# Bridging distances in technology and regulation

Leenes, Ronald; Kosta, Eleni

# BRIDGING DISTANCES IN TECHNOLOGY AND REGULATION

edited by

RONALD LEENES & ELENI KOSTA

**Bridging Distances in Technology and Regulation**
Ronald Leenes & Eleni Kosta (eds.)
ISBN: 978-90-5850-986-4

Published by Wolf Legal Publishers (WLP)
P.O. Box 313
5060 AH Oisterwijk
The Netherlands
E-Mail: info@wolfpublishers.nl
www.wolfpublishers.com

Cover design: Ronald Leenes
Cover illustration: still from the film Metropolis, 1925 – 26, director: Fritz Lang
Copyright: Horst von Harbou - Deutsche Kinemathek

*Bridging Distances in Technology and Regulation* originates in a conference with the same title, which was held at Tilburg University on 25 and 26 April 2013. The editors wish to thank the following sponsors, for making this event possible:

# Foreword

Information and Communication Technologies allow us to bridge space and time. New services and industries are constantly being created and people no longer depend on the here and now for their development, but can tap into resources across the globe. Cloud Computing, for instance, allows users to make use of remote services and store their data far from home. Healthcare increasingly makes use of diagnosis and care at a distance. Drones and remote cameras replace the physical presence of police and other vigilantes. Robots will increasingly be deployed to act on our behalf.

The mediation in space and time by technology also raises new questions. How will distance work out in daily life, in work, in friendships, and in care? How will people adjust to the paradoxical distance and closeness created by technologies? Will the distribution of responsibilities and liability change if activities take place at distances in space and time in complex systems and global environments? What are best practices in multi-level governance to address the rise of distant interconnectivity?

*Bridging distances in technology and regulation* is a textbook of papers that deal with diverse issues in the fields of regulation, technology and ethics. This book is divided in four parts and is organised as follows: the **first part** examines how technologies challenge regulation. The **second part** deals with the legal assessment of normative phenomena. The **third part** presents case studies on ethical dimensions of distance. The **fourth part** focuses on the managing of access to information. The individual chapters included in this book are briefly discussed below.

The first part (coping with technologies) consists of four chapters. In **Chapter 1** Gregory Mandel and Gary Marchant tackle the issue of governance in relation to emerging technologies, using as an example the case of synthetic biology. They discuss the regulation of synthetic biology under the US legal framework and they present how 'soft-law' could present sufficient advantages over the current mechanisms. **Chapter 2**, by Lyria Bennett Moses, examines the European and the Australian paradigms in technology regulation. While Australia has relied on law reform commissions to approach the regulation of new technologies, Europe has mainly put emphasis on technology assessment. Bennett Moses compares these two approaches and explores opportunities for mutual learning. Hans Ebbers, Huub Schellekens, Hubert Leufkens and Toine Pieters in **Chapter 3** focus on the regulation of pharmaceuticals. They present the European framework on copycut biological, so-called 'biosimilars', focusing especially on erythropoiesis-stimulating agents and the pure red cell aplasia (PRCA) safety controversy. Their analysis shows that the European regulatory framework for biosimilars stimulates innovation, while it manages to maintain high safety standards and it illustrates the role of regulation and regulators in creating new pharmaceuticals. **Chapter 4** by Johan Söderberg deals with the cat and mouse game between legislators and makers of intoxicating drugs. Each time a drug is added to the list of controlled substances, new ones with similar intoxicating effects as those already prohibited by law are created. These 'legal highs' obviously cause problems for regulators who have a hard time to keep up with development. Söderberg discusses ways for regulators to keep up with innovations without hampering innovation.

The second part (the scope of law) contains two chapters. **Chapter 5** by Michael Anthony C. Dizon draws attention to regulation by other means than classical law. He argues that to under-

stand how the networked information society is organized and operates we need to develop and adopt a pluralist, rule-based approach taking into account plural legal and extra-legal rules, norms, codes and principles that influence behaviour. He illustrates this idea by discussing hackers showing that hacking is not simply a problem that needs to be solved, but rather that it is a complex, techno-social complex that flips from socially desirable to socially undesirable and back all the time and thus requires a more nuanced assessment. In **Chapter 6** Robin Hoenkamp, Adrienne de Moor – van Vugt and George Huitema discuss the odd role (technical) standards play in the modern networked society. Often standards are being developed without a clear legal mandate, yet they have a profound normative effect on manufacturers and consumers. The authors discuss the legal status of different types of standards and illustrate the importance of providing clear procedural standards and legal status for standards in the domain of smart grids.

The third part (ethical reflection on distance: case studies) comprises of four chapters. Mark Coeckelbergh in **Chapter 7** takes us into the world of killer drones and surveillance in public spaces and discusses the often-heard argument that the distance in these environments between the killer/observant and their targets makes killing/observation easier. The technology between drone crew and target seems to increase moral distance making killer easier. Coeckelbergh argues that the fact that the crew builds up stories about their targets over time which may mitigate the increased moral distance. In other words, he shows that practice of drone fighting is more complex than often thought and calls for more reflection on how technologies could create the conditions under which moral metamorphosis and interpretative freedom can be promoted to keep a proper balance.

In **Chapter 8** Esther Keymolen presents collaborative consumption as a characteristic of the 21$^{st}$ century. One of the basic principles of collaborative consumption is that it is based on trust between strangers, expressed for instance via online peer-to-peer platforms or user rating systems. Such trust is however not free of failures, which raises the need to tackle with the complexities of online environments. Keymolen proposes the concept of *interpersonal system trust* to open up a new perspective on the workings of collaborative consumption. **Chapter 9**, authored by Federica Lucivero and Lucie Dalibert discusses trust in the context of point-of-care devices such as the Nanopil, an ingestible capsule that contains a miniaturized chip that performs an in vivo analysis of intestinal fluid, detects the presence of biomarkers for colorectal cancer, and communicates the result to the outside via radiosignalling. Lucivero and Dalibert elaborate on the potential tension users of such point-of-care devices may experience between trusting their experience of a symptom and trusting the technology. They show how the Nanopil provides a hybrid of proximity and detachment from the user and argue that such close-yet-distant relationship requires careful consideration in the innovation process. In **Chapter 10** Anton Vedder deals with the relation between technological innovation and the sustainability of the health care system. He examines the possible impact of the use of e-health applications on the respective roles of patients and care providers and on the care provider-patient relationship.

The fourth part (managing access to information) consists of two chapters. In **Chapter 11**, Maurice Schellekens discusses the problem arising by the use of robots to collect information from the internet and the use of robots.txt protocols to regulate de facto the access by bots. Schellekens discusses the two legal action that can be taken to vindicate a prohibition of access, presenting the criminal act of unauthorised access foreseen in Article 2 of the Convention of Cybercrime of the Council of Europe on the one hand and the protection under US civil law action of trespass to chat-

tels on the other. **Chapter 12,** by Gergely Alpár and Bart Jacobs, discusses attribute-based credentials, the basic building blocks of many upcoming privacy-enhancing technologies and user-centric identity management systems. They elaborate realistic on-line and off-line use cases in attribute-based identity management and identify and analyse some of the design issues that require a decision or solution.

The editors wish to thank the following persons: first and foremost the authors of this book for their invaluable contributions and their enthusiasm. We also wish to thank the reviewers for their time, effort and motivation to provide feedback on all the papers. We thank Anton Vedder, who, as the Director of the Tilburg Institute for Law, Technology, and Society (TILT), made it possible to organise the conference that was the starting point for this book. A deep thank you to Bert-Jaap Koops and to the members of the organising team, who helped us in realising the conference and the book, Leonie de Jong, Femke Abousalama and Irene Aertsen. And last but not least, we would like to thank our publisher, Simone Fennell, for her support in turning this book into reality.

Ronald Leenes & Eleni Kosta
Tilburg, The Netherlands, April 2013

# Contents

# Author biographies

**Gergely Alpár** started in 2010 his PhD project, titled 'Identity Management for Mobile Devices', within the Digital Security group of the Computer Science department at the Radboud University Nijmegen. Participating in this project, he also has the opportunity to work at TNO, the Dutch organisation for applied scientific research. His main research interests are applied cryptography, privacy-enhanced technology, and their practical aspects. In these fields he has published conference papers and participated in workshops in Europe and in the US. He holds two master degrees, Master of Science in mathematics and Master of technological design in applied mathematics, and he also has practical business experience, as he ran his own successful IT company for seven years. He has given lectures at several universities in Europe since he had earned his first master degree.

**Lyria Bennett Moses** is a Senior Lecturer at the University of New South Wales in Sydney Australia. She has a JSD from Columbia Law School on the topic 'The Impact of Technological Change on Law'. Lyria's research engages with issues such as the relationship between law and technological change (what kinds of legal issues arise as technology changes and how such issues are managed) and the appropriate scope of property law in new contexts. She is also Sydney co-ordinator of the IEEE Society for the Social Implications of Technology, co-editor of the blog 'The Social Interface' and a member of the Editorial Board of the Property Law Review.

**Mark Coeckelbergh** (Ph.D., University of Birmingham) teaches philosophy at the Philosophy Department of the University of Twente, the Netherlands, and is managing director of the 3TU.Centre for Ethics and Technology. He is the author of Liberation and Passion (2002), The Metaphysics of Autonomy (2004), Imagination and Principles (2007), Growing Moral Relations (2012), Human Being @ Risk (2013), and numerous articles in the area of ethics and technology, including ethics of information technologies and robotics.

**Lucie Dalibert** received a Master degree in Women's and Gender Studies in 2009, and she is currently doing a PhD in philosophy of technology at the University of Twente, where her research is part of Prof.dr.ir. Peter-Paul Verbeek's NWO/VIDI project 'Technology and the Limits of Humanity: The Conceptual, Anthropological, and Ethical Aspects of Posthumanism.' As she relies upon two case studies, prosthetics and neuromodulation, Lucie Dalibert investigates what kinds of bodies materialise with/in these technologies while attending to the conceptions of humanness that are being convened and conveyed in these materialisation processes. Indeed, her project is an attempt at conceptualising the material intertwinement of technologies, bodies, and humanness. Lucie Dalibert is a member of the WTMC graduate school and of the 3TU Centre for Ethics and Technology.

**Adrienne de Moor-van Vugt** is professor of Constitutional and administrative law at the Law Faculty of the University of Amsterdam. She set up the Research Group on Market Regulation in the

Law Faculty, is co-director of the Amsterdam Center for Energy Research and faculty at the Amsterdam Center for Law & Economics. De Moor-van Vugt's recent research includes regulation and supervision in the gas and electricity sector, the banking crisis and the role of national and European banking authorities, state aid under EU law, EU subsidies, and competition law. Her inaugural address in May 2010 dealt with the EU rules of good repute for bankers and its implementation in the Netherlands and the UK.

**Michael Anthony C. Dizon** is a PhD researcher at the Tilburg Institute for Law, Technology, and Society (TILT) doing research on open source hardware hackers and hacktivists. For a number of years, he was a lecturer at the University of the Philippines College of Law. He has conducted research at the UP Law Internet & Society Program (UP Law-ISP) and the AHRC Research Centre for Studies in Intellectual Property and Technology Law (SCRIPT) at the University of Edinburgh.

**Hans Ebbers**, PhD, is a researcher at the department of pharmaceutical sciences. His research interests are related to regulatory challenges of biologicals, mainly the safety of biological medicines and regulatory challenges posed by the arrival of biosimilars.

**Robin A. Hoenkamp** studied Dutch Law at the University of Maastricht and the University of Utrecht, where she obtained her Bachelor degree. She studied one semester at the University of Washington, Seattle, where she focused on Environmental and Comparative Law. She took her LLM in Constitutional and Administrative Law at the University of Utrecht and wrote her Master thesis on Constitutional Law. Since September 2010 she is working on her PhD thesis for the Amsterdam Centre for Energy of the University of Amsterdam on safeguarding public interests in smart grid technical standardization. This study is part of the research of the Smart Energy Systems Group of the Netherlands Organization for Applied Scientific Research, TNO.

**George B. Huitema** is Professor of Telematics at the Faculty of Economics and Business at the University of Groningen. Furthermore he is Senior Research Scientist and member of the Smart Energy Systems Group of the Netherlands Organization for Applied Scientific Research TNO. At present, he develops strategic guidelines for next generation billing in telecommunications, public transport and utilities. He is member of the Revenue Management Initiative and Energy Smart Grid initiative of the Tele Management Forum. At TNO he coordinates EU FP7 projects in the energy domain and is project member of the EU FP7 EcoGrid project, which demonstrates a real-time energy market with high penetration of many and variable renewable energy resources.

**Bart Jacobs** is a professor of computer security at the Radboud University Nijmegen. With his research group he has worked over the last decade on a number of societally relevant security topics such as chipcards (eg. in passports and transport), electronic voting, smart metering, road pricing and privacy. He is a member of the National Cyber Security Council in the Netherlands that provides cabinet level advice in the Netherlands on strategic computer security matters.

**Esther Keymolen** has research interests in the Philosophy of Technology, Philosophical Anthropology, and policy and ICT. Currently, she is a PhD student at the Faculty of Philosophy at the Erasmus University Rotterdam (EUR). In her dissertation she examines the impact of new technol-

ogies on the development of trust in interpersonal interactions. Before starting her doctoral research in 2010, Esther worked at the Scientific Council for Government Policy (WRR). She completed her Master's degree with distinction in 2008 as well as her Bachelor's degree with honours in 2007 in philosophy at the EUR.She also holds a Bachelor's degree in Music (2004).

**Hubert G. Leufkens** is professor in pharmacoepidemiology, chair of the Dutch Medicines Evaluation Board and Co-opted member of the Committee of Human medicinal products of the European Medicines Agency. He has a broad interest in drug safety and the workings of drug regulatory systems.

**Federica Lucivero** (PhD) is a post-doctoral researcher at TILT, the Tilburg Institute for Law Technology, and Society (Tilburg University, The Netherlands). Federica completed the Nederlands Graduate Research School of Science Technology and Modern Culture (WTMC) and has been conducting research at the crossroad of philosophy and ethics of emerging technologies and science & technology studies. In her studies, Federica tries to combine theoretical and methodological analysis with empirical studies. Her PhD thesis, completed in 2012 at the University of Twente (the Netherlands), addresses the methodological question of assessing the plausibility of expectations surrounding emerging technologies within the context of Technology Assessment.

**Gregory N. Mandel** is the Peter J. Liacouras Professor of Law and Associate Dean for Research at Temple Law School. He specializes in intellectual property law and the interface among technology, science, and the law.Professor Mandel's articles have been selected as top intellectual property and top patent law articles of the year, and his experimental studies have been cited by the Court of Appeals for the Federal Circuit and in several briefs filed before the United States Supreme Court. Professor Mandel served on the Executive Committee of the Intellectual Property Section of the American Association of Law Schools, an American Bar Association task force to brief the Environmental Protection Agency on arising nanotechnology legal issues, and is the recipient of a Fulbright Senior Specialist grant to teach U.S. intellectual property law to foreign law students. He is a frequent speaker on intellectual property and technology law issues, having given over one hundred presentations in a dozen countries internationally, including for the United Nations, Second Circuit, Environmental Protection Agency, American Bar Association, American Psychology Association, and National Academy of Science, as well as at Stanford, NYU, Penn, and Berkeley law schools. Before entering academia, Professor Mandel practiced law with Skadden, Arps, Slate, Meagher & Flom LLP, and clerked for Judge Jerome Farris, United States Court of Appeals for the Ninth Circuit. He worked on NASA's Hubble Space Telescope prior to attending law school. Professor Mandel received his J.D. from Stanford Law School and his undergraduate degree in physics and astronomy from Wesleyan University.

**Gary Marchant** is Regent's Professor and the Lincoln Professor Emerging Technologies, Law and Ethics at the Sandra Day O'Connor College of Law at Arizona State University. He is also Faculty Director of the ASU Center for Law, Science and Innovation, Professor of Life Sciences and a Senior Sustainability Scientist in the Global institute of Sustainability at ASU. Professor Marchant has a Ph.D. in Genetics from the University of British Columbia, a Masters of Public Policy degree from the Kennedy School of Government, and a JD from Harvard Law School.Prior to joining the ASU

faculty in 1999, he was a partner in the Washington, D.C. office of the law firm Kirkland & Ellis where his practice focused on regulatory issues. Professor Marchant teaches and researches in the subject areas of environmental law, risk assessment and risk management, genetics and the law, biotechnology law, food and drug law, legal aspects of nanotechnology, and law, science and technology.

**Toine Pieters** is professor of the history of pharmacy (Descartes Centre for the History and Philosophy of the Sciences and the Humanities, Utrecht University) and senior lecturer in the medical humanities (VU Amsterdam Medical Centre). He has published extensively on the history of pharmacy and medicine, and on science, technology and society (STS). His broader interests include digital humanities, pharmaceutical policy analysis, pharmacology and pharmacoepidemiology.

**Huub Schellekens** is professor in medical biotechnology at Utrecht University in the Netherlands and has a long-standing interest in the safety questions surrounding biological medicines. He has published extensively on the topic of immunogenicity of therapeutic proteins and works as an advisor of biosimilar legislation in various countries around the world.

**Maurice Schellekens** is an Assistant Professor at the Tilburg Institute for Law, Technology, and Society (TILT) at Tilburg University, The Netherlands. He studied law (Maastricht University) and computer science (Eindhoven University of Technology). In 2001, he defended his thesis about liability of ISPs for copyright infringement and criminal offences on the Internet. His research topics include legal aspects of modern biotechnology, intellectual property law, and regulation of new technologies. In the last few years, Maurice published extensively on information and communication technology and law. Subjects include: starting points for regulation of ICT, intellectual property in the information society, reliability of Internet information, the legal status of authentication technology and on line dispute resolution.

**Johan Söderberg** is a post-doc researcher at Institute for Research and Innovation in Society (IFRIS) and Laboratoie Techniques, Territoires et Sociétés (LATTS). Previously he has studied wireless network activists in Czech Republic and hobby-engineers developing an open source 3D printer. His current research focus is on legal highs. What unites the empirical cases is a theoretical interest in the antagonistic aspects of innovation processes.

**Anton Vedder** is an Associate Professor of Ethics and the Regulation of Innovative Technologies at TILT, the Tilburg Institute for Law Technology, and Society (Tilburg University, The Neherlands). The main topics of his research and teaching are the interactions between technological developments and the articulation of values, antiterrorism regulation and fundamental human rights, and normative aspects of the adoption of healthcare technology. Anton is the general director of TILT since 2011.

# PART I: COPING WITH TECHNOLOGIES

# Evolving technology regulation: Governance at a temporal distance

Prof. Gregory N. Mandel
Temple Law School
✉gmandel@temple.edu

Prof. Gary E. Marchant
Arizona State College of Law
✉gary.marchant@asu.edu

**Abstract** Emerging technologies can place great strain on extant regulatory systems. Regulatory systems are hard-pressed to adapt quickly enough to technological development, particularly as both the benefits and risks of emerging technologies often cannot be known until a technology develops further. In such circumstances, 'soft law' alternatives can more rapidly provide flexible measures to help fill regulatory gaps in a manner that allows a promising technology to develop while still adequately protecting human health and the environment.

**Keywords** emerging, technology, governance, regulation, synthetic biology

## Introduction

The biotechnology revolution has changed our lives, transforming medicine, agriculture, and energy. Rapid developments in biotechnology over the past several decades, from genetically modified crops to biologic pharmaceuticals have placed tremendous strain on extant regulatory systems. Regulatory systems are designed to handle the technology in place at the time of their promulgation, often decades in the past, and have been hard-pressed to evolve to govern emerging innovation (Mandel 2009; Brownsword 2008). New developments in biotechnology may fall into gaps not covered by existing regulation, or be unintentionally trapped in regulatory schemes poorly designed for certain products and governed by happenstance by a regulatory agency that lacks expertise in a given area. Successful governance of an emerging technology, with biotechnology as a prime example, requires governance across time of a technology whose development is as yet unknown. It requires technology governance at a technological and temporal distance.

The challenge of adapting historic regulatory schemes to emerging technologies can be daunting. Statutory and regulatory evolution is slow, expensive, and often politically difficult or futile. In many circumstances, law is simply incapable of evolving as rapidly as technological advance. In these cases, "soft law" alternatives may provide a valuable alternative, one that can provide faster and more flexible governance that achieves a balance between the desire to enable promising technologies to develop further while adequately guarding against their potential risks.

This paper discusses the challenge of technology regulation at a distance by presenting a case study on synthetic biology. Synthetic biology is one of the fastest developing and most promising emerging technologies. It will permit scientists to design living organisms unlike any found in nature, and to redesign existing organisms to have enhanced or novel qualities. While traditional biotechnology involves the transfer of a small amount of genetic material from one species to another, synthetic biology will permit the purposeful assembly of an entire organism. Synthetically designed organisms, it is hoped, might be put to myriad beneficial uses, including better detection and treatment of disease, the remediation of environmental pollutants, and the production of new sources of energy, medicines and other valuable products. Engineered life forms, however, also

might pose risks to human health and the environment. And, exactly what those hazards are and how they might be controlled cannot be fully determined in advance of the very research necessary to develop this novel science in the first instance.

In order to ground and concentrate the analysis, the paper focuses on the first synthetic biology organisms that are anticipated to be commercialized and on governance under the U.S. regulatory system. The analysis reveals that although the extant U.S. regulatory system is capable of handling sufficiently several aspects of novel synthetic biology organisms, there are also a number of potentially troubling regulatory gaps. These gaps arise because synthetic biology presents particular challenges for the existing regulatory regimes due to three atypical characteristics of this nascent technology: synthetic biology organisms can evolve; the traditional relationship between mass and risk may break down for synthetic biology products; and the conventional regulatory focus of existing statutes on end-product chemicals may be a poor match in certain instances for a technology that produces novel organisms, with their own attendant risks, that, in turn, produce the end-product chemicals. Critically, the lessons learned and recommendations offered have generalizable implications for how to govern an array of emerging technologies under a variety of regulatory systems.

The article begins with an overview of synthetic biology and an examination of the potential benefits and risks of expected early synthetic biology products. The paper then discusses existing U.S. regulatory authority concerning the potential human health and environmental impacts of synthetic biology. The final part introduces several innovative “soft law” governance approaches that could shore up certain gaps in the existing regulatory framework for synthetic biology, with a goal of permitting this promising technology to develop as rapidly as possible consistent with adequately guarding against its potential environmental and human health risks.[1]

## Synthetic biology

Synthetic biology brings the concept of engineering to biology in order to design living organisms. Synthetic biology is based on the understanding that DNA sequences can be assembled together like building blocks, producing a living entity with any desired combination of traits, much as one can assemble a car by putting together many individual pieces with different functions.

Synthetic biology is in its infancy as a technological field. This emerging technology will use genes and other DNA sequences as interchangeable biological parts to build a target organism. The BioBricks Foundation is developing a catalog of standardized genetic sequences that perform specified biological functions when inserted into a microorganism. Concurrently, other scientists are trying to develop a simplified genome, designed to contain the minimal genetic code necessary to survive and replicate (Erickson 2011; Schmidt 2010). This minimal genome could then be used as a chassis to which genetic material coding for particular desired traits can be attached (Hylton 2012). In this manner, synthetic organisms could be designed to perform myriad functions.

Synthetic biology represents a giant leap forward from the current generation of genetically modified organisms created by recombinant DNA. Current genetic modification methods involve

[1] Many emerging technologies, including synthetic biology, raise certain non-physical concerns, including economic and ethical questions. This paper focuses on the regulatory authority concerning science-based human health and environmental risks.

adding, modifying or deleting one, or at most a few, genes within an organism. Synthetic biology, on the other hand, will involves the creation of novel DNA sequences that may never have existed before in living organisms, or the widespread substitution or addition of entire or partial genomes. Synthetic biology is expected to provide significant benefits across a wide variety of fronts. Medical advances may include better disease detection, molecular devices for tissue repair and regeneration, molecules utilizing a sensor and enzymes to identify and attack disease targets such as tumors, personalized medicine, rapid development of vaccines, and cells with new properties to improve human health (Ruder 2011; Chopra & Kamma 2006). As one example, synthetic biology may allow for less expensive production of biopharmaceuticals (European Commission 2005). Drugs that are currently expensively produced from natural sources, such as the anti-cancer drug taxol and the anti-HIV compound prostratin, could be produced inexpensively through engineering cells to produce the compounds in large quantities (Tucker & Zilinskas 2006).

Synthetic biology is expected to produce a variety of environmental and energy benefits, including the production of chemicals in more environmentally friendly manners, bioremediation, pollutant detection, and less expensive and more efficient energy production (Erickson 2011). Biosensors could be designed to signal the presence of environmental contaminants, including chemical pollutants and weapons (Khalil & Collins 2010; Bhutkar 2005). Engineered microorganisms may be able to remediate some of the most hazardous environmental pollutants, such as heavy metals, hazardous waste, and nuclear waste, or to recycle waste such as converting agricultural waste into useful products such as ethanol (Jarrell 2010; Chopra & Kamma 2006; European Commission 2005). Microorganisms such as algae, bacteria or yeast could be redesigned using synthetic biology to produce a new generation of biofuels that reduce pollution from both the production and use of the fuel (You-Kwan Oh 2011; Chopra & Kamma 2006; European Commission 2005).

Synthetic cells may provide a future generation of faster, less expensive, and even self-repairing, computers and robotic technologies (Balmer & Martin 2007; Tsuda 2005). For example, synthetic biologists have recently figured out how to program proteins to perform basic calculations, producing the first “cellular calculator” (Boyle 2012). Other scientists have been able to get an amoeba’s cellular structure to interface with, and process sensory signals from, a robot (Tsuda 2005). Synthetic organisms may also be designed to biologically produce other proteins and chemicals with a variety of industrial, agricultural, or environmental applications, all more efficiently, for lower cost, and using fewer natural resources than is currently possible (Erickson 2011; Krivoruchko 2011; Keasling 2010).

For all its potentially wondrous advances, synthetic biology also poses a variety of potential risks. A primary concern involves the accidental or intentional release of synthetic organisms into the environment.[2] Uncontrolled release raises concerns that range from environmental damage to bioterrorism. For engineered organisms intended to be released into the environment, scientists are developing potential controls, such as making synthetic organisms dependent on non-naturally occurring nutrients or designing the organisms to self-destruct if a population spurt or density oc-

[2] Society’s approach to synthetic biology raises other potential areas of concern beyond direct risks to human health or the environment, including concerns regarding global trade, justice, intellectual property rights, and other issues, as well as social, religious, and philosophical questions regarding modifying or creating life forms. These issues raise a variety of questions that have few simple answers. This article focuses on the human health and environmental risks of synthetic biology.

curs (Balmer & Martin 2007). Such controls instituted for synthetic organisms deliberately released into the environment to serve as biosensors, for agricultural purposes, or for bioremediation could fail, leading to environmental or human health impacts (Pollack 2010). For example, intentionally released synthetic organisms could mutate or interact with other organisms and the environment in unexpected ways leading to unanticipated proliferation or to synthetic organisms passing their synthetic genes to natural species (Balmer & Martin 2007). Thus, controls are not guarantees; living systems are very complex and can be unpredictable (Chopra & Kamma 2006). Synthetic circuits developed so far, for instance, have tended to mutate rapidly and become nonfunctional (Tucker & Zilinskas 2006).

As with other emerging technologies, the challenge of guarding against synthetic biology risks while maintaining a safe environment in which the potentially enormous benefits of synthetic biology can be pursued will fall primarily upon federal regulatory agencies. These agencies will have to seek this delicate balance while operating pursuant to a statutory and regulatory system designed largely prior to the advent of synthetic biology, or even the advent of the earlier generation of conventional genetically modified products. Unsurprisingly, uncertainty surrounding emerging synthetic biology technology, and its attendant potential benefits and risks, will create significant challenges for the U.S. regulatory system. Regulatory systems, almost necessarily, are designed for technologies existing at the time of the regulatory systems' formation and are based on the then-current understanding of that technology. Such systems often face difficulty and disruption when applied to newly emerging technologies (Mandel 2009).

The first synthetic biology organisms expected to be commercialized include microorganisms engineered to produce biofuels, for chemical production, and for bioremediation. The following sections provide background on each of these nascent technologies, describe how each may be used, and evaluate potential scenarios for exposure and risks to human health or the environment.

### *Synthetic Biology Algae for Biofuel Production*

Biofuels are one of the most promising new sustainable energy technologies for meeting rising energy needs worldwide, particularly in the transportation sector (Carriquiry 2011; Parmar 2011). First generation biofuels such as ethanol from corn have important limitations, including competition with food uses of the corn, loss of ecosystems, increases in food prices, and depending on the production method limited or even negligible environmental benefits over their lifecycle (Parmar 2011). Accordingly, second and third generation biofuels produced from non-food biomass are being pursued as a more sustainable, long-term solution, and single-cell algae (or microalgae) and cyanobacteria (or blue-green algae) (collectively, "algae") are leading candidates for the production of biofuels (Carriquiry 2011; Singh & Gu 2010). While many researchers and companies are pursuing the development of algal cells for biofuel production using naturally occurring or genetically engineered strains, synthetic biology may offer the greatest potential for producing large quantities of sustainable biofuels by creating new strains of algae.

Genetic engineering of algae, particularly using the more powerful techniques of synthetic biology, has enormous potential to improve biofuel production in algae and help make it economically competitive with other fuel types and sources (Biello 2011; Parmar 2011). There are many types of algae, but of particular importance for the production of biofuels are microalgae and cyanobacteria, which are single-cell organisms that capture sunlight through photosynthesis and use the stored energy to convert inorganic substances into simple sugars (Parmar 2011; National Renew-

able Energy Laboratory 1998). As the primitive ancestors of modern plants, algae and cyanobacetria have relatively simple cellular systems, and as a result they can devote virtually all their cellular resources to the conversion of solar energy into biomass. Additionally, the lack of multicellular structure allows algae and cyanobacetria to remain in aqueous suspension where their cellular surface area has maximum contact with nutrients such as $CO_2$ (NREL 1998).

In recent years there has been a surge of interest in utilizing algae for renewable fuel production, catalyzed by policy objectives including slowing increases in greenhouse gas emissions. As a report for the U.S. Department of Energy noted, "[p]ut quite simply, microalgae are remarkable and efficient biological factories capable of taking a waste (zero-energy) form of carbon ($CO_2$) and converting it into a high density liquid form of energy (natural oil)." (NREL 1998). Microalgae and cyanobacteria can provide many environmental benefits—for example, "[b]iodiesel performs as well as petroleum diesel, while reducing emissions of particulate matter, CO, hydrocarbons and SOx. Emissions of NOx are, however, higher for biodiesel in many engines." (NREL 1998). Through their photosynthetic metabolism, algal cells take in carbon dioxide and release oxygen as a metabolic byproduct. This carbon sequestration quality makes them attractive to renewable fuel advocates. Although the biofuel will release greenhouse gasses when burned for energy, the fuel was created by cells that sequestered carbon dioxide from the atmosphere, making biofuel from algae nearly carbon neutral. The high production capability of algae also makes them an attractive source for biofuels. Algae can produce up to 58,700 liters of oil per hectare of cultivation, which is one to two magnitudes higher than what is possible from other energy crops (Chen 2011). Algae grow to high densities and have high per-acre productivity, providing for efficient mass cultivation (Parmar 2011). They are also extremely hearty organisms that thrive all over the planet and can survive in extreme conditions, such as salt water, waste water and on land otherwise ill-suited for agriculture (Biello 2011; Parmar 2011).

Due to their simple structure, algae make easy targets for extensive genetic manipulation compared to higher plants. A number of helpful traits could be engineered into algae to improve their biofuel production, including traits for producing different types of hydrocarbons that could be used for improved biofuels, for secreting oils into the environment so the cells don't need to be harvested to extract their products, for better utilizing atmospheric $CO_2$ as a carbon source, and to grow faster and stronger in a variety of different environments, including salt water and stressed environments (Biello 2011; Savage 2011).

There are, however, also significant safety and regulatory concerns about synthetic biology algae, including the potential environmental release, exposure and risks of the engineered organisms. A key factor influencing such concerns will be whether the algae are grown in open (i.e. open pond systems) or closed (bioreactor) systems (Chen 2011). Most commercial cultivation of algae is currently carried out in open pond systems (Chen 2011). Open cultivation utilizes uncovered 'ponds' that can be either man made or naturally occurring. By their nature, these ponds are open and exposed to the external environment.

The other principal cultivation method involves photobioreactors to create a closed environment for cultivation, where conditions can be monitored and controlled. Consequently, cultivation can be maximized through a careful, controlled balancing of the variables. For example, algae grown in plastic tubes in ponds provide up to seven times the productivity of open ponds (Singh & Gu 2010). Another comparative advantage of closed systems is the protection against unintended

contamination or release (NREL 1998). Even with contained uses, however, the risk of accidental environmental release is not zero, although it is less than open cultivation.

If synthetic biology algae products are released accidentally into the environment, there is likely to be much uncertainty about the resultant likelihood and nature of risks to the natural environment or human health. Modified synthetic biology algae could be transported through the air for long distances, and could survive a variety of harsh environments in dormant form (Parmar 2011). The risks of the release of most genetically engineered organisms into the environment creates some uncertainty, and given the more substantial modifications made possible by synthetic biology, it is likely that any environmentally-released synthetic biology algae will create even greater uncertainties. Some of the uncertainties include the likelihood and rate of accidental release, the survivability of the synthetic biology algae in the surrounding environment, its ability to reproduce, spread, and compete in the natural environment, and the mechanisms and magnitude of any possible risks to the environment or human health.

### *Synthetic Biology Organisms Designed for Chemical Production*

Synthetic biology may also permit microorganisms to be engineered as “living factories” designed to produce valuable chemical products. Traditional genetic engineering is already used to produce natural chemical products through metabolic engineering. This is accomplished by transferring genetic material that produces a particular substance, such as a useful enzyme or protein, to a host microorganism that can be readily manipulated to express that substance. Current biological production, however, often relies on nonrenewable resources and limited natural resources (Keasling 2010).

Synthetic biology will permit the design of microorganisms that produce chemicals metabolically with greater precision than currently possible and will allow the engineering of microorganisms to produce chemicals that cannot currently be manufactured biologically. These designed microorganisms can be tailor-made for particular chemical production processes that rely on widely available and inexpensive starting materials (primarily certain sugars) to produce a broader array of valuable output chemical products (Erickson 2011; Keasling 2010). The great advantage of the biological production of chemicals is that it can be accomplished at lower cost, using fewer natural resources, and with lower environmental impact, than certain traditional chemical production methods (Krivoruchko 2011).

Microorganisms may be designed to produce basic commodity chemicals such as solvents, feed additives, agricultural chemicals, and certain polymers (Keasling 2010). More advanced chemical products, including enzymes, vitamins, antibiotics, and nutraceuticals may also be manufactured (Erickson 2011). DuPont has developed a semi-synthetic bacterium that lives on cornstarch and produces a chemical useful for manufacturing high-tech fabrics. This synthetic bacterium may become the first $1 billion non-pharmaceutical biotechnology product (Weiss 2007). Other developments include a synthetic antibiotic, a building block for Spandex, and work on a synthetic biology microorganism that would produce rubber (Erickson 2011).

Pharmaceutical ingredients that are too complex to be chemically synthesized may also be produced. For example, a number of alkaloids, compounds that are found in or derived from plants and commonly used in drugs, are likely targets for synthetic biology production (Keasling 2010). Synthetic biology may be used to more efficiently produce a precursor to artemisinin, a naturally occurring drug that is highly effective in treating malaria, but is in short supply (Krivoruchko 2011).

The Bill and Melinda Gates Foundation donated over $40 million to promote research concerning the development of synthetic artemisinin (van Noorden 2010). Taxol, a widely used anticancer compound, and hydrocortisone are other examples of pharmaceuticals that may be produced less expensively and more efficiently through synthetic biology than current methods (Krivoruchko 2011).

While manufacturers have a long history of synthetic chemical production, using synthetic biology microbes to produce chemicals biologically creates new risks. As the Presidential Commission on the Study of Bioethical Issues found, "Unlike synthetically produced chemicals, which generally have well-defined and predictable qualities, biological organisms may be more difficult to control" (Presidential Commission on Bioethical Issues 2010). Although much synthetic biology chemical production is expected to take place in contained environments, this does not eliminate potential risks from unintentional release into the environment.

Further, the development of synthetic biology for chemical production also creates a risk that individuals with malicious intent could try to use toxic or pathogenic synthetic biology microorganisms for illegal activities, such as bioterrorism (Erickson 2011). The U.S. government has developed certain recommendations to try to reduce these risks, but the synthetic biology field is in an early stage of development and understanding the contours of potential risks necessarily remains at a developmental stage as well (Presidential Commission on Bioethical Issues 2010).

### *Synthetic Biology Microorganisms Designed for Bioremediation*

In addition to the production of biofuels and chemicals, one of the most promising fields of synthetic biology involves the potential to revolutionize the remediation of hazardous substance. Bioremediation refers to the use of microorganisms to reduce or remove contaminants from the environment. Bioremediation is already common in oil spills as several species of bacteria naturally consume and degrade certain petroleum components into less toxic by-products (Schmidt 2010). To date, however, traditional genetic engineering of bacteria for bioremediation has been a bit of a disappointment as there have been significant difficulties with how the bacteria interact in the environment, the ability of the bacteria to compete and survive in the wild, and the low bioavailability of certain compounds (Viebahn 2009). In most cases, genetically modified bacteria have not done any better at bioremediation than their naturally occurring counterparts (Cases & de Lorenzo 2005).

Synthetic biology may permit the redesign of microbes to better remediate petroleum based contamination and the engineering of novel microorganisms that can break down more recalcitrant contaminants, such as dioxins, pesticides, and radioactive compounds (Schmidt 2010; Viebahn 2009). Because synthetic biology microorganisms could be designed from scratch, as opposed to being dependent on naturally-occurring genetic material, they could be engineered to be more viable in the natural environment and to target particular pollutants of concern. These microorganisms may be able to more efficiently remediate a variety of environmental contaminants while having less of a negative impact on the environment than traditional remediation methods (Schmidt 2010).

Synthetic biology microbes engineered for bioremediation raise particular concerns because their use necessarily entails the intentional release of synthetic organisms into the environment. Synthetic biology microbes released into the environment could mutate or interact with other organisms and the environment in unexpected ways leading to unanticipated proliferation or to synthetic microbes passing their non-natural genes to natural species (Presidential Commission on Bioethi-

cal Issues 2010; Balmer & Martin 2007). In a worst-case scenario, synthetic biology microbes could compete or cross-breed with natural organisms, threatening the existence or ecosystem of those natural organisms (Presidential Commission on Bioethical Issues 2010). Exacerbating this concern, to survive in the natural world, as opposed to a laboratory environment, synthetic biology microbes designed for bioremediation will need to be designed to be particularly robust, which could make them more competitive vis-à-vis natural organisms, as well as more difficult to control (Ferber 2004). The lack of any evolutionary or ecological history, and the potential for unpredicted and unpredictable properties and interactions, will make evaluating the consequences of a release difficult (Presidential Commission on Bioethical Issues 2010).

Scientists are developing potential controls, such as designing "terminator genes," making synthetic organisms dependent on non-naturally occurring nutrients, or designing organisms to self-destruct if a population spurt or density occurs (Presidential Commission on Bioethical Issues 2010; Callura 2010; Balmer & Martin 2007). But, controls are not guarantees. Living systems are complex and unpredictable, uncertainty that is only exacerbated by the unknown interaction between an organism and an ecosystem. Because a synthetic biology organism could evolve or exchange genetic material with another organism, the potential controls may not be fully secure (Presidential Commission on Bioethical Issues 2010; Callura 2010). Finally, because they are living microorganisms and may be able to reproduce, synthetic biology microbes, once released, may be extremely difficult or even impossible to eliminate from the environment (Tucker & Zilinskas 2006). For these reasons, synthetic biology microbes may present additional challenges beyond traditionally genetically modified microbes, including microbes developed for bioremediation.

## Regulating synthetic biology

As with other technologies, synthetic biology is not regulated as a technology per se in the United States. Rather, pursuant to the 1986 Coordinated Framework for Regulation of Biotechnology, synthetic biology, like earlier generations of biotechnology products before it, will be regulated based on particular products and particular uses (Office of Science and Technology Policy 1986). As such, any synthetic biology microbes will be regulated pursuant to existing environmental and human health protection statutes. The primary responsibility for governing the risks of synthetic biology products in the United States will fall to the U.S. Environmental Protection Agency ("EPA") under the Toxic Substances Control Act ("TSCA").

### *The Toxic Substances Control Act*

The Toxic Substances Control Act regulates the production, use, and disposal of hazardous chemical substances (15 U.S.C. §§ 2601–95d). TSCA was intended as a "gap filling" statute to fill in the regulatory interstices that are not covered by other statutes. Thus, unlike most other environmental statutes in the U.S., TSCA is not limited by the medium in which the chemicals are released or the manner in which the chemicals are used, and therefore is one of the broadest environmental statutes in scope. In addition, TSCA permits regulation of chemical substances before, during, and after their use. For these reasons, TSCA is likely the most important statute concerning the regulation of synthetic biology microbes engineered for biofuel production, chemical production, and bioremediation in the United States. Under the Coordinated Framework for Regulation of Biotechnolo-

gy, the EPA has primary responsibility for regulating most genetically engineered microbes under TSCA (Office of Science and Technology Policy 1986).

The most important provision of TSCA for purposes of the oversight of synthetic biology products is section 5, which requires manufacturers of new chemical substances, or significant new uses of existing chemicals, to submit a "pre-manufacturing notice" ("PMN") to EPA before commercial production. Dating back to the Coordinated Framework in 1986, EPA has treated genetically engineered microorganisms slightly differently than other new chemical substances under TSCA. Unless otherwise exempted by EPA regulations, manufacturers of new intergeneric engineered microorganisms must submit a Microbial Commercial Activity Notice ("MCAN") to EPA for review at least ninety days prior to the commercialization of the product.[3] The MCAN thus functions as a PMN for intergeneric genetically engineered microorganisms, but not for non-intergeneric microorganisms, based on the assumption that only the former are likely to present novel risks.

Also distinct for genetically modified microorganisms, for pre-commercialization field trials, the manufacturer must submit a TSCA Experimental Release Application ("TERA") to EPA at least sixty days prior to commencing field testing. While these pre-market notification requirements of TSCA have been the primary focus of EPA's oversight of genetically engineered microbial products to date, other provisions of TSCA could apply to genetically engineered microbes in certain circumstances, and are discussed below.

**Threshold Authority Concerns**

There are two threshold regulatory authority concerns regarding the regulation of synthetic biology organisms pursuant to TSCA: whether living microorganisms are subject to TSCA in the first instance, and whether the definition of intergeneric engineered microorganisms under TSCA might restrict EPA's authority with respect to synthetic biology organisms.

First, TSCA was enacted to regulate the release of "chemical substances" into the environment (15 U.S.C. § 2601). "Chemical substance" is defined broadly under TSCA to include "any organic or inorganic substance of a particular molecular identity, including." (15 U.S.C. § 2602(2)(A)). While the EPA has concluded that Congress intended "chemical substance" to be defined broadly to encompass living microorganisms, and consequently has relied on TSCA to regulate biotechnology products for over twenty-five years (EPA 1997a; EPA 1997b), Congress gave no indication when it enacted TSCA in 1976 that it anticipated the inclusion of living microorganisms within the definition of "chemical substance." (Chadwick 1995). EPA's definition of "chemical substances" to include living microorganisms is thus open to challenge, and while EPA's definition would likely prevail,[4] this is not a guarantee and the mere possibility of an adverse outcome could deter the EPA from regulating as aggressively as it otherwise might consider appropriate.

Second, EPA's regulations under TSCA that require manufacturers of new intergeneric engineered microorganisms to submit an MCAN define intergeneric microorganisms as "organisms

---

[3] This notice requirement functions as the equivalent of a pre-manufacturing notice ("PMN") for traditional chemical substances under section 5 of TSCA. The EPA regulations for the MCAN and TERA contain a number of full or partial exemptions, which are unlikely to apply synthetic biology-produced microbes, and thus are not discussed here.

[4] Under the *Chevron* doctrine, which requires reviewing courts to defer to an agency's "reasonable" interpretation of an ambiguous statutory provision (Chevron, U.S.A., Inc. v. Natural Res. Def. Council 1984).

formed by combining genetic material from organisms in different genera." (40 C.F.R. §§ 725.1(a), 725.3). EPA's policy is based on traditional genetic modification techniques and the premise that the transfer of genetic information from more distantly related organisms (i.e., organisms from different genera) are more likely to create new or modified traits that could present a risk (EPA 1997a). Synthetic biology, however, raises the possibility of introducing wholly synthetic genes or gene fragments (i.e., DNA sequences that do not exist in nature) into an organism. Similarly, synthetic biology may allow scientists to remove a gene fragment from an organism, modify that fragment, and then reinsert it back into the same organism. In either case, such organisms may not be "intergeneric" under EPA's definition because they would not include genetic material from organisms of different genera.[5] Because the MCAN regulations state that they "establish […] all reporting requirements [for] microorganisms," (40 C.F.R. §§ 725.1(a)) non-"intergeneric" genetically modified microorganisms currently are not covered by any TSCA premanufacture notice requirements. Synthetic biology modifications, however, may have a greater probability of creating a novel risk than most intra-generic transfers exempt from regulation.

Due to the unforeseen evolution of biotechnology across time, synthetic biology microorganisms thus create potential gaps in the current regulatory structure that do not exist for traditional genetically modified organisms. Roger Brownsword has developed the concept of regulatory disconnection to refer to this mismatch that can develop (Brownsword 2008). Because the law does not evolve as rapidly as technology, regulation governing technology can become disconnected from the attributes of the technology. Such circumstances can leave a void until the judiciary or legislature act to reconnect the law (Brownsword 2008).

**Life-Cycle Analysis of Synthetic Biology Microbes under TSCA**

Like any product, synthetic biology microbes have the potential to create environmental or health risks across various stages of their life-cycle. Although no specific risks for synthetic biology microbes have been identified to date, if such risks emerge, EPA will need to use its existing TSCA authority to address those risks. This section evaluates the potential application of, and possible challenges in applying, the pertinent regulatory provisions of TSCA to each stage of the synthetic biology microbelife-cycle.

At the research and development stage, the manufacturer of a synthetic biology microbe strain generally must submit a TSCA Experimental Release Application ("TERA") to EPA at least sixty days prior to any field testing of a new strain. EPA then has sixty days to review the submission. A key challenge for this field testing requirement for all genetically engineered microbes, including synthetic biology ones, is that any risks that escape EPA's notice at the field testing stage could result in a permanent and even growing problem given the capability of living microorganisms to reproduce and proliferate. Thus, the consequences of any problem at the field testing stage could be much larger for microbes than for the traditional chemical substances for which TSCA

[5] With the advent of synthetic biology, the EPA's distinction between intergeneric and non-intergeneric microorganisms actually runs afoul of the dictate of the Coordinated Framework that the products of bioltechnology should be regulated based on the product itself, not based on the process by which it was made (Office of Science and Technology Policy 1986).EPA's current MCAN regulations would differentiate between an intergeneric microorganism produced by traditional genetic modification techniques (which would be subject to MCAN regulations) and a synthetically produced identical microorganism (potentially not subject to MCAN regulations).

was designed, where a problem at this stage would generally be limited to the usually small quantity of chemical used in a field test.

Because many products in the research and development stage are not successful and may never be commercialized, however, imposing significant regulatory costs and burdens at this early stage of product development could have adverse impacts on innovation. EPA must strike a delicate (and inevitably not always optimal) balance between precaution and innovation in implementing the TERA review for synthetic biology microorganisms. The increased uncertainties about the risks from synthetic biology relative to "traditional" genetically modified microbes will exacerbate this tension.

A related challenge in the research and development stage is how thoroughly and effectively EPA can identify and address any risks created by field testing of synthetic biology microbe products in the sixty-day TERA window. Unlike other products, such as traditional chemicals, that can be quickly evaluated by existing models,[6] there are no such screening methods for synthetic biology products. Given the variety and complexity of genetic manipulations made possible by synthetic biology, combined with the lack of a methodology or even track record on which to base its determinations, EPA's capability to reliably assess risks of field testing synthetic biology microbes in the sixty days provided by TERA is questionable.

Moreover, chemical substances used in research and development that are not manufactured for "commercial purposes" are exempt from TSCA's premanufacture notice requirements (40 C.F.R. § 720.22(a)(1)).[7] "Commercial purpose" is defined broadly by the EPA under TSCA to include any production of chemical substances with the purpose of obtaining an immediate or eventual commercial advantage (40 C.F.R. § 720.3(r)). Private, non-"commercial purpose" activities, however, are beyond TSCA's scope (Presidential Commission on Bioethical Issues 2010; Rodemeyer 2009). This is a particular concern for synthetic biology because many expect synthetic biology to popularize and decentralize the development of new organisms (National Science Advisory Board for Biosecurity 2010). Traditional genetic engineering requires substantial expertise, expensive laboratory equipment, and funding. Synthetic biology is likely to be available to anyone with a spare room and a few hundred dollars, spawning the so-called "DIY Bio" movement (Hsu 2010). The inability to reach non-commercial activities thus presents a significant gap in the regulation of synthetic biology microbes. As one example, the International Genetically Engineered Machine (iGEM) competition is an annual synthetic biology competition that involves thousands of undergraduate students building biological systems out of a set of biological parts (Hsu 2010). Because this or similar competitions may not involve a "commercial purpose," the engineered microbes developed as part of such activities may not be subject to TSCA.[8]

The most significant regulatory controls EPA possesses under TSCA concerning synthetic biology microbes are the pre-commercialization notification requirements. TSCA section 5 authorizes the EPA to regulate new hazardous chemical substances where the manufacture, processing,

---

6 EPA screens new chemicals based on structure-activity relationships, which informs the agency of potential risks of a new chemical based on an extensive experiental database on the relationship between various molecular chemical structures and toxicity.

7 *See also* 40 C.F.R. § 725.234 (providing an exemption from TSCA Experimental Release Application requirements for certain enclosed research and development activities).

8 Indeed, there is no record that iGEM participants have applied for TERA approvals.

distribution in commerce, use, or disposal of the substance presents an unreasonable risk of injury to health or the environment (15 U.S.C.§ 2605). Where a chemical substance presents an unreasonable risk, the EPA may prohibit or limit the amount of its manufacture or use (15 U.S.C.§ 2605). Even this authority, however, is limited and could be problematic if synthetic biology microbes present significant risks.

As noted above, the developer of a new synthetic biology microbe involving the intergeneric transfer of genetic material must submit a Microbial Commercial Activity Notice ("MCAN") to EPA at least ninety days prior to commercialization. EPA then has ninety days to make a determination on whether the product will present an unreasonable risk to human health or the environment. Like the traditional pre-manufacture notice ("PMN") requirement for conventional chemicals from which it is derived through TSCA section 5, the MCAN imposes no affirmative duty on the product developer to generate any safety information, but rather only requires the developer to submit known and reasonably ascertainable data. In contrast, the European Union's analogous chemical regulation law, the Regulation on the Registration, Evaluation, and Authorization of Chemicals (REACH), places greater data production requirements on chemical manufacturers, depending in part on the quantity of chemical substance produced (Fleurke & Somsen 2011).

There are ongoing concerns that the EPA lacks sufficient authority to provide a meaningful safety review in ninety days in the absence of mandatory data requirements, and such concerns are even greater for synthetic biology microbes. Unlike traditional chemicals, which EPA usually evaluates using already existing risk assessment models using structure-activity relationships and other computational biology approaches, EPA lacks any existing methodology or data set against which to evaluate the risks of novel synthetic biology products. Moreover, while PMN analyses for chemicals focus on human toxicity, most significant risk scenarios for synthetic biology algae and bioremediation products involve environmental releases that may result in some form of ecological harm. Such concerns are much more difficult to study and predict than human health risks. Because the burden of proof of establishing a reasonable basis is on the EPA, reaching a finding of an unreasonable risk to health or the environment from synthetic biology microbes, particularly within this limited time frame, will be a significant challenge, especially in the early stages of synthetic biology development, as the data and understanding concerning synthetic biology risk analysis are lacking or are limited. In many cases, it may be impossible to understand certain synthetic biology microbe risks well until the technology develops further. Accordingly, there are serious doubts about EPA's ability to identify and manage any risks that may be presented by synthetic biology microbes using the existing MCAN mechanism.

Pursuant to TSCA section 4, the EPA may require that a product manufacturer conduct and report testing with respect to human health and environmental effects if a chemical substance either (1) may present an "unreasonable risk of injury to health or environment"; or (2) "will be produced in substantial quantities" and "may reasonably be anticipated to enter the environment in substantial quantities" or "result in substantial human exposure." (15 U.S.C. § 2603(a)(1)(A)(i), (B)(i)). Such testing, however, can only be required after the EPA has sufficient data to meet its burden to show there may be a problem and EPA makes a finding that existing available data are "insufficient" to determine or predict the health and environmental effects of the product (15 U.S.C. § 2603 (a)(1)(A)(ii), (B)(ii)). These requirements put a substantial evidentiary burden on EPA before it can require a product manufacturer to conduct testing. Based on historical precedent, it often takes EPA approximately ten years from start to finish to adopt and implement a test rule under

TSCA section 4 (GAO 2007). The first finding ("unreasonable risk") is often the biggest obstacle for such a test rule, and this will likely also be the case for synthetic biology microbes. EPA is rarely able to make a finding that a chemical substance for which it is seeking more safety data presents an "unreasonable risk"—if EPA had sufficient data to make such a finding, it would not need to undertake more testing, but rather proceed with more direct regulatory action. The European REACH Regulation again provides an alternate model, providing a burden-shifting mechanism in certain conditions (Fleurke & Somsen 2011).

For these reasons, EPA almost always supports section 4 testing requirements using the second trigger—that the product "will be produced in substantial quantities" and "may reasonably be anticipated to enter the environment in substantial quantities" or "result in substantial human exposure." The substantial quantity measures, however, are set by statute and regulation based upon traditional chemical quantities and a direct relationship between mass and risk, thresholds that are inappropriate for synthetic biology microbes. The REACH regulation in Europe faces similar limitations (Fleurke & Somsen 2011). In addition, the expectation is that in many cases synthetic biology microbes will be in controlled and contained environments, unlike traditional chemical substances, and thus if substantial environmental release and human exposure occurs, the regulatory and risk management systems will have already failed. It is likely that for many synthetic biology microbes the EPA will be unable to meet the Section 4 threshold requirements. In these cases, the EPA lacks statutory authority to require further testing concerning human health and environmental impacts of synthetic biology microbes.

TSCA provides limited authority for EPA to conduct post-market surveillance and risk management of regulated products such as synthetic biology microbes. TSCA section 8 provides a series of reporting and recordkeeping requirements, some of which could be important for oversight of synthetic biology microbes. For example, section 8(c) requires the manufacturer or distributor of a product to keep records of significant adverse effects to human health or the environment alleged to have been caused by their product. However, the effectiveness of this provision is limited in two key ways. First, a company is only required to maintain records of allegations of such effects, and not to itself identify or mitigate such effects. Second, the company is only required to retain the information and is not required to report the allegations to EPA unless specifically requested to do so by the Agency.

Section 8(e) of TSCA requires the manufacturer or distributor of a product to report to EPA any information that "reasonably supports the conclusion that the chemical substance or mixture presents a substantial risk of injury to health or the environment." (15 U.S.C. § 2607(e)). EPA has not issued regulations implementing section 8(e) to date, so it is not clear precisely what type of scenarios relating to synthetic biology microbes would trigger reporting requirements under this provision. However, given the statutory language of "substantial risk," as well as the historical implementation of this provision, it is likely that results showing actual or serious potential for harm would be required, and this may not encompass some of the key incidents that would be important to report to EPA about synthetic biology microbes, such as unintended environmental releases that may not trigger section 8(e) but which nevertheless may be of concern to EPA.

If EPA identifies potential post-marketing risks associated with synthetic biology microbes, it potentially could take regulatory action under section 6 of TSCA to attempt to manage those risks. Section 6 of TSCA gives EPA an extensive menu of potential risk management options including prohibition of a product, restrictions on the quantity or use of a product, requirements for labeling or

communicating the risks of a product, restrictions on product disposal, testing requirements, and reporting requirements (15 U.S.C. § 2605(a)). However, to impose such a requirement, EPA must make a finding based on a quantified cost-benefit calculation that the product poses an "unreasonable risk," and moreover that the proposed regulatory action is the least burdensome for protecting against the unreasonable risk (15 U.S.C. § 2605(c)(1)). As enforced by the courts, these requirements are very difficult for the agency to satisfy (Corrosion Proof Fittings v. EPA 1991)). Indeed, EPA has issued rules under section 6 for only five chemicals since the statute was enacted in 1976 (polychlorinated biphenyls, fully halogenated chlorofluoroalkanes, dioxin, asbestos, and hexavalent chromium) (GAO 2005). One of these, a proposed ban on certain asbestos products, was based on ten years of study and a 45,000 page record, but was struck down by a federal appeals court in 1991 for lacking sufficient cost-benefit analysis and not imposing the least burdensome regulation (Corrosion Proof Fittings v. EPA 1991). The EPA has not tried to exercise this authority subsequently. For these reasons, TSCA (or the judicial interpretation of TSCA) has been criticized by commentators for imposing unrealistic data and certainty requirements (Lin 2007). Considering the limited scientific knowledge concerning the risks of synthetic biology microbes, it would be difficult, if not impossible, for EPA to conduct the necessary cost-benefit analysis to satisfy the least burdensome regulation requirement.

The lack of serious post-commercialization surveillance or authority represents a significant concern for synthetic biology microbes, particularly bioremediation or algae products that may be intentionally placed into the open environment. One of the hallmark characteristics of organisms is that they evolve. A synthetic biology microbe thus may mutate, creating both a new organism and new chemical products produced by that organism, all without the manufacturers' or EPA's knowledge. These new organisms and chemical products could have different risk profiles than the intended products. Synthetic biology microbes may be able to be designed so that the risk of evolution is low, but biological controls can fail. In addition, because of some of the potential regulatory gaps and exemptions discussed above, the original synthetic biology microbe may not have been appropriately evaluated in the first instance regarding risks related to evolution or other concerns.[9] This represents a major gap for the regulatory oversight of synthetic biology microbes under TSCA—if a risk exists and EPA fails to identify and address that risk in the brief MCAN window of opportunity, or if EPA never had an opportunity to assess the risk, the agency may be without any effective regulatory authority to recognize or manage subsequent events.

EPA's ability to assess the risks of new synthetic biology organisms is a particularly daunting task. EPA generally evaluates the risks of a new organism based upon the known relatives of that organism (Presidential Commission on Bioethical Issues 2010). This method may be insufficient for synthetic biology microbes, given that such microbes may be derived from a large number of existing organisms, with no particular organism providing a close enough relative for pertinent risk assessment purposes. Further, a significant manner in which the EPA has evaluated traditionally genetically engineered microbes depends on the presumption that the basic biology of the microbe had not changed though genetic engineering. This presumption may not be true for a variety of synthetic biology microbes. Even a synthetic biology microbe that may be similar to an existing

[9] It is possible that there have already been genetically modified microbes produced through traditional rDNA techniques that raise similar issues, but there does not appear to be any publicly available information on such.

organism in many ways could contain significant differences with unknown effects on risk. These risks will be exacerbated for any microbe released into the environment, given the uncertainty of the organism's interaction with various external environmental stimuli. Risk assessment for synthetic biology is in its infancy, raising substantial challenges for much of EPA's analyses (Tucker & Zilinskas 2006). Given the limits inherent in the current statute and regulations, EPA will have a very difficult role to play under TSCA both in adequately protecting against human health and environmental risks, and in balancing the need to conduct adequate risk assessments against the desire to permit this nascent technology to develop without undue regulation.

### *National Institutes of Health Guidelines*

The U.S. National Institutes of Health (NIH) could also play a role in managing synthetic biology risks, but its authority is limited in this regard. NIH has guidelines for constructing and handling recombinant DNA organisms generally, but these guidelines apply only to research conducted by or funded by federal agencies, and do not reach private industry (Presidential Commission on Bioethical Issues 2010). Although private researchers may voluntarily follow the guidelines, compliance is not required unless the research is federally funded (DHHS 2011). Thus, private research concerning synthetic biology microbes engineered for chemical production may substantially take place outside of agency oversight.

As discussed above, governance of private research activities is a particular concern for synthetic biology because one of the much-anticipated features of synthetic biology is that it will permit a broader spectrum of small private entities and individuals to engage in the engineering of new organisms. While traditional genetic engineering techniques require substantial monetary and laboratory resources, individuals are expected to be able to engage in synthetic biology activities in their home and with limited resources.

Finally, the NIH guidelines only concern contained research and do not give any guidance concerning the deliberate release of microbes into the environment. A private researcher seeking to study microbes in the environment would not even have any best practices or guidance available concerning appropriate protective measures to take.

## Innovative Synthetic Biology Governance through 'Soft-Law'

The previous sections reveal that, as was the case with the first generations of genetically engineered products (Mandel 2004), the existing statutory and regulatory matrix has certain concerns regarding synthetic biology. These concerns arise from statutory and regulatory gaps, inadequate regulatory authority, and uncertain technology characteristics, all produced by unforeseen technological development. Though this case study focused on synthetic biology governance under U.S. law, similar circumstances and challenges exist for other emerging technologies in jurisdictions around the world (Brownsword 2008; Lin 2007).

Emerging technologies disrupt extant regulatory systems and do not fit neatly into their historically created schemes. This mismatch can produce regulatory disconnection between evolving technology and the law (Brownsword 2008). In spite of the potential concerns of regulatory disconnection, however, absent some unexpected tragedy or disaster, there often is not sufficient impetus for major statutory overhaul. This is not surprising: major change is not only politically difficult, time-consuming, and expensive, but due to the challenges of regulating at a technological and

temporal distance, uncertain to achieve success. Synthetic biology likely fits this pattern. The uncertainties about the technological trajectory and risks of synthetic biology, the wide range of products and applications, and the promising environmental, health and economic benefits of synthetic biology all counsel against major new regulatory impositions at this time, as the U.S. President's Commission on Bioethics recently concluded (Presidential Commission on Bioethical Issues 2010).

While new regulatory provisions may be premature for nascent technologies, other types of innovative "soft law" measures can help to fill current gaps until such time as the need for, and focus of, formal regulation has been better delineated. Soft law measures can produce flexible interim (or long-term) measures that can more rapidly enable a sound oversight system. In addition to allowing a promising technology to develop while protecting human health and the environment, such measures can also help to maintain public confidence, provide industry with some certainty concerning regulatory requirements, and assure investors that the technology will be developed safely and without unduly restrictive/regulatory burdens.

One soft law initiative for synthetic biology would be a type of "issue manager" that could help coordinate the research and regulatory actions of the various governmental agencies that may have some oversight responsibilities for synthetic biology. Though not discussed in detail above, the myriad products and potential impacts of synthetic biology mean that synthetic biology products and uses will likely fall within the regulatory purview of numerous agencies and services. An instructive precedent for an issue manager might be the U.S. National Nanotechnology Initiative ("NNI"), including its National Nanotechnology Coordination Office ("NNCO") that provides administrative and coordination and the Nanoscale Science, Engineering, and Technology ("NSET") Subcommittee composed of representatives of federal agencies with an interest in nanotechnology. The NNI with its various subcomponents serves as a focus for media, industry and interested stakeholders to interact with the government and each other on issues relating to nanotechnology, including safety and regulatory issues. The NNI also coordinates important initiatives such as research & development planning and coordination, and even issues such as a common definition of nanotechnology. A similar coordinating body for synthetic biology would likewise help to provide some coherence and central organization for the rapidly evolving and sprawling field of synthetic biology.

Another useful step forward would be a private-public partnership to develop the data and risk assessment models that agencies such as EPA need to provide effective regulatory oversight. While statutes such as TSCA do have various deficiencies as outlined above, the biggest impediment agencies are likely to face with synthetic biology are the uncertainties and novelty in trying to assess product risks. Not all synthetic biology products are likely to be dangerous, and thus across-the-board restrictions would likely to do more harm than good. Rather, agencies need the capability to identify the products most likely to present significant risks, and to identify risk management options that can adequately control those risks. To achieve this, agencies need better data and risk assessment methods. Much of the data necessary for adequate risk assessment is often in industry's hands, but it is also in industry's interest for government to develop this more fine-tuned and effective regulatory focus and to implement a governance structure that maintains public confidence in the technology. There should be opportunity and common interest in industry and government pooling their expertise and resources to develop the tools necessary to better predict and manage synthetic biology risks.

Regulatory agencies may be able to leverage some of the uncertainty concerning their regulatory authority in certain regards to such an end. For example, notwithstanding the limitations on EPA's authority under section 5 of TSCA, EPA could be innovative in using this potential authority to engage product manufacturers in more proactive and collaborative safety measures. EPA's use of TSCA section 5 authority for nanomaterials could serve as a potential model, as nanomaterials have some similarities to synthetic biology microbes in that they present greater uncertainties about risk that are not amenable to being addressed using conventional risk modeling techniques. EPA has used its TSCA section 5 authority to persuade product manufacturers to enter into consent decrees in which the manufacturers agree to undertake additional safety measures, such as various worker protection measures (e.g., use of personal protective equipment), conduct subchronic toxicity studies on the products, and impose restrictions on product use. A similar approach could be developed for synthetic biology products that might come under EPA's TSCA authority, but the challenge will be in developing a set of reasonable safety measures that can help assure the safety of the products without unduly burdening the product's commercialization. In addition, because certain synthetic biology microbes primarily involve potential ecological rather than human health risks, this might be a more difficult undertaking than was the case for EPA's treatment of nanomaterials.

Other soft law measures could be developed to incentivize industry to disclose useful information related to potential synthetic biology risks. For example, also in the context of nanotechnology, the U.S EPA developed the Nanoscale Materials Stewardship Program (NMSP) as a voluntary reporting program designed to promote data-sharing by industry (Abbott et al. 2012). Interested parties were invited to comment and participate at each stage of development of NMSP, and over thirty companies participated, submitting information on 132 nanomaterials. Four companies went beyond data provision to actually conduct testing on their nanomaterials. Though the program was only a partial success, with less participation and lower quality data than anticipated, EPA still reported that it received "a significant amount of data through NMSP submissions," which allowed it to develop "a considerably stronger and better informed understanding of the issues and commercial status of nanoscale materials in the United States" (EPA 2009). A similar program, building on lessons from NMSP, could be developed for synthetic biology products. For example, the NMSP suffered in participation because industry perceived the program to offer few benefits and was unsure how the data would be used (Abbott et al. 2012). The latter issue could be resolved with clearer disclosure and the former by offering tangible benefits, such as fast-tracked permit review or other concrete benefits for program participants.

Valuable soft law initiatives could also be developed at the international level. For example, the Intergovernmental Panel on Climate Change (IPCC) is an intergovernmental scientific body, set up to provide comprehensive scientific assessment of scientific, technical and socio-economic information worldwide about the risk of climate change caused by human activity, its potential environmental and socio-economic consequences, and possible options for adapting to these consequences or mitigating the effects (IPCC 2006). Thousands of scientists and other experts contribute on a voluntary basis to producing IPCC reports, which are reviewed by representatives from approximately 120 participating governments (IPCC 2010). Though the IPCC has had certain problems concerning the use of non-peer reviewed data, potential conflicts of interest, and policy neutrality, in an area rife with dissensus, the IPCC has become a generally widely-respected international authority on climate change (Simon & Pentland 2012). A similar intergovernmental scientific

body could be created for synthetic biology to investigate and report on its potential risks. This body could learn from the structural problems with the IPCC's organization to provide a reliable international scientific body for assessing scientific risks and concerns surrounding synthetic biology. Because synthetic biology policy appears to be less culturally and ethically charged that the climate change debate, and because it concerns a more discrete field of technology, an international panel in this context may have a greater opportunity for success.

Soft law measures should not be considered a panacea. They have been criticized in differing contexts for failing to require serious commitments, advance implementation of protective measures, or provide sufficient incentives for compliance (Abbott et al. 2012). However, the issue is not whether soft law can provide a perfect governance structure, but whether it offers sufficient advantages over current mechanisms. Given the uncertainty surrounding emerging technology opportunities and risks, and public and political limitations on the extent of regulatory change that is feasible, soft law mechanisms will often offer the most practical means to develop an early-stage governance structure that can be adaptable as a technology develops further, adequately protect human health and the environment, and not unduly hinder the development of promising new technologies. These measures can help maintain public confidence in the protective structure of the governance system and provide industry and investors with needed certainty for further investment in a technology at the early stages of technological development. Soft law measures can then evolve into a sound oversight system as a technology develops further, and its benefits and risks are better understood (Malloy 2012). All of these factors make the soft law options surveyed above, and others, worthy of serious consideration for emerging synthetic biology technologies.

## Conclusion

It is not surprising that a technology as potentially revolutionary as synthetic biology would raise a number of concerns under a regulatory system developed largely prior to its inception. Regulatory systems, almost by definition, are designed for technologies existing at the time of the regulatory systems' formation and are based on the then-current understanding of that technology. Unsurprisingly, regulatory systems often face difficulty and disruption when applied across time to newly emerging technologies. These challenges, however, can also represent opportunities. Opportunities to reenvision governance at a technological and temporal distance to utilize soft law mechanisms that can provide more efficient and more comprehensive risk protection. Addressing the regulatory concerns surrounding synthetic biology microbes early and proactively can permit synthetic biology to continue to develop in as rapid a manner as possible consistent with the need to adequately protect human health and the environment.

## References

Abbott K.h W., G.E. Marchant, & E.A. Corley (2012). Soft Law Oversight Mechanisms for Nanotechnology, 52 *Jurimetrics* J. 279.

Balmer A. & P. Martin (2008). Synthetic Biology: Social and Ethical Challenges, Institute for Science and Society, University of Nottingham 17.

Bhutkar A. (2005). Synthetic Biology: Navigating the Challenges Ahead, 8 *J. Biolaw & Bus*. 19

Biello D. (2011). The False Promise of Biofuels, *Scientific American.*

Boyle R. (2012) Swiss Scientists Program Mammalian Cells to Work as Logic Gates, *Popular Science*.

Brownsword R. (2008) The Challenge of Regulatory Connection, in *Rights, Regulation, and the Technological Revolution*.

Callura J.M., et. al. (2010). Tracking, Tuning, and Terminating Microbial Physiology using Synthetic Riboregulators.

Carriquiry M., X. Du, G.R. Timilsina (2011) Second Generation Biofuels: Economics and Policies, 39 *Energy Pol'y* 422.

Cases I. & V. de Lorenzo (2005). Genetically Modified Organisms for the Environment: Stories of Success and Failure and What We Have Learned from Them, 8 *Int'l Microbiology* 213.

Chadwick R.A. (1995). Regulating Genetically Engineered Microorganisms Under the Toxic Substances Act, 24 *Hofstra L. Rev.* 223, 234-35.

Chen C.-Y., et al. (2011) Cultivation, Photobioreactor Design and Harvesting of Microalgae for Biodiesel Production: A Critical Review, 102 *Bioresource Technology* 71.

Chevron, U.S.A., Inc. v. Natural Res. Def. Council, Inc., 467 U.S. 837 (1984).

Chopra P. & Kamma A. (2006). Engineering Life through Synthetic Biology, 6 In *Silico Biology* 401

Corrosion Proof Fittings v. EPA, 987 F.2d 1201 (5th Cir. 1991).

DHHS (2011). NIH Guidelines for Research Involving Recombinant DNA Molecules § 1-C-1.

EPA (2009). Nanoscale Materials Stewardship Program: Interim Report.

EPA, Microbial Products of Biotechnology; Final Regulations under the Toxic Substances Control Act; Final Rule, 62 Fed.Reg. 17,910 (April 11, 1997).

EPA, Microbial Products of Biotechnology: Final Regulation Under the Toxic Substances Control Act – A Summary of the Public's Comments and the Agency's Response (Mar. 26, 1997).

Erickson B. et al. (2011) Synthetic Biology: Regulating Industry Uses of New Biotechnologies, 333 *Science* 1254.

European Commission (2005), Synthetic Biology: Applying Engineering to Biology, Report of a NEST High-Level Expert Group.

Ferber D., Time for a Synthetic Biology Asilomar?,303 *Science* 159,Jan. 9, 2004

Fleurke F. & H. Somsen (2011). Precautionary Regulation of Chemical Risk: How REACH Confronts the Regulatory Challenges of Scale, Uncertainty, Complexity, and Innovation, 48 *Common Market L. Rev*. 357.

GAO (2005). Chemical Regulation: Options Exist to Improve EPA's Ability to Assess Health Risks and Manage Its Chemical Review Program.

GAO (2007) Chemical Regulation: Comparison of US and Recently Enacted European Union Approaches to Protect Against the Risks of Toxic Chemicals 20.

Hsu J. (2010). The Wild World of DIY Synthetic Biology, *Popular Science*, Feb. 12, 2010.

Hylton W.S. (2012). Craig Venter's Bugs Might Save the World, *N.Y. Times Mag.*, May 30, 2012.

Intergovernmental Panel on Climate Change, Principles governing IPCC work (2006).

Intergovernmental Panel on Climate Change, Understanding Climate Change: 22 years of IPCC assessment (2010).

Jarrell K. et al. (2010). Synthetic Biology: Challenges, Opportunities, Feature Commentary: Industry Survey, 6 Indus. *Biotechnology* 321.

Keasling J. D. (2010) Manufacturing Molecules Through Metabolic Engineering, 330 Sci. 1355

Khalil A. S. & J. J. Collins (2010). Synthetic Biology: Applications Come of Age, 11 *Nature Revs. Genetics* 367.

Krivoruchko A., V. Siewers, & J. Nielsen (2011). Opportunities for Yeast Metabolic Engineering: Lessons from Synthetic Biology, 6 *Biotechnology J.* 262.

Lin A. C. (2007). Size Matters: Regulating Nanotechnology, 31 *Harv. Envtl. L. Rev.* 349.

Malloy T. F. (2012). Soft Law and Nanotechnology: A Functional Perspective, 52 *JurimetricsJ.* 347.

Mandel G. (2004). Gaps, Inexperience, Inconsistencies, and Overlaps: Crisis in the Regulation of Genetically Modified Plants and Animals, 45 *Wm. & Mary L. Rev.* 2167.

Mandel G. (2009). Regulating Emerging Technologies, 1 *Law, Innovation, & Tech.* 75.

National Renewable Energy Laboratory (NREL) (1998).A Look Back at the U.S. Department of Energy's Aquatic Species Program—Biodiesel from Algae.

National Science Advisory Board for Biosecurity (2010). Addressing Biosecurity Concerns Related to Synthetic Biology.

Office of Science and Technology Policy, Coordinated Framework for Regulation of Biotechnology, 51 Fed.Reg. 23,302 (June 26, 1986).

Oh Y.-K. (2011). Current Status of the Metabolic Engineering of Microorganisms for Biohydrogen Production, 102 *Bioresource Tech.* 8357.

Parmar A. et al. (2011). Cyanobacetria and Microalgae: A Positive Prospect for Biofuels, 102 *Bioresource Tech.* 10163.

Pollack A. (2010). U.S. Bioethics Commission Gives Green Light to Synthetic Biology, N.Y. Times, Dec. 10, 2010.

Presidential Commission for the Study of Bioethical Issues (2010). New Directions: The Ethics of Synthetic Biology and Emerging Technologies 94.

Rodemeyer M. (2009). New Life, Old Bottles, Synthetic Biology Project 23.

Ruder W. C. et al. (2011) Synthetic Biology Moving into the Clinic, 333 *Science* 1248.

Savage N. (2011) Algae: The Scum Solution, 474 *Nature* S15, S16.

Schmidt Ch.W. (2010). Synthetic Biology: Environmental Health Implications of a New Field, 118 *Envtl. Health. Perspectives* A118.

Simon M. S. & W. Pentland (2012). Reliable Science: Overcoming Public Doubts in the Climate Change Debate, 37 *Wm. & Mary Envtl. L. & Pol'y Rev.* 219.

Singh J. & S. Gu (2010). Commercialization Potential of Microalgae for Biofuels Production, 14 *Renewable& Sustainable Energy Revs.* 2596.

Tsuda S. et al. (2005). Robot Control with Biological Cells, 87 *Biosystems* 215.

Tucker J. & R.A. Zilinskas (2006). The Promise and Perils of Synthetic Biology, 12 *The New Atlantis* 25.

Van Noorden R. (2010). Demand for Malarial Drug Soars, 466 *Nature* 672.

Viebahn M. et al. (2009). Effect of Genetically Modified Bacteria on Ecosystems and Their Potential Benefits for Bioremediation and Biocontrol of Plant Diseases—A Review, Climate Change, Intercropping, Pest Control, and Beneficial Microorganisms, 2 *Sustainable Agricultural Reviews* 45.

Weiss R. (2007). Creation 2.0, *Wash. Post*, 31 Dec. 2007.

# Bridging distances in approach: Sharing ideas about technology regulation

Lyria Bennett Moses
University of New South Wales
✉lyria@unsw.edu.au

**Abstract** New technologies pose a range of challenges for regulators – do existing regulatory frameworks apply appropriately (and clearly) in new contexts and are new rules and practices required to address new concerns? Although existing rules and values will vary across jurisdictions, technological change causes similar questions to be raised in different jurisdictions at a similar time. However, institutional approaches to answering them differ. On many occasions, Australia has relied on law reform commissions to consider these questions, while in Europe the emphasis has been primarily on technology assessment (although both utilise a range of other mechanisms as well). This paper compares the approaches of law reform and technology assessment, exploring opportunities for mutual learning.

**Keywords** technology regulation, technological change, law reform, technology assessment

## Introduction

Although legal systems and regulatory structures vary across borders, much technological change is increasingly synchronised around the developed world. Thus concern about the regulation of such things as nanotechnology and synthetic biology tends to begin at approximately the same time. The desire to regulate stems from a range of concerns from health, safety and environmental risks to the protection of important and fundamental values, as well as to a sense that 'we' ought to intentionally shape our socio-technical environment to achieve more desirable outcomes. Although goals may be similar in Australia and Europe, the means employed to achieve these goals differ substantially. In Australia, law reform commissions have been a prominent role in designing rules for new technologies whereas, in Europe, parliamentary technology assessment has been important. While neither of these operate alone (with parliamentary committees, government departments and agencies, ad hoc commissions and so forth playing a role), they are important within their own spheres.

Law reform and technology assessment each have their own literatures, exploring problem definition, function, methodology and impact. With the exception of the United Kingdom, they tend to operate in different jurisdictions – with law reform prominent in Australia and some Pacific countries, while technology assessment dominants in Europe. Technology assessment and law reform are not the same thing, but they operate in an overlapping space. In particular, both can be a useful means of exploring and evaluating possible approaches to the regulation of new technologies.

At a transnational level, there may be benefits from developing an approach that draws on the best aspects of diverse national responses to managing the interface between law and regulation on the one side and new technologies and socio-technical change on the other. The significant distances between law reform and technology assessment practitioners, which are both geographical and disciplinary, means that there has been little opportunity for mutual learning to date. The goal of this paper is to introduce law reform and technology assessment, to highlight some similarities and differences and to explain how transnational, cross-disciplinary dialogue might be of benefit.

The questions discussed here are as important as, albeit separate from, questions of an international response to technologies as such. There has been some discussion in the literature about the need for or design of a better framework for international law to develop rules and norms to govern new technologies (Abbott 2011; Picker 2001). An agreed international governance framework for a new technology may be sought where no single country acting alone has the capacity to manage a problem (as is arguably the case with on-line child pornography) or where a technology risks encroaching on internationally agreed rights (as is arguably the case with some genetic technologies). The importance of recognising the relationship between human rights and technology has been addressed in the literature (Hildebrandt & Gutwirth 2008; Kirby 1986; Murphy 2009). This paper focuses on circumstances where the issue is not 'international' as such, in particular where there are legitimate national differences as to whether and how a particular practice ought to be regulated. In the case of the Internet, for example, different countries have stronger or weaker preferences for freedom of speech, elimination of various types of problematic content (in particular hate speech and pornography), individual privacy, and surveillance as a means of reducing criminal activity. While some positions may fall foul of international human rights norms, others are within the bounds of ordinary disagreement. International agreement will be possible (and desirable) on some issues, but not others. However, even where issues are left for individual states, there is still scope for transnational learning on how such questions can be approached. This paper explores the kinds of mutual learning that may be beneficial in the face of substantive disagreement. In particular, it explores differences between a law-oriented and technology-oriented approach and suggests areas where transnational dialogue may lead to improved outcomes.

The paper comprises five further sections. The following section briefly describes why regulators are interested in issues at the technological frontier, thus setting up the types of questions raised in different jurisdictions. The third and fourth sections describe two methodologies that are the focus of this paper – law reform as practiced in Australia and technology assessment as practiced in Europe. The fifth section summarises the limited transnational and inter-disciplinary scholarship, while the last section explains the ways in which these two different approaches might learn from each other. Throughout, I have drawn on the example of law reform and technology assessment reports concerning privacy for information and communication technologies to illustrate differences in approach and outcome.

## The regulation of emerging technologies

Before going further, it is necessary to define what is meant by the *regulation* of *technology* and why it may be felt necessary. While the term regulation can carry different meanings, a useful starting point is Julia Black's definition as "the sustained and focussed attempt to alter the behaviour of others according to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information-gathering and behaviour modification" (Black 2002). This deliberately excludes non-intentional 'regulation', as when behaviour is restricted as a result of market forces. While regulation need not stem from government (and may include self-regulation or professional codes), this paper will often take a government *perspective* in that it focuses on the means employed, directly or indirectly, by government to direct the course of evolving technological practice in desired directions (which may include promotion of non-government regulation or funding of privately run programs).

Defining technology poses greater difficulties, as the term has multiple meanings, which focus on different aspects of an increasingly important phenomenon. In defining technology as such, one can focus on the fact that they are 'tools' or means to achieve an end (Koops 2010) or on the fact that they enable new forms of conduct (Schon 1967). Alternatively, one can adopt a multi-dimensional approach that considers technology as technological artefacts, technological knowledge, technological activities of using and making, and volition (Mitcham 1994). A commonly employed shortcut, that in a sense avoids the need for a definition, is to think about *technology* regulation in terms of 'hot topics' drawn from fields such as nanotechnology, information and communication technology, biotechnology, neurotechnology, robotics, and so forth (Allenby 2011). The realness of such categories (especially in the case of nanotechnology) can be the subject of dispute, but the regulatory issues that arise can nevertheless be identified (Ludlow, Bowman, & Hodge 2007). This is because new socio-technical practices commonly raise legal and regulatory issues (Bennett Moses 2007). In particular, if people can do or make new things, then questions arise as to whether such things ought to be prohibited, permitted, encouraged, discouraged or co-ordinated (if they are not already under broadly framed rules).

Thus one tends not to see too much navel gazing, in legal literature at least, about the definition of technology. People have a general sense of what it is and why, in many cases, regulation is desirable. At a simple level, it is recognised that technological artefacts and activities can bring benefits, but can also cause harms. For instance, the production and use of technology may be associated with negative environmental consequences or health and safety risks. These risks have been said to be of a different order in the case of modern technologies (Beck 1992). As well as such quantifiable problems, technological practices can also impinge on other values, as when there are concerns about a diminution in privacy associated with information and communication technologies, a loss of respect for human dignity associated with human cloning or distributive concerns that arise in both the direction of inventive efforts and ownership of and responsibility for outcomes. There is commonly a strong desire to preserve current values in the face of new technological possibilities that may undermine them (Cockfield 2004), at least initially (Bernstein 2002). At a deeper level, new technologies can challenge us to re-examine our commitment to particular values and their meaning, as when reproductive technologies force us to rethink the importance of 'natural' conception (Bernstein 2002) or the Internet forces us to rethink the meaning and importance of democracy (Klang 2006). Values are rarely static and, even at one time, are the subject of disagreement, in particular as to their relative priority.

Bringing these strands together, technology regulation is a means of exercising *intentional* control over the shape of (new) technological artefacts and practices in order to decrease the likelihood of a negative outcome or increase the likelihood of a positive outcome, as assessed by reference to particular values. In other words, the 'regulator' takes the perspective of wanting to extract the maximum benefit and minimise the harms from a particular technology. This is done through direct or indirect encouragement, facilitation, regulation, prohibition or co-ordination of particular new things, activities and relationships.

In terms of the path actually taken, there will usually be no single 'best answer', at least if it is accepted that there is scope for disagreement about the relative importance of different values. Even where risks can be quantified using an agreed methodology (which is only sometimes the case), an assessment of a particular proposal for regulation (or non-regulation) will depend on different preferences in terms of both risk tolerance and value priorities (such as whether one is more

comfortable with environmental or economic risks) (Renn 1999). One can attempt to work within a particular risk framework, and may be required to so in some jurisdictions.[1] But, generally speaking, spheres of agreement will be surrounded by contentious ground.

Not every new technology requires particular new regulation. In many cases, broadly applicable rules applying to contracts, property, competitive markets and so forth will be sufficient. In fact, much socio-technical change takes place without any regulatory crisis. However, existing regulations are sometimes inadequate – they may fail to apply in the new context, or their applicability may be uncertain (Bennett Moses 2007). Sometimes adjustments can be made to existing regimes in order to encompass changes in socio-technical practices. Other times, it is not simply a question of tweaking, as where the challenges posed are sufficiently unique or have not been addressed. The threat to a particular value may be new, and different in kind from those posed previously. Many new technologies are not within jurisdiction of an existing agency and the types of problems raised may not covered by existing law (Mazur 1981).

Although existing practices and value preferences vary across jurisdictions, the kinds of technologies that pose these types of problems will be similar. Due to globalisation, similar questions will thus arise at similar times across different jurisdictions. There are three distinct areas where transnational learning may be of use. The first, which occurs through the international scientific community, is to establish the 'facts' on which decisions about regulation can be based. This involves identifying possible benefits and harms (at least the known knowns and known unknowns), quantifying those that can be quantified in terms of magnitude and probability (and specifying where quantification is not possible, or not possible *yet*), and being clear about what is certain and what remains uncertain (as well as how and when ascertainable uncertainties might be resolved). The second is to determine areas of predetermined international agreement by applying international rules and norms to the particular situation, where applicable, or creating new ones. The third is to explore appropriate methods through which different jurisdictions can explore normative disagreement within their own communities and design appropriate regulations at the local, state or national level.

This paper focuses on the third task. There are many different institutions that play a role in exploring how technologies may impinge on particular values, attitudes to such tensions and appropriate regulatory responses (by government and/or non-government actors). These include government-sponsored institutions conducting law reform, technology assessment and policy analysis. Bodies such as parliamentary committees, government departments, judges, professional bodies, ad hoc and specialist commissions also play a role. This is not the occasion for examining the diversity of roles played (Bennett Moses 2011). Rather this paper focuses on two that have been subject to extensive examination in the literature in terms of purpose and methodology – law reform and technology assessment.

## Technology assessment

Technology assessment was first institutionalised in the now defunct Office of Technology Assessment in the United States in 1972 (Bimber 1996). Before it was defunded by a cost-cutting Congress, the Office of Technology Assessment often worked on similar issues to law reform

[1] E.g., Treaty on European Union, Official Journal C 115, 09/05/2008 P. 0001 – 038.

commissions in Australia (Australian Law Reform Commission 1983, 2004; New South Wales Law Reform Commission 1988; OTA 1986a, 1986b, 1987, 1988). While technology assessment is still practiced to some extent in the US Government Accountability Office (Sclove 2010), members of the European Parliamentary Technology Assessment network (EPTA) have overtaken the United States to become world leaders in technology assessment (Russell, Vanclay, Salisbury, & Aslin 2011; Vig & Paschen 2000). EPTA and its members have considered similar issues, albeit from a different angle, to the Australian Law Reform Commission, for example in relation to privacy in the information age (Australian Law Reform Commission 2008; European Parliamentary Technology Assessment 2006).

Definitions and approaches to technology assessment differ between different organisations and also across history. Developments in technology assessment have been closely tied to evolving views in social science about the relationship between technology and society. In particular, the realisation that particular technological futures are not inevitable implies that an understanding of different possibilities (and their consequences) might enable better choices. Classical definitions of technology assessment focus on systematic expert evaluation of technological possibilities to determine benefits as well as potential harms (including indirect, unintended or delayed impacts) of particular technological developments and trajectories (Armstrong & Harman 1980; Coates 1976; Hetman 1973; Vig & Paschen 2000). In this classical version, policy-makers would be informed of an assessment, and could use it to design better policy. Although technology assessment still incorporates scientific analysis of risk, it now increasingly recognises non-quantitative (Hansson 2011) and aesthetic (Pitt 1989) approaches, as well as the importance of non-expert participation. Following extended dialogue amongst the technology assessment community in Europe, technology assessment has recently been defined as "a scientific, interactive and communicative process which aims to contribute to the formation of public and political opinion on societal aspects of science and technology." (Decker & Ladikas 2004). Thus technology assessment no longer focuses exclusively on providing rationally derived technical information to policy audiences, but rather promotes understanding, reflexivity and debate amongst designers, policy makers and broader publics.

Within the technology assessment community, there is extensive discussion of approach and methodology (Decker 2010; Decker & Ladikas 2004; Joss & Durant 1995). From technocratic approaches, there is now a strong focus on different techniques that can be used to enable broad participation in decisions around technological design and regulation linked to ideas such as citizen juries (Dunkerley & Glasner 1998), consensus conferences (Joss & Durant 1995), discursive technology assessment (Renn 1999), interactive technology assessment (Rathenau Institute 1997), real-time technology assessment (Guston & Sarewitz 2002; Sarewitz 2005), among others. This does not mean that there is no role for expertise – expertise is still required to inform participatory technology assessment and evaluate its implications – only that it does not operate in isolation (Sclove 2010).

A report on technology assessment on the issue of information and communication technologies and privacy helps illustrate the diversity of approaches to methodology (European Parliamentary Technology Assessment 2006). Nine technology assessment institutions in Europe joined together to summarise related technology assessment exercises and propose some policy options. Participatory techniques included focus groups, consensus conferences, citizen and stakeholder workshops, and consultation with citizen and expert panels. There were also technolo-

gy assessment reports that did not employ participatory techniques, relying instead on expertise or analysis. Where the public were involved, they were actively recruited. They did not act as stakeholders so much as citizens, with Leisner and Cas (representing technology assessment institutions in Denmark and Austria) writing that "[w]hen citizens participate in technology assessment projects they tend to have a democratic interpretation of their role, and they will reflect on the consequences not only for themselves but for other members of society, such as the underprivileged."

Whether or not a technology assessment results in new law, it is clearly designed to regulate (or influence) technological practices. It engages with those who design and manufacture technologies, encouraging thinking about the link between design decisions and broader public values and concerns. This is particularly so in real time technology assessment (Guston & Sarewitz 2002; Sarewitz 2005). By enhancing informed public debate and consciousness about technological possibilities, choices and consequences, it may also make users more conscious of technological choices they make. In some cases, government regulation or industry codes of practice will also emerge from the process, for example setting limits in order to prevent particular outcomes. But, whether or not this occurs, the goal of technology assessment includes influence over (and in that sense regulation of) technological design and use. In line with this goal, technological uncertainties and possible trajectories are explicitly discussed, together with advantages and disadvantages, for example in relation to ubiquitous computing, privacy enhancing technologies and RFID tags (European Parliamentary Technology Assessment 2006).

There are differences between technology assessment as it exists in the world (with limited resources and limited spheres of influence) and an idealised technology assessment. Ideally, technology assessment would be carried out for every significant or larger technological project beginning at an early stage of its development and continuing throughout (Wilsdon & Willis 2004). It should be closely linked with funding mechanisms, to ensure that funding goes to projects with proven future benefits and confined future risks (Lin 2010-2011). Multiple parties should be involved, including designers and affected stakeholders as well as policy-makers. General citizens ought to have a say through mechanisms such as citizen juries combined with national referenda (Lin 2010-2011). It should be an ongoing process, alongside technological development (Rip, Misa, & Schot 1995). Needless to say, in practice these goals have not always been achieved (Goven 2003; Jensen 2005; Sclove 2010).

Although technology assessment is centred in Europe, there have been moves in the United States and Australia to re-establish technology assessment capabilities (Bennett Moses 2011). Despite the demise of the Office of Technology Assessment, there has been some technology assessment in the United States – in the Government Accountability Office, the National Research Council, and through academic projects. Political efforts to revive the former Office of Technology Assessment, however, have thus far proved unsuccessful (Sclove 2010). In Australia, the Department of Industry, Innovation, Science, Research and Tertiary Education has been exploring ways in which citizens can become involved in policy-making around new technologies through the STEP framework (STEP 2012). Despite its geographical location, this approach has more in common with European technology assessment than Australian law reform.

## Law reform

Law reform has a long history in Australia, with the first New South Wales Law Reform Commission being established by Letters Patent in 1870. It has waxed and waned over the intervening years in the various states and territories. At a federal level, the Australian Law Reform Commission has been operating since 1975, with the task of reviewing, simplifying and modernising Australian law. Formally, its work program is dictated by the Attorney-General, although consultation is common.

Like technology assessment, law reform has different roles and there are disputes as to how law reform ought to be defined, what its goals ought to be and what methods are the most appropriate (Burrows 2003; Macdonald 1997; Samek 1977). Within Australia at least, law reform generally includes (but is not limited to) recommendations for legislative changes in a field of concern. Many law reform reports have little to do with emerging technologies but involve the resolution of various issues from technical legal questions to important national questions such as the role of indigenous law. Nevertheless, particularly in Australia, there has been a strong emphasis on ensuring law's responsiveness to new technologies and, in particular, designing regulations that will preserve important values (such as privacy) in the face of technological change. Bringing law 'up to date' is one of the statutory functions of law reform commissions.[2] But much of the emphasis on this aspect of its role is due to the early influence of Michael Kirby who emphasised the Australian Law Reform Commission's responsibilities in this area (Kirby 1988). In Australia, significant numbers of reports directly address 'technology regulation' issues including the regulation of human tissue transplants (Australian Law Reform Commission 1977), genetic testing (Australian Law Reform Commission 2003), Internet content (Australian Law Reform Commission 2012b) and reproductive technologies (New South Wales Law Reform Commission 1988).

Although law reform institutions have partnered with other bodies where appropriate, their own expertise is primarily legal (Burrows 2003; Hurlburt 1986). Technology assessment, at least in the sense of understanding a technology and its anticipated effects, is seen as an input into a law reform report, and is generally addressed in background chapters. Technology tends to be "black boxed" for most of a report, in that it is taken as the current state of affairs. There is minimal horizon-scanning and minimal mention of potential technological trajectories or alternative pathways. For example the 2008 Australian Law Reform Commission Report into privacy focussed on technology already in commercial use such as databases that were already in existence (for genetic information, property holdings, financial transactions, credit worthiness, consumer preferences, and so forth) (Australian Law Reform Commission 2008, 151-153). Horizon technologies, such as ubiquitous computing, were mentioned briefly but not subjected to the same analysis as currently existing technologies.

Not only does law reform focus on current technologies, it also tends to begin late in a technological development timeline. It tends to follow, rather than proceed, technology assessment elsewhere. For example, the inquiry on gene patenting (which published its report in 2004) concluded that the time to recommend that gene sequences should not be patentable had "long since past" (Australian Law Reform Commission 2004). While European technology assessment organi-

[2] E.g., Australian Law Reform Commission Act 1996 (Aust) ss 21(1)(a), (c).

sations had completed extensive reports on privacy issues around information and communication technologies prior to 2006 (European Parliamentary Technology Assessment 2006), including in relation to horizon technologies (such as ubiquitous computing), the Australian Law Reform Commission did not complete its report on issues relating to current commercial practices in this area until 2008.

Technology assessment and law reform manage the problem of ongoing technological change (requiring repeated regulatory changes) in different ways. An ideal technology assessment will continue to monitor technological developments, and seeks to begin discussion early in a technology's development. While technology assessment engages actively in horizon scanning, law reform seeks to manage ongoing technological change through a preference for technology-neutral (Australian Law Reform Commission 2008, 422) or principles-based regulation (Australian Law Reform Commission 2008, 235-242). This approach is possibly the only solution in a context where law reform reports on a particular issue are large scale, once-off events. The Australian Law Reform Commission has expressed the view that it would be "undesirable" to design legislation to accommodate technologies which are yet to be invented or deployed, although it can recommend that continuing monitoring be done by others (Australian Law Reform Commission 2008, 422, 430).

The idea of "technology regulation" as such is less prominent in law reform than in technology assessment. The output of a law reform report is generally (but not always) proposed changes in legislation along with recommendations for guidelines, education programs and changed practices directed to government, independent agencies, industry and other groups. Nevertheless, despite not being framed in terms of 'technology regulation', that is the impact of many of the Australian and state law reform commission recommendations. One advantage of the law reform approach is that they show awareness of the fact, sometimes ignored in technology assessment (Edquist 1994), that regulation targeted at something other than the technology in question can indirectly influence that technology. Thus, after introducing a technology, a law reform report will attempt to summarise how existing rules apply to a new technology within relevant spheres, whether or not those rules were originally intended to 'regulate' the technology as such. The starting point is thus the current legal framework. For example, in its privacy inquiry, the ALRC described its task as being "to review an existing piece of legislation…and to consider emerging areas that may require privacy protection" (Australian Law Reform Commission 2008, 150). This was reflected in the layout of its report – after an introductory chapter, five chapters explored the existing legal regime (including the extent to which new technological practices are covered by existing statutory categories), two chapters discussed some specific limitations of that regime, after which were four chapters under the overarching heading "Developing Technology", and further chapters exploring specific issues, including recommendations for legal change. Changes to law and regulation are thus proposed in the context of deep analysis of the existing framework, and are very specific.

Law reform also differs from technology assessment in how it engages with publics. For longer than technology assessment, law reform has recognised the importance of public input. In its opening Annual Report for 1975, the federal Law Reform Commission adopted the words of the Law Reform Commission of Canada in recognising that

> ... there must be dialogue and consultation with the public in order to unearth and to articulate public opinion on the law – discussing with the public the values they think the law should enshrine, the functions it should perform, the aims it should pursue. (Law Reform Commission of Canada 1973-1974; The Law Reform Commission (Australia) 1975).

Law reform has always allowed significant *opportunity* for comment from interested members of the public. Law reform generally involves an issues paper, a discussion paper which makes tentative proposals for reform, followed by a final report. A variety of mechanisms, including podcasts, information sheets, media interviews, social media and public fora are used to publicise these reports. People can also ask to be added to a mailing list for a particular inquiry.

However, while there is plenty of opportunity for public comment on issues and proposals, there is less emphasis on seeking to engage with members of the public who are not already engaged on an issue. The result is that the level of engagement with the general public, as opposed to stakeholders and advocacy groups, varies significantly across different reports. In its gene patenting report, the Australian Law Reform Commission paid lip service to the need for public consultation, but spent its time actually meeting with stakeholders and advocacy organisations rather than the public directly (Australian Law Reform Commission 2004). A similar pattern can be seen in the report on privacy, with consultations focused on government (and related bodies), private sector agencies, advocacy groups, lawyers and academics (Australian Law Reform Commission 2008, Appendix 2). In the latter case, there were some roundtables, fora, workshops and a phone-in on specific issues with members of the public. In some reports there have been public fora involving a "set presentation" followed by comments and questions from the floor or members of the Commission sitting on panels at general public fora (Australian Law Reform Commission 2003). The usual focus, however, is on consulting with those who can 'speak for' the public, rather than the public directly. This is sometimes explained by the additional costs as well as the lack of democratic legitimacy in any event (North 1985). There is also reliance on quantitative and qualitative data prepared by other organisations (Opeskin 2002). For example, in the privacy report, the ALRC relied on external reports on questions of community attitudes to privacy and cost implications of its recommendations and recommended further study on the attitudes of young Australians to privacy (Australian Law Reform Commission 2008, 114, 129, 475). While members of the public do sometimes prepare submissions on topics of interest to them, as was the case with respect to classification of video games in a recent inquiry (Australian Law Reform Commission 2012b), these are often organised by more established groups. There are some recent moves in a positive direction, with the commission announcing a strategy to engage with people from diverse backgrounds (Australian Law Reform Commission 2012a). Still, compared to the vast literature on participation in technology assessment, engagement with the public directly, where it happens, lacks a fully developed methodology. That is not to say that public consultation by law reform commissions is not worthwhile or effective, only that it operates without reference to the kinds of justificatory theories and evaluations that one finds in technology assessment. This has led to criticism that the Commission can end up relying too much on anecdotes from vocal stakeholders (Graycar 2000).

Another difference between technology assessment and law reform is with respect to implementation rates. The implementation rates for law reform reports are high, with the most recent annual report of the Australian Law Reform Commission stating that 59% of its reports have been substantially implemented, 30% partially implemented, 6% currently under consideration and only 5% not implemented (Australian Law Reform Commission 2012a). While technology assessment can point to some successes in this regard, the rates are far lower. Of course, technology assessment has other aims, so this is not a critique, only an observation.

## Engagement across national and disciplinary lines

Law reform and technology assessment literatures, in the sense of discussion around goals, problem definition, methodologies and influence, are mostly separate, with different journals, conferences and authors involved. Part of the reason for this is geographical – other than the United Kingdom, there are few jurisdictions that recognise a significant role for both kinds of institutes. However, it is primarily disciplinary – law reform commissions and technology assessment bodies recruit on the basis of different qualifications and see themselves as doing different things (which, in part, they are). Thus although there are some cross references between technology assessment and law reform reports *on particular issues*, there is no discussion across the disciplinary/geographical divide about how the task of deliberately shaping technological practice in which both play a role ought to be carried out.

Lawyers have shown relatively little interest in technology assessment and the technology assessment community has largely ignored law reform. Legal interest in technology assessment as a process is mostly historical (Burns 1976; Green 1967, 1983; Portnoy 1969; Tribe 1971, 1973), although there is always interest in the outcomes of particular technology assessments. Such legal commentary as exists looks at technology assessment in itself – exploring proposals to improve it (Lin 2010-2011), critiquing particular approaches (Tribe 1973) or arguing that particular procedures meet technology assessment standards (Kritikos 2009). Where comparisons are made to legal processes, it has been to formal procedural processes such as criminal trials rather than law reform (Hildebrandt & Gutwirth 2008).

Unlike the poor links between technology assessment and law reform, there is significant mutual learning among those seeking to optimise regulatory design generally. The cohesion around regulatory studies has meant that there are significant parallels between, for instance, the European Union's "Better Regulation" initiative[3] and Australia's "Best Practice Regulation".[4] But transnational conversations about the best way to design regulation generally does not seem to have carried over to conversations about how to manage the law/regulation/technology interface.

## Opportunities for engagement

Technology assessment and law reform operate in an overlapping space. As discussed in Section 2 above, there are diverse circumstances in which one wishes to consider regulating a new technology. Ultimately, one is dealing with (possibly contested) values that may be enhanced or challenged by potential technological practices where existing legal and regulatory structures are insufficient for managing the conflict, either because they are under-inclusive or because the nature of the challenge is new. In short, one is dealing with tensions in a socio-techno-legal space (Dizon 2012), and a desire to deliberately shape its future in accordance with particular value preferences (whether assumed or derived through the process itself). It is therefore not surprising to find similar topics being examined by institutions in Europe and Australia.

While the technology assessment and law reform sometimes address similar problems, their perspective and approach are different. Technology assessment typically starts from a technology,

---

3 http://ec.europa.eu/governance/better_regulation/index_en.htm.

4 http://www.finance.gov.au/obpr/proposal/gov-requirements.html

charts its possible and probable implications. Different methods dictate to some extent how this is achieved – whether directly through influence over designers or indirectly through government regulation (although each is a kind of 'regulation' in its broad sense). Law reform generally assumes a state of technology, and is unwilling to venture as far into future possibilities. It builds on an analysis of existing law and regulation to identify gaps and problems raised by (existing) new practices and propose solutions. Its proposals, and in particular those that relate to recommendations for new law, are generally detailed and commonly enacted in accordance with what was proposed. Law reform also makes recommendations to non-government institutions, but does not make recommendations about technological design as such. While technology assessment tends to less detail on its recommendations (in a sense black boxing law), law reform tends to black box technology itself. Each focuses more closely on one part of the socio-techno-legal dynamic.

The shared role explains the fact that law reform and technology assessment have approached related debates about how technological practice ought to be made to align with particular values. What is more difficult to explain is why these two ways of thinking about the problem have rarely been compared. A deep understanding of both technological and legal histories and possibilities would surely be an advantage in formulating recommendations for how a socio-techno-legal space ought to be shaped. Mutual learning in this context would not necessarily lead to similar outcomes. Technology assessment in Europe and law reform in Australia both fulfil an advisory function. In both cases, recommendations are ultimately adopted (or not) by other actors (including government and industry). The kind of mutual learning I am proposing is thus not an avenue to harmonisation of technology regulation internationally – it will not dissolve disagreement. Rather, it is a proposal that might lead to improvements in the tools used within different jurisdictions for deciding how to regulate technology in light of each jurisdiction's own values and preferences.

In particular, there are two areas in which Australian law reform commissions could learn from European technology assessment. The first is by considering approaches to public engagement used in participatory technology assessment. Both law reform and technology assessment invoke the importance of broad community involvement. Both do so for similar reasons – for normative reasons related to democratic ideals, substantive reasons (to improve decision-making) and pragmatic reasons (for example, to enhance compliance) (Opeskin 2002; Wilsdon & Willis 2004).Among its other benefits, public participation facilitates learning about value preferences (Skene 1985). To date technology assessment practitioners have generated a more extensive discussion about how this is best achieved, and law reformers, despite having been interested in public participation for longer, could benefit from considering means by which a broad range of citizens can be engaged. Secondly, law reform could benefit from a better understanding of the contingency of technological development and the potential for regulation (in the sense of intentional influence or control) to shape development pathways.

Conversely, technology assessment practitioners could benefit from considering how law reform commissions operate. Typically, a law reform report ends not merely with a sense of what problems exist, but specific proposals for change, both to legislation and in other areas, that build on existing law and practice. In technology assessment, conclusions are often expressed in more general terms such as the need for (better or updated) legislation to protect particular rights such as privacy, the desirability of regulation of particular technologies or requirements to use better technologies, and the need for better enforcement of existing laws and consumer education

(European Parliamentary Technology Assessment 2006). By increasing specificity, it is may be possible for technology assessment institutions to exercise greater influence over policy. By building on a detailed understanding of existing general regulatory frameworks, it may be possible to avoid unnecessary technology specificity in its proposals.

Both technology assessment and law reform employ a combination of expertise (scientific/technical and legal respectively), public engagement (described respectively in terms of consultation or participatory technology assessment) and communication in order to achieve their goals. In both cases, reports may recommend legislative changes in light of technological developments. However, due to the lack of overlap between law reform and technology assessment literatures and the lack of opportunities for mutual engagement between practitioners of law reform and practitioners of technology assessment, there has been little opportunity for mutual learning. While interest in technological assessment has existed within Australia, it is rarely referred to by Australian legal scholars. In particular, the extensive literature on methodologies of public engagement (or participatory technology assessment) (Joss and Durant 1995; Decker 2010) has not been discussed in relation to Australian law reform commissions. The fact that law reform and technology assessment work in an overlapping space suggests that a comparison of methodologies, and suggestions for integrating these approaches would be fruitful.

## References

Abbott, Kenneth W. (2011). An International Framework Agreement on Scientific and Technological Innovation and Regulation. In G. E. Marchant, B. R. Allenby & J. R. Heckert (Eds.), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight: The Pacing Problem*: Springer.

Allenby, Braden R. (2011). Governance and Technology Systems: The Challenge of Emerging Technologies. In G. E. E. Marchant, B. R. R. Allenby & J. R. R. Herkert (Eds.), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight* (Vol. 7): Springer.

Armstrong, Joe E, & Harman, Willis W. (1980). *Strategies for Conducting Technology Assessments*. Boulder Colorado: Westview Press.

Australian Law Reform Commission. (1977). Human Tissue Transplants.

Australian Law Reform Commission. (1983). Privacy.

Australian Law Reform Commission. (2003). Report 96. Essentially Yours: The Protection of Human Genetic Information for Australia.

Australian Law Reform Commission. (2004). Genes and Ingenuity: Gene patenting and human health.

Australian Law Reform Commission. (2008). For Your Information: Australian Privacy Law and Practice (Vol. 108).

Australian Law Reform Commission. (2012a). Annual Report 2011-2012. Sydney.

Australian Law Reform Commission. (2012b). Classification - Content Regulation and Convergent Media.

Beck, Ulrich. (1992). *Risk Society: Towards a New Modernity* (M. Ritter, Trans.): Sage.

Bennett Moses, L. (2007). Recurring Dilemmas: The Law's Race to Keep Up with Technological Change. *University of Illinois Journal of Law, Technology and Policy, 7*, 239.

Bennett Moses, L. (2011). Agents of Change: How the Law "Copes" with Technological Change. *Griffith Law Review, 20*(4), 263-294.

Bernstein, Gaia. (2002). The Socio-Legal Acceptance of New Technologies: A Close look at Artificial Insemination. *Washington Law Review, 77*, 51.

Bimber, Bruce. (1996). The Politics of Expertise in Congress: The Rise and Fall of the Office of Technology Assessment. Albany NY: SUNY Press.

Black, Julia. (2002). Critical reflections on regulation. *Australian Journal of Legal Philosophy, 27*, 1-35.

Burns, Stephen G. (1976). Congress and the Office of Technology Assessment. *George Washington Law Review, 45*, 29.

Burrows, Andrew. (2003). Some Reflections on Law Reform in England and Canada. *Canadian Business Law Journal, 39*, 17.

Coates, Joseph F. (1976). The Role of Formal Models in Technology Assessment. *Technological Forecasting and Social Change, 9*.

Cockfield, Arthur J. (2004). Towards a Law and Technology Theory. *Matinoba law Journal, 30*(3), 32.

Decker, M (Ed.). (2010). Interdisciplinarity in Technology Assessment: Implementation and its Chances and Limits. Berlin Heidelberg: Springer-Verlag.

Decker, M, & Ladikas, M (Eds.). (2004). Bridges between Science, Society and Policy: Technology Assessment - Methods and Impact (Vol. 22). Berlin Heidelberg: Springer.

Dizon, Michael Anthony C. (2012). From Regulating Technologies to Governing Society: Towards a Plural, Social and Interactive Conception of Law. In H. Morgan & R. Morris (Eds.), *Moving Forward: Tradition and Transformation*: Cambridge Scholars Publishing.

Dunkerley, David, & Glasner, Peter. (1998). Empowering the public? Citizens' juries and the new genetic technologies. *Critical Public Health, 8*(3), 181-192.

Edquist, Charles. (1994). Technology Policy: The Interaction between Government and Markets. In G. Aichholzer & G. Schienstock (Eds.), *Technology Policy: Towards an Integration of Social and Ecological Concerns* (pp. 67). Berlin, New York: Walter de Gruyter.

European Parliamentary Technology Assessment. (2006). ICT and Privacy in Europe.

Goven, Joanna. (2003). Deploying the Consensus Conference in New Zealand: Democracy and De-Problematization. *Public Understanding of Science, 12*(4), 423-440. doi: 10.1177/0963662503124006.

Graycar, Regina. (2000). Law Reform by Frozen Chook: Family Law Reform for the New Millennium? *Melbourne University Law Review, 24*(3), 737-755.

Green, Harold P. (1967). Technology Assessment and the Law: Introduction and Perspective. *George Washington Law Review, 36*, 12.

Green, Harold P. (1983). Should Technology Assessment Guide Public Policy *American Bar Association Journal, 69*, 5.

Guston, David H, & Sarewitz, Daniel. (2002). Real-Time Technology Assessment. *Technology in Society, 24*, 16.

Hansson, Sven Ove. (2011). Coping with the Unpredictable Effects of Future Technologies. *Philosophy & Technology, 24*(2), 137-149.

Hetman, Francois. (1973). Society and the Assessment of Technology. Paris: OECD.

Hildebrandt, M, & Gutwirth, S. (2008). Public Proof in Courts and Jury Trials: Relevant for pTA Citizens' Juries? *Science, Technology and Human Values, 33*(5), 582-604.

Hurlburt, William H. (1986). Law Reform Commissions in the United Kingdom, Australia and Canada. Edmonton, Canada: Juriliber.

Jensen, Casper Bruun. (2005). Citizen Projects and Consensus-Building at the Danish Board of Technology: On Experiments in Democracy. *Acta Sociologica, 48*(3), 221-235. doi: 10.1177/0001699305056564.

Joss, Simon, & Durant, John (Eds.). (1995). Public participation in science: the role of consensus conferences in Europe. England: Science Museum.

Kirby, Michael. (1986). Human Rights – The Challenge of the New Technology. *Australian Law Journal, 60*, 170.

Kirby, Michael. (1988). Law Technology and the Future. *Australian Journal of Forensic Sciences, 21*.

Klang, Mathias. (2006). Disruptive Technology: Effects of Technology Regulation on Democracy. (PhD), Göteborg University, Göteborg.

Koops, Bert-Jaap. (2010). Ten Dimensions of TEchnology Regulation: Finding your bearings in the research space of emerging technologies. In M. Goodwin, B.-J. Koops & R. Leenes (Eds.), *Dimensions of Technology Regulation* (pp. 309): Wolf.

Kritikos, Mihail. (2009). Traditional risk analysis and releases of GMOs into the European Union: space for non-scientific factors? *European Law Review, 34*(3), 405-432.

Law Reform Commission of Canada. (1973-1974). Third Annual Report.

Lin, Albert. (2010-2011). Technology Assessment 2.0: Revamping our Approach to Emerging Technologies. *Brooklyn Law Review, 76*, 1309-1370.

Ludlow, K, Bowman, D, & Hodge, G. (2007). A Review of Possible Impacts of Nanotechnology on Australia's Regulatory Framework: Final Report: Australian Office of Nanotechnology.

Macdonald, Roderick A. (1997). Recommissioning Law Reform. *Alberla Law Review, 35*(4), 48.

Mazur, Allan. (1981). *The dynamics of technical controversy*. Washington, D.C.: Communications Press.

Mitcham, Carl. (1994). Thinking Through Technology: The Path between Engineering and Philosophy. Chicago: University of Chicago Press.

Murphy, Thérèse. (2009). Repetition, Revolution, and Resonance: An Introduction to New Technologies and Human Rights. In T. Murphy (Ed.), *New Technologies and Human Rights*. Oxford OUP.

New South Wales Law Reform Commission. (1988). Artificial Conception: In vitro fertilization (Vol. 58).

North, PM. (1985). Law Reform: Processes and Problems. *Law Quarterly Review 101*, 338-358.

Opeskin, Brian. (2002). Engaging the public: community participation in the genetic information inquiry. *Reform, 80*, 53-58, 73.

OTA. (1986a). Electronic Record Systems and Information Privacy.

OTA. (1986b). Intellectual Property Rights in an Age of Electronics and Information.

OTA. (1987). New Developments in Biotechnology: Ownership of Human Tissues and Cells.

OTA. (1988). Infertility: Medical and Social Choices.

Picker, Colin B. (2001). A View From 40,000 Feet: International Law and the Invisible Hand of Technology. *Cardozo Law Review, 23*, 70.

Pitt, Joseph. (1989). Technology and the Objectivity of Values. In T. Curry & L. Embrey (Eds.), *Technology and the Life World* (pp. 165-180): The Centre for ADvanced Study in Phenomenology.

Portnoy, Barry M. (1969). Role of the Courts in Technology Assessment *Cornell Law Review, 55*, 18.

Rathenau Institute. (1997). Technology Assessment through Interaction - A Guide.

Renn, Ortwin. (1999). Participative technology assessment : meeting the challenges of uncertainty and ambivalence *Futures research quarterly, 15*(3), 81-97.

Rip, Arie, Misa, Thomas J., & Schot, Johan (Eds.). (1995). *Managing Technology in Society: The Approach of Cosntructive Technology Assessment*. London and New York: Pinter Publishers.

Russell, Wendy A, Vanclay, Frank M, Salisbury, Janet G, & Aslin, Heather J. (2011). Technology assessment in Australia: the case for a formal agency to improve advice to policy makers. *Policy Science, 44*, 157-177.

Samek, Robert. (1977). A Case for Social Law Reform. *Canadian Bar Review, 55*(3), 27.

Sarewitz, Daniel. (2005). This Won't Hurt a Bit: Assessing and Governing Rapidly Advancing Technologies in a Democracy. In M. Rodemeyer, D. Sarewitz & J. Wilsdon (Eds.), *The Future of Technology Assessment*. Washington DC: Woodrow Wilson International Center for Scholars.

Schon, Donald. (1967). *Technology and Change*. Oxford: Pergamon Press.

Science and Technology Pathways (STEP): Community Involvement in science and technology decision making. (2012).Canberra.

Sclove, Richard. (2010). Reinventing Technology Assessment: A 21st Century Model. *Woodrow Wilson International Centre for Scholars*.

Skene, Loane. (1985). Consultation: Asking law reform questions and listening to the answers. *Law Institute Journal, 59*, 453-455.

The Law Reform Commission (Australia). (1975). Annual Report. Canberra.

Tribe, Laurence H. (1971). Legal Frameworks for the Assessment and Control of Technology. *Minerva, 9*, 243.

Tribe, Laurence H. (1973). Technology Assessment and the Fourth Discontinuity: The Limits of Instrumental Rationality. *Southern California Law Review, 46*, 617.

Vig, Norman J, & Paschen, Herbert (Eds.). (2000). *Parliaments and Technology - The Development of Technology Assessment in Europe*. Albany: State University of New York Press.

Wilsdon, James, & Willis, Rebecca. (2004). See-Through Science: Why Public Engagement Needs to Move Upstream: Demos.

# The challenge of regulating biologicals; the PRCA controversy and the creation of the European biosimilar regulatory framework

Hans. C. Ebbers
Utrecht University
Utrecht Institute for Pharmaceutical Sciences (UIPS)&Copernicus Institute of Sustainable Development
✉h.ebbers@uu.nl

Huub Schellekens
Utrecht University
Utrecht Institute for Pharmaceutical Sciences (UIPS)&Copernicus Institute of Sustainable Development
✉h.schellekens@uu.nl

Hubert G. Leufkens
Utrecht University
Utrecht Institute for Pharmaceutical Sciences (UIPS)
✉H.G.M.Leufkens@uu.nl

Toine Pieters
Utrecht University & VU Amsterdam Medical Centre
Utrecht Institute for Pharmaceutical Sciences (UIPS) & Department of Metamedica (Vumc)
✉t.pieters@uu.nl

**Abstract** Pharmaceutical regulators have a dual responsibility. On the one hand, they need to protect and promote public health, while on the other hand, they have a role in stimulating pharmaceutical innovation through scientific advice, regulatory guidelines and other forms of regulatory dialogue. Although regulators are acclaimed for their scientific expertise and independence, they are also criticized for being a source of bureaucracy and thus stifling innovation. Here we analyse the emergence of the EU biosimilar regulatory framework with a specific focus on erythropoiesis-stimulating agents and the pure red cell aplasia (PRCA) safety controversy. We demonstrate that in an uncertain environment, European regulators have created a regulatory framework for biosimilars that stimulates innovation while attempting to maintain high safety standards. This case study provides valuable lessons on how to handle controversies in a highly volatile pharmaceutical sector and within a specific regulatory framework.

**Key words** Biosimilar, biologicals, drug regulation, EMA, Pure red cell aplasia, erythropoietin, controversy

## Introduction

Substances derived from **biological** sources to *diagnose, treat,* cure or*preventdisease*—so-called biological—have existed in medicine's therapeutic arsenal for centuries. Biologicals form a heterogeneous group of medicinal products including tissue, extracts, and purified hormones. In the 1980s, the development of biotechnologies, such as recombinant DNA and hybridoma technology, gave rise to the creation of biotechnological drugs or biologicals (Walsh 2003). In the past decade, the first generation of these biologicals, which include recombinant human interferons, insulin, growth hormone and erythropoietin, have lost or are about to lose their patent protection and market exclusivity. This has opened the door for the introduction of competing copies of biologicals.

For conventional synthetic molecules, regulations are in place that allow for the approval of competing generic products based on abbreviated application dossiers that demonstrate equivalence to the innovator product. However, unlike conventional synthetic "small molecule" products, the size and complexity of biologicals, together with the inherent variability of their production process, prevents the application of existing regulations. Although the technology for characterizing biologicals has greatly improved since their introduction in the 1980s, their immunogenic properties cannot be predicted using currently available analytical methods**.** This has created a need for tailored regulatory requirements to assess copycat biologicals—so-called biosimilars. The require-

ments of efficacy and safety data have provoked strong debate among regulators, innovative companies and producers of non-innovator versions of existing biologicals (Schellekens & Moors 2010). On one side, it is argued that biosimilar manufacturers should provide full safety dossiers; while on the other side, there is a call for abridged requirements, such as the ones that apply to conventional synthetic molecules. To settle this debate, regulatory standards are needed for biosimilars.

In 2001, an adverse drug reaction, pure red cell aplasia (PRCA), occurred in patients receiving the recombinant erythropoietin-α (EPO) product Eprex, a product marketed only outside the USA. This adverse drug reaction occurred unexpectedly following changes in the Eprex formulation and manufacturing process and clearly showed the industry's inability to predictchangesin immunogenic properties of biologicals. The drug reaction also evoked an increased interest in the possible consequences of immunogenicity for biologicals and particularly biosimilars. By analyzing the development of the biosimilar guidelines, we aim to illustrate the role of regulation and regulators in creating new pharmaceuticals. This case holds lessons for regulators who govern pharmaceutical innovations around the globe. We focus on the creation of the biosimilar regulatory framework of the European Union (EU), and will reflect on the institutional processes and outcomes using the PRCA case to illustrate the challenges of building a regulatory framework for biosimilars. This case is an important example of the dual role of regulators to protect and promote public health while simultaneously facilitating innovation in the pharmaceutical sector.

## Roles of regulation

Regulation serves as a means to exercise control over the quality, efficacy and safety of pharmaceuticals. Pharmaceutical regulators act as gatekeepers to ensure that medicines have a positive benefit-to-risk balance when they enter the market and throughout their lifecycle. Increased regulatory pressure is often regarded as a barrier to innovation and thus criticized for delaying the introduction of useful medicines and weakening industrial competitiveness (Miller & Henderson 2007). However, regulation can also provide positive incentives for innovation, e.g. providing guidance to improve the quality of pharmaceuticals. Furthermore, the regulatory 'norm of acceptability' has a profound influence on decisions for whether or not to develop medicines. A powerful example of this is the development of many new pharmaceuticals for orphan diseases following the adoption of orphan legislation(Braun et al. 2012), or the role of regulation to direct tissue engineering (Hogle 2009). This double bind between the management of the benefit-risk balance and innovation is characteristic of modern drug regulation cultures (Carpenter 2010; Daemmrich 2002; Pieters & Snelders 2012).

The process of creating and adopting regulation is far from straightforward. Rather than a rational response to a perceived public health problem, creating drug regulation standards is a highly political process as many competing interests collide on the efficacy, safety, and affordability of medicines and other economic interests (Hüntelmann 2008; Timmermans & Berg 2003). Stakeholders with conflicting interests have long exerted their influence on the process of creating regulations(Abraham 2002; Pieters 2005; Wiktorowicz & Deber 1997). This can result in differing views of what should be regulated and to what extent. Furthermore, the development of regulation is a subtle process, which may promote the integration of views and perspectives from opposing stakeholders—a process that has been called 'facilitation' (Black 1998; Jasanoff 1990). Incorporat-

ing the arguments of scientists, regulators, health technology assessors and patients, regulation may facilitate the acceptance of the outcome of the regulatory process.

How is it then that regulatory agencies can manage to perform these seemingly conflicting tasks in the highly political pharmaceutical sector? The creation of a novel framework for biosimilar regulation in the EU provides a case example of how regulators have managed these challenges in the field of biologicals.

## Introducing EU regulations

### *EU biological legislation*

Following the Thalidomide tragedy in the 1960s, European regulation established norms for drug-approval procedures in 1965 with the adoption of Directive 65/65EEC. In 1975, Directives 75/318/EEC and 75/319/EEC were adopted and stipulated extensive pre-marketing testing and regulatory agency review to assess drugs (Pignatti, Boone, & Moulon 2004). These regulations applied to all medicinal products. The 1980s witnessed the advent of biotechnology and the first recombinant biological products entered the market. Many member states lacked the knowledge to assess these technologically advanced products. Therefore, in 1987, a concertation procedure was established that required biological marketing applications to be reviewed by the Biologics Working Party (BWP) of the scientific committee of the EMEA, the committee of proprietary medicinal products (CPMP), whose name was changed to the Committee of Medicinal Products for Human Use (CHMP) in 2004 (Jefferys & Jones 1995). The BWP reviewed the application dossiers for quality, safety and efficacy and issued an advisory opinion; the final decision was left to the individual EU member states. In 1995, this procedure was replaced by a centralized procedure via the newly established European Medicines Evaluation Authority (EMEA), which was renamed European Medicines Agency (EMA) in 2010. This procedure allows for a single drug authorization, valid in all EU member states, which is mandatory for all biologicals that are intended to be marketed in the EU.

### *First steps toward a regulatory pathway for biosimilars*

At the end of 1997, the ‘centralized procedure’ for the approval of pharmaceuticals for the EU using a single application to the EMA was well established. Fifteen biological products had received approval through the centralized procedure and 10 more were approved through the concertation procedure. By then, the first products developed using recombinant technologies were approaching the loss of their patent protection in the EU. At this time, the EMA received inquiries from potential manufacturers about criteria for the approval of a competing version of an existing recombinant protein on the market (European Medicines Agency 1998). For chemically synthesized ‘small molecules’, generic versions may receive marketing authorization by demonstrating “essential similarity” to the originator product (European Commission 2001).This option was introduced in USA legislation in 1984 through the adoption of the Hatch-Waxman Act and similar regulation was established in EU through Directive 87/21/EEC. Essential similarityis demonstrated by performing studies on the quality of the new ‘small molecule’ and limited pharmacokinetic studies demonstrating bioequivalence. Given the inability to fully characterize biologicals and the inherent variability in their production process, it was clear that competing versions of biological could not be considered under existing legislation. Although regulation existed for establishing the comparability of products originating from a single manufacturer, these could not be applied to products from various manu-

facturers (International Conference on Harmonisation 2004). De facto, this resulted in unlimited market exclusivity for originator biological products. The question was forwarded to the European Commission, who returned it to EMEA as a scientific question asking what information was needed to demonstrate the comparability of two biological products. The CHMP deferred to its expert committee, the biologics working party (BWP), which resulted in a concept paper in 1998 outlining the first steps for the creation of regulatory guidance on minimal requirements for the quality, non-clinical and clinical issues for these new products (European Medicines Agency 1998). Just as the first steps for creating a regulatory pathway were taken, an adverse event occurred in patients receiving epoetins that would have important implications for the discussion surrounding the regulatory requirements for biosimilars.

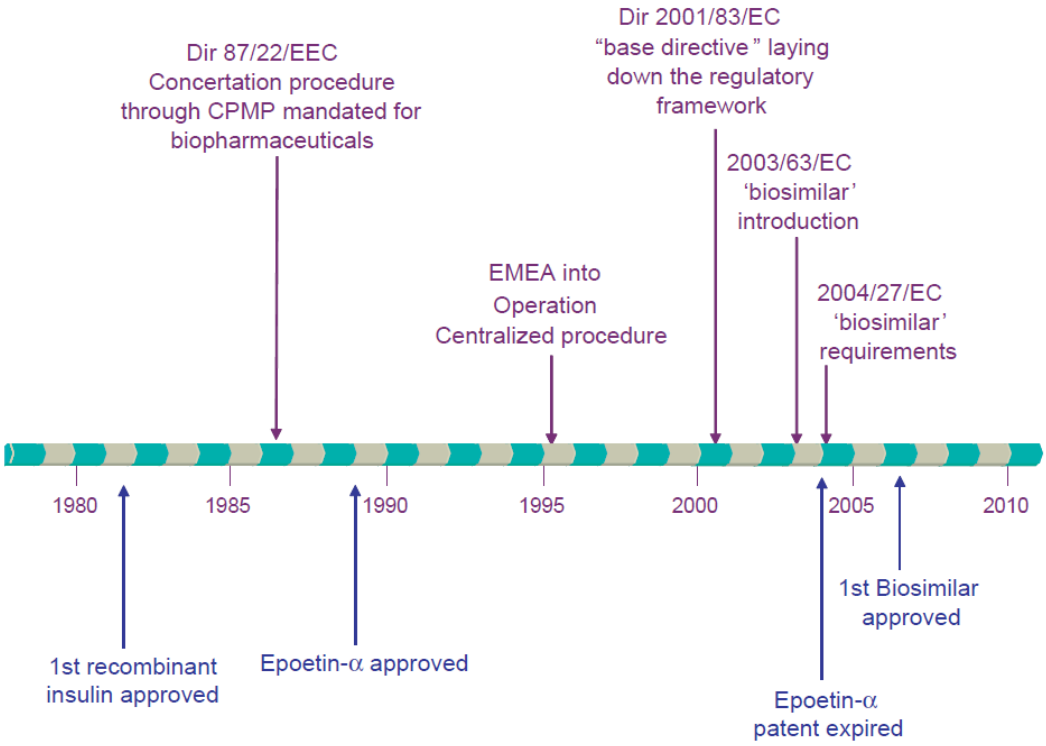



**Figure 1**: Overview of key EU legislation and events concerning biologicals and biosimilars. All legislation related to the development and utilization of pharmaceuticals was combined in the "Community code relating to medicinal products for human use", Directive 2001/83/EC thereby replacing all previous directives.

## The case of pure red cell aplasia

### The unexpected occurrence of pure red cell aplasia

In 1988, epoetin-α, the first recombinant erythropoietin (EPO), was approved in Europe for treating anemia associated with renal failure. In the following years, the approved use of epoetin-α was extended to include the treatment of anemia in patients with non-myeloid cancer receiving chemotherapy(Bennett et al. 2008; Gascon 2005). In November 2001, a warning was issued by Ortho-Biotech, the manufacturer of Eprex (epoetin-□), to alert physicians to an increase in the number of reported cases of pure red cell aplasia (PRCA). PRCA is ahematological disorder characterized by severe anemia and an almost complete absence of erythroid precursor cells, while other bone marrow colonies are unaffected(Pollock et al. 2008). PRCA is very rare and from the approval of epo-

etin-α until 1998, only three cases of PRCA associated with the occurrence of anti-erythropoietin antibodies had been published (Bergrem, Danielson, Eckardt, Kurtz, & Stridsberg 1993; Peces, de la Torre, Alcazar, & Urra 1996; Prabhakar & Muhlfelder 1997). The majority of new cases of PRCA were found to be associated with a particular brand of epoetin-α—Eprex, produced by Ortho Biotech and only marketed outside the USA. In early 2002, three months after the first regulatory warnings, a landmark publication heightened the awareness of PRCA around the globe (Casadevall et al. 2002). The publication described 13 patients who had received epoetins and developed PRCA and conclusively confirmed the role of anti-erythropoietin antibodies in causing this adverse reaction. The number of cases reported to regulatory agencies across the EU, Canada and Australia increased significantly. The majority of these cases occurred in renal patients who were receiving subcutaneous Eprex. As the number of reported cases of PRCA increased, a second regulatory warning was issued along with the recommendation that physicians administer Eprex intravenously whenever possible. When these measures did not result in a decrease in the number of reported cases of PRCA, regulators contraindicated the use of subcutaneous Eprex in patients with chronic renal failure. Following these measures, the number of newly reported cases declined, resulting in a total of over 200 confirmed PRCA cases (Bennett et al. 2004).

### *Investigations into the cause of the increased incidence of PRCA cases*

Along with actions from regulatory agencies in the EU, Canada and Australia, the Marketing Authorization Holder (MAH) in Japan investigated the PRCA cases associated with Eprex use. How could a sudden increase in this otherwise extremely rare adverse drug event be explained? The origin of the problem was traced back to the 1990s when Europe was reaching the peak of the 'Mad Cow Disease' crisis. The agent responsible for transmitting the human form of bovine spongiform encephalopathy, Creutzfeldt-Jakob disease, could not be inactivated in donor blood. The CHMP was concerned with possible contamination of the plasma-derived products and excipients used to stabilize the formulations of biological products, including human serum albumin (HSA). In 1998, it adopted the position that although the chance of transmission of a new variant of Creutzfeldt-Jakob disease was highly unlikely, it was prudent to withdraw batches of products containing (donor-derived) HSA at risk for contamination (Committee of Proprietary Medicinal Products 1998). The CHMP advised manufacturers to refrain from using HSA as an excipient whenever possible and encouraged the use of alternatives. The manufacturer of Eprex for the European market, Ortho Biotech, responded to this revised position and changed the formulation of Eprex. HSA was replaced as a stabilizer by the widely used detergent polysorbate 80 and glycine, which are extensively used in biological formulations. It is now widely accepted that removing HSA as an excipient, along with other changes introduced in the manufacturing process, were the most likely causes of the sudden increased incidence of PRCA cases. Nevertheless, the question of the exact mechanism of drug induced PRCA has remained the subject of intense debate.

Two hypotheses have been brought forward by the MAH to explain the increase in the immunogenicity of Eprex (Boven et al. 2005). First, it was suggested that polysorbate from the uncoated plunger stoppers of prefilled syringes were 'leaching' organic compounds that could have adjuvant properties. Second, the replacement of HSA by polysorbate 80 and glycine decreased the stability of the formulation making it more susceptible to improper handling and temperature changes. Measures were implemented to ensure proper handling of Eprex.

In April 2003, the teflon-coated stoppers were replaced by uncoated rubber stoppers in prefilled syringesto prevent leaching. Following these measures, the number of reported PRCA cases declined to the levels seen before 1998. However, the hypothesis of organic leachates put forward by the MAH was heavily debated and other mechanisms were suggested (Schellekens & Jiskoot 2006). Most notable, the new formulation may have made Eprex more susceptible to the formation of aggregates of recombinant protein formation, which in turn could have induced immunologic reactions. This process may have been further induced by improper storage and handling conditions. No definitive answer has yet been found and this issue remains a matter of scientific debate.

### *After the regulatory actions*

In 2006, the subcutaneous route for Eprex administration was reinstated, but only for patients for whom intravenous access was not readily available. However, since the exact cause of PRCA was not yet determined, regulatory authorities were not assured that the measures to prevent PRCA would be effective over time. Therefore, efforts were made to assess the safety of Eprex including a large prospective observational study to monitor the incidence of PRCA cases. The study had been initiated in 2003, but was prematurely stopped having failed to detect any new cases of PRCA due to anti-erythropoietin antibodies (Rossert et al. 2006). The uncertainty about the cause of the increased incidence of PRCA cases and the unpredictability of immunogenicity-associated adverse events had obvious implications for biosimilar regulatory requirements. The adverse experiences with Eprexclearly demonstrated how changes in a product that are not apparent in quality control can have severe consequences for the safety of biologicals. As the market exclusivity of some key biologicals including EPOs, was coming to an end, the creators of the biosimilar regulatory framework needed to create safety standards without closing the door on biosimilars.

## The emergence of a regulatory framework for similar biological medicinal products

### *Lack of agreement on global guidance*

The BWP 1998 concept paper for recombinant proteins was the first step towards creating a regulatory framework for similar biological medicinal products (European Medicines Agency 1998). The patents for EPOs and granulocyte colony stimulating factors were due to expire first in the EU and later in the USA (Ledford 2007). An obvious platform for the development of global regulation on this topic would have been the International Conference of Harmonization (ICH). The ICH has representatives from regulating agencies and the pharmaceutical industry in the three major pharmaceutical markets, i.e. USA, Europe and Japan. The ICH proposes topics for harmonization that are implemented in local legislation after consultation within the regions (Buono 1995). The ICH platform operates by finding consensus on subjects to address with guidelines. However, the ICH decided that the safest approach was to limit the scope of their guidance to the manufacturing processes of products already on the market and produced by the ‘original’ manufacturers. The pharmaceutical industry is represented in the ICH by associations that generally act on behalf of innovative companies who may have been less receptive to guidance on this topic. Regardless of the underlying reasons, the ICH decided not to provide guidance on the requirements of biological products produced by companies other than the innovator(International Conference on Harmonisation 2004). This left a gap in the global regulatory framework and the EMA needed to address the dilemmas posed by the arrival of biosimilars.

## Basic principles of the EU biosimilar approach

Since 'essential similarity' cannot be demonstrated for biologicals, rather than using the term 'generic', the term 'similar biological medicinal products' or 'biosimilars' was coined in the EU legislation in 2003 (European Commission 2003). EU legislation states that biosimilars must demonstrate a comparable quality, efficacy and safety compared to a chosen reference product (European Commission 2004)Comparative clinical data are needed to demonstrate the safety and efficacy of the product and biosimilar manufacturers must provide extensive risk management plans to monitor their safety after receiving marketing authorization. Like all biologicals, biosimilars must be approved through the EU centralized procedure. The exact requirements for specific products were to be determined on a case-by-case basis and would be outlined in CHMP guidelines. The guidelines were drafted by the expert working parties advising the CHMP. These working parties include scientists from each EU country who are selected for their particular expertise. An 'overarching' guideline was released that described the basic principles underlying the biosimilar regulatory framework. This was followed by guidelines detailing requirements on quality, non-clinical issues and comparability issues. Initially, four guidelines were issued that described the requirements for specific product classes, i.e. insulins, human growth hormones, granulocyte colony stimulating factors and EPOs. Draft versions of these guidelines were released for review in May 2005.

After a consultation period, in December 2005, a workshop was organized to share the experience of biosimilar regulation, discuss the prospective conclusions included in the guidelines and highlight any evolving scientific factors that might influence the review, risk management and post-marketing surveillance of these products. The final versions of the four guidelines were adopted in February 2006.A separate guideline specifically addressed the immunogenicity of therapeutic proteins and states:"Immunogenicity issues should be further addressed in the Risk Management Plan"(European Medicines Agency 2007). As for all new pharmaceutical products, biosimilars are subject to a five-year assessment; at this time the marketing authorization may be renewed. Since 2006, specific guidelines have been adopted for interferon alpha, low-molecular-weight heparins and monoclonal antibodies, and draft guidance has been released for recombinant follicle stimulating hormones and recombinant interferon-β.

## The market situation of EPOs at the time of the drafting of biosimilar guidelines

At the time that the PRCA adverse events associated with Eprex use emerged, the market for EPOs was valued at more than $10 billion and over three million patients had received EPOs worldwide, making it by far the best selling biological in the world (Evens, Bennett, & Luminari 2005). Johnson & Johnson, the company responsible for marketing Eprex, earned $4.3 billion in revenues for the product, accounting for 11.8% and 10.6% of the total company revenue in 2001 and 2002 respectively (Johnson & Johnson 2002). Even though sales of Eprex declined from 2002 to 2005, the drug still generated significant of revenue for the company. Similarly, sales of Amgen's EPOs rose to over $5 billion in 2004—more than 50% of the total company revenue (Amgen 2004). In the EU, the patent for the production of epoetin-α expired at the end of 2004 opening the way for competitor products (Ledford 2007; Lin 1984). Obviously, the stakes were high and creating hurdles for manufacturers to enter the market increases the cost of developing competitor products. Traditionally, the key attribute of generic medicines to secure a market share is lower cost. However, given the higher development costs and the limited number of competitors that would enter the

market, the price of biosimilars was expected to be approximately 80% of originator products and biosimilars were predicted to capture 30-75% of the anemia market (Melnikova 2006). Biosimilars have the potential for high financial returns despite taking longer, costing more and requiring more biotechnological expertise to develop than conventional drugs. Early biosimilar manufacturers had strong ties to companies with extensive experience developing innovative biologicals. Both innovative companies and companies interested in developing biosimilars participated in discussions surrounding the creation of the biosimilar regulatory framework in Europe.

## Guidelines creating controversies

### *Public consultation on the draft guidelines*

The first draft of the biosimilar EPO guidelines was circulated for public consultation in June 2005. According to European procedures, stakeholders could offer feedback on this draft until October 2005. Responses came from innovator companies, generic companies, regulatory agencies, scientists and patient organizations. Interestingly, no input was provided by any medical association or individual physician (Ebbers, Pieters, Leufkens, & Schellekens 2012). Discussion of biosimilar safety included more than just biosimilar EPOs, but the PRCA adverse events provided the perfect example of the unpredictable nature of immunogenicity and the potential harmful responses resulting from unwanted immunogenicity. While guidelines on biosimilars and immunogenicity were drafted in Europe, the exact mechanisms of PRCA adverse drug events were under investigation. Various stakeholders stressed that the unknown cause of the increased incidence of PRCA cases illustrated the need for specific guidance on biosimilars. Both innovative companies and patient organizations insisted that patient safety should be of prime importance (CEAPIR 2005; EuropaBio 2005). The use of placebo-controlled trials for products that have a known efficacy and safety profile was considered unethical. It was generally accepted that comparative clinical studies of a biosimilar versus the innovator product should be a necessary part of any application dossier. This would enable a comparison of the immunogenicity of a product under investigation with that of the innovator product.

### *How many patients should be studied?*

Key points for discussion on the guidelines included: the number of patients in the clinical studies, the number of studies to be performed and the duration of studies to provide adequate premarketing safety data. The draft version of the final guidelines specifically stated that safety data from the efficacy trials of at least 300 patients would be sufficient to exclude “excessive immunogenicity” (European Medicines Agency 2005). The rationale for 300 patients was not clear and in addition, applicants needed to provide 12 months of immunogenicity data from patients receiving biosimilar EPO. Stakeholder comments were diverse; some recommended increasing the minimum number of patients to 1000, while others suggested that a single study would provide sufficient safety data. Still others, including the European Kidney Patients Foundation, advocated that the same criteria should be required for biosimilars as the reference product. In the final guideline text, the minimum number of patients in a clinical trial was removed.

### *Route of administration*

Another part of the guideline discussion focused on the need to perform separate studies to demonstrate the therapeutic equivalence of both the subcutaneous and intravenous routes. Since the subcutaneous route for the comparator product Eprex was contraindicated (because of PRCA), only studies comparing the biosimilar to intravenously administered Eprex were possible. Unfortunately, PRCA had only been identified in patients receiving subcutaneously administered Eprex. A consensus was reached to require one study using an intravenous route and to grant approval only for that route (Schellekens 2008). To obtain approval for the subcutaneous indication, additional studies would be required once the contraindication for subcutaneous Eprex was lifted.

### *Which indications should be studied?*

A second point of the guideline discussion was whether or not clinical data should be required for all authorized indications for the reference product, or if demonstrating comparability for one indication could extrapolate to mean that the product was equally efficacious and safe in all other indications. Although some stakeholders argued that separate clinical data should be provided for each indication for which approval was sought, the CHMP decided that well-designed trials in the "most sensitive" therapeutic indication would suffice (European Medicines Agency 2006). Patients with anemia resulting from renal failure are more sensitive to the effects of EPO than patients receiving EPO for the treatment of chemotherapy-associated anemia. Furthermore, patients with renal failure require long term, continuous treatment that places them at a higher risk for developing anti-EPO antibodies. Indeed, there were no reported cases of antibody-dependent PRCA for patients receiving EPOs to treat chemotherapy-associated anemia. Therefore, patients with renal anemia are considered the most sensitive model, both from an efficacy and safety perspective. It was recognized that the number of patients included in the clinical studies would likely be too small to establish the 'true' immunogenicity of the product. European legislation requires biosimilar producers to provide a detailed description of pharmacovigilance and risk minimization activities in so-called Risk Management Plans. The *need* for pharmacovigilance activities was not contested, although the extent of post-authorization activities to identify potential risk was. As became clear from the Eprex-associated PRCA case, immunogenicity was the key safety concern for biosimilar EPOs. Both manufacturers of a biosimilar EPO committed to performing post-marketing observational studies, which included studies with a planned enrollment of 1500 patients to monitor the incidence of "relevant" adverse events, including PRCA (European Medicines Agency 2007). Because of the specific safety concerns for EPOs, the pharmacovigilance requirements, as specified in the guideline, were more extensive than for other biosimilars. This demonstrates that the regulatory authorities established the guidelines on a case-by-case basis taking a risk-based approach.

### *Controversies beyond the scope of the guidelines*

The CHMP considered some final points of concern to be beyond the scope of the guidelines including: the traceability and naming of biosimilars and the interchangeability of biosimilars with innovative EPOs. The traceability issue was raised to ensure that any immunogenicity-related adverse reactions could be clearly traced to either the comparator product or the biosimilar. The World Health Organization (WHO) is responsible for naming biologicals through their International Nonproprietary Name (INN) program. For EPOs, this proved to be a challenge—how to capture the

diversity of differences in glycosylation patterns in a single Greek letter? The various glycosylation patterns of EPOs are indicated by distinct Greek suffixes; however, the inherent variability of the production of biologicals resulted in differences in glycosylation patterns. Whereas some biosimilars (e.g. Binocrit) received the same INN as its comparator product, others for various reasons have received alternative suffixes. This situation has led to confusion and discussion within WHO and efforts are ongoing to resolve this issue. Innovative companies argued that no protein is identical, so specific suffixes should be applied to biosimilars to distinguish them from the originator products or that the originator products be referred to by their brand names (EuropaBio 2006). Also, worries were expressed that brand products, like generic products, would be automatically substituted for biosimilars at pharmacies, thereby causing confusion about the source of a possible immunogenic reaction. In many countries, laws exist for the automatic substitution of branded products for (cheaper) generics in the case of 'small molecules'. After the regulatory approval of biosimilars, discussions emerged to address the question—should this practice also apply to biosimilars (Rossert 2007)? Rules for substitution have always been a national affair and the EMA clearly stated that this issue was outside of the scope of their guidelines. In several countries, automatic substitution was explicitly forbidden, at least for several years after the introduction of the biosimilar. Thus, the substitution of EPO continued to be the choice of the treating physician (Covic et al. 2008).

## Following the adoption of the EU regulatory framework

### *Biosimilar regulations are being developed around the world*

The EU biosimilar regulations have in been in place now since 2006 and seven biosimilar products (sold under 13 trade names), have received marketing approval in the EU. Overall, the consultation procedure was welcomed by all stakeholders and has received positive acclaim. Other countries and organizations are following the path taken by the EMA. In 2009, WHO issued a set of draft guidelines that serves as a basis for national requirements for biosimilars (Hodgson 2009). Australia adopted the European framework and many of the principles devised for biosimilars have been copied by countries such as Canada and Switzerland (Kresse 2009). According to some, the new EU framework has reached the status of the 'gold standard' for biosimilar drug regulation (Fox 2010). In early 2010, the USA adopted the 'Biologics Price Competition and Innovation Act', which amends the Public Health and Safety Act to enable a regulatory route for an abridged procedure for the approval of what has been termed 'follow-on biologics'(U.S. Senate 2009). Some notable differences apply to the USA law when compared to EU law. The USA legislation has gone one step further in creating two possible applications: one that is comparable to the EU approval procedure and may deem a product "biosimilar", a second option is to demonstrate interchangeability. To obtain this qualification, data must be provided that demonstrate biosimilarity and "can be expected to produce the same clinical result as the reference product in any given patient"(U.S. Senate 2009). In early 2012, the FDA released draft guidance on biosimilar product development and the final guidelines are expected to be released soon.

As more experience was gained with biosimilars, the norms specified in the biosimilar EPO guidelines were subject to discussion once again. The CHMP responded with a concept paper to revise the existing guidelines, in which the issues of immunogenicity and the need for two separate clinical studies were questioned. In March 2010, revised guidelines were adopted (European Medi-

cines Agency 2010). By then, subcutaneous Eprex had been reinstated and the requirement for two separate trials was replaced by a single trial studying the efficacy and safety of both the intravenous and subcutaneous route of administration. After the release of the draft version of the guidelines in July 2009, two cases of neutralizing antibodies occurred in a study that evaluated the efficacy of the subcutaneously administered biosimilar Binocrit (Haag-Weber et al. 2012). While this led to renewed controversy about the adequacy of the authorization requirements for biosimilars, the EMA decided that demonstrating comparability in a single trial involving patients receiving subcutaneously administered EPO would suffice to receive marketing authorization as a biosimilar. Clearly, the case is not closed and continues to challenge regulators.

### *Barriers to the uptake of biosimilars*

Despite the adoption of extensive regulation and the development of several biosimilar products, thus far, their uptake in clinical practice has been fairly slow (IMS Health 2011). Many factors play a role here. Compared with small molecule generics, the price difference between originator products and biosimilars is modest; in many cases biosimilars are less than 20% cheaper than innovator products. This is partly due to the relative high development costs of biosimilars, but also because the prices of innovator products were lowered. Furthermore, physicians are still doubtful about the safety of biosimilars (Zelenetz et al. 2011). Learned societies of clinicians need to determine a position on the use of biosimilars and provide advice to physicians who use biosimilars in clinical practice. Criticism has arisen from clinicians with various clinical backgrounds (Declerck et al. 2010; Niederwieser & Schmitz 2011). The European regulators were and are engaged in active discussion with the medical field to explain the concept of the biosimilar framework, thereby highlighting that the 'reduced' data package does not lead to additional safety risks (Weise et al. 2012). Nevertheless, several EU countries have adopted regulations that prohibit the automatic substitution of innovator products with biosimilars. Altogether, this has prevented the rapid uptake of biosimilars as is usually the case for small molecule generics. With regard to EPOs, the restriction of the biosimilar approval to IV use may have prevented a quick uptake. In addition, the use of the entire class of EPOs has been greatly restricted as a result of various studies that implied an increased mortality due to EPO treatment both in cancer and renal patients (Unger, Thompson, Blank, & Temple 2010). Clearly, the further uptake of biosimilars will depend on a multitude of context-dependent factors that should be closely monitored by regulators as part of a stakeholder feedback mechanism that is essential to maintain gatekeeping authority in a rather competitive and challenging regulatory environment

## Discussion

In our case study, we analyzed how EU regulators laid out standards by which a specific category of drugs, biologicals, are deemed equivalent or not to one another. The regulators succeeded in rendering a host of development issues, health assessment questions and economic exchanges more predictable and hence manageable. The EU regulatory framework provided a solution to the controversy that emerged with the arrival of biosimilars; as such it proved to be a *sine qua non* for their adoption. Even in an uncharted environment where there was much uncertainty about possible safety issues and many competing interests, the EU biosimilar regulatory framework has gained widespread acceptance from multiple stakeholders. Competing biosimilar versions have

been approved for recombinant human hormone growth hormone and granulocyte colony stimulating factors. Three biosimilar EPOs have been approved in Europe while seven more are currently under review.

The conflicting roles of regulators to protect patients while facilitating innovation and supporting cost-effectiveness were a leitmotiv in the biosimilar case. Containing health expenditure is formally no task of EU pharmaceutical regulators and creating an abbreviated pathway for the approval of products, for which alternatives exist, is a new step in regulatory responsibilities. Regulators were faced with the question of how to ensure that biosimilars were held to the same standards of quality, safety and efficacy that exists for all biologicals without preventing the access of these products to the EU market. The EU Commission forwarded the question of the scientific feasibility of such a framework to the CHMP. But what started with a scientific question, in effect gave responsibility to the CHMP and its working parties for paving the way for biosimilars. The regulatory trajectory of the biosimilars demonstrates how regulators were able to support the introduction of these products to the European market based on scientific considerations and through extensive dialogue involving all stakeholders. This highlights the key role EU regulators have played as intermediaries between science, medicine and industry. Process consultation with the various stakeholders could not prevent the regulators from being confronted with unanticipated issues related to product safety and being forced on the defensive by persistent safety concerns on the part of prescribers and patients. Hard work and diplomacy on the part of the regulators was required to address the safety concerns and build in safety measures without knowing the ultimate effects on the market uptake of biosimilars in medicine.

So what can be learnt from the regulation trajectory in this case study? First clear goals were set and communicated to all the stakeholders. The first concept paper that was released in 1998 proposed to address the question of specific information needed to demonstrate comparability of two biologicals, rather than the possibility of demonstrating equivalence of two biologicals. It was clear to all stakeholders that the goal of the EU Commission was to create an abbreviated approval process for biosimilars. In the consultation period that followed, there was little discussion on the need for a separate regulatory route for biosimilars. The discussion focused mainly on specifics that would be part of the requirements for approval. The EU rules with regard to public consultation ensured that input was sought from a wide variety of stakeholders. Representatives of innovator companies, producers of biosimilars, national regulatory agencies and patient organizations seized the opportunity to participate in the process of reviewing the draft guidelines. Surprisingly, physicians or medical associations hardly participated in this process consultation. This may reflect a disturbing aspect of the growing distance between doctors and drug regulators (Ebbers et al. 2012; Horton 2003). For the stakeholders who did participate, the reactions were generally in line with expectations, with innovator companies advocating more stringent regulatory requirements for biosimilars, while producers of biosimilars advocated abbreviated procedures. The EMA provided ample opportunity for debate and dialogue. Through this way of governance by means of process consultation the regulators succeeded in mobilizing and maintaining broad support for biosimilar regulations. An important part of the stakeholder dialogue strategy was to take seriously the opposition from doctors and patients. Establishing a platform to facilitate dialogue with European medical associations on issues of common interest could promote the acceptance of regulation. In the end, regulation not only aims to ensure that medicinal products have an appropriate benefit/ risk balance, but also that promising products become available to patients. When regulators fail to in-

volve doctors in their activities, this will impede the acceptance of the cost effective and innovative medicinal products of the future (Ebbers et al. 2012).

The PRCA case is exemplary in showing a direct need to anticipate on the occurrence of adverse safety events and the emergence of public safety concerns by the means of a structural consultation process with all stakeholders and a state of the art drug vigilance system. The occurrence of PRCA during the process may have resulted in a more prudent approach for EPOs when compared to other biosimilars, because of doubts remaining about the immunogenic properties EPO after the clinical development program. This clearly shows the dilemmas that regulatory scientists face. Regulators are in a constant struggle between facilitating and restricting products and both courses of action may be a source of criticism for regulators. Allowing drugs on the market always leaves questions of benefit and risk. Allowing a biosimilar product on the market that might eventually prove to be unsafe will raise public concern and criticism. On the other hand, withholding a product from entering the market will lead to criticism of bureaucracy, stifling innovation and warm ties between regulators and producers of innovative products. The case we describe illustrates the tightrope that regulators walk to maintain their authority in managing these highly complex situations. The confidence in regulatory agencies is fragile and needs constant attention. Events such as PRCA demonstrate that the position of the regulators is continuously under public scrutiny. Conflict between existing regulations, knowledge production and technology development should be embraced and demands an open attitude and a willingness to adapt regulatory standards to current thinking, especially for regulations in uncharted terrain such as biosimilars. Challenges to existing regulations and continuous dialogue are needed to ensure that the regulators can maintain their role as gatekeepers and as intermediaries between science, government, industry and the public sphere.

**Acknowledgements**: The authors would like to thank Julia Challinor for her English manuscript correction services and the reviewers for their constructive comments.

## References

Abraham, J. (2002). The pharmaceutical industry as a political player. Lancet, 360(9344), 1498-502.

Amgen (2004). Annual report. Available from: http://investors.amgen.com/phoenix.zhtml?c=61656&p=irol-reportsannual. [accessed 8 November 2011].

Bennett, C. L., Luminari, S., Nissenson, A. R., Tallman, M. S., Klinge, S. A., McWilliams, N., … Casadevall, N. (2004).Pure red-cell aplasia and epoetin therapy.N Engl J Med, 351(14), 1403-8.

Bennett, C. L., Silver, S. M., Djulbegovic, B., Samaras, A. T., Blau, C. A., Gleason, K. J., Henke, M. (2008). Venous thromboembolism and mortality associated with recombinant erythropoi-etin and darbepoetin administration for the treatment of cancer-associated anemia. JAMA, 299(8), 914-924. doi: 10.1001/jama.299.8.914.

Bergrem, H., Danielson, B. G., Eckardt, K. U., Kurtz, A., & Stridsberg, M. (1993). A case of antierythropoietin antibodies following recombinant human erythropoietin treatment. In C. Bau-

er, K. M. Koch, P. Scigalla & L. Wieczorek (Eds.), Erythropoietin: Molecular physiology and clinical applications. New York: Marcel Dekker.

Black, J. (1998). Regulation as facilitation: Negotiating the genetic revolution.Modern Law Review, 61(5), 621-660.

Boven, K., Knight, J., Bader, F., Rossert, J., Eckardt, K. U., & Casadevall, N. (2005). Epoetin-associated pure red cell aplasia in patients with chronic kidney disease: Solving the mystery. Nephrol Dial Transplant, 20 Suppl 3, iii 33-40.

Buono, T. P. (1995). Biotechnology-derived pharmaceuticals: Harmonizing regional regulations. Suffolk Transnat'l L. Rev., 18, 133.

Carpenter, D. (2010). Reputation and power. organizational image and pharmaceutical regulation at the FDA. Princeton: Princeton University Press.

Casadevall, N., Nataf, J., Viron, B., Kolta, A., Kiladjian, J. J., Martin-Dupont, P., … Mayeux, P. (2002). Pure red-cell aplasia and antierythropoietin antibodies in patients treated with recombinant erythropoietin. The New England Journal of Medicine, 346(7), 469-475. doi: 10.1056/NEJMoa011931.

CEAPIR. (2005). Guideline on similar biological medical products (CHMP/437/04) comment of the European kidney patients' federation (CEAPIR) available from: http://www.ceapir.org.

Committee of Proprietary Medicinal Products. (1998). CPMP position statement on new variant CJD and plasma-derived medicinal products. available from: www.emea.europa.eu/pdfs/human/press/pos/020198en.pdf.

Covic, A., Cannata-Andia, J., Cancarini, G., Coppo, R., Frazao, J. M., Goldsmith, D., … London, G. (2008). Biosimilars and biopharmaceuticals: What the nephrologists need to know – a position paper by the ERA-EDTA council. Nephrol Dial Transplant, 23(12), 3731-7.

Daemmrich, A. (2002). A tale of two experts: Thalidomide and political engagement in the United States and West Germany. Social History of Medicine, 15(1), 137-158. doi: 10.1093/shm/15.1.137.

Declerck, P. J., Darendeliler, F., Goth, M., Kolouskova, S., Micle, I., Noordam, C., … Ranke, M. B. (2010). Biosimilars: Controversies as illustrated by rhGH.Curr Med Res Opin, 26(5), 1219-29.

Ebbers, H.C., Pieters, T., Leufkens, H.G., & Schellekens, H. (2012). Effective pharmaceutical regulation needs alignment with doctors. Drug Discovery Today, 17(3-4), 100-103. doi: 10.1016/j.drudis.2011.09.018; 10.1016/j.drudis.2011.09.018.

EuropaBio. (2005). Draft guideline on similar biological medicinal products containing biotechnology-derived proteins as active substance: Non-clinical and clinical issues, ref. EMEA/CHMP/42832/2005. comments from EuropaBio. Available from: www.europabio.org.

EuropaBio. (2006). Europabio position paper.naming and labelling requirements for biosimilar medicines. available from http://www.europabio.org [accessed 01 February 2009].

European Commission. (2001). Directive 2001/83/EC; Official Journal L 311, 28/11/2001, p. 67

European Commission. (2003). In The Commission of the European Communities (Ed.), (2003) Directive 2003/63/EC. Official Journal L 159, 27/6/2003 p. 46 – 94.

European Commission. (2004). Directive 2004/27/EC. Official Journal L 136, 30/4/2004 p. 34 - 57

European Medicines Agency. (1998) concept paper on the development of a CPMP guideline on comparability of biotechnology-derived products. Available from: http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500003966.pdf[ accessed 13 February 2013].

European Medicines Agency. (2007). Guideline on immunogenicity assessment of biotechnol-ogy-derived therapeutic proteins. Available from: Http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500003947.pdf [accessed 3 July 2011].

European Medicines Agency. (1998). Concept paper on the development of a CPMP guide-line on comparability of biotechnology-derived products. Available from: http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500003966.pdf [accessed 14 February 2013].

European Medicines Agency. (2005). Submission of comments. Guideline on similar biological medicinal products containing biotechnology derived products as active substance: Non-clinical and clinical issues annex: Recombinant erythropoietin containing products EMEA/CHMP/945626/2005. Available from http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500003923.pdf [accessed May 10, 2011].

European Medicines Agency. (2006). Guidance on biosimilar medicinal products containing re-combinant erythropoietins. Available from: http://www.ema.europa.eu/docs/en_GB/document_library/Scientific_guideline/2009/09/WC500003921.pdf [accessed 2 February 2011].

European Medicines Agency. (2007). Binocrit: European public assessment report. Scientific dis-cussion. Available from: http://www.ema.europa.eu/humandocs/Humans/EPAR/binocrit/binocrit.htm [accessed 14 September 2011].

Evens, A. M., Bennett, C. L., & Luminari, S. (2005). Epoetin-induced pure red-cell aplasia (PRCA): Preliminary results from the research on adverse drug events and reports (RADAR) group. Best Practice & Research Clinical Haematology, 18(3), 481-489. doi: 10.1016/j.beha.2005.01.017.

Fox, A. (2010). Biosimilar medicines--new challenges for a new class of medicine. J Biopharm Stat, 20(1), 3-9.

Gascon, P. (2005). Evaluating erythropoietic agents for the treatment of anaemia in the oncology setting. European Journal of Cancer 41(17):2601–12. doi: 10.1016/j.ejca.2005.04.046

Haag-Weber, M., Eckardt, K. U., Horl, W. H., Roger, S. D., Vetter, A., & Roth, K. (2012). Safety, immunogenicity and efficacy of subcutaneous biosimilar epoetin-alpha (HX575) in non-dialysis patients with renal anemia: A multi-center, randomized, double-blind study. Clinical Nephrology, 77(1), 8-17.

Hodgson, J. (2009). WHO guidelines presage US biosimilars legislation? Nat Biotech, 27(11), 963-965.

Hogle, L. F. (2009). Pragmatic objectivity and the standardization of engineered tissues. Social Studies of Science, 39(5), 717-742.doi: 10.1177/0306312709103478

Horton, R. (2003). Second opinion. doctors, diseases and decisions in modern medicine. London: Granta Publications.

Hüntelmann, A. C. (2008). Ways of evaluation. therapeutic agents between standardization and in-stitutionalization. Berlin: Max-Planck-Institut für Wissenschaftsgeschichte.

IMS Health. (2011). Shaping the biosimilars opportunity: A global perspective on the evolving bio-similars landscape. Available from:

http://www.imshealth.com/ims/Global/Content/Home%20Page%20Content/IMS%20News/Biosimilars_Whitepaper.pdf[accessed, 11 April 2012].

International Conference on Harmonisation. (2004). Comparability of biotechnologi-cal/biological products subject to changes in their manufacturing process Q5E. Available from: http://www.ich.org/products/guidelines/quality/quality-single/article/comparability-of-biotechnologicalbiological-products-subject-to-changes-in-their-manufacturing-proc.html [accessed 13 October 2011].

Jasanoff, S. (1990).The fifth branch: Science advisors as policy makers. Cambridge, MA: Harvard University Press.

Jefferys, D. B., & Jones, K. H. (1995). Emea and the new pharmaceutical procedures for Europe. European Journal of Clinical Pharmacology, 47(6), 471-476.

Johnson & Johnson. (2002). Annual report. Available from: http://www.investor.jnj.com/annual-reports.cfm [accessed 9 November 2011].

Kresse, G. B. (2009). Biosimilars--science, status, and strategic perspective. Eur J Pharm Biopharm, 72(3), 479-86.

Ledford, H. (2007). Biotechs go generic: The same but different. Nature, 449(7160), 274-6.

Lin, F. K. (1984). In KIRIN AMGEN INC [US] (Ed.), Production of erythropoietin.

Melnikova, I. (2006). Anaemia therapies. Nat Rev Drug Discov, 5(8), 627-628.

Miller, H. I., & Henderson, D. R. (2007). Governmental influences on drug development: Striking a better balance. Nat Rev Drug Discov, 6(7), 532-539.

Niederwieser, D., & Schmitz, S. (2011). Biosimilar agents in oncology/haematology: From approval to practice. European Journal of Haematology, 86(4), 277-288. doi: 10.1111/j.1600-0609.2010.01566.x; 10.1111/j.1600-0609.2010.01566.x.

Peces, R., de la Torre, M., Alcazar, R., & Urra, J. M. (1996). Antibodies against recombinant human erythropoietin in a patient with erythropoietin-resistant anemia. N Engl J Med, 335(7), 523-4.

Pieters, T., & Snelders, S. (2012). Managing double binds in the pharmaceutical prescription market: The case of Halcion. Ways of regulating drugs in the 19th and 20th centuries. (In, Gaudillière JP.; Hess, V. ed., pp. 270-286). London: Palgrave Mac Millan.

Pieters, T. (2005). Interferon. the science and selling of a miracle drug. New York: Routledge.

Pignatti, F., Boone, H., & Moulon, I. (2004). Overview of the European regulatory approval system.The Journal of Ambulatory Care Management, 27(2), 89-97.

Pollock, C., Johnson, D. W., Horl, W. H., Rossert, J., Casadevall, N., Schellekens, H., … Toffelmire, E. (2008). Pure red cell aplasia induced by erythropoiesis-stimulating agents. Clin J Am Soc Nephrol, 3(1), 193-9.

Prabhakar, S. S., & Muhlfelder, T. (1997). Antibodies to recombinant human erythropoietin causing pure red cell aplasia. Clin Nephrol, 47(5), 331-5.

Rossert, J. (2007). EMEA guidelines on biosimilars and their clinical implications.Kidney Blood Press Res, 30 Suppl 1, 13-7.

Rossert, J., Muirhead, N., White, L., Ramlow, W., Stryker, S., Boven, K., & Denys, N. (2006).An active postmarketing surveillance (pms) plan to prospectively monitor the incidence of pure red cell aplasia (prca) among patients receiving epoetin alfa therapy or other erythropoietins. Nephrol Dial Transplant, 21 (Suppl 4), iv 153.

Schellekens, H. (2008). The first biosimilar epoetin: But how similar is it? Clin J Am Soc Nephrol, 3(1), 174-178.doi: 10.2215/cjn.04251007.

Schellekens, H., & Jiskoot, W. (2006). Erythropoietin-associated PRCA: Still an unsolved mystery.J Immunotoxicol, 3(3), 123-30.

Schellekens, H., & Moors, E. (2010). Clinical comparability and European biosimilar regulations. Nat Biotechnol, 28(1), 28-31.

Timmermans, S., & Berg, M. (2003). The gold standard. The challenge of evidence-based medicine and standardization in health care. Philadelphia: Temple university press.

U.S. Senate. (2009). Biologics price competition and innovation act of 2009 111th Cong., 2nd sess. S7001.

Unger, E.F., Thompson, A.M., Blank, M.J., & Temple, R. (2010). Erythropoiesis-stimulating agents – time for a reevaluation. N Engl J Med, 362(3), 189-192. doi: 10.1056/NEJMp0912328

Walsh, G. (2003). Pharmaceutical biotechnology products approved within the european union. European Journal of Pharmaceutics and Biopharmaceutics: Official Journal of Arbeitsgemeinschaft Fur Pharmazeutische Verfahrenstechnik e.V, 55(1), 3-10.

Weise, M., Bielsky, M. C., De Smet, K., Ehmann, F., Ekman, N., Giezen, T. J., … Schneider, C. K. (2012). Biosimilars: What clinicians should know. Blood, doi: 10.1182/blood-2012-04-425744

Wiktorowicz, M., & Deber, R. (1997). Regulating biotechnology: A rational-political model of policy development. Health Policy, 40(2), 115-138.doi: 10.1016/s0168-8510(96)00889-5.

Zelenetz, A. D., Ahmed, I., Braud, E. L., Cross, J. D., Davenport-Ennis, N., Dickinson, B. D., Hoffman, J. M. (2011). NCCN biosimilars white paper: Regulatory, scientific, and patient safety perspectives. Journal of the National Comprehensive Cancer Network: JNCCN, 9 Suppl 4, S1-22.

# Legal Highs
# legal definitions versus 'open innovation'

Johan Söderberg
Écoles des Ponts/Paris-Est
Institut francilien recherche, innovation et société (IFRIS)
johan.soderberg@univ-mlv.fr

**Abstract** The name 'legal highs' is given to drugs which have the same intoxicating effects as controlled substances, but which have not (yet) been prohibited by law. The impossibility of describing in advance every possible variation of a psychoactive molecule is mobilised by grassroots activists, entrepreneurs and organised crime to circumvent existing legal definitions. The case study provides a stepping stone for reflecting over the difficulties of regulating innovation in an economy centred on 'open innovation' and user-centred innovation models.

**Keywords** open innovation, user-centred innovation, designer drugs, legal highs, law enforcement, antagonism

## Introduction and overview of argument

The economy of drug trafficking holds up a mirror image to the official economy (Ruggieroand & South 1997). It can therefore help us to catch sight of phenomena, which have grown too familiar or are clouded behind euphemisms. For instance, the organisation of local drug trafficking in the Baltimor district in the US in the 1990s closely resembled an idealised notion of a 'cottage industry' (Eck & Gersh 2000). Likewise, the wheeling-and-dealing pusher can be said to personify the entrepreneurial subject *avant-la-lettre* (South 2004). This goes to suggest that one can learn much about how officially recognised, white markets operate by studying illegal drug markets. In a similar vein, I call upon legal highs to throw a new light on a phenomenon that has variously been labelled 'open innovation' (Chesbrough 2003), democratisation of innovation (von Hippel 2005), or 'research in the wild' (Callon & Rabeharisoa 2003). Although the scholars mentioned above belong to different intellectual traditions and their objectives diverge a great deal, they are all trying to encircle the same phenomenon. The object of study is an economy where the tools and know-how to innovate have been dispersed beyond the confines of firms and state institutions, and, subsequently, beyond the confines of experts and professionals. To Chesbrough, this offers an opportunity for companies to diversify innovation processes and lower in-house incumbents. To von Hippel, user-consumers can now invent products that better approximate their consumer needs and fancies. As for Callon and Rabeharisoa, they cherish an end to the epistemological superiority claimed by experts and professionals in the foregone, modernist era.

All the aforementioned scholars describe a trend, which they consider, on average to be benevolent. Evidence hereof is sought in empirical case studies of users who improve the functionality of mountain bikes (Luthje, Herstatt, and von Hippel 2005), create new juvenile products (Shah and Tripsas 2007), or develop medical instruments destined for legally recognised pharmaceutical companies (Lettl, Herstatt, and Gemuenden 2006). A common trait of the case studies mentioned above is that they start with a background assumption about the market economy as directed towards the production of goods for the benefit of society at large. The relation between firm and user is assumed to be consensual and cooperative. As a consequence, with the exception of licens-

ing regimes and intellectual property rights, questions about regulation and law enforcement have rarely been evoked in relation to 'open innovation' or lay expertise (cf. Söderberg 2010). Such *naïveté* is quickly put to shame when the users in question are tweaking molecule structures for the sake of circumventing legal definitions. The purpose of this paper is *to present an empirical case which compels us to adopt a more antagonistic perspective on the market economy, thus mandating a different theoretical apparatus than the ones now commonly drawn upon in studies of open innovation and/or user innovation*.

In order to foreground aspects of antagonism and contradiction in the regulation of (open) innovation processes, I point to Carl Schmitt, the infamous legal theorist in Nazi-Germany, and two of his contemporary critics, Franz Neumann and Otto Kirchheimer. The latter, associates of the Frankfurt School and emigrants, anchored their reflections over law and legal order in transformations of the economy. Like them, my inquiry into the regulation of legal highs falls back on an analysis of the economy. By making a comparison with activists and entrepreneurs developing filesharing tools, typically with the intent of violating copyright law, I hope to demonstrate that legal highs is not a stand-alone case. Rather, it gives indication of contradictions at the heart of an economy centred on fostering innovation and 'creative destruction'.

In the first section of the paper, I give an overview of the phenomenon of legal highs. In the next paragraph, the surge of legal highs is related to a longer debate about drugs and the problem of definitions. After having provided a summary of the empirical field, my theoretical apparatus will be introduced. Thereafter I move on to draw parallels with similar developments elsewhere in the economy. The main arguments of the paper are summarised at the end.

## Overview of legal highs

The defining trait of 'legal highs' is that the substance has not yet been defined in law as a controlled substance. Hence the production, possession and sale of the substance is not subject to law enforcement. Everything hinges on timing and novelty. When a substance has been prohibited, a small change of the molecule structure might suffice to circumvent the legal definition. What kinds of changes are required depends on the legal procedures in the country in question. A recurrent finding in Innovation Studies is that lead users often are ahead of firms in discovering new products and emerging markets. Quite so, for decades, legal highs was a marginal phenomenon chiefly engaged in by a subculture of ‘psychonauts’. Pioneers in underground chemistry like Nicholas Sand started in the 1960s to synthesise DMT and LSD, and they have since been followed by generations of aspiring chemist students. However, again confirming a wisdom from Innovation Studies, instances of on-off innovation by individuals for the sake of satisfying intellectual curiosity, personal consumption habits, or an urge to win recognition from one’s peers, takes on a different significance when the market grows bigger. Some of the chemistry students decided at one point to become full-time entrepreneurs, producing drugs not primarily for use but for sale. A major inflow came with the rave scene in the UK in the 1980s and early 1990s (McKay 1994). The outlawing of ecstasy and ‘magic mushrooms’ triggered a quest for novel substances among a larger section of the population. Concurrently, information became easier to come by. Back in the day, information about how to synthesise or extract substances were disseminated in obscure fanzines such as *Journal of Psychodelic Drugs*, *High Times* and *The Enthogen Review*, to mention three of the most renowned, and reaching an audience of a thousand readers at most. With the spread of the Inter-

net in the 1990s, information about fungus and herbs from all the corners of the world could be broadcast to a global audience. Thanks to the legally uncertain status of legal highs, the products can be advertised and sold by webshops that ship internationally. According to a recent survey, more than half of the shops were registered in UK, and more than a third in the Netherlands (Hillebrand, Olszewski & Sedefov 2010). In Ireland, drugs were sold openly in retail stores, so-called 'head shops', until a law was passed banning this practice (Ryall & Butler 2011). Globalisation has reshaped this market like any other. Most synthetic substances today are believed to have been produced in China, and, to a lesser extent, in India (Vardakou, Pistos, Spiliopoulou 2011b).

To provide an exhaustive taxonomy of something as ephemeral as legal highs is self-defeating from the start. To get a rough overview of the phenomenon under discussion, however, some highlights need to be given. A major group of legal highs classifies as synthetic cathinones. The source of inspiration comes from Khat, a plant traditionally used in East African countries. One derivative of this substance that has made it to the headlines is mephedrone. The first known instance of its use was in 2007 but it became widespread in 2009, in response to a new legislation in the UK that banned some other designer drugs. Subsequently, mephedrone was banned in UK in 2010, as well as in Netherlands and the Nordic countries (Winstock et al. 2010). Just a few months later, however, a new synthetic cathinone called Naphyrone took its place (Vardakou et al. 2011a). Another major class of drugs are synthetic cannabinoids. On the street they go under the name 'Spice' and are marketed as a legal alternative to marijuana. The synthetic extract of cannabis has been sprayed on herbal leaves. It took a long time for drug prevention authorities to realise that the active substance did not stem from the plant mixture but from added chemicals. In fact, it appears as some of the chemicals have been added to the compound simply to lead researchers astray and avoid detection (Griffiths et al. 2010). Piperazines, finally, have effects that are said to mimic ecstacy. One version of this substance, 1-benzylpiperazine (BZP) became a celebrity cause after New Zealand recognised its legal status. From 2005 till 2008, it was permitted to sell BZP if some restrictions on advertisement and age limits were respected. The drug could be obtained from all kinds of outlets—corner shops, petrol stations and conveniences stores (Sheridan & Butler 2010)

## Drugs and definitions

Definitions were always key in discussions about drugs and addiction. The ambiguities start with the binary separation between legal drugs (tobacco, alcohol, pharmaceuticals) and illegal ones. It has often been commented on that the harm caused by a drug only in a remote way relates to the legal status of that substance. All the major drugs, opium, cocaine, cannabis and amphetamine, were initially considered to be therapeutic and still have some medical uses. Consequently, the intoxicating effects of a drug itself do not give an exhaustive answer to the question why it has been banned. Conventions, public perceptions and entrenched interests carry a heavy weight in defining what belongs to the right or the wrong side of the law. The centrality of definitions in this discussion is old hat among the scholars studying misuse and addiction (Klaue 1999; Derrida 2003). However, in the case of legal highs, the inherent limitations of definitions and language take on a heightened importance. For instance, to avoid health and safety regulations, the drugs are often labelled 'research chemicals' or 'bath salt' and the containers carry the warning 'not for human consumption'. The drawback with this strategy is that no instructions can be given on the container about dosages or how to minimise risks when administrating the drug.

Legal highs thrives on phony definitions that reflect an ambiguity in the law as such. Ultimately, what legal highs points to is the limits and contradictions of modern sovereignty in one of its incarnations, the rule of law. At the heart of the legal order lies a mismatch between, on the one hand, general and universal concepts of rights, and, on the other, the singularity in which those rights must be defined and enforced. Examples abound of how this gap can be exploited to turn the law against itself. Tax evasion and off-shore banking comes to mind as examples from an altogether different field. This is to say that the case with legal highs is not exceptional. Nor is it novel. Perhaps the urge to play out the letter against the spirit of the law and find loopholes is as old as the law's origin in divine commandments. However, if the aim is to escape prosecution by the state, then the effectiveness of such practices presupposes a society bound by the rule of law. Rule-bending preys on the formalistic character of the law, which is specific to the secular, democratic and liberal society. Some core principles of the rule of law are as follows: The effects of a new law may only take place after the law has been passed. The law must be made known to the subjects that are ruled by it. What counts as a violation of the law must be clearly defined, as must the degree of enforcement and the punitive measures that is merited by a violation. In addition to the principles for how laws must be formulated, considerable time-lags are imposed by the recognised, democratic process for passing laws.

The original 1961 United Nation Single Convention on Narcotic Drugs laid down that unauthorized trade in a controlled substance should be made a criminal offence in signatory countries. It included a list of substances that were from now on to be held as illegal. Ten years later, more substances had been identified as problematic and were added to the list drawn up in the Convention on Psychotropic Substances. In the last years, however, the number of intoxicating and psychoactive substances is snowballing. According to the annual report by European Monitoring Centre for Drugs and Drug Addiction, there were almost one new substance discovered every week during 2011, and the trend is pointing steadily upward (ECNN 2012). It has become untenable to proceed along the default option of classifying each new substance individually. There is a wide variation in European countries how long time it takes to make a drug controlled (from a few weeks to more than a year), depending on what legislative procedures are required. The time-lag in the different jurisdictions are made the most of by the web-shops selling legal highs to the ‘EU common market’. Hence, pressure is building up for changing the procedures by which new substances are classified. The ordinary, parliamentary route of passing laws needs to be sidestepped if legislators are to keep pace with developments in the field. Already in 1986, United States introduced an analogue clause that by default includes substances structurally similar to recognised and classified substances (Kau 2008). Recently, UK and Ireland took a similar route, adopting generic, catch-all definitions of classified substances. Other countries have hesitated to follow suit, out of fear of introducing too much ambiguity in a law which carry heavy penalties (EMCCDA 2009). Alternative routes have been to put in place fast-track systems for classifying new substances, or to expand the use of consumer safety and/or medicine regulation, which can be used more flexibly (Hughes & Winstock 2011).

The fact that legal highs are not prohibited in law might give the impression that such drugs are less dangerous than known and illegal substances. The case is often the opposite. The toxicity of amphetamine, cocaine etc. are well known to medical experts. One doctor specialised in aesthetics told me that he receives almost one patient each week at his hospital in Göteborg, Sweden, that have become unconscious from the intake of a novel substance. It is hard to treat those cases

as the chemical content is unknown to the medical expertise. In 2012, it was reported in Swedish media that 14 people had died from just one drug, called 5-IT.

## A theoretical excursion: the sovereign and law

While the medical risks of legal highs are easy enough to appreciate, other kinds of risk stem from the responses by legislators and law enforcement agencies. The collateral damage of international drug prevention has been thoroughly documented by scholars in the field. Especially in developing countries, the war on drugs has contributed to human rights abuses, corruption, political instability, and the list goes on (Barrett 2010). Given this shoddy history, it is merited to ask what negative consequences a 'war on legal highs' might bring. Almost every country in the European Union have revised their laws on drug prevention, or are in the process of doing so, in direct response to the surge of legal highs. The laws need to be made more agile to keep pace with the innovativeness of users and organised crime, or else law enforcement will be rendered toothless. Such flexibility is bought at a high price, though, as the constraints are part and parcel of rule of law.

It is in this light that it becomes relevant to recall Carl Schmitt's reflections over the sovereign, alluded to in the introduction of the paper. Schmitt identified the punitive system as the nexus where the self-image of pluralistic, liberal democracy has to face its own contradictions. Thus he called attention to the fact that peaceful deliberation always presupposes the violent suppression of hostile elements. The delimitation of the violence monopoly of the state laid down by the rule of law is, at the end of the day, limits that the sovereign chooses to impose on himself (or not) (Schmitt 2007; Zizek 1999). Carl Schmitt's radical challenge to the liberal and formalist legal tradition has been extensively commented on in recent years. Many thinkers on the left are attracted to his ideas as an antidote to what they consider to be an appeasing, post-political self-understanding in liberal societies (Mouffe 2005).

Here I am less interested in present-day appropriations of Carl Schmitt's thinking, than to use him as an entry point to discuss the works of two of his contemporary critics, Franz Neumann and Otto Kirchheimer. They lived through the same convulsions of the Weimar Republic as Carl Schmitt did, but drew very different conclusions from that experience. Before saying anything more, let me first make clear that I am *not* suggesting comparing the historical situation in Germany during the 1930s and the current one, a claim that would be hyperbolic and misleading. What interests me with their writings is that they anchored the rule of law in a transformation of the economy. In a ground-breaking essay, Franz Neumann argued that formalistic modes of law and legal reasoning had enjoyed broad support from privileged business interests in an era of competitive capitalism, epitomised by nineteenth century Britain. Competing firms wanted the state to act as an honest broker. Neumann did not take the self-descriptions of the rule of law at face value. He knew full well that law did not apply equally to all the subjects of the land. Still, he also recognised that subjugated groups had something to lose if this pretence was given up. As a labour organiser in the Weimar Republic, he had seen first-hand how the German business elite begun to cede their commitments to strict, clear, public and prospective forms of general law. Neumann explained this change of heart with an ongoing transition from competitive to monopolistic capitalism. Monopolies did not rely on the state as a broker. Rather, universally applicable laws were perceived as an encumbrance and a source of inflexibility (Neumann 1996).

If Neumann's reasoning is pushed too far, it turns into crude economism. It is merited to bring him up, nonetheless, because his ideas provide a missing piece of the puzzle to discussions about open innovation. Recently, William Scheuerman defended the actuality of Neumann's thinking on law in light of globalisation. Multinational companies do not depend on national legislation to the same extent as before, while national parliaments are struggling to keep ahead and passings laws in response to developments in financial trading and global markets (Scheuerman 2001). If the word ‘globalisation’ is replaced with ‘innovation’, then Scheuerman's argument concurs with the case I am trying to make here. The actors involved in developing legal highs stand as examples of how the speed of innovation places demands on legislators and parliaments that are difficult to reconcile with the principles of rule of law and democratic decision making. Furthermore, the example with legal highs should not be understood as an isolated phenomenon. As I will argue in the next paragraph, legal highs is indicative of broader transformations in an economy mandating innovation and technological change, including, crucially, open innovation. It can be worthwhile to recall that in 1950, Carl Schmitt too expressed concerns about how the legal system would cope with the acceleration of society, which he claimed to see evidence of on all fronts. He divined that this would result in a 'motorization of law':

> “Since 1914 all major historical events and developments in every European country have contributed to making the process of legislation ever faster and more summary, the path to realizing legal regulation ever shorter, and the role of legal science ever smaller.” (Schmitt 2009, p.65)

## Regulating innovation in an economy of innovation

The ongoing efforts to circumvent legal definitions are carried out through innovation. The property looked for in a novel string of molecules or a new family of plants is the quality of not having been classified by regulators. Innovation is here turned into a game of not-yet and relative time-lags. Legislation is the planet, which this frenetic activity gravitates around. This contrasts sharply with the mainstream discourse about the relation between legal institutions and innovation. It is here assumed that the institutions of law and contractual agreement serve to foster innovative firms by providing stability and predictability for investors (Waarden 2001). However, a closer examination will reveal that legal highs are not such an odd-one-out after all. A lot of the innovation going on in corporate R&D departments is geared towards circumventing one specific kind of legal definition, that is to say, patents. The drive to increase productivity, lower costs and creating new markets are only part of the history behind innovation. As important is the drive to invent new ways to achieve the same-same old thing, simply for the sake of avoiding a legal entitlement held by a competitor. Perhaps this merits a third category in the taxonomy of innovations, besides radical and incremental innovations, which I elect to call ‘phony innovations’. Note to be taken, I do not intend this term to be derogative. What ‘phony’ refers to is something specific: innovation that aims to get as close as possible to a pre-existing function or effect, while being at variance with how that function is defined and described in a legal text. A case in point is naphyrone, made to simulate the experience that user previously had with mephedrone.

To regulate innovation, something non-existent and unknown must be made to conform with what already exists: the instituted, formalised and rule-bound. Activist-minded members of the ‘psychonaut’ subculture, as well as entrepreneurs selling legal highs, seize on this opportunity to circumvent state regulation, which they tend to perceive as a hostile, external force. The image of

an underdog inventor who outsmarts an illegitimate state power through technical ingenuity is widely spread, also among subcultures engaged in publicly accepted activities, such as building wireless community networks (Söderberg 2011). In a time when the whole of Earth has been mapped out and fenced in by nation states, often with science as a handmaid, innovation and science turns out to be the final frontier. In popular writings about science in the ordinary press, science is portrayed as the inexhaustible continent, offering land-grabs for everyone at no-ones expense. The colonial and scientistic undertones of such rhetoric hardly need to be pointed out. What is more interesting to note is that the frontier rhetoric also calls to mind folktales about the outlaw (and, occasionally, a social bandit or two, in Hobsbawn's sense of the word). Science and innovation turns into the last hide-out from the sheriff, as it were. The official recognition granted to this cultural imagination is suggested by the term 'shanzhai innovation'. It used to be the name of some marshlands in China where bandits could evade authorities, but nowadays 'shanzhai' designates product innovations made by manufacturers of counterfeited goods (Lindtner & Li 2012).

Twenty years ago, the no-mans-land opened up by innovation had a permanent address, it was 'cyberspace'. John Perry Barlow declared its independence vis-à-vis the governments of the industrial world. His declaration has (rightly) been ridiculed. These days, cyberspace has as much independence from states as an encircled, indian reservation. That being said, temporality is built-into the frontier notion from the start. New windows open up as the old ones are closed down. Concurrently, there is a historical continuity which links the subcultures dedicated to filesharing, crypto-currencies (such as BitCoin) etc. thriving on the Internet, and the psychonaut subculture experimenting with legal highs. Both technologies where pioneered by the same cluster of people, stemming from the same 1960s American counter-culture. Hence, the subcultures associated with either technology have inherited many of the same cultural tropes. This is particularly evident from a shared hostility towards state authority and state intervention, experienced as an unjust restriction of the freedom of the individual to do as he pleases. There is also a practical link, as the surge of legal highs would be unthinkable without the Internet. Discussion forums are key for sharing instructions for how to administrate a drug. And reviews of retailers and novel substances on the Internet provide a minimum of consumer power (Walsh & Phil 2011; Thoër & Millerand 2012).
The comparison between crypto-anarchism and psychonauts is merited also because both puts in relief the troubled relation between innovation and law. A closely related case is the struggle over filesharing. In much the same way as with the relentless search for unclassified drugs, legal definitions of what constitutes a copyright violation are continuously circumvented by programmers/hackers. They do so by rewriting the way the filesharing network operates. To take one example out of the hat: the Swedish court case against one of the world's largest filesharing sites, the Pirate Bay (Andersson 2011). Swedish and international copyright law specifies that an offence consists in the unauthorised dissemination of a file containing copyrighted material. Strictly speaking, however, not a single file was up- or downloaded on the Pirate Bay site that violated this definition of copyright law. Pirate Bay relies on the BitTorrent protocol, which means that the file has been broken up into a torrent of thousands of fragments scattered all over the network. This protocol qualifies as a 'phony innovation' in the sense defined above. When the fragments are combined by the end-user/computer, an effect is produced on the screen (an image, a sound, etc.) indistinguishable from that which would have happened, had a single file been transmitted to the user. As it now stands, there is not a single person responsible for uploading the file and against whom charges can be pressed. The three men behind the Pirate Bay (and an additional fourth one whose

involvement is highly questionable), were nevertheless found guilty by the Swedish court, on the grounds of having assisted in copyright violation. Technically speaking, however, the Pirate Bay provided a search engine service similar to Google, though specialised in BitTorrent files. A user bent on violating copyright law could just as effectively have used the latter. Such technical niceties create a dilemma for the entire juridical system: either stick with legal definitions and risk having the court procedure grinding to halt, or arbitrarily override the principles of rule-of-law.

## Conclusion

The development of legal highs is exceptional on at least one count, namely in that governments try very hard to prevent it from happening. When those initiatives fail, the response from policy makers and legislators has been to scale up the efforts. Changes are introduced in legislative procedures, international cooperation is strengthened, and more power is given over to law enforcement agencies. In most other cases, the official stance on innovation and technology development is *laissez-faire*. The underlying assumption is that whatever unfortunate side-effects a technology might have, unemployment, health risks, environmental degradation, etc., it is due to a technical imperfection, something that can be set right through more innovation. Of course, the importance given to innovation owes to the belief that innovation is the royal road for staying competitive in global markets. Everyone must bow to this imperative, be it a worker, a firm or a nation state. Subsequently, firms are forced by competition to follow after innovative lead-users, no matter where it leads. This might sound like old hat to Innovation Studies scholars. But there is a twist to the tale. Some lead users end up on the wrong side of the law, or at least in a grey-zone between legality and illegality (Flowers 2008). The important point to stress here is that, although the motives of the delinquent innovator may be despicable and self-serving, he is also very, very productive. The appropriation of filesharing methods by the computer industry gives a pointer. The distributed method for storing and indexing files in a peer-to-peer network has proven to be advantageous over older, centralised forms of data retrieval. The technique has become an industrial standard. Even the practice of filesharing itself has been incorporated in the marketing strategies of some content providers, including those who are pressing charges against individual filesharers (MediaDefender being the celebrity case). While filesharers and providers of filesharing services are fined or sent to prison, the innovations stemming from their (illegal) activities are greasing the wheels of the culture industry. By the same token, one can expect that some of the discoveries made by clandestine chemists and psychonauts will be added to the patent portfolio of respected pharmaceutical companies. It suffices to recall that the practice of methamphetamine cooking in the US has driven up over-the-counter sales of cold medicine (in which a key precursor for methamphetamine can be found, ehpedrine), far beyond what any known cold epidemic could account for (Redding 2009). In conclusion, the legal grey zone has become an incubator for innovation. It acquires a structural importance in the so-called 'knowledge economy'. The interesting questions to ask about 'open innovation' are therefore: what possibilities remain for a society wanting to prohibit particularly harmful innovations, and how can this be done without sacrificing some of the core principles of rule-of-law?

## References


A. Alexander & M. Roberts (Eds.). (2003). *High Culture – Reflections on Addiction and Modernity.* Albany, State University of New York Press.

Andersson, J. (2011). The origins and impacts of Swedish filesharing: A case study. *Journal of Peer Production. R*etrieved from http://peerproduction.net/issues/issue-0/peer-reviewed-papers/

Barrett, D. (2010). Security, development and human rights: Normative, legal and policy challenges for the international drug control system. *International Journal of Drug Policy,21*, 140–144 .

*Callon, M. & Rabeharisoa, V. (2003). Research "in the wild" and the shaping of new social identities Technology in Society 25, (2), 193–204.*

*Chesbrough, H. (2003). The era of open innovation.MIT Sloan Management Review,* 44 (3), 35-41.

Derrida, J. (2003). The rhetoric of drugs. In: A. Alexander & M. Roberts (Eds.), *High Culture— Reflections on Addiction and Modernity* (pp. 19-44) Albany: State University of New York Press.

Eck, J & Gersh, J. (2000). Drug trafficking as a cottage industry.*Crime Prevention Studies, 11*, 241-271.

EMCDDA (2009) Legal responses to new psychoactive substances in Europe, available: http://eldd.emcdda.europa.eu/

Flowers, S. (2008) Harnessing the hackers: The emergence and exploitation of Outlaw Innovation. *Research Policy*, 37 (2), 177–193.

Griffiths, P, Sedefov, R., Gallegos, A. & Lopez, D. (2010). How globalization and market innovation challenge how we think about and respond to drug use: 'Spice' a case study. *Addiction,105*, 951–953.

Hillebrand, J., Olszewski, D. & Sedefov, R. (2010) Legal Highs on the Internet.*Substance Use & Misuse*, *45*, 330–340.

Hughes, B. &Winstock , A. (2011). Controlling new drugs under marketing regulations. *Addiction*, 107 (11), 1894-1899.

Kau, G. (2008) Flashback to the Federal Analogue Act of 1986: Mixing rules and standards in the Cauldron, *University of Pennsylvania Law Review*, 156 (4), 1077-1115.

Klaue, K. (1999). Drugs, addictions, deviance and disease as social constructs.*Bulletin on Narcotics*, 1–2.

Lettl, C., C. Herstatt, and H. Gemuenden (2006). Users' contributions to radical innovation: Evidence from four cases in the field of medical equipment technology. *R&D Management*, *36*, 251-72.

Lindtner, S. & Li, D. (2012) *Created in China: the makings of China's hackerspace community. Interactions, 19 (6), 18-22.*

Luthje, C., C. Herstatt, and E. Hippel (2005). User-innovators and ''local'' information: The case of mountain biking. *Research Policy*, 34, 951-956.

McKay, G. (1994). Senseless acts of beauty: Cultures of resistance . London: Verso.

Mouffe, C. (2005). *On the Political.*London: Routledge.

Neumann, F. (1996) The change in the function of law in modern society. In: Scheuerman, W. *The rule of law unders siege: Selected essays of Franz Neumann and Otto Kirchheimer* (101-141) Los Angeles: California University Press.

Reding, N. (2009) Methland: The death and life of an American small town. New York: Bloomsury.

Ruggieroand, V. & South, N. (1997). The late-modern city as a bazaar: Drug markets, illegal enterprise and the 'barricades'. *The British Journal of Sociology*, *48* (1), 54-70.

Ryall, G. & Butler, S. (2011). The great Irish head shop controversy.*Drugs: education, prevention and policy*. 18 (4), 303–311.

Scheuerman, W. (1996). The rule of law under siege: Selected essays of Franz L. Neuman and Otto Kirchheimer. Berkeley: University of California Press.

Scheuerman, W. (2001) Franz Neumann: Legal Theorist of Globalization? *Constellations*, 8 (4), 503-520.

Schmitt, C. (2007). *The Concept of the Political*. Chicago: University of Chicago Press.

Schmitt, C. (2009). The Motorized Legislator. In: Rosa, H. & Scheuerman, W. (Eds.) *High-speed society: social acceleration, power, and modernity*. (65 – 76) Pennsylvania: The Pennsylvania State University

Shah, S., & Tripsas, M. (2007). The accidental entrepreneur: The emergent and collective process of user entrepreneurship. *Strategic Entrepreneurship Journal 1*, 123-140.

South, N. (2004). Managing work, hedonism and 'the borderline' between the legal and illegal markets: Two case studies of recreational heavy drug users. *Addiction Research and Theory, 12* (6), 525–538.

Sheridan, J. & Butler, R. (2010). “They’re legal so they’re safe, right?” What did the legal statusof BZP-party pills mean to young people in New Zealand? *International Journal of Drug Policy*, 21 (1), 77–81.

Söderberg, J. (2010). Misuser Inventions and the Invention of the Misuser: Hackers, Crackers and Filesharers. *Science as Culture*, *19* (2), 151-179.

Söderberg, J. (2011). Free Space Optics in the Czech Wireless Community: Shedding Some Light on the Role of Normativity for User-Initiated Innovations. *Science, Technology & Human Values*, 36 (4), 423-450.

Thoër, C. & Millerand, F. (2012). Enjeux éthiques de la recherche sur les forums Internet portant sur l'utilisation des médicaments à des fins non médicales. *Revue International: Communication Sociale et Publique*, 7, 1-22

Vardakou, I., Pistos, C., Dona, A., Spiliopoulou, C. & Athanaselis , S. (2011). Naphyrone: a “legal high” not legal any more. *Drug and Chemical Toxicology*, 1–5 .

Vardakou, C., Pistos, C. and Spiliopoulou, C. (2011). Drugs for youth via Internet and the example of mephedrone. *Toxicology Letters,201*, 191-195.

von Hippel, E. (2005). *Democratizing innovation*. MIT Press.

Waarden, F. (2001). Institutions and Innovation: The Legal Environment of Innovating Firms. *Organisation Studies*, 22 (5), 765-795.

Walsh, C. & Phil, M. (2011). Legal Highs on the Internet. *Journal of Psychoactive Drugs*, *43* ( I ), 55-63.

Whalen, J. (2010). Keeping it legal. *Chemistry & Industry* 24 (5).

Winstock, A, Mitcheson, L, Deluca, P, Davey, Z, Corazza, O & Schifano, F. (2010). New kid for the chop? *Addiction* 106, 154–161.

Zizek, S. (1999). Carl Schmitt in the age of post-politics. In: C. Mouffe (Ed.), *The Challenge of Carl Schmitt* (18-37). London: Verso.

Zizek, S. (2000). The Ticklish Subject: The Absent Centre of Political Ontology. New York: Verso.

# PART II: THE SCOPE OF LAW

# Rules of a networked society: Here, there and everywhere

Michael Anthony C. Dizon
Tilburg University
Tilburg Institute for Law, Technology, and Society (TILT)
✉m.a.dizon@uvt.nl

**Abstract** With the ever-increasing informatization and technologization of society, technological rules and actors are playing a greater role in the governance of the digital and connected world. This paper argues that, in order to better understand how the networked information society is organized and operates now and in the near future, it is important to develop and adopt a pluralist, rules-based approach to the study of law and technology. This means coming to terms with and taking seriously the plural legal and extra-legal rules, norms, codes, and principles that influence behavior and determine the state and degree of normativity in society. The proposed approach can be handily applied to the case of hackers. From a pluralist perspective, hacking is not simply a problem to be solved but a complex, techno-social phenomenon that needs to be properly observed and understood. Adopting a pluralist approach to law and technology study can be valuable since multiple persons, things and rules do profoundly shape the world we live in. This rules-based approach can potentially bridge the distance between law and technology and bring them ever closer together.

**Keywords** rules, pluralist, normative, technology, hackers

## Impact of technological rules and actors on society

At the height of the dot-com boom in the late 1990s, Lawrence Lessig expressed and popularized the idea that technical code regulates (Lessig 2006). Since then, together with rapid technological developments and widespread dissemination of technologies in all aspects of people's lives, the growing influence on the behavior of people and things of technological rules and actors other than and beyond the law and the state has become all the more apparent. The behaviors of people online are to a certain extent determined by the technical protocols and standards adopted by the Internet Engineering Task Force (IETF) and other non-governmental bodies that design the architecture of the internet (see Murray 2007, 74; Bowrey 2005, 47). The Arab Spring has proven that the use of internet-based communications and technologies can enable or have a role in dramatic political and social change (Howard 2011; Stepanova 2012).[1] Making full use of their technical proficiency, the people behind the whistleblower website Wikileaks and the hacktivist group Anonymous have become influential albeit controversial members of civil society who push the boundaries of what democracy, freedom and civil disobedience mean in a digital environment (Ludlow 2010; Hampson 2012, 512-513; Chadwick 2006, 114). Technology-related rules even had a hand in one of the most significant events of the new millennium, the Global Financial Crisis. It is claimed that misplaced reliance by financial institutions on computer models based on a mathematical algorithm (Gaussian copula function) was partly to blame for the miscalculation of risks that led to the crisis (Salmon 2009; MacKenzie&Spears 2012). The fact that a formula (i.e., a rule expressed in symbols) can affect the world in such a momentous way highlights the critical role of rules in a 'networked information society' (Cohen 2012, 3) or 'network society' (Castells 2001, 133).

[1] But see Morozov (2011a; 2011b) for more somber assessments of technology's role in political change.

This paper argues that, in order to better understand how a networked society is organized and operates now and in the near future, it is important to develop and adopt a pluralist, rules-based approach to law and technology research. This means coming to terms with and seriously examining the plural *legal and extra-legal rules*, norms, codes, and principles that influence and govern behavior in a digital and computational universe (see Dyson 2012), as well as the persons and things that create or embody these rules. Adopting this rules-based framework to technology law research is valuable since, with the increasing informatization and technologization of society (Pertiera 2010, 16), multiple actors and rules – both near and far – do profoundly shape the world we live in.

## From 'what things regulate' to 'what rules influence behavior'

A pluralist and distributed approach to law and technology is not new (see Schiff Berman 2006; Hildebrandt 2008; Mifsud Bonnici 2007, 21-22 ('mesh regulation'); Dizon 2011). Lessig's theory of the four modalities of regulation (law, social norms, the market, and architecture) serves as the foundation and inspiration for many theories and conceptualizations about law, regulation and technology within and outside the field of technology law (Lessig 2006, 123; Dizon 2011). Modifying Lessig's model, Murray and Scott (2002, 492) come up with what they call the four bases of regulation: hierarchy, competition, community, and design. Similarly, Morgan and Yeung (2007, 80) advance the five classes of regulatory instruments that control behavior, namely: command, competition, consensus, communication, and code.

Lessig's conception of "*what things regulate*" (Lessig 2006, 120) is indeed insightful and useful for thinking about law and technology in a networked society. I contend, however, that his theory can be remade and improved by: (1) modifying two of the modalities; (2) moving away from the predominantly instrumentalist concerns of 'regulation' and how people and things can be effectively steered and controlled to achieve stated ends (Morgan & Yeung 2007, 3-5; Black 2002, 23, 26); and (3) focusing more on how things actually influence behavior rather than just how they can be regulated. I prefer to use the term 'technology' rather than 'architecture' since the former is a broader concept that subsumes architecture and code within its scope. By technology, I mean the '*application of knowledge to production from the material world. Technology involves the creation of material instruments (such as machines) used in human interaction with nature*' (Giddens 2009, 1135). The regulatory modality of 'the market' is slightly narrow in its scope since it pertains primarily to the results of people's actions and interactions. This modality can be expanded to also cover the 'naturaland social forces and occurrences' (including economic ones) that are present in the physical and material world. In the same way that market forces have been the classic subject of law and economics, it makes sense for those studying law and technology issues to also examine other scientific phenomena. As will be explained in more detail below, social norms are distinguished from natural and social phenomena since the former are composed of prescriptive (ought) rules while the latter are expressed as descriptive (is) rules. Based on the above conceptual changes to Lessig's theory, the *four things that influence behavior* are: (1) law, (2) norms, (3) technology, and (4) natural and social forces and occurrences.

The four things that influence behavior can be further described and analyzed in terms of the rules that constitute them. From a rules-based perspective, law can be conceived of as being made up of *legal rules*, and norms are composed of specific *social norms*. On their part, technolo-

gy consists of *technical codes and instructions*, while natural and social forces and occurrences are expressed in *scientific principles and theories*. By looking at *what rules influence behavior*, one can gain a more detailed, systematic and interconnected picture of who and what governs a networked society. Lessig's well-known diagram of what constrains an actor can be reconfigured according to the four types of rules that influence behavior. The *four rules of a networked society* therefore are *legal rules*, *social norms*, *technical codes*, and *scientific principles* (see Figure 1).

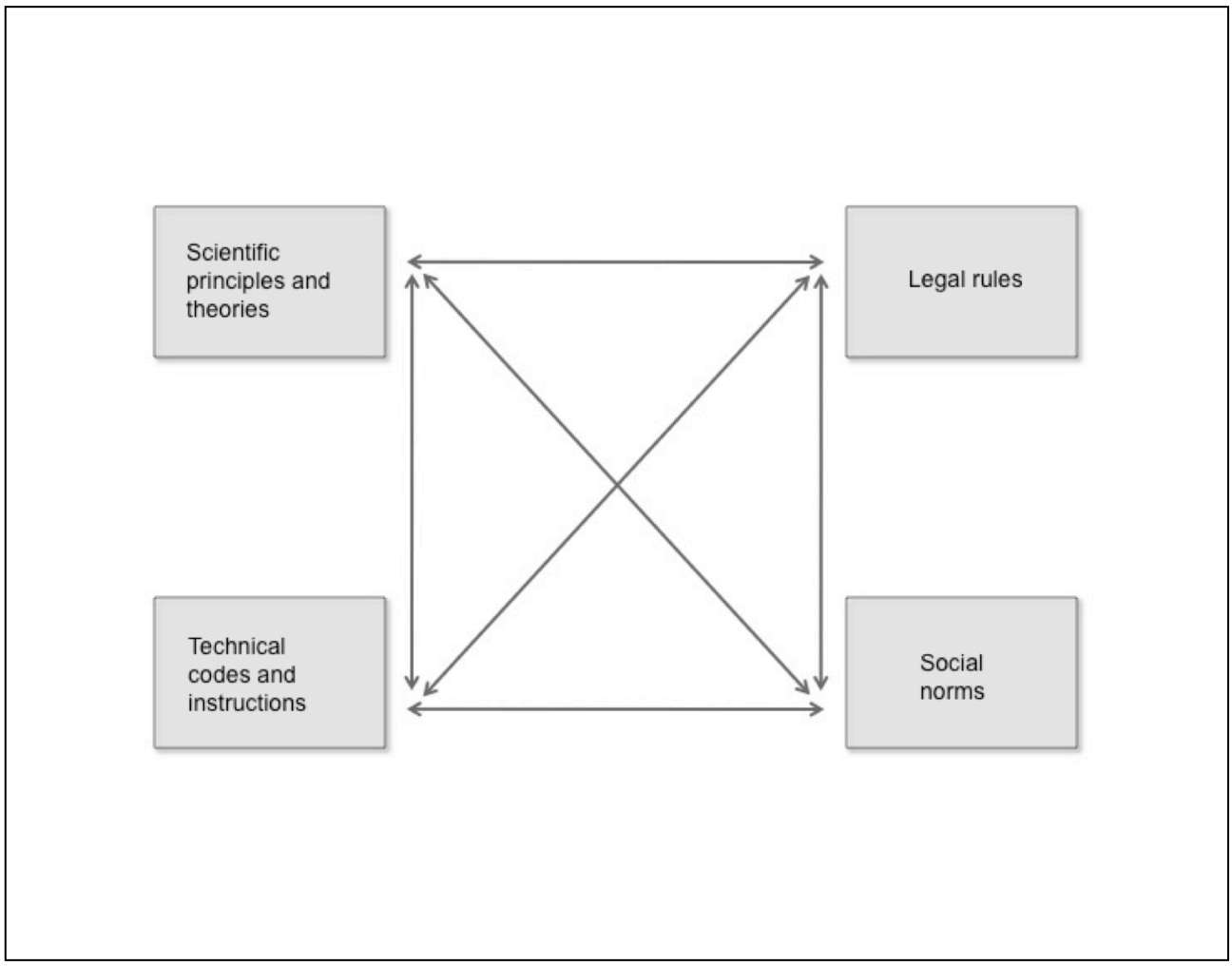



**Figure 1:**The four rules of a networked society

## Rules of a networked society

### *Plurality of rules*

How the various rules of a networked society relate to and interact with each other is very important to understanding how the informational and technological world works. Having a clear idea of how and why the rules are distinct yet connected to one another is paramount given that, in most cases, there are multiple overlaps, connections, intersections and even conflicts among these rules. More often than not, *not one but many rules* are present and impact behavior in any given situation.

The presence of two or more rules or types of rules that influence behavior in a given situation gives rise to a condition of *plurality of rules*. Plurality of rules resembles the concept of 'legal pluralism', which is described by John Griffiths as "*that state of affairs, for any social field, in which behavior pursuant to more than one legal order occurs*" (Griffiths 1986, 2; von Benda-Beckmann & von Benda-Beckmann 2006, 14). Legal pluralism generally considers both descriptive and normative/prescriptive rules as falling within the ambit of the term law (von Benda-Beckmann 2002, 48). As a result, legal pluralism has been subject to the perennial criticism that, due to its more expansive conception of law, the distinction between law and other forms of social control has been blurred (Merry 1988, 871, 878-879, 858; Griffiths 1986, 307; von Benda-Beckmann 2002, 47, 54, 56). In order to avoid a similar critique, while still maintaining a pluralist perspective, I deliberately use the term 'rule' (*regula*) rather than 'law' (*lex*) to characterize and describe the things that influence and govern behavior. Unlike law, which is inherently normative, a rule has greater flexibility and can cover both is and ought statements. In this way, the important distinction between descriptive rules and normative rules is retained, and the term rule can still be used in two discrete senses: (1) as an observed *regularity*[2] and (2) as a *standard* that must be observed. The concept of rules is thus sufficiently robust and nuanced that it can serve as the basis for constructing a new way of perceiving the state and degree of normativity in the networked information society (Riesenfeld 2010). Far from conflating the four things that influence behavior, a rules-based perspective is able to integrate and find important interconnections between and among them while, at the same time, preserving and taking in account their uniqueness.

The different types of rules of a networked society and how they connect with each other are explained in greater detail below.

### *Legal rules and social norms*

Legal rules and social norms are both prescriptive types of rules. A social norm has been defined in a number ways: as 'a statement made by a number of members of a group, not necessarily by all of them, that the members ought to behave in a certain way in certain circumstances' (Opp 2001, 10714), as 'a belief shared to some extent by members of a social unit as to what conduct *ought to be* in particular situations or circumstances' (Gibbs 1966, 7), and as 'generally accepted, sanctioned prescriptions for, or prohibitions against, others' behavior, belief, or feeling, i.e. what others *ought* to do, believe, feel – *or else*' (Morris 1956, 610). Dohrenwend proffers a more detailed definition:

> A social norm is a rule which, over a period of time, proves binding on the overt behavior of each individual in an aggregate of two or more individuals. It is marked by the following characteristics: (1) Being a rule, it has content known to at least one member of the social aggregate. (2) Being a binding rule, it regulates the behavior of any given individual in the social aggregate by virtue of (a) his having internalized the rule; (b) external sanctions in support of the rule applied to him by one or more other individuals in the social aggregate; (c) external sanctions in support of the rule applied to him by an authority outside the social aggregate; or any combination of these circumstances. (Dohrenwend 1959, 470)

From the above definitions, the attributes of social norms are: '*(1) a collective evaluation of behavior in terms of what it* ***ought to be****; (2) a collective expectation as to what behavior* ***will be****; and/or*

[2] In relation to social norms, behavioral regularities that lack a normative element are also called "conventions" (see McAdams & Rasmusen 2007, 1576).

*(3) particular **reactions** to behavior, including attempts to apply sanctions or otherwise induce a particular kind of conduct*'. (Gibbs 1965, 589)

Norms are a key element to a rules-based approach to law and technology. This is especially evident when one recognizes that law is '*a type of norm*' and '*a subset of norms*' (Gibbs 1966, 315; Opp 2001, 10715; Posner 1997, 365[3]) Laws may be deemed to be more formal norms. Galligan holds the inverse to be true: '*some rule-based associations are mirrors of law and as such may lay some claim to be considered orders of **informal laws***' (Galligan 2007, 188). Norms and laws can therefore be imagined as forming a *continuum* and the degree of formality, generality, certainty and importance (among other things) is what moves a rule of behavior from the side of norms to the side of law (see Ruby 1986, 591).

Legal rules and social norms have a close and symbiotic relationship. Cooter explains one of the basic dynamics of laws and norms, '*law can grow from the bottom up by [building upon and] enforcing social norms*' (Cooter 1996, 947-948), but it can also influence social norms from the top down – "*law may improve the situation by enforcing a beneficial social norm, suppressing a harmful social norm, or supplying a missing obligation*" (ibid 1996, 949). Traditional legal theory has settled explanations of how laws and norms interact. Social norms can be transformed into legal norms or accorded legal status by the state through a number of ways: incorporation (social norms are transformed or codified into law by way of formal legislative or judicial processes), deference (the state recognizes social norms as facts and does not interfere with certain private transactions and private orderings), delegation (the state acknowledges acts of self-regulation of certain groups) (Michaels 2005, 1228, 1231, 1233 and 1234), and recognition (the state recognizes certain customary or religious norms as state law) (van der Hof & Stuurman 2006, 217).

### *Technical codes and instructions*

Technical codes like computer programs consist of descriptive rather than prescriptive instructions. However, the value of focusing on rules of behavior is that the *normative effects* of technical codes can be fully recognized and appreciated. Despite the title of his seminal book and his famous pronouncement that '*code is law*', Lessig (2006, 5) does not actually consider technical or computer code to be an actual category or form of law, and the statement is basically an acknowledgement of code's law-like properties. As Leenes (2011, 145) points out, '*Although Lessig states that 'code is law', he does not mean it in a literal sense*'. Even Reidenberg's earlier concept of Lex Informatica, which inspired Lessig, is law in name only (Lessig 2006, 5). Reidenberg explicitly states that Lex Informatica can be '*a useful **extra-legal** instrument that may be used to achieve objectives that otherwise challenge conventional laws and attempts by government to regulate across jurisdictional lines*' (1997, 556 emphasis added). While Lex Informatica '*has analogs for the key elements of a legal regime*', it is still '*a **parallel rule system***' that is '*distinct from legal regulation*' (Reidenberg 1997, 569, 580 emphasis added). But if '*code is not law*' as some legal scholars conclude (Dommering 2006, 11, 14), what exactly is the relationship between technical codes and law, and what is the significance of code in the shaping of behavior in a networked society?

Using the above definition and characterization of norms, technical code *in and of itself* (i.e., excluding any such norms and values that an engineer or programmer intentionally or unintention-

[3] "law is older than political society, which means that it originates as a set of norms" Posner (2000, 365).

ally implements or embodies in the instructions) is *neither a legal rule nor a social norm* because: (1) it is not a shared belief among the members of a unit; (2) there is no *oughtness* (must or should) or a sense of obligation or *bindingness* in the *if-then* statements of technical code (they are simply binary choices of on or off, true or false, is versus not); (3) there is no 'or else' element that proceeds from the threat of sanctions (or the promise of incentives) for not conforming (or conforming) with the norm; (4) the outcome of an if-then statement does not normally call for the imposition of external sanctions by an authority outside of the subject technology; (5) and, generally, there is no collective evaluation or expectation within the technical code itself of what the behavior ought to be or will be (a matter of *is* and not *ought*).

Even though technical codes and instructions are not per se norms, they can undoubtedly have normative effects (van der Hof & Stuurman 2006, 218, 227). Furthermore, technologies are socially constructed and can embody various norms and values (Pinch & Bijker 1984, 404). A massively multiplayer online role-playing game (MMORPG) such as World of Warcraft has its own rules of play and can, to a certain extent, have normative effects on the persons playing it (they must abide by the game's rules and mechanics). A virulent computer program such as the 'ILOVEYOU' virus/worm (or the Love Bug) that caused great damage to computers and IT systems around the world in 2000 can have a strong normative impact; it can change the outlooks and behaviors of various actors and entities (Cesare 2001, 145; Grossman 2000). As a result of the outbreak of the Love Bug, employees and private users were advised through their corporate computer policies or in public awareness campaigns not to open email attachments from untrustworthy sources. In the Philippines, where the alleged author of the Love Bug resided, the Philippine Congress finally enacted a long awaited Philippine Electronic Commerce Act, which contained provisions that criminalized hacking and the release of computer viruses.[4] The Love Bug, which is made up of technical instructions, definitely had a strong normative impact on computer use and security.

Digital rights management (DRM) is an interesting illustration of the normative effects of technology since, in this case, technical code and legal rules act together to enforce certain rights for the benefit of content owners and limit what users can do with digital works and devices (see Brown 2006). DRM on a computer game, for example, can prevent users from installing or playing it on more than one device. Through the making of computer code, content owners are able to create and grant themselves what are essentially new and expanded rights over intellectual creations that go beyond the protections provided to them under intellectual property laws (van der Hof & Stuurman 2006, 215; McCullagh 2005). Moreover, supported by both international and national laws,[5] DRM acts as hybrid techno-legal rules that not only restrict the ability of users to access and use digital works wrapped in copy protection mechanisms, but the circumvention of DRM and the dissemination of information about circumvention techniques are subject to legal sanctions (see Dizon 2010).[6] When users across the world play a computer game with 'always-on' DRM like

---

4 Philippine Electronic Commerce Act, s 33(a); Disini, Jr. & Toral (2000, 36-37; Sprinkel 2001, 493-494; Pabico & Chua 2001).

5 See WIPO Copyright Treaty and the World Performance and Phonograms Treaty (together the WIPO Internet Treaties).

6 Another noteworthy example of hybrid techno-legal rules are those relating to "privacy by design", which are being advanced in the privacy and data protection regulations of Canada and the European Union (see Cavoukian 2009; see European Commission COM(2010) 245 final/2 and COM(2010) 609 final.

Ubisoft's *Driver*, it is tantamount to people's behavior being subjected to a kind of transnational, technological control, which users have historically revolted against (Hutchinson 2012; Doctorow 2008).

Another example of hybrid techno-legal rules is the so-called Great Firewall of China. This computer system that monitors and controls what users and computers within China can access and connect to online clearly has normative effects since it determines the actions and communications of an entire population (Karagiannopoulos 2012, 155). In fact, it does not only control what can be done within China but it also affects people and computers all over the world (e.g., it can prevent a Dutch blogger or a U.S. internet service such as YouTube from communicating with Chinese users and computers). In light of their far-reaching normative impact, technical codes and instructions should not be seen as mere instruments or tools of law (Dommering 2006, 13-14), but as a distinct type of rule in a networked society. Code deserves serious attention and careful consideration in its own right.

### *Scientific principles and theories*

There is a whole host of scientific principles, theories and rules from the natural, social and formal sciences that describe and explain various natural and social phenomena that influence the behavior of people and things. Some of these scientific principles are extremely relevant to understanding the inner workings of a networked society. For example, Moore's Law is the observation-cum-prediction of Intel's co-founder Gordon Moore that '*the number of transistors on a chip roughly doubles every two years*',[7] and can be expressed in the mathematical formula $n = 2^{((y - 1959) \div d)}$ (Ceruzi 2005, 585)[8] Since 1965, this principle and the things that it represents have shaped and continue to profoundly influence all aspects of the computing industry and digital culture particularly what products and services are produced and what people can or cannot do with computers and electronic devices (Ceruzzi 2005, 586; Hammond 2004; see Anderson 2012, 73, 141). Ceruzzi rightly claims, '*Moore's law plays a significant role in determining the current place of technology in society*' (2005, 586). However, it is important to point out that Moore's Law is not about physics; it is a self-fulfilling prophecy that is derived from 'the confluence and aggregation of individuals' expectations manifested in organizational and social systems which serve to self-reinforce the fulfillment of Moore's prediction' for some doubling period (Hammond 2004, citations omitted)and is '*an emergent property of the highly complex organization called the semiconductor industry*' (ibidem). This statement reveals an important aspect of Moore's Law and other scientific principles and rules – that they are also *subject to social construction*. As Jasanoff eruditely explains:

> science is *socially constructed*. According to a persuasive body of work, the "facts" that scientists present to the rest of the world are not simple reflections of nature; rather these "facts" are produced by human agency, through the institutions and processes of science, hence they invariably contain a social component. Facts, in other words, are more than merely raw observations made by scientists exploring the mysteries of nature. Observations achieve the status of "facts" only if they are produced in accordance with prior agreements about the rightness of particular theories, experimental methods, instrumental techniques, validation procedures, review processes, and the like. These agreements, in turn, are socially de-

---

7 <http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_2pg.pdf> accessed 7 September 2012;see also Ceruzzi (2005, 584).

8 n is the number of circuits, y is the current year and d is the doubling time.

> rived through continual negotiation and renegotiation among relevant bodies of scientists (Jasanoff 1991, 347; see also Polanyi 2000).

Since the construction of scientific rules and facts is undertaken by both science and non-science institutions, "what finally counts as 'science' is influenced not only by the consensus views of scientists, but also by society's views of what nature is like – views that may be conditioned in turn by deep-seated cultural biases about what nature should be like" (Jasanoff 1991, 347). Due to "the contingency and indeterminacy of knowledge, the multiplicity and non-linearity of 'causes', and the importance of the narrator's (or the scientific claims-maker's) social and cultural standpoint in presenting particular explanations as authoritative" (Jasanoff 1996, 411-412), science is without doubt a 'deeply political' and 'deeply normative' activity (Jasanoff 1996, 409, 413; see Geertz 1983, 189; Hoppe 1999). It reveals as much about us as it does the material world.

The 'constructedness' (Jasanoff 1991, 349) of science can also been seen in the history of the use of and meaning ascribed to the term 'scientific law'. The use of the term 'law' in reference to natural phenomena has been explained as '*a metaphor of divine legislation*", which "*combined the biblical ideas of God's legislating for nature with the basic idea of physical regularities and quantitative rules of operation*' (Ruby 1986, 341, 342,358 (citations omitted). Ruby argues, however, that the origins of the use of the term law (*lex*) for scientific principles is not metaphorical but is inherently connected to the use and development of another term, rule (*regula*) (Ruby 1986, 347, 350). Through the changing uses and meanings of *lex* and *regula* and their descriptive and/or prescriptive application to the actions of both man and nature throughout the centuries, law in the field of science became more commonly used to designate a more fundamental or forceful type of rule, which nevertheless pertains to some 'regularity' in nature. At its core, a scientific principle or law is about imagining '*nature as a set of intelligible, measurable, predictable* ***regularities***' (Ruby 1986, 350 (emphasis added)).

Another important characteristic of scientific principles is that they act as signs, and consist of both signifier and signified. Moore's Law is both the expression and the embodiment of the natural and social forces and occurrences that it describes. As Ruby (1986, 347) explains, "*in the case of natural phenomena it is not always possible to distinguish the use of lex for formulated principles from that for regularities in nature itself*". Thus, from a practical standpoint, natural and social phenomena are reified and can be referred to by the labels and formulations of the relevant scientific principles that they are known by. For example, rather than saying, 'the forces described by Moore's Law affected the computer industry', it can be stated simply as 'Moore's Law affected the computer industry'.

There is much that can be learned about how the world works if we take as seriously the influence of scientific rules on behavior as we do legal ones. Scientific principles are descriptive and not prescriptive rules, but, like technical codes, they too are socially constructed and have significant normative effects on society and technology, and are thus worth studying in earnest (see Jasanoff 1996, 397 'co-production of scientific and social order'). People who are aware of the descriptive 'theory of the Long Tail' (Anderson 2007, 52)[9] would *conform* their actions to this rule and build

---

[9] The Long Tail is the phenomenon where consumption and production "are increasingly shifting away from a focus on a relatively small number of hits (mainstream products and markets) at the head of the demand curve, and moving towards a huge number of niches in the tail".

businesses that answer the demands of niche markets. Scientists and engineers are obviously cognizant of the "law of gravity" and they know that they *ought* to design rockets and airplanes based on this important descriptive principle. Competition authorities know that they *must* take into account market forces and relevant economic principles before imposing prescriptive rules on a subject entity or market. These and many other examples show how descriptive rules can also give rise to or be the basis of ought actions and statements.[10] Descriptive rules as such can influence behavior and have normative effects.

Being able to incorporate scientific principles within the purview of law and technology research is important since it creates connections that bring the fields of law and science and technology ever closer together. If there is value in a sociologist of science and technology studying law-making processes (Latour 2010), there is equal merit in law and technology researchers examining scientific principles and technical codes since rules that govern the networked society can similarly be made and found in laboratories and workshops (Latour 2010; Callon 1987, 99).

### *Significance of rules*

On a theoretical level, a rules-based approach is very useful and valuable to law and technology research in a number of ways. First, it distinguishes but does not discriminate between normative and descriptive rules. While the key distinction between is and ought is maintained, the role and impact of descriptive rules on behavior and order is not disregarded but is, in fact, fully taken into account. By focusing as well on descriptive rules and regularities that are not completely subject to human direction, a rules-based framework can complement and support the more instrumentalist, cybernetic and state-centric theories and methods to law and technology (Morgan & Yeung 2007, 3-5, Black 2002, 23, 26). Rather than concentrating solely or mainly on how state actors and the law directly or indirectly regulate behavior, a rules-based approach creates an awareness that problems and issues brought about by social and technological changes are often not completely solvable through man-made, top-down solutions alone, and more organic and bottom-up approaches should also be pursued. By placing equal emphasis on descriptive rules such as technical codes and scientific principles and their normative effects, the complexity and unpredictability of reality can be better understood, and the people, things and phenomena within and beyond our control are properly considered, addressed or, in some case, left alone.

Second, conceptualizing the networked society in terms of is and ought rules makes evident the 'duality of structure' that recursively constitutes and shapes our world (Giddens 1984 25, 375). As Giddens explains,

> The constitution of agents and structures are not two independently given set of phenomena, a dualism, but represent a duality. According to the notion of duality of structure, the structural properties of social systems are both medium and outcome of the practices they recursively organized. Structure is not "external" to individuals…. Structure is not to be equated with constraint but is always both constraining and enabling. (Giddens 1984, 25)

Applying Giddens' 'theory of structuration', a networked society is thus not constituted solely by one dimension to the exclusion of another – agency versus structure, human against machine,

[10] Hume's law, which states that one cannot derive ought from is, is not applicable since the examples do not involve morality but conclusions based on experience and empirical data (see Hume (1739, Book III, Part I, Section 1)).

man versus nature, instrumentalism or technological determinism, society or technology – but it is the action-outcome of the mutual shaping of any or all of these dualities (Giddens 1984).

Finally, a rule can be a key concept for an interdisciplinary approach to understanding law, technology and society. A rule can serve as a common concept, element or interface that connects and binds different academic fields and disciplines (Therborn 2002, 863). With the increasing convergence of different technologies and various fields of human activity (both inter and intra) and the multidisciplinary perspectives demanded of research today, a unifying concept can be theoretically and methodologically useful. The study of rules (particularly norms) has received serious attention from such diverse fields as law (see Posner 2000; Sunstein 1996; Lessig 1995; Cooter 2000), sociology (Hecter 2001), economics (McAdams & Rasmusen 2007; Posner 1997), game theory (Bicchieri 2006; Axelrod 1986), and even information theory (Boella et al. 2006; Floridi 2012). The study of '*normative multiagent systems*' illustrates the interesting confluence of issues pertaining to law, technology and society under the rubric of rules (Boella et al. 2006; Savarimuthu & Cranefield 2011).

## Rules of hacking

In addition to its conceptual advantages, a rules-based approach can be readily applied to analyze real world legal and normative problems that arise from technical and social changes. There can be greater clarity in determining what issues are involved and what possible actions to take when one perceives the world as being '*normatively full*' (Griffiths 2002, 34) and replete with rules. For instance, the 'problem' of computer hacking[11] is one that legislators and other state actors have been struggling with ever since computers became widely used. Using the rules of a networked society as a framework for analysis, it becomes evident that hacking is not simply a problem to be solved but a complex, techno-social phenomenon that needs to be properly observed and understood.

### *Laws on hacking*

Early attempts to regulate hacking seemingly labored under the impression that the only rules that applied were legal rules. Thus, despite the absence of empirical data showing that hacking was an actual and serious threat to society, legislators around the world enacted computer fraud and misuse statutes that criminalized various acts of hacking, particularly unauthorized access to a computer (Hollinger 1991, 8). Some studies have shown, however, that these anti-hacking statutes have mostly been used against disloyal and disgruntled employees and only seldom in relation to anonymous outsiders who break into a company's computer system, the oft-cited bogeyman of computer abuse laws (Hollinger 1991, 9; Skibbel 2003, 918). Not all laws though are opposed to all forms of hacking. The Software Directive upholds the rights to reverse engineer and to decompile computer programs to ensure interoperability subject to certain requirements.[12] The fair use doc-

[11] To "hack" is to produce a surprising result through deceptively simple means, which belies the impressive mastery or expertise possessed by an actor who is neither bound nor excluded by the rules of the subject technology or technological system. This is a paraphrasing and refinement of Turkle definition of a hack (see Turkle 2005, 208).

[12] Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs [2009] OJ L111/416, art 5(3), 6, and 8.

trine and similar limitations to copyright provide users and developers with a bit of (but clearly not much) space and freedom to hack and innovate (see Rogers & Szamosszegi 2011).

### *Norms of hackers*

Another thing that state actors fail to consider when dealing with hacking is that computer hackers belong to a distinct culture with its own set of rules. Since the social norms and values of hackers are deeply held, the simple expedient of labeling hacking as illegal or deviant is not sufficient to deter hackers from engaging in these legally prohibited activities. In his book *Hackers*, Levy codified some of the most important norms and values that make up the hacker ethic:

- Access to computers should be unlimited and total.
- All information should be free.
- Mistrust Authority – Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better (Levy 2010, 28-34).

These norms and values lie at the very heart of hacker culture and are a source from which hackers construct their identity. Therborn (2002, 869) explains the role of norms in identity formation, "*This is not just a question of an 'internalization' of a norm, but above all a linking of our individual sense of self to the norm source. The latter then provides the meaning of our life*". While hacker norms have an obviously liberal and anti-establishment inclination, the main purposes of hacking are generally positive and socially acceptable (e.g., freedom of access, openness, freedom of expression, autonomy, equality, personal growth, and community development). It is not discounted that there are hackers who commit criminal acts and cause damage to property. However, the fear or belief that hacking is intrinsically malicious or destructive is not supported by hacker norms. In truth, many computer hackers adhere to the rule not to cause damage to property and to others (Levy 2010, 457). Among the original computer hackers in the Massachusetts Institute of Technology (MIT) and the many other types and groups of hackers, there is a '*cultural taboo against malicious behavior*' (Williams 2002, 178). Even the world famous hacker Kevin Mitnick, who has been unfairly labeled as a '*dark-side hacker*' (Hafner & Markoff 1991, 15), never hacked for financial or commercial gain (Mitnick & Siomon 2011; Hollinger 2001, 79; Coleman & Golub 2008, 266).

It is not surprising then that the outlawing and demonization of hacking inflamed rather than suppressed the activities of hackers. After his arrest in 1986, a hacker who went by the pseudonym of The Mentor wrote a hacker manifesto that was published in Phrack, a magazine for hackers, and became a rallying call for the community.[13] The so-called 'hacker crackdown' in 1990 (also known as Operation Sun Devil, where U.S. state and federal law enforcement agencies attempted to shut down rogue bulletin boards run by hackers that were allegedly "*trading in stolen long distance telephone access codes and credit card numbers*") (Hollinger 2001, 79) had the unintended effect of spurring the formation of the Electronic Frontier Foundation, an organization of digital

[13] The Mentor, "The Hacker Manifesto" <http://www.phrack.org/issues.html?issue=7&id=3> accessed 4 December 2012.

rights advocates (Sterling 1992, 12). Similarly, the suicide of a well-known hacker, Aaron Schwartz, who at the time of his death was being prosecuted by the US Justice Department for acts of hacktivism, has spurred a campaign to finally reform problematic and excessively harsh US anti-hacking statutes that have been in force for decades.[14]

It may be argued that Levy's book, which is considered by some to be the definitive account of hacker culture and its early history, was a response of the hacker community (with the assistance of a sympathetic journalist) to counteract the negative portrayal of hackers in the mass media and to set the record straight about the true meaning of hacking (Levy 2010, 456-457, 464; Sterling 1992, 57, 59; Coleman & Golub 2008, 255). Through Levy's book and most especially his distillation of the hacker ethic, hackers were able to affirm their values and establish a sense of identity and community (Williams 2002, 177-178). According to Jordan and Taylor,

> Rather than hackers learning the tenets of the hacker ethic, as seminally defined by Steven Levy, they negotiate a common understanding of the meaning of hacking of which the hacker ethic provides a ready articulation. Many see the hacker ethic as a foundation of the hacker community. (Jordan & Taylor 2008, 774-775)

To illustrate the importance of Levy's book as a statement for and about hacker culture, the well-known German hacker group Chaos Computer Club uses the hacker ethic as their own standards of behavior (with a few additions).[15]

### *Technologies of hacking*

Hackers do not only practice and live out their social norms and values, but the latter are embodied and upheld in the technologies and technical codes that hackers make and use. This is expected since hackers possess the technical means and expertise to route around, deflect or defeat the legal and extra-legal rules that challenge or undermine their norms. Sterling notes, "*Devices, laws, or systems that forbid access, and the free spread of knowledge, are provocations that any free and self-respecting hacker should relentlessly attack*" (1992, 66). The resort of hackers to technological workarounds is another reason why anti-hacking laws have not been very successful in deterring hackingactivities.

Despite the legal prohibition against different forms of hacking, there is a whole arsenal of tools and techniques that are available to hackers for breaking and making things. There is not enough space in this paper to discuss in detail all of these hacker tools, but the following are some technologies that clearly manifest and advance hacker norms. Free and open source software (FOSS) is a prime example of value-laden hacker technology (Coleman & Golub 2008, 262). FOSS is a type of software program that is covered by a license that allows users and third party developers the rights to freely run, access, redistribute, and modify the program (especially its source code).[16] FOSS such as Linux (computer operating system), Apache (web server software), MySQL

---

14 Electronic Frontier Foundation, "Computer Fraud And Abuse Act Reform" <https://www.eff.org/issues/cfaa> accessed 4 March 2013; see Olivenbaum (1996).

15 See Chaos Computer Club, "hackerethics" <http://www.ccc.de/hackerethics> accessed 7 November 2012

16 Free Software Foundation, "What is free software?" <http://www.gnu.org/philosophy/free-sw.html> accessed 5 December 2012; Open Source Initiative, "The Open Source Definition" <http://opensource.org/osd> accessed 5 December 2012.

(database software) WordPress (content management system), and Android (mobile operating system) are market leaders in their respective sectors and they exert a strong influence on the information technology industry as a whole. The freedoms or rights granted by FOSS licenses advance the ideals of free access to computers and freedom information, which arealso the first tenets of the hacker ethic. What is noteworthy about FOSS and its related licenses is that they too are a convergence of legal rules (copyright and contract law), social norms (hacker values), technical codes (software) and scientific principles (information theory) (Coleman 2009; Benkler 2006, 60). In order to grasp the full meaning and impact of FOSS on society, one mustengage with the attendant plurality of rules. Other noteworthy examples of hacking technologies that hackers use with higher socio-political purposes in mind are Pretty Good Privacy (PGP, an encryption program for secret and secure communications) (Coleman & Golub 2008, 259), BackTrack (security auditing software that includes penetration testing of computer systems), Low Orbit Ion Cannon (LOIC, network stress testing software that can also be used to perform denial-of-service attacks), and circumvention tools such as DeCSS (a computer program that can decrypt content that is protected by a technology protection measure).

Technical codes are an important consideration in the governance of a networked society since "technology is not a means to an end for hackers, it is central to their sense of self – making and using technology is how hackers individually create and how they socially make and reproduce themselves" (Coleman & Golub 2008, 271). While technical codes are not themselves norms, they can embody norms and have normative effects. As such, technical codes too are essential to understanding normativity in a networked society.

### *Science of hacking*

The norms and normative effects of hacking tend to be supported and often magnified by scientific principles and theories. Hackers, for instance, can rely on Moore's Law and the principle of 'economies of scale' (Lemley & McGowan 1998, 494) to plan for and develop technologies that are exponentially faster and cheaper, which can receive the widest distribution possible. Being cognizant of Schumpeter's 'process of creative destruction' (Schumpeter 1962) and Christensen's related 'theory of disruptive innovation' (Christensen 2006), hackers, as innovators and early adopters of technology, are in an ideal position to take advantage of these principles and create new technologies or popularize the use of technologies that can potentially challenge or upend established industries. Creative destruction is Schumpeter's theory that capitalist society is subject to an evolutionary process that "*incessantly revolutionizes the economic structure* ***from within****, incessantly destroying the old one, incessantly creating a new one*" (Schumpeter 1962, 82). Schumpeter argues that today's monopolists industries and oligopolistic actors will naturally and inevitably be destroyed and replaced as a result of competition from new technologies, new goods, new methods of production, or new forms of industrial organization (Schumpeter 1962, 82-83). The revolutionary Apple II personal computer, the widely used Linux open source operating system, the controversial BitTorrent file-sharing protocol, and the ubiquitous World Wide Web are some notable technologies developed by hackers,[17] which through the process of creative destruction profoundly changed not

[17] Steve Wozniak, Linus Torvalds, Bram Cohen, and Tim Berners-Lee, creators of the Apple II, Linux, BitTorrent and the World Wide Web, respectively, view themselves as hackers and participate in hacker culture (see Levy 2010, 249; see Himanen 2001; see Thompson 2005; see Berners-Lee 2013).

just the economic but the legal, social and technological structures of the networked society as well.

Furthermore, because of their proclivity for open standards, resources and platforms that anyone can freely use and build on, hackers can naturally benefit from principles of network theory such as network effects. According to Lemley,

> "Network effects" refers to a group of theories clustered around the question whether and to what extent standard economic theory must be altered in cases in which "the utility that a user derives from consumption of a good increases with the number of other agents consuming the good." (Lemley & McGowan 1998, 483 (citations omitted))

This means that the more people use a technology, the greater the value they receive from it and the less likely they will use another competing technology. A consequence of network effects is a

> natural tendency toward de facto standardization, which means everyone using the same system. Because of the strong positive-feedback elements, systems markets are especially prone to 'tipping,' which is the tendency of one system to pull away from its rivals in popularity once it has gained an initial edge (Lemley & McGowan 1998, 483 (citations omitted)).

Network effects and the openness of the Android open source mobile operating system may partly explain how Android became dominant in the smartphone market despite the early lead of Apple's iPhone and iOS. While Apple's iOS operating system is proprietary, closed and can only be used on Apple's own devices, developers are free to use, modify and improve the open source software components of Android, and manufacturers can use Android on their devices subject to certain limitations. The success of Android confirms a view that hackers will have no trouble agreeing with – "*open always wins… eventually*" (Downes 2009).

Creative destruction and network effects are a few of the important scientific principles and theories that influence the networked information society that hackers are able to benefit from. These principles do not merely remain in the background, quietly establishing the conditions and contexts of action, but, as cognitive statements about observed phenomena in nature and the market, they have strong normative effects in their own right and people tend to conform their behavior to these principles.

## Rules, rules everywhere

As illustrated in the case of hacking, a pluralist and rules-based approach can be very useful in describing and analyzing legal problems and normative issues brought about by new or disruptive technologies. Attempts by state and non-state actors to adapt to the changing digital environment or to change people's behaviors can derive much benefit from knowing how the world works. The workings of the networked society can be framed in infinite ways, but, as explained above, seeing these operations in relation to the presence, action and interaction of rules is extremely helpful in making sense of reality. The formation and implementation of laws must therefore take into account the social, technical and scientific rules that govern a subject area or field. This is necessary because behavior in a technology-mediated and scientifically validated world is not only shaped by laws, but equally by norms, technologies, and natural and social phenomena. These four rules, whether as norms as such or through their normative effects, determine the state and degree of normativity in a networked society.

This paper has enlarged the domain of technology law to cover not just legal rules but also extra-legal rules such as social norms, technical code, and scientific principles. The expanded scope should not be bemoaned but instead embraced as a challenge since there are now more interesting people, things and phenomena which technology lawyers and legal scholars can and ought to study. There is nothing wrong with perceiving the networked society in relation to rules. Other academic fields have no problem seeing the world through their own distinct and widely-encompassing disciplinary lenses – for anthropologists it is all about culture, evolutionary biologist focus on the gene, physicists perceive the universe in terms of matter and energy, and information theorists unabashedly see everything as bits. Technology law researchers should not hesitate to say that everything could potentially be about rules. In a world where normative and descriptive rules pervade all aspects of our lives and we have to constantly negotiate all sorts of rules, norms, codes and principles, a pluralist and rules-based approach brings law and technology study much closer to the messy reality that it seeks to understand and explain. Just look around and it is evident that the world is truly normatively complex and full of rules.

## References


Anderson, Chris (2007). The Long Tail: How Endless Choice is Creating Unlimited Demand, Random House Business Books.

Anderson, Chris (2012). *Makers: The New Industrial Revolution,* Random House Business Books.

Axelrod, Robert (1986). "An Evolutionary Approach to Norms", 80 *American Political Science Review,* 1095.

Benkler, Yochai (2006). The Wealth of Networks: How Social Production Transforms Markets and Freedom, Yale University Press.

Berman, Paul Schiff (2006). "Global Legal Pluralism", 80 *Southern California Law Review* 1155.

Berners-Lee, Tim (2013). "Aaron is dead" W3C mailing list <http://lists.w3.org/Archives/Public/www-tag/2013Jan/0017.html> accessed 4 March 2013.

Bicchieri, Cristina (2006). The Grammar of Society: The Nature and Dynamics of Social Norms, Cambridge University Press.

Black, Julia (2002). "Critical Reflections on Regulation", 27 *Australian Journal of Legal Philosophy* 1.

Boella, Guido, Leendert van der Torre and Harko Verhagen (2006). "Introduction to normative multiagent systems", 12 *Computation & Mathematical Organization Theory* 71.

Bowrey, Kathy (2005). *Law and Internet Cultures,* Cambridge University Press 2005.

Brown, Ian (2006). "The Evolution of Anti-Circumvention Law", 20 *International Review of Law, Computers & Technology* 239.

Callon, Michel (1987). "Society in the Making: The Study of Technology as a Tool for Sociological Analysis" in WE Bijker, TP Hughes and TJ Pinch (eds), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*, The MIT Press.

Castells, Manuel (2001). The Internet Galaxy: Reflections on the Internet, Business, and Society, Oxford University Press.

Cavoukian, Ann (2009). "Privacy by Design: The 7 Foundational Principles" <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf> accessed 4 March 2013.

Ceruzzi, Paul E. (2005). “Moore's Law and Technological Determinism”, 46 *Technology and Culture* 584.

Cesare, Kelly (2001). “Prosecuting Computer Virus Authors: The Need for an Adequate and Immediate International Solution”, 14 *The Transnational Lawyer* 135.

Chadwick, Andrew (2006). Internet Politics: States, Citizens, and New Communication Technologies, Oxford University Press.

Chaos Computer Club, “hackerethics” <http://www.ccc.de/hackerethics> accessed 7 November 2012.

Christensen, Clayton M. (2006). “The Ongoing Process of Building a Theory of Disruption”, 23 *The Journal of Product Innovation Management* 39.

Cohen, Julie E. (2012). Configuring the Networked Self: Law, Code, and the Play of Everyday Practice, Yale University Press.

Coleman, Gabriella (2009). “Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers”, 24 *Cultural Anthropology* 420.

Coleman, E. Gabriella and Alex Golub (2008). “Hacker Practice: Moral genres and the cultural articulation of liberalism”, 8 *Anthropological Theory* 255.

Cooter, Robert (1996). “Normative Failure Theory of Law”, 82 *Cornell Law Review* 947.

Cooter, Robert D. (2000). “Three Effects of Social Norms on Law: Expression, Deterrence, and Internalization”, 79 *Oregon Law Review* 1.

Directive 2009/24/EC of 23 April 2009 on the legal protection of computer programs [2009] OJ L111/416.

Disini, Jr., Jesus M. and Janette C (2000). Toral, Annotations on the Electronic Commerce Act and its Implementing Regulations (Philexport 2000).

Dizon, Michael Anthony C. (2011). “Laws and Networks: Legal Pluralism in Information and Communications Technology”, 15 *Journal of Internet Law* 1.

Dizon, Michael Anthony C. (2010). “Participatory democracy and information and communications technology: A legal pluralist perspective”, *European Journal of Law and Technology*, Vol. 1, Issue 3.

Doctorow, Cory (2008). “Amazon reviewers clobber Spore DRM” <http://boingboing.net/2008/09/07/amazon-reviewers-clo.html> accessed 6 December 2012.

Dohrenwend, Bruce P. (1959). “Egoism, Altruism, Anomie, and Fatalism: A Conceptual Analysis of Durkheim’s Types”, 24 *American Sociological Review* 466.

Dommering, Egbert (2006). “Regulating Technology: Code is not Law” in E Dommering and L Asscher (eds), *Coding Regulations: Essays on the Normative Role of Information Technology,* TMC Asser Press.

Downes, Larry (2009). The Laws of Disruption: Harnessing the New Forces that Govern Life and Business, Audible.

Dyson, George (2012). Turing’s Cathedral: The Origins of the Digital Universe, Random House Audio.

Electronic Frontier Foundation, “Computer Fraud And Abuse Act Reform” <https://www.eff.org/issues/cfaa> accessed 4 March 2013.

European Commission, “Communication on a comprehensive approach on personal data protection in the European Union” COM(2010) 609 final.

European Commission, “Communication on a Digital Agenda for Europe” COM(2010) 245 final/2.

Floridi, Luciano (2012). "Norms as Informational Agents and the Problem of their Design", *SCRIPT Conference: Law and Transformation*, Edinburgh, June 2012.

Free Software Foundation, "What is free software?" <http://www.gnu.org/philosophy/free-sw.html> accessed 5 December 2012.

Galligan, D.J. (2007). *Law in Modern Society,* Oxford University Press.

Geertz, Clifford (1983). Local Knowledge: Further Essays in Interpretative Anthropology, Basic Books, Inc.

Gibbs, Jack P. (1981). Norms, Deviance, and Social Control: Conceptual Matters, Elsevier.

Gibbs, Jack P. (1965). "Norms: The Problem of Definition and Classification", 70 *American Journal of Sociology* 586.

Gibbs, Jack P. (1966). "The Sociology of Law and Normative Phenomena", 31 *American Sociological Review* 315.

Giddens, Anthony (2009). *Sociology,* 6th edn, Polity Press.

Giddens, Anthony (1984). The Constitution of Society: Outline of the Theory of Structuration, Polity Press.

Griffiths, Anne (2002). "Legal Pluralism" in R Banakar and M Travers (eds), *An Introduction to Law and Social Theory*, Hart.

Griffiths, John (1986). "What is Legal Pluralism?", 24 *Journal of Legal Pluralism & Unofficial Law* 1.

Grossman, Lev (2000). "Attack of the Love Bug",*TIME* (15 May 2000).

Hafner, Katie and John Markoff (1991). Cyberpunk: Outlaws and Hackers of the Computer Frontier, Corgi Books.

Hammond, Martin L. (2004). "Moore's Law: The First 70 Years", *Semiconductor International* (1 April 2004).

Hampson, Noah C.N. (2012). "Hacktivism: A New Breed of Protest in a Networked World", 35 *Boston College International and Comparative Law Review* 511.

Hecter, Michael and Karl-Dieter Opp (eds) (2001). *Social Norms*, Russel Sage Foundation.

Hildebrant, Mireille, "A Vision of Ambient Law" in R. Brownsword and K. Yeung (eds) (2008). *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes,* Hart Publishing.

Himanen, Pekka (2001). The Hacker Ethic and the Spirit of the Information Age, Secker & Warburg.

Hollinger, Richard C. (2001). "Computer Crime" in David Luckenbill and Denis Peck (eds), *Encyclopedia of Crime and Juvenile Delinquency (Vol. II),* Taylor and Francis.

Hollinger, Richard C. (1991). "Hackers: Computer Heroes or Electronic Highwaymen", 21 *Computers & Society* 6.

Hoppe, Robert (1999). "Policy analysis, science and politics: from 'speaking truth to power' to 'making sense together'", 26 *Science and Public Policy* 201.

Howard, Philip N. and others (2011). "Opening Closed Regimes: What Was the Role of Social Media During the Arab Spring?" <http://pitpi.org/index.php/2011/09/11/opening-closed-regimes-what-was-the-role-of-social-media-during-the-arab-spring/> accessed 7 December 2012.

Hume, David (1739). *A Treatise of Human Nature*<http://www.gutenberg.org/files/4705/4705-h/4705-h.htm> accessed 7 March 2013.

Hutchinson, Lee (2012). “Ubisoft backtracks on PC DRM, citing customer feedback” Ars Technica <http://arstechnica.com/gaming/2012/09/ubisoft-backtracks-on-pc-drm-citing-customer-feedback/> accessed 6 December 2012.

Intel, “Moore’s Law” <http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_2pg.pdf> accessed 7 September 2012.

Jasanoff, Sheila (1996). “Beyond Epistemology: Relativism and Engagement in the Politics of Science”, 26 *Social Studies of Science* 393.

Jasanoff, Sheila (1991). “What Judges Should Know About the Sociology of Science”, 32 *Jurimetrics* 345.

Jordan, Tim and Paul Taylor (2008). “A sociology of hackers”, 46 *The Sociological Review* 757, 774-775.

Karagiannopoulos, Vasileios (2012). “China and the Internet: Expanding on Lessig’s Regulation Nightmares”, 9:2 *SCRIPTed* 150 <http://script-ed.org/?p=478> accessed 2 October 2012.

Latour, Bruno (2010). The Making of Law: An Ethnography of the Conseil D’Etat (Polity Press 2010).

Leenes, Ronald (2011). “Framing Techno-Regulation: An Exploration of State and Non-state Regulation by Technology”, 5 *Legisprudence* 143.

Lemley, Mark A. and David McGowan (1998). “Legal Implications of Network Economic Effects”, 86 *California Law Review* 479.

Lessig, Lawrence (2006). *Code: version 2.0,* Basic Books.

Lessig, Lawrence (1995). “Social Meaning and Social Norms”, 144 *University of Pennsylvania Law Review* 2 181.

Levy, Steven (2010). *Hackers: Heroes of the Computer Revolution*, O’Reilly Media, Inc.

Ludlow, Peter (2010). “Wikileaks and Hacktivist Culture”,*The Nation* (New York, 4 October 2010).

MacKenzie, Donald and Taylor Spears “‘The Formula That Killed Wall Street’?: The Gaussian Copula and the Material Cultures of Modelling” <http://www.sps.ed.ac.uk/__data/assets/pdf_file/0003/84243/Gaussian14.pdf> accessed 7 December 2012.

McAdams, Richard H., and Eric B. Rasmusen (2007).“Norms and the Law” in A Polinsky and S Shavell (eds), *Handbook of Law and Economics, Volume 2*, Elsevier.

McCullagh, Declan and Milana Homsi (2005). “Leave DRM Alone: A Survey of Legislative Proposals Relating to Digital Rights Management Technology and Their Problems”, *Michigan State Law Review* 317.

Merry, Sally Engle (1988). “Legal Pluralism”, 22 *Law & Society Review* 869.

Michaels, Ralf (2005). “The Re-*State*-Ment of Non-State Law: The State, Choice of Law, and the Challenge from Global Legal Pluralism”, 51 *The Wayne Law Review* 1209.

Mifsud Bonnici, Jeanne Pia (2007). *Self-Regulation in Cyberspace*, TMC Asser Press.

Mitnick, Kevin and William L. Simon (2011). Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker, Blackstone Audio.

Morgan, Bronwen and Karen Yeung (2007). *An Introduction to Law and Regulation: Text and Materials*, Cambridge University Press 2007.

Morozov, Evgeny (2011a). "Facebook and Twitter are just places revolutionaries go", *The Guardian* (7 March 2011) <http://www.guardian.co.uk/commentisfree/2011/mar/07/facebook-twitter-revolutionaries-cyber-utopians> accessed 5 March 2013.

Morozov, Evgeny (2011b). The Net Delusion: How Not to Liberate the World, Penguin Books.

Morris, Richard T. (1956). "A Typology of Norms", 21 *American Sociological Review* 610.

Murray, Andrew D. (2007). The Regulation of Cyberspace: Control in the Online Environment, Routledge-Cavendish.

Murray, Andrew and Colin Scott (2002). "Controlling the New Media: Hybrid Responses to New Forms of Power", 65 *The Modern Law Review* 491.

Olivenbaum, Joseph M. (1996). "<CTRL><ALT><DEL>: Rethinking Federal Computer Crime Legislation", 27 *Seton Hall Law Review* 574.

Open Source Initiative, "The Open Source Definition" <http://opensource.org/osd> accessed 5 December 2012.

Opp, K.D. (2001). "Norms" in N Smelser and P Baltes (eds), *International Encyclopedia of the Social & Behavioral Sciences*, Elsevier.

Pabico, Alecks P. and Yvonne T. Chua (2001). "Cyberspace has become the playground of high-tech criminals"<http://pcij.org/imag/Online/cybercrimes.html> accessed 2 October 2012.

Pertierra, Raul (2010). "The Anthropology of New Media in the Philippines", Institute of Philippine Culture 2010.

Philippine Electronic Commerce Act, adopted 14 June 2000.

Pinch, Trevor J. and Wiebe E. Bijker (1984). "The Social Construction of Facts and Artefacts: or How the Sociology of Science and the Sociology of Technology might Benefit Each Other" 14 *Social Studies of Science* 399.

Polanyi, Michael (2000). "The Republic of Science: Its Political and Economic Theory", 38 *Minerva* 1.

Posner, Eric A. (2000). *Law and Social Norms,*Harvard University Press.

Posner, Richard A. (1997). "Social Norms and the Law: An Economic Approach", 87 *AEA Papers and Proceedings* 365.

Reindenberg, Joel R. (1997). "Lex Informatica: The Formulation of Information Policy Rules Through Technology", 76 *Texas Law Review* 553.

Riesenfeld, Dana (2010). *The Rei(g)n of "Rule"*, Ontos verlag.

Rogers, Tomas and Andrew Szamosszegi (1986). "Fair use in the U.S. Economy: Economic Contribution of Industries Relying on Fair Use", Computer & Communications Industry Association.

Ruby, Jane E. (1986). "The Origins of Scientific 'Law'", 47 *Journal of the History of Ideas* 341.

Salmon, Felix (2009). "Recipe for Disaster: The Formula That Killed Wall Street", *Wired Magazine* Issue 17.03.

Savarimuthu, Bastin Tony Roy and Stephen Cranefield (2011). "Norm creation, spreading and emergence: A survey of simulation models of norms in multi-agent systems", 7 *Multiagent and Grid Systems* 21.

Schumpeter, Joseph A. (1962). "The Process of Creative Disruption" in *Capitalism, Socialism and Democracy*, Harper Torchbooks.

Skibbel, Reid (2003). "Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act", 18 *Berkeley Technology Law Review* 909.

Sprinkel, Shannon C. (2001). “Global Internet Regulation: The Residual Effects of the ‘ILOVEYOU’ Computer Virus and the Draft Convention on Cyber-Crime”, 25 *Suffolk Transnational Law Review* 491.

Stepanova, Ekaterina (2012). “The Role of Information Communication Technologies in the ‘Arab Spring’” <http://www.gwu.edu/~ieresgwu/assets/docs/ponars/pepm_159.pdf> accessed 7 December 2012.

Sterling, Bruce (1992). *The Hacker Crackdown*, Bantam Books.

Sunstein, Cass R. (1996). “Social Norms and Social Roles”, 96 *Columbia Law Review* 903.

The Mentor, “The Hacker Manifesto” <http://www.phrack.org/issues.html?issue=7&id=3> accessed 4 December 2012.

Therborn, Goran (2002). “Back to Norms! On the Scope and Dynamics of Norms and Normative Action”, 50 *Current Sociology* 863.

Thompson, Clive (2005). “The BitTorrent Effect”,*Wired Magazine* Issue 13.01.

Turkle, Sherry (2005). *The Second Self: Computers and the Human Spirit* (Twentieth anniversary edition), the MIT Press.

Van der Hof, Simone and Kees Stuurman (2006). “Code as Law” in BJ Koops and others (eds), *Starting Points for ICT Regulation: Deconstructing Prevalent Policy One-Liners*, TMC Asser Press.

Von Benda-Beckmann, Franz (2002). “Who’s Afraid of Legal Pluralism”, 47 *Journal of Legal Pluralism* 37.

Von Benda-Beckmann, Franz and Keebet von Benda-Beckmann (2006). “The Dynamics of Change and Continuity in Plural Legal Orders”, 53-54 *Journal of Legal Pluralism* 1, 14.

Williams, Sam (2002). Free As In Freedom: Richard Stallman’s Crusade for Free Software, O'Reilly.

WIPO Copyright Treaty, adopted on 20 December 1996.

World Performance and Phonograms Treaty, adopted on 20 December 1996.

# Law and standards
# Safeguarding societal interests in smart grids

R.A. Hoenkamp
University of Amsterdam
Amsterdam Centre for Energy
✉r.a.hoenkamp@uva.nl

A.J.C de Moor- van Vugt
University of Amsterdam
Amsterdam Centre for Energy
✉a.de.moor@uva.nl

G.B. Huitema
University of Groningen
Operations
✉g.b.huitema@rug.nl

**Abstract** This chapter examines the relationship between technical standards and law in light of developments in ICT technologies. As standards have grown greater in quantity and influence over the last decade, this paper analyses how standards relate to the legal system of the European Union. The chapter demonstrates the similarities between law and standards, and reviews ways in which standards are binding for users and obtain a legal effect. It is argued that the only way to ensure that sufficient attention is paid to societal interests like those of the users and EU policy aims is to design and apply procedural criteria for standardization. The paper shows that these criteria are specifically important for the imminent introduction of smart grids[1] in the electricity market of Europe, for which many new standards are currently in development.

**Keywords** Standardization, smart grids, EU law

## Introduction

Standardization in general plays a fundamental role in our society because of the impact technology has on our lives. As we will see, standardization does not merely involve technical aspects, but also political decisions and user options. Though standards are not delegated acts under EU law, the EU Commission can mandate the European Standardization Organizations (ESOs) to develop standards. Furthermore, as we will see, standards have a binding effect on the makers of the relevant product, as well as on the users of the product. In network environments such as the Internet and smart grids, current developments show that standards have developed from regulating technical form (such as the electricity voltage) to regulating user behaviour (Benoliel 2004, 1077). Once standards have been implemented, their negative effects are hard to reverse. It is therefore desirable to anticipate those effects during the standardization process, especially where they concern user interests and policy aims. The EU Commission attempts to safeguard these interests by requiring the process to be open for societal interests representatives, next to the market parties. However, these parties lack the power to influence the process substantially.

Standardization in the area of smart grids is currently one of the most important standardization processes. Because different areas such as the electricity system, telecom system and several other markets need to be integrated, standards play an exceptionally important role in smart grid

[1] Smart grids can support the transition to the use of renewable energy by applying ICT in favor of information management on energy supply and use.

developments. Networking technologies will support the physical electricity system to balance renewable intermittent energy sources on the network. Smart grids encompass different layers: a component layer, a communication layer, an information layer, a function layer and a business layer and they all need to be interoperable.[2] Therefore, standardization is a key element in developing smart grids. Because of this important role of standards in smart grids, safeguarding user interests and policy aims as well as the commercial interests of the parties involved in standardization, is crucial. The role technology currently plays in combination with the legal requirements from energy directives[3], introduces the question whether there is a need to develop legal rules for the standardization process. The European Commission mandated the European ESOs to develop smart grids' technical and ICT standards to achieve interoperability between various components and to facilitate smart grid services.[4] However, the Commission Mandate holds few safeguards to ensure policy aims are met through standardization.

In this paper we investigate whether there is a need, from a legal perspective, to provide more procedural safeguards than is currently the case in smart grid standardization. We approach this issue by viewing four different relationships between standards vis-á-vis legal rules.

First, we describe the developments of ICT, the characteristics of standards and how these exist *independent* from the traditional legal system, against the background of the theory of 'code is law' (Lessig 2006). It will become clear that standards are not law as such, but can be equally binding in effect. Subsequently, we examine cases that are comparable to standards, yet contrary to standards, are established legal concepts. We discuss whether there are *similarities* between standards and those existing legal concepts, by analysing how they comply with public and/or private law. The concepts of self-regulation and declaration of universal applicability seem to be the most parallel to that of standards, when it comes to their genesis and binding force. It becomes apparent that these concepts comply with either public- or private law principles, while standards comply with neither. In the third part we will explore which safeguards do exist. We view how EU law *influences and restricts* standardization demonstrating the present legal framework for standardization. Finally, we describe how the traditional legal system *reinforces* the power of standardization by incorporating standards in the legal system. By or exploration on these different relations we intend to clarify the position of standards in the current legal system.

We will see that our analysis leads to the conclusion that standards are binding but do not yet have a well-defined place in the legal system. Hence, there is a need for additional regulatory safeguards for the standardization process. Because of the important role of standards in smart grid developments future research is necessary to examine how these safeguards can be achieved.

---

2 CEN/CENELEC and ETSI Smart Grids Coordination Group.

3 Requiring for example, reliability, affordability and the transition to renewable energy.

4 Standardization Mandate to European Standardisation Organisations (ESOs) to support European Smart Grid deployment, Brussels 1st March 2011, M/490 retrieved from http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/2011_03_01_mandate_m490_en.pdf.

## Standards vis-á-vis the law in the information society

Standards have come to play an increasingly important role in society, especially in the last decades. However, legal systems were developed in a time where none of the technology that plays a crucial role in our lives today existed. Standards were for the most part regarded as a voluntary agreement between companies that only affects the companies using those particular standards. However, as we will see, standards bind the users of the standardized products as well. Standards can actually have such a powerful binding force that they become akin to laws. In this section we will study the similarities between standards and law, and their consequences.
Directive 98/34/EC defines a standard in the following way:

> "A technical specification approved by a recognized body for repeated or continuous use, with which compliance is not compulsory."[5]

We use the term standards in this paper in a broader sense, including also de facto standards. A standard is a technical specification that is used to provide interoperability in repeated use. It expresses technical uniformity (Burk 2005, 551).

In general, laws are orders that bind citizens of a jurisdiction. From a legal positivist perspective there are four requirements for orders to be regarded as *law,* according to Hart.[6] They are first of all either a command that is backed by a threat of sanction, a condition for an entitlement to something, a creation of legal relations or a specification of legal powers. Furthermore, these rules acquire their status of law because they are recognised as such by a legal system. Moreover the rules have to be ordered by some form of sovereign. Finally, the rules are written and accessible for the individuals they concern.

Next to these four general conditions there is are two distinct ways in which citizens can be bound through law, namely through public or private law.

Public law defines and controls the power of governments over the people (Bell 2002). These controls are relevant at the legislative level, as well as the executive and administrative levels. Public law is aimed at the well being of its subjects, which in EU law is expressed in art 2 of the Treaty of Lisbon. Its implementation occurs within a framework and limitations of competence on the relevant authority (art. 3b Treaty of Lisbon.) An important characteristic of public law is that citizens do not have to consent to the rule in order for it to become binding, the hypothesis being that the consent is incorporated in the democratic process of rule making. Next to legal rules, governments can also raise restrictions for people by carrying out tangible acts. For example when a municipality closes down a street. When the person affected by that act has a relevant interest, because for instance it prevents him from entering his house, he can object to that decision.

If a law on itself does not bind citizens, they can be bound through the effect of private law. Private law creates legal relations. It is law characterized by the fact that citizens can only be restricted in their actions or bound by obligations towards each other through mutual consent. The parties involved will have to agree to a restriction or obligation through the offer and acceptance of

---

5 Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998, Laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on Information Society services; (OJ L 204, 21.7.1998, 37).

6 This description is in line with Hart (1961).

a contract.[7] Thus, the principle of freedom to contract is leading and therefore contracts are voluntary (von Bar 2009, 212).

At first glance standards show many similarities to law, yet as we will see, some crucial aspects are different. Standards are difficult to categorize in either the legal framework of public- or private law, when it comes to the relation between the users of a standard and a standardized product. The user of the standardized product never agreed with the standard, yet he is bound by it. They are not bound in law by the standard and its possibilities and restrictions, yet they are bound in fact. Once a standard is generally accepted, it is virtually impossible to circumvent it. The use of standards has markedly increased since the introduction of the Internet and they play an exceedingly large role in networked environments, such as smart grids.

We will review the introduction of the use of the Internet, to understand the relationship between standards and laws today. The example of the Internet offers a suitable example to do so, because it has caused important changes, both socially and legally, in the last decades.

Originally, the Internet was perceived as something that governments could not and should not regulate. Pioneers saw it as a phenomenon where companies and individuals could enjoy total freedom from any government interference. They felt that the Internet or 'Cyberspace' should just evolve by itself without any interference or supervision from the outside. This view is also called the cyber-libertarian perspective (Winner 1997). The exceptionalist approach, on the contrary, assumed that a new set of rules was needed to regulate cyberspace. The *unexceptionalist* approach held that existing rules were sufficient for cyberspace (Shiff Berman 2007, 14). In that sense the law concerning the Internet is not a separate regulatory domain. More recently, scholars have suggested that there ought to be hybrid solutions with new interfaces between government regulation and self-regulation of the Internet (Farrel 2002). This debate about whether and who should regulate the Internet gives rise to the question whether there should be an international legal body to govern the Internet (Tauberman 2009).

Irrespective of the question of who is best placed to regulate the Internet, several organizations have coordinated aspects of the Internet from an early stage. The Internet Society (ISOC), a non-profit organization encompasses several organizations, such as for example the Internet Engineering Task Force (IETF), which sets most of the international Internet Protocol (IP) standards. The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization established by California law. It manages all domain names and the top-level domains such as .com, .org, .eu, .fr etc. and allocates the domains of browser URL's. These organizations have in common that they are non-profit organizations that decide upon general rules and policies that apply to the Internet worldwide. They are, however, not legal authorities of the international legal system. In response to these US centred organization the World Summit on the Information Society (WSIS) brought up the discussion of more global governance for the Internet wit state and non-state actors (Mueller 2010, 55-80).

On a national level the Internet Service Providers (ISPs) are an entity that regulates the use of the Internet. The contract with the ISP allows the customer access with the help of a modem. The contracts explain the rights and obligations of parties, and the exclusions of accountability for

[7] E.g. article 2:205 Principles of European contract law part I, II and III 2002.

web content. Some ISP contracts contain terms that directly influence the way the customer uses the Internet.

Furthermore, people, companies and other organizations automatically set restrictions by determining the capabilities of their websites. There are of course no restrictions when these websites merely provide information. However when they offer an online service, such as social media, they will inherently create certain barriers for their users.

The architecture of the Internet and its content determines the activities of users as well as the limitations thereof. Thus, the architecture can be seen as a form of law of the Internet, because users are automatically bound by its possibilities, impossibilities and restrictions. This perspective differs from that of the cyber libertarian and exceptionalist perspectives and it can be placed against the background of the discussion that started 15 years ago with Joel Reidenberg's theory of 'Lex Informatica' (Reidenberg 1998). Lawrence Lessig built upon this theory by introducing the concept of 'Code is Law', strengthening the debate on the role of the Internet in society. The debate leaves open many questions on how to deal with the development of the Internet today (Lessig 2006). We will review this theory and debate, while applying it to standards specifically. The debate stems from a U.S. context, yet the aspect of how codes bind users is applicable for the EU system as well.

Obvious examples that illustrate how code functions as the 'law' of the Internet is the use of IP addresses for access to the Internet and the use of cookies on websites to recognize recurring visitors.

Code restrictions can also come through algorithms designed by specific websites. YouTube, for instance, enforces copyright law by removing certain videos from their website when the content is assumed to infringe on a copyright. This IP content management tool however is less sophisticated than the law on copyright itself. This became clear in the case where Michelle Obama's speech during the Democratic National Convention (DNC) was embedded in the DNC's website through a YouTube video. The video was blocked for a couple of hours after it was placed on the website because of assumed copyright infringements. However, the DNC website owned the video itself and therefore broadcasting it on its own website did not actually infringe on the copyright. Even though media companies have a great advantage in this tool, it restricts users and in this case, the contributor as well.

The impact that technology has on society creates restrictions and threats for users. The level of interference these 'rules' have on individual Internet users can occur in varying degrees. Obviously not all codes are standards, nor are all standards codes. However a great part of the code of the Internet is standardized. Moreover, what code does for the user is exactly the same as what standards, be it technical – or ICT – standards, do for the users of a standardized product. It determines their possibilities for Internet usage. Standards do this even more so, as the option to use a different provider of the product or service in most cases will either not exist or be hard to find. The DVD standard, for example, determines that its recording provides the possibility to only be able to be played on one continent and not the other (Leenes 2011). It also determines the amount of times a video can be played until its quality deteriorates (Burk 2005, 541).In a similar way, smart grids standards can cause restrictions for users. The code in the standard can for example decide how often certain information about electricity usage will be sent to an external party. A technical standard can also include a feature to shut-off household solar production when the frequency on the network comes within a certain spectrum. Whether an electricity meter of an electric car is

standardized to be in the car or at the charging station can have many consequences. Numerous other decisions will have to be made in the standardization process of smart grids, that in the theory of code is law, will have a great regulating impact on users.

Undoubtedly several arguments contradict the theory that code is law. One argument is that, as a general rule, people can make their own choices regarding hardware and software and therefore they are free from restrictions (Post 2000, 1453). As mentioned earlier, when a person buys a product, he accepts its constraints, including the underlying standard. In cyberspace people can, for example, still easily choose whether they use the prominent Facebook as a social network, or another, perhaps more nationally oriented website to contact their friends online. Nevertheless, if people really have this kind of 'choice' in smart grids, it would mean that users of smart grids could easily go around a standard. Yet, this is not the case as once the smart grid standard is introduced, and accepted, all products will most likely comply with it. Therefore choice becomes virtually non-existent in smart grids. Standards thus become generally binding without real, deliberate consent from users, as opposed to a voluntary contract.

The approach of analysing whether code is (a substitute of) law can take many different forms. Some authors use Fuller (Asscher 2006), others look at code from the perspective of legitimacy (Koops & Leenes 2005). We take a legal positivist perspective. Not to analyse code in general, but to analyse standards more specifically. Hart's four requirements mentioned above, suit this approach. In essence, standards form *a condition for an entitlement to something*. The entitlement is the use of the standardized product feature, and the condition is set by the developer of the standard. The second requirement is obviously not met as standards are not recognised as law by a legal system. The third criterion is not completely met. When a 'sovereign' is as Hart formulates it:

> "a person or body of persons whose orders the great majority of society habitually obey and who does not habitually obey any other person or persons." (Hart 1961)

In the case of the Internet this requirement would not be met as there is not one 'legislator' of the internet (Shah & Kesan 2004, 281). However the *body of persons* does apply to smart grid standards in the case of the Commission Mandate. This mandate clearly states that CEN/CENELEC and ETSI are the standard bodies. Finally, standards are written, yet not accessible by the individuals governed by the standards. The users of the Internet have no idea what standards they are complying with. Standards are a way of social shaping, which does not allow for the option of not obeying (Latour 1992). When the regulatory force comes from the environment or architecture, as is the case with standards, it is even harder to recognize that one is being regulated (Schiff Berman 2000).

Even though some requirements of law are met, even more so than Internet code, in a strict sense, standards are undoubtedly not law. So what are they? The division of public and private law sheds some light on the issue. When looking from the point of view of the standard setters, standards belong to the area of private law. By setting a standard, the involved parties at least invoke expectation that they will comply with it. They do this voluntarily. When observing the effect on the parties that are not part of the process, there is a distinction between the product developer of a relevant product in the first place, and the user of the standardized product. Once a standard becomes widely accepted, the product developer will not be able to circumvent the standard if he wants to have access to the networked market. The user of the standardized product will be bound to the restrictions and possibilities of the standard, as well to make use of the product. Neither of

them consented to the requirements of the standard, so for them the standards do not fall within the framework of private law.

In the end, it is clear that standards are not law. The problem is however, that they have a similar effect as laws. The fact that we have to do what a standard determines does furthermore not follow from a private contract. Standards thus sit awkwardly in the division of public and private law. If the standard of an information system is to be based on public law, it must be done through democratically legitimized rules. If it were a civil law information system, there would have to be an explicit consent (Franken 2004, 28). Neither is the case. As legal systems are always changing, it might be time that the regulating nature of technology is recognized today, to adequately handle its consequences.

## Comparing standardization to existing legal concepts

Since standards do not comply with the requirements that typically apply to legal rules, there could be grounds for governments to intervene (Asscher 2006, 88). In order to understand whether this is the case, we will compare standards with certain concepts recognized in legal research, which are also not clearly a public or private law, yet have binding force. The legal system adjusted to these concepts, and it could be the same for standards. These concepts are self-regulation and the concept of declarations of universal applicability of contracts. We will examine to what extent standards are similar as these concepts and whether they fall within the public or private framework. This comparison helps us to develop a deeper understanding of the position of standards and what is needed for standards to be in line with either public or private law.

The main reasons for choosing these two concepts for a comparison is, first of all, that they have binding effect but have no conventional status in either public or private law. Another important similarity to standards is the fact that these concepts were introduced in order to involve private parties in rulemaking. The reason that ESOs set standards, and not the EU Commission, is that the ESOs can bring together the relevant expertise necessary to set a technical standard. With self-regulation and declaration of universal applicability of contracts, governments likewise do not simply impose rules, but instead let private decide what rules suit best.

In this section we utilize the principles of the western public law systems of public and private law to examine standards. Regarding public law we use the two principles for EU law that where mentioned in the previous section. We first study whether those rules work in favour of the public good. Furthermore we examine whether there is a legal competence to set the rule. If they do not meet the principles of public law, we assess whether the principle of the voluntary nature of contracts applies.

Many researchers assume that standardization is a mode of self-regulation (Weiser 2001, 822); however, this is not necessarily the case. We will give three descriptions of self-regulation so as to analyse whether standard setting is actually a form of self-regulation:

1. “Non-governmental rules that are determined in cooperation or without cooperation with others by those for whom the rules are intended respectively their representatives, and whereas the supervision of compliance is executed by these groups.” (van Driel 1989, 2)
2. “[T]he disciplining of one’s own conduct by oneself, regulation tailored to the circumstances of particular firms, and regulation by a collective group of the conduct of its members or others.” (Black 1996, 26)

3. "(a) a type of regulation; (b) a set of rules voluntary developed and accepted by those who are taking part in an activity; and (c) a rule-making process followed to develop and apply the set of norms." (Mifsud Bonnici2007, 7)

Although it does not immediately follow from the definitions, self-regulation often has the aim of achieving some public interest. Self-regulation is in many ways also encouraged by states to achieve a public objective (Mifsud Bonnici2007, 33), for instance in the case of complying with self-regulatory waste dumping provisions. Therefore, the first requirement of public law is met. There does not, however, have to be a legal basis for self-regulation. Thus self-regulation is not within the public law framework. The voluntary nature of contracts of private law, however, does apply. Only when a company wants to be bound by the regulation it will be bound. Thus, without consent to a self-regulatory rule, the rule does not apply.

Standards are different. They are not necessarily set to achieve a public interest, although as we will see later on, this can be the case. Similar to self-regulation, there is no legal basis for the authority to set the rule. Most importantly, self-regulation is valid only to the extent that it binds the parties actually involved in the standardization process. However, standards can also tie in the previously mentioned producer and user of standardized products. In those cases the ones that need to comply with the standard practically, had no role in setting the standard.

An alternative situation where a binding force for third parties is created is where contracts between two parties obtain effect on a third party. A common example is Declarations of Universal Application (DUA)of contracts. Contracts will in these cases obtain universal effect for certain groups who were not a contracting party.In this case, contrary to self-regulation, the decisions dobind parties that were not part of the process of designing the rule. An example is the Dutch situation in which the Minster of Employment and Social Affairs assigns the status of DUA to sections of collective working agreements.The motivation for introducing such provisions was to stimulate cooperation between employers and employees.[8]The precondition for such a decision is that the provision does not conflict with any general interests or the legitimate interest of a third party. The affected parties can request dispensation from the decision. Similar practices can be found in other areas, such as the general applicability of waste disposal fees.

First of all, before the decision to issue a DUA, the contracts are obviously part of the private law system, as DUAs clearly concern underlying contracts that before universal application are voluntary. When the minister makes the declaration of universal application the position shifts to public law. The DUA is in favour as of public good, in this case stimulating the cooperation between employers and employee. Moreover the safeguard of relevant competence (the Minister), and its boundaries (not conflicting with general or third party interest) come into effect. With that, the fundamental principles of public law are met. Moreover, many safeguards come into force. When someone requests dispensation and it is refused, this can for example be objected to through an administrative appeal. Legal certainty is also covered as these provisions are announced in the Official Journal and/or recorded in a registry (Dresden 2004, 153). The conditions under which a DUA can be issued are codified in relevant legislation, providing for instance that a committee is heard about the decision (Dresden 2004, 49).

[8] *Kamerstukken II* 1936/1937 274 §1.

The previous comparisons first of all show that standards are a concept different from these already existing legal concepts. It is exactly from these differences that we can learn something. Self-regulation shows similarities with public law, but in the end has private law as a frame because of its voluntary nature. The DUA case is a private law concept when it only concerns the parties involved. Yet when others become bound by it, the principles, plus many more safeguards of public law come into force. This way, standards are very similar to DUAs. They start of as a private agreement between companies, but when they become a de facto standard, everyone is bound to them. Unfortunately, in the case of smart grid standards, the European Commission gives the ESOs the freedom to develop the standards, with very little safeguards of public law. It is noticeably unnecessary for standards to be completely in line with public law in the sense that they only serve a public good and that the authority setting it has the relevant authority. Yet, observing the effect the standards can have on users we established in the previous section, especially the requirements of process of DUA can be relevant for standards. That would mean that the Commission would first of all have to provide a framework to which standards have to comply up front, and secondly ensure that a standard does not conflict with any general interest or the relevant interest of a third party. This in general is not the case is standardization.

There exist some exceptions, where the compliance with policy is crucial. In these cases governments in fact do set a framework for standardization up front. This was for example the case in the US CALEA, where a legislative act ensured that standards complied with requirements that preserved the ability of law enforcement in the changes in technology (Koops & Leenes 2005, 141). A similar system supports the current Dutch standardization of smart meters, in which an Order in Council sets elaborate legal requirements to which all smart meter standards need to comply (Hoenkamp et al. 2011, 279). Moreover, at EU level, New Approach standards enjoy a clear context, which is set in a directive through essential requirements to which the relevant standards need to comply. Unfortunately, in the case of smart grids no such system exists.

## The influence of the EU legal framework on standards

The previous section has shown that some desirable elements for decisions that are generally binding are lacking. In this section we study what the existing EU regulatory framework for the standardization process does entail. The examination of the current legal framework for standardization will show how the EU influences and restricts standardization processes at this moment, and to what extend it provides a frame that public law requires. We will start with a general approach on what restrictions competition law creates for standardization, and subsequently elaborate on specific regulation regarding standardization. This will provide an overview of relevant law, and clarify to what extent standards are influenced by EU law.[9]

Different types of standards exist. Regulatory standards are a policy means, which on a EU level are used in the *New Approach* to standardization. In that case a European Standardization Organization (ESO) creates standards based on certain policy objectives such as safety or quality, which are translated into essential requirements that are laid down in a directive. Other standards

[9] To note, it could be argued that copyright law is also part of the laws regulating standards. However, copyright law in the light of standardization only deals ex- ante with the question whether a standard should be released, or whether some technology should be standardized. E.g. Van Rooijen (2010, 48). As in this section we focus on the process of standardization itself, dealing with copyright is irrelevant.

can be developed within ESOs, sometimes initiated by a Commission mandate. Further, industry standards are developed within for a and consortia on the sole initiative of market parties. Finally, standards can be developed when certain technical requirements are adopted as de facto standards without a previous standardization process.

All types of standards can conflict with competition law in certain circumstances. Articles 101 and 102 of the Treaty of the Functioning of the European Union (TFEU) pursue the aim of effective competition on the market (Wijckmans& Tuytschaever 2011, 8). Article 101(1) prohibits agreements that could disrupt free competition in the internal market. As most standards promote technical and economic progress they are exempted from the provision through art. 101(3).

Article 101(1) TFEU concerning horizontal co-operation agreements states that agreements aiming at restricting the internal market are prohibited. In relation to this article the Guidelines on the applicability of art. 101 state as the primary objective of a standard the definition of quality or technical requirements.[10]

There are three main types of situations that can give rise to restrictive effects on competition. First, there is the situation where companies engage in anti-competitive discussion in the standardization process, reducing or eliminating price competition. Second, when standards oblige parties to exclusively use the particular standard it limits competition, especially when certain parties are unjustifiably excluded from the process. Third, when companies are restricted from obtaining effective access to the result of the standardization process. This in particular leads to anti-competitive results when certain parties enjoy intellectual property rights to components that are essential for the standard as it might result in the gain of market share. Such practices are also referred to as patent ambush (Staniszewski 2007, 670). The company will in that case only reveal the patent after the standard has gained popular recognition, thus locking in its competitors. This practice can even constitute an abuse of their dominant position when those property rights are highly restrictive. Whether it constitutes an infringement however, needs to be evaluated on a case-by-case basis.[11]

To understand how this provision is applied to standardization in practice, we will study cases brought before the Commission that concern the infringement in competition through standardization. The following cases illustrate the scope of competition law regarding standardization, beginning with the older cases and ending with more recent ones.[12]

The first time the European Commission had to decide on a matter of standards was the X/Open Group case. The question at hand was whether the agreement between market parties establishing a common application environment for UNIX software restricted competition in the light of art. 101(1).[13] The restrictions on participation to the process posed a threat to competition. However, this disadvantage was easily outweighed by the advantages for economic growth through the

---

10 Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ 2011 C11, article 257.

11 Guidelines on the applicability of Article 101 of the Treaty on the Functioning of the European Union to horizontal co-operation agreements, OJ 2011 C11, arts 264-269.

12 We will refer to the articles of the current TFEU, which means that art. 81 and 82 (old) will be referred to as 101 and 102 TFEU in order to make the reference more comprehensible.

13 X/Open Group, Decision 1987/69, OJ 1987 L 35.

wider availability of software and greater flexibility for software from different sources as in art. 101 (3).

In the IMS Health case[14], NDC Health presented a claim before the Commission regarding the fact that IMS Health refused to give NDC Health a license for the use of structure for the regional sale in the pharmaceutical industry (called the 1860 brick structure). Next to that, the Landgericht Frankfurt posed a prejudicial question concerning the breach of competition to the ECJ on this case. The structure had obtained the status of the facto standard and was necessary for NDC to compete in the market. The Commission ruled that IMS Health was guilty of abuse of dominant market power as in art. 102.[15] The ECJ explained that in certain cases, if the entity requesting the license will provide a new product for which consumers potentially have a demand, the licence needs to be granted.

The notorious Microsoft case dealt with an infringement of art. 102. Microsoft refused to make essential standards for their server operating system available to competing Sun Microsystems, and therefore interoperability with new technology was impossible. Thus applications from other companies could not be added, and users were bound to applications owned by Microsoft. The Commission ruled that this was an abuse of dominant market power by Microsoft. Refusing transparency of their standards restrained innovation by other companies in the network operating system market. Their dominant position in the relevant market was established by their market share in PC operating systems of more than 90% in that time. The Commission decided that Microsoft should make the standards at issue available under reasonable and non-discriminatory (RAND) conditions to companies active in the network operating system market.[16] After Microsoft did not comply with the Commissions' requirements, Microsoft was fined 899 million Euro.[17]

Another case is related to the abuse of dominant market position through intentional deceptive conduct during the standardization process through not disclosing patents.[18] In the case of Rambus Inc., the company did not disclose the existence of patents that were relevant for the standards until after the standard was adopted. This is a form of patent ambush as mentioned earlier. In the preliminary ruling the Commission concluded that certain practices might constitute an abuse of dominant position under art. 102. In this case the fact that Rambus engaged in intentional deceptive conduct in the context of the standard-setting process and subsequently claimed unreasonable royalties for the use of their patent, constituted an abuse of dominant market position.[19] In response Rambus Inc. lowered their royalty rates and committed themselves to a maximum rate for future royalty rates in order to provide new entrants to the market a clear perspective of costs. Due to these commitments there were no further grounds for the commission to pursue their action.

---

14 IMS Health v NDC Health 2002/165 OJ 2002 L 59.

15 NDC Health v IMS Health Commission Decision 2001/165 OJ 2001 L 59

16 Microsoft v Commission, Decision 2007/53, OJ 2007 L 32.

17 European Commission Decision 2009/ C 166/ 08,OJ 2009 C 166.

18 European Commission decision 2010/C 30/09, OJ 2010 C 30.

19 Status of Objections 23 August 2007, MEMO/07/330.

Finally, the case of EMC concerned a complaint of EMC Development, a cement producing company, arguing that the EN-197-1 standard for cement favoured Portland Cement, and excluded alternative products from the market. They moreover claimed that they did not have sufficient access to the standardization process and that the cooperation between CEN and Cemburo, the European Cement Association led to an illegal horizontal cooperation. The Commission ruled that the possibility of participation is provided at national level, through the possibility of being involved in the national standardization process, and there was national representation in the EU process. There were therefore no restrictions for EMC to participate.[20]

| Case | Infringement of competition | Infringement through the standardization process |
|---|---|---|
| X/Open Group | No | No |
| IMS Health | Yes | No |
| Microsoft case | Yes | No |
| Rambus Inc. | Yes | Yes |
| EMC case | No | No |

These cases show that infringements on competition will not be assumed very often based on faults in the standardization process. It is hard to prove that the during the process there was anti-competitive discussions as the process is closed and parties will never do this explicitly, and cover it up. Only in the extreme case of patent ambush can the process give rise to a breach of competition law.

Furthermore, the free movement of goods invokes on standardization specific restrictions as well. The case of Cassis de Dijon provides a well-known example.[21] In this case a national standard restricted free movement of goods. To avoid such incident in which national standards restricted cross-border trade because of the difference between standards in member states, the Council introduced the New Approach to standardization.[22] Through this approach harmonized standards concerning quality and safety requirements are developed on a European level, facilitating the completion of the internal market. The ESOs are then mandated by the Commission to transpose certain safety or quality levels set by a directive into technical standards. These standards are published in the Official Journal of the EU, and become a European Standard (EN), requiring member states to adopt it as a national standard. The Information Directive regulates how member states

20 Case C-367/10P in appeal to Case T-432/05, EMC Development AB v European Commission.

21 ECJ C12/78 Rewe-Zentral AG v Bundesmonopolverwaltung für Branntwein.

22 Council Resolution 85/C136/01 on a new approach to technical harmonization and standards. New Approach, OJ 1985 C 136.

have to deal with these standards.[23] First of all, the Information Directive determines that National Standardization Bodies (NSB) may not develop any national competing standard. Market parties can develop other standards alongside a New Approach standard, but they will have to prove that they comply with technical requirements of the Directive. This rarely happens in practice, as this takes intensive testing. Collecting evidence that such a deviating standard fulfils the EU requirements is a long and cumbersome activity. If companies do not comply with the New Approach directive, the national authority will authorise to sanction them on the basis of the New Legislative Framework, Regulation EC 765/2008 article 41. Member states are obliged to enforce penalties that are effective, proportionate and dissuasive in case of infringements.[24] This system provides an important instrument to ensure that certain EU policy requirements are achieved through standardization.

Regardless the New Approach, member states cannot apply technical restrictions without informing the Commission. The Securitel case[25], in which a Belgian standard concerning security systems discriminated against the security systems of CIA Security International, illustrates this. As the Belgian government had not informed the Commission of the National Standard –which was not unusual at the time – other member states had not been able to contest the standard, and the standard was declared void. This way, member states have an obligation to communicate all technical regulation to the Commission, currently on the ground of art. 8 of the Information Directive. The New Approach and Legislative Framework in general emphasize the relationship between the directives, standards, and what the obligations of national authorities are.

The General Guidelines of Cooperation for the ESOs form another relevant document for standardization.[26] These guidelines provide a frame for standardization. The document is not legally binding.[27] It refers to principles of consensus, openness and transparency. There are no definitions for the principles in the document. The principles are based on the WTO principles that are found in the Agreement on Technical Barriers to Trade (TBT), which is necessary for the standards to be accepted on an international level.

The WTO principles are not legally binding.[28] It goes beyond the scope of this article to explain the WTO rules on standardization, as we focus on EU law. However, as the ESOs have signed the TBT agreement, these principles have an influence on European standardization. The meaning of the principles is not explained as such in the agreement. According to ISO/IEC guide

---

23 Directive 98/34/EC laying down a procedure for the provision of information in the field of technical standards and regulations, OJ 1998 L 204.

24 Regulation EC 765/2008: Commission Decision on a common framework for the marketing of products, OJ 2008L 218.

25 ECJ C-194/94, CIA Security International SA v. Signalson SA and Securitel Sprl.

26 Such as transparency, access and efficiency. General Guidelines for the Cooperation between CEN, CENELEC and ETSI and the European Commission and the European Free Trade Association, 28 March 2003, OJ 2003 C 91.

27 Commission staff working document, “The challenges for European standardization”, p. 7 retrieved from http://ec.europa.eu/enterprise/policies/european-standards/files/standards_policy/role_of_standardisation/doc/staff_working_document_en.pdf

28 Vademecum on European Standardization Part IV, European standardisation in the International context (Internal EC Working Document) retrieved from http://ec.europa.eu/enterprise/policies/european-standards/documents/vademecum/

2:2004 1.7 consensus is a “general agreement, characterized by the absence of sustained opposition to substantial issues by any important part of the concerned interests and by a process that involves seeking to take into account the views of all parties concerned and to reconcile any conflicting arguments”. Openness in relation to standards is a term that is highly ambiguous, and no useful definition exists (West 2007). Furthermore, the Code of Good Practice, under annex 3 sub L of the TBT sets out a procedure in which the WTO must be notified of draft standards that must be made available to the public upon request, giving meaning to the principle of transparency.

A final EU influence on standardization regards the new regulation of standardization.[29] In the EUROPE 2020 strategy for smart, sustainable and inclusive growth states that the standardization process is one of the key subjects that that need policy changes in order to boost innovation.[30] In response the Commission submitted a proposal for regulation of European standardization that amends the aforementioned existing directives concerning standards.[31]

The regulation addresses three major problems of the current European standardization process. To start, the de jure European standardization process takes far too long. Consequently, conflicting standards are set by non-ESOs that create technical barriers to trade. Furthermore, several stakeholders are underrepresented in the process. This, according to the proposal, is mainly a problem for SMEs, as they do not have the means to fully participate in the process. Moreover, societal stakeholders are unable to have their interests incorporated in the standardization process as their technical knowledge and financial means are insufficient to contribute to the process. Finally, instead of official ESOs, for a and consortia are the main producers of ICT standards. This is caused by the lack of expertise and slow pace of ESOs. As it is typically only allowed to refer to official ESO standards in public procurement, authorities refrain from referring to fora and consortia. This results in a lack of cross-border interoperability standards coming from different organizations.

The regulation on European standardization attempts several actions to solve these problems. The most important improvement is that ICT-standards from non-ESOs can be permitted in public procurement processes, provided that they comply with the WTO principles of openness, transparency and consensus for international standardization processes. This is a big step away from the non-binding reference, which stemmed from the WTO principles of the General Guidelines of Cooperation mentioned earlier. Next to that the proposal requires that National Standardization Bodies establish annual work programs containing new and prospective standards, which should be made publicly available online. It also requires ESOs to ensure appropriate representation of societal stakeholders. This includes the involvement in certain stages of and financial support for SMEs and societal stakeholders. Unfortunately, these societal stakeholders, as we will see in a following section, do not have the means or expertise to effectively protect those societal interests.

---

29 Regulation No 1025/2012 on European standardization OJ 2012 L316

30 Communication from the Commission: EUROPE 2020, A strategy for smart, sustainable and inclusive growth, COM(2010)311.

31 Proposal for a regulation on European standardization COM(2011)0315

In line with the new regulation, CEN/CENELEC introduced a new guide on membership criteria. It is a reference document based on 'a voluntary approach of self-imposed requirements'.[32] The guides are informative documents that are not legally binding. They address more specifically the involvement of societal stakeholders. The regulation is only just implemented, so it is impossible to determine what the effects exactly will be on standardization.

All in all, EU law only minimally affects the European standardization process. Competition law provides some crucial safeguards against unfair practices such as patent ambush. Regrettably, patent ambush is the only case in which breach of competition is clear enough to have an effect on the standardization process. Apart from that, standardization specific rules provide some minimal restrictions that mainly affect New Approach standards. As smart grid standards are not based on the New Approach, yet merely on a mandate, there exists little framework for standardization work. The Commission merely created a mandate, which, to a certain extent, functions as a contract to the ESOs. However, the mandate only sets certain requirements for deadlines and some aspects of privacy and security. The relevant policy for smart grids as of for example the reduction of $CO_2$ emissions only recurs in the 'background' and therefore has no legally binding force whatsoever. The new regulation can have a positive influence on the standardization process in the sense that it puts more focus on inclusion of stakeholders and transparency. Unfortunately it does not provide more support to take relevant policy, ad the policy on smart grids into account. Therefore the current EU framework does not provide relevant safeguards to comply with principles of public law. Standards are not set in the public interest and there are no set rules for competence for the ESOs. There thus is a need for more procedural safeguards to incorporate user interests and policy aims.

## How standards can become legally binding when implemented at a national level

The preceding sections have described standards in the case where they operate next to legal rules. Although the legal consequences of standards standing alone might not be obvious, the issue changes when they are laid down in legislation. At a member state level the inclusion of standards in laws can bestow legal binding force to these standards. In some cases, national statutes refer to standards, which can then change the status of the standards. In this section we will concentrate on certain national cases where standards play a role in the legal system. We will demonstrate how EU standards can find their way into national law and what the consequences are. As potentially the smart grid standards will be incorporated in national law, we need to view the consequences of this situation.

Generally there are three different ways in which statutes refer to standards.[33] First is the rigid reference, when the law refers to a specific version of a standard. The second is a dynamic reference, when the standard number and title are given, but the version is not mentioned. Finally, open clauses make general reference to standards without specifying a title or version. An example of such an open reference is art. 3 of Commodities Act Decree on electro technical products regarding electro-technical products (Warenwetbesluit elektrotechnische producten), which refers to 'applicable safety regulation' from the International Electrotechnical Commission. Furthermore, there

32 CEN/CENELEC Guide 20, Guide on membership criteria of CEN and CENELEC edition2, 2012-06, retrieved from http://www.cen.eu/boss/supporting/Reference%20documents/guides/Pages/default.aspx

33 These differences were first mentioned in Marburger (1979).

is a difference between on the one hand standards that are essential for the law to have meaning in the sense that the standard specifies the statute, and on the other hand standards that merely complement a provision.

In the second section it already became clear that standards are not law as such. Most scholars agree that isolated standards are not legally binding (e.g., Joerges & Micklitz 2010, 363). However, research shows that when they are incorporated in laws, and especially when the standard specifies the norm, the standard is held to have legal effect as they work externally and are of general scope (Elferink 1998).

Contrary, in the Dutch Building Decree (Bouwbesluit 2003) case, the Dutch Council of State (Raad van State) has countered this reasoning through a judgement in which it decided that standards do not constitute generally binding regulation.[34] The Building Decree refers to almost 70 Dutch 'NEN' standards directly. The standards mostly influence the process of granting building permits. In order to obtain a permit, one has to comply with the relevant standard. The legal basis for referring to standards in this decree lies in article 3 of the Housing Act (Woningwet), which states that references to standards can be made through an Order in Council. One has to comply with these standards, but – in line with the EU criteria –, their use is not compulsory. This means that in theory one could abide with the specifications without obtaining the standard.

In this case the status of referred standards in the Building Decree was questioned. The case concerned the company Knooble that intended to publish relevant standards from the Decree on their website free of charge. This prompted the question of what the legal status of such standards is. If the standards in the Decree should be considered as 'generally binding regulation' it meant that they should be published following the *Publication Act (PA, Bekendmakingswet)* and, moreover, art. 11 of the *Copyright Act (CA, Auteurswet)* would exempt the standard from copyright, allowing Knooble to publish the standards. Initially, the court at The Hague decided that as the standards were not yet published according to the Publication Act, they were not generally binding, and therefore the exemption of art. 11 CA did not apply. However, the statement that the standards in the Building Decree were not generally binding would imply that they could not be enforced through the building permit application process.

On appeal, the Council of State decided that even though standards cannot be considered as 'generally binding regulation', they are still generally binding and therefore can be enforced. The Council of State used the following reasoning: In the Explanatory Memorandum of the Housing Act it appears that the NSB, the Netherlands Standardization Institute (NEN), has no legislative powers and is not a body authorized to make 'generally binding regulation', and therefore the NEN standards cannot be regarded as such. However, from the Explanatory Memorandum of the PA follows that standards can become part of the law, which should be published and available to stakeholders.[35] Referring to the location where the standard can be found is enough to comply with the requirement of availability. Consequently this decision means that the standards are not 'generally binding regulation', and therefore do not have to be publically available, yet they are binding for the public wishing to obtain building permits. Knooble eventually took the case to the Supreme Court

34 ABRvS 2 februari 2011, NJB 2011, 698.

35 *Kamerstukken II*, 1985/86 19583, no. 3, p. 5.

(Hoge Raad), which did not alter the decision.[36] After this case, a similar case came before the Trade and Industry Appeals Tribunal (College van Beroep voor het bedrijfsleven).[37] The plaintiff appealed a decision of the Ministry of Economics denying an energy investment deduction (energie-investeringsaftrek) because a heat pump did not comply with the relevant NEN standard.

If we look at this case from the perspective of the four requirements of law from the second section of this paper, the position of standards changes. The requirement that standards are recognized by a legal system is now met. First of all, by including a reference in an Order, and second of all by the recognition of the Court that all citizens have to comply with the standard. The requirement of the rule to be set by a sovereign is again probably not met. Though the NEN itself is a clear body of persons, the NEN itself, but technical committees do not set the actual standards. Finally, obviously these standards are not accessible, so that requirement is also not met.

Should these courts have found that the standards were actually 'generally binding regulation', the NEN would have to be attributed rule making powers. That would subsequently lead to the NEN having to observe general principles of regulation, such as the principle that rules must be generated in the general interest and the principle of legal equality (Stuurman 1995, 162-186). This would make standards in line with public law, just like the case of DUA as we already saw. The current decision saves the NEN from these complications.

In the end the courts' argument boils down to the statement that the NEN can set permit conditions, and because they do not have the formal power to set these conditions, they are not accountable, nor do they have to comply with the regular publication rules to boot. This seems like aworrisome ruling, especially when observing the role of standards in current society. Several new questions arise through this decision. For one, it remains unclear on what basis the standards become generally binding? It can be argued that, instead of just accepting any given standard up front, the government in these cases has a duty to monitor the process and the standard itself (van Gestel 2012, 251). Furthermore, the question why certain rules that bind citizens do not have to be made publicly available remains unanswered.[38] As was found in previous research, when standards work externally and are of general scope, they are part of the law (Stuurman 1995, 162-185). One can hardly imagine that the Council of State sought to make the standards generally binding without somehow becoming part of the law.

Interestingly a U.S. Court of Appeals for the Fifth Circuit case dealt with a very similar case.[39]In that case a website published parts of the building code online. This decision solely dealt with copyright law, and not with the legal status of the building code standards. In direct contrast to the Dutch court, this court came to the decision that as part of the Building Code the standards enter the public domain and no copyright is applicable.

There are many other ways in which technical standards find their way into Dutch law through orders or specific conditions in, for example, the electricity market. This can be donefor example by the reference to the technical codes in the electricity market, where they use network

36 HR, LJN: BW0393, 22 juni, 2012.

37 CBB 3 april 2012, AWB 09/1272.

38 AB 2012/228: Verwijzing in wetgeving naar NEN-normen. Geen algemeen verbindende voorschriften. Publiekrechtelijk algemeen geldende normen met noot van F. Van Ommeren.

39 Vreeck vs SBCCI, 99-40632, United States Court of Appeals, June 7 2002.

codes that are 'generally binding regulation' for the network operators (Pront- van Bommel 2011, 53).

This practice of referring to standards in acts and orders shows that the use of standards is mandatory in some cases. On the EU level standards are often distinguished from regulation, as they are voluntary and therefore exempted from procedural safeguards. When standards become mandatory on a national level, however, it raises the question of whether the reasons for not providing procedural safeguards can hold up to scrutiny? European standards can find their way into national law, changing their voluntary status. This alters the legal status of standards more broadly. Where in previous sections the de facto binding force became apparent, in this circumstance they also become legally binding. This invokes an even stronger reason for the necessity of procedural safeguards for user interests and policy aims. The EU framework as described in the previous section will therefore not be sufficient in the case of mandatory standards.

## Conclusion

This chapter examined the relationship between the legal system and standards from different perspectives to the legal system. It firstly showed that because of the role technology currently plays in society, standards can have the same effect as laws in that they are equally binding. This presents the question of how the legal system should deal with standards. To answer that question we reviewed existing legal concepts that are similar to standards. In this review we learned that standards are different, but show the most similarities to the DUA. The DUA have several safeguards that provide protection for parties affected by those decisions, yet smart grid standards do not. We therefore are in favour of a similar preset clear framework to protect the interests of those affected by smart grid standards. In order to understand what relevant framework is already in place we reviewed the EU framework for standards. This review shows that the current system has a limited influence on standardization, and does not provide enough safeguards for user interests and EU policy objectives for smart grids. Finally the reference to standards by governments in national laws shows that the legal system in some cases even legally reinforces standards, while escaping the safeguards of the legal system. In these cases the status of standards shifts from binding in effect, which was demonstrated in the second paragraph, to being legally binding. As this type of transference of EU standards into national law is likely to occur with smart grid standards as well, the demand for a framework to ensure user interests and policy objectives increases drastically.

There is a need to extend the current legal framework to ensure that policy aims are not impaired and user interests are not put at risk by standardization. Especially given the important role standards play in the development of the smart grid architecture, it is crucial to ensure that procedural safeguards support policy goals and non-commercial interests in this process. If the sole document to base smart grid standards continues to be the standardization mandate, the standardization process will pose threats for the future of our energy system. An example of a threat is that that the targets of the EU Climate and Energy Package are ignored in the standardization process. As smart grids are one of most important EU developments to achieve those targets, this is a serious risk. Furthermore the values that play a key role in EU energy policy such as reliability and efficiency are not part of the mandated work and are therefore at risk with the current standardization system.

The standardization process is based on market initiatives, and led by technical experts. This technical expertise is absolutely crucial in order to develop good standards. Our message is therefore unquestionably not that standardization should be abolished our taken over by a public authority. Nevertheless, the absence of a public authority in standard setting has led to a process dominated by market interests and little checks on whether the standards developed take public interest into account sufficiently.

## References


Asscher, L. (2006). 'Code' as law- using Fuller to assess code rules In E. Dommering & L. Asscher (eds)*Coding Regulation, Essays on the Normative Role of the Information society* 61-90, The Hague: TMC Asser Press.

Bell, J. (2002). Comparing Public Law, in A. Harding, and E. Örücü, (eds.), *Comparative Law in the 21st Century*. London: Kluwer.

Benoliel, D. (2004), Comment, Technological Standards, Inc.: Rethinking Cyberspace Regulatory Epistemology, *Cal. L. Rev*. 92 1069-1086.

Black, J. (1996). Constitutionalising Self-Regulation, *The Modern Law Review*, 59(1), 24–55.

Burk, D.L. (2005) Legal and technical standards in digital rights management technology, *Fordham Law Review* 74 537-573.

Dresden, M.J. (2004). *Algemeen verbindendverklaring van overeenkomsten*, (Dissertation Universiteit van Amsterdam) 's-Gravenhage: Sdu.

Elferink, M.H. (1998). Verwijzing in wetgeving. Over de publiekrechtelijke en auteursrechtelijke status van normalisatienormen, Deventer: Kluwer.

Farrel, H. (2002) Hybrid Institutions and the law: Outlaw arrangements or interface sollutions?, *Zeitschrift fur Rechtssoziologie*, 23(1).

Franken, H. (2004) et al., *Recht en Computer*, Deventer: Kluwer.

Hahn, R. & Weidtmann (2011), Transnational Governance and the Legitimacy of ISO 26000: Analyzing the Case of a Global Multi-Stakeholder Process, *Academy of Management 2011 Annual Meeting*, August 2011, San Antonio, TX, USA.

Hart, H.L.A. (1961). *The Concept of Law*, Oxford: Oxford University press.

Hoenkamp, R.A., Huitema, G. B. & de Moor- van Vugt, A.J.C. (2011) The Neglected Consumer: The Case of the Smart Meter Rollout in the Netherlands, *Renewable Energy Law and Policy Review* 4 269-282.

Joerges, C. & Micklitz, H.W. (2010), The need to supplement the new approach to technical harmonization and standards by a coherent European product safety policy, *HanseLR* 6(2).

Koops, B. & Leenes, R. (2005). 'Code' and the slow erosion of privacy, *Michigan Telecommunications and Technology Law Review*, 12(115), 115-188.

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In W. Bijker & J. Law (eds.), *Shaping Technology* (pp. 225-258), Cambridge, MA: The MIT Press.

Leenes, R.E. (2011). Framing techno-regulation: An exploration of state and non-state regulation by technology. *Legisprudence*, *5*(2), 143-169.

Lessig, L.(2006). *Code, version 2.0*, New York: Basic Books.

Marburger, M. (1979). *Die Regeln der Technik im Recht*, Köln:Carl Heymans Verlag.

Mifsud Bonnici, J.P. (2007). *Self-Regulation in Cyberspace*, (Dissertation Rijksuniversiteit Groningen).

Mueller, M. L. (2010).Networks and States, The Global Politics of Internet Governance, Cambridge, MA: The MIT Press.

Post, D. G. (2000). What Larry Doesn't get: Code, Law and Liberty in cyberspace, *Stan. L. Rev.* 52(5) 1439-1459 p. 1453.

Pront- van Bommel, S. (2011) De elektriciteitsconsument centraal? In: Pront- van Bommel, S. eds. *De consument en de andere kant van de elektrciteitsmarkt*, Amsterdam: Universiteit van Amsterdam.

Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules Through Technology, *Tex. L. Rev*, 76(3), 554-584.

Schiff Berman, P. (2000). Cyberspace and the state action debate: the cultural value of applying constitutional norms to "private" regulation, *U. Colo. L. Rev.*, 71, 1263-1300.

Shah, R.C. & Kesan, J.P. (2004).Deconstructing Code, *Yale Journal of Law and Technology*, 6, 277-389, p. 281.

Shiff Berman, P. (2007). Law and Society Approaches to Cyberspace, *University of Connecticut School of Law Articles and Working Papers* 72.

Staniszewski, P. (2007). The interplay between IP rights and competition law in the context of standardization, *Journal of Intellectual Property Law & Practice*, 2(10), p. 670.

Stuurman, C. (1995) *Technische Normen en het Recht*, (Dissertation Universiteit van Amsterdam), Deventer: Kluwer.

Tauberman, A. (2009). International Governance and the Internet, in Adward & Waelde eds.,*Law and the Internet*, Portland: Hart Publishing.

van Driel, M. (1989). *Zelfregulering: Hoog spelen of thuisblijven*, (Dissertation Katholieke Universiteit Brabant), Deventer: Kluwer.

van Gestel, R.(2012). Hoge Raad is duur, over het verwijzen naar normalisatie normen in wetgeving, *Regelmaat*, nr. 4 (27).

van Rooijen, A. (2010). The Software Interface between copyright and Competition Law, A Legal Analysis of Interoperability in Computer Programs, (Dissertation University of Amsterdam).

von Bar, C. et al. (2009). (eds.), Principles, Definitions, and Model Rules of European Private Law; Draft Common Frame of Reference, Munich: Sellier.

Weiser, P.J. (2001). Internet governance, standard- setting, and self regulation, *N. Ky. L. Rev.* 822-846.

West, J. (2007). The economic realities of open standards: black, white, and many shades of gray. In S. Greenstein & V. Stango (Eds.), *Standards and Public Policy*, Cambridge: Cambridge University Press.

Wijckmans, F. and Tuytschaever, F. (2011). *Vertical Agreements in EU Competition Law*, Oxford University Press: New. York.

Winner, L. (1997). Cyberlibertarian Myths And The Prospects for Community, *Computers and Society*, September.

# PART III: ETHICAL REFLECTION ON DISTANCE: CASE STUDIES

# Too close to kill, too far to talk
# Interpretation and narrative in drone fighting and surveillance in public places

Mark Coeckelbergh
University of Twente
Department of Philosophy
✉m.coeckelbergh@utwente.nl

**Abstract** Like other teletechnological practices, drone fighting as remote fighting gives rise to a paradox with regard to the relation between ethics and distance: on the one hand, it bridges physical distance in the sense that it enables spying on people and killing people in other parts of the world. On the other hand, it seems to increase *moral* distance: if you are far away from your target, it becomes easier to kill. However, based on interviews with drone crew as published in the media, I show that the current surveillance technologies used in drone fighting might mitigate this effect since they allow the viewer to build up a kind of intimacy with (potential) targets. Then I argue that this moral proximity is only possible if we assume that interpretation and the construction of narrative play a key role in the epistemology of surveillance. I compare military surveillance to surveillance in public spaces to elaborate this point and explore the relation between automated surveillance, distance, and interpretation. I also argue that given the lack of shared sociality and communication, moral distance in surveillance and drone fighting can only *partly* be bridged by technology-mediated interpretation and narration. I conclude that we need more reflection on how technologies could create the conditions under which moral metamorphosis and interpretative freedom is not only possible but also probable.

**Keywords**drones; ethics; surveillance technology; distance; interpretation; narrative

## Introduction

Unmanned aerial vehicles, also known as 'drones', are increasingly deployed by military organizations all over the world, for example for surveillance but also for killing people. Some argue that drones enable more precision, and that they are therefore better at avoiding killing of civilians. Whether or not this is true, the technology has certainly one important advantage over previous methods: it inflicts damage on the enemy but does not risk the lives of one's own people and material damage is also limited (see for example Valdes 2012). However, drone fighting also raises many ethical issues (see for example Asaro 2008; Singer 2009; Arkin 2008; Lin et al. 2008; Sparrow 2007; 2009; Sullins 2010). An important and interesting one has to do with the same reason why drones incur less risk for those who deploy them: distance. The worry is that because of the distance, killing becomes easier: it becomes a 'video game': "operators sit at game consoles, making decisions about when to apply lethal force" (Sharkey 2012, 113). This claim seems plausible and seems to be illustrative of a paradox that is applicable to all teletechnologies: such technologies bridge physical distance, but at the same time they create (more) moral distance. However, in this paper I will nuance this thesis by focusing on contemporary surveillance technology and its epistemic and moral implications. I will argue that under certain conditions such technology might enable the user to get 'closer' – not only in a physical but also in a moral sense. I will show that these conditions have to do with the need for, and our capacity of, interpretation and narration, which may at least *partly* bridge the distance in drone fighting and surveillance. Thus, I will show that the role of the new surveillance technologies is much more ambiguous than assumed in the 'easy kill-

ing' argument: they create moral distance but at the same time offer ways to mitigate this effect. However, comparing drone surveillance to surveillance in public places, I will also argue that the moral distance cannot be fully bridged due to a lack of a shared physical-social and communicative space. This will lead me to further reflection on ethics, transfiguration, and ambiguity. But let me start with offering support for the 'easy killing' argument.

## The phenomenology of fighting and killing: Support for the 'easy killing' view

In fighting, as in other practices, other humans can be experienced and appear in various ways, depending on all kinds of conditions. It is well-known that killing is more difficult at short range. If a fighter can see the other's eyes, if he touches the other's body, if indeed he has 'intimate' knowledge of the other's body, his opponent appears like a human being, a person not too dissimilar to himself. In this case, fighting itself is a personal matter. Because of this proximity, intended killing of the other is difficult. We have psychological barriers to kill at close range. Psychological evidence suggests that there is "a direct relationship between the empathic and physical proximity of the victim, and the resultant difficulty and trauma of the kill" (Grossman 1995, 97). A shorter physical distance means more *moral* distance. Grossman writes:

> ''At close range the resistance to killing an opponent is tremendous. When one looks an opponent in the eye, and knows that he is young or old, scared or angry, it is not possible to deny that the individual about to be killed is much like oneself. […] As men draw thisnear it becomes extremely difficult to deny their humanity. Looking in a man's face, seeing his eyes and his fear, eliminate denial.' (Grossman 1995, 118)

In philosophy, a similar point has been made by Levinas, who argued that there is an ethical demand that arises directly in relational situations: the face of the other shows the other's vulnerability, which renders killing impossible. When we see the other's "defenceless eyes", the other's "nudity", we cannot kill (Levinas 1961, 199-200).

Historically, the 'solution' to this 'problem' has been the development of weapons, which can be understood as *teletechnologies*, that is, tools that are intended to increase and bridge physical distance – the idea is that you can strike while minimizing risk for yourself – but also to maximize moral distance: they are meant to render it easier to kill. First stones, spears, knives and swords were used for this purpose, then longer-range weapons such as guns were developed. This meant that the person and the human being became a 'target' – a 'something' one can aim at with one's weapon. To kill a 'target' is much less traumatic to the fighter and the killer, who has now become a 'shooter'. Moreover, the increased distance protects the fighter against being killed, or so he thinks. Sharkey summarizes the point: "attacking from a distance […] gets around two of the fundamental obstacles that war fighters must face: fear of being killed and resistance to killing.'(Sharkey 2012, 111) A typical teletechnological military practice is airstrike: there is a huge distance between bomber and bombed, which renders killing easier, and risk of losing (many) lives is lower than with (ground) artillery. Consider the bombings in World War II, including the nuclear attacks on Hiroshima and Nagasaki in 1945: the immense distance also made the mass killings possible. Drone fighting, then, seems to be the 'ultimate' distance technology for killing (unless one would fight from space), since it maximizes the distance between fighter and opponent, thus maximizing protection of the fighter and rendering killing as easy as it can get.

But is this true for drone fighting? How easy is it really to kill when you are part of a drone crew? In order to find out more, we need to look more closely to drone fighting as a practice and how that practice is mediated by current surveillance technologies.

## Interpretation and Narrative in the Drone Cockpit: Questioning the 'easy killing' view

What kind of knowledge is generated in the drone fighting practice? What does the drone crew know about their 'targets'? In order to fine-tune the phenomenology of drone surveillance and fighting we first have to attend to the particular surveillance technologies used by the drone crew. Let us focus on how the images operators see on their screens are produced. Surveillance drones are outfitted with high definition (gigapixel) cameras that enable tracking of many different targets. Drones may also carry infrared cameras, heat and movement sensors, automated license plate readers, etc. Use of this equipment does not only raise obvious privacy issues when it comes to military and non-military use; in so far as the cameras enable operators to see individual people, they also shape how drone crew experience their targets, and this has moral consequences. Let me show why these technologies are neither epistemologically nor morally neutral, and how they mediate and shape the experience of the crew and 'construct' the experience knowledge they have of their 'targets'.

We do not see neutral 'facts' or 'data'. To use these terms is already a particular construction of reality. When drone operators see their 'target', the epistemic framing has already been done. To call a particular person a 'target' and to experience her *as* a target is *already* a particular kind of construction. The other may also appear as a human being or indeed *as an other*. Which appearance prevails is morally significant. It is also a *moral* framing. If I see a 'person', I am less likely to kill than if I see a 'target'. Thus, how the other appears to the fighter is highly morally significant: it can mean the difference between life and death. What happens in 'traditional' airstrikes, it seems, is that the combination of technologies (airplane, surveillance technology, etc.) makes possible that the people on the ground do not appear as people, as human beings, or as others, but as enemies, as objects, as targets that have to be destroyed. The technology does not make possible any other appearance. The moral distance is unbridgeable. In a sense, before the victim is physically killed, he is first killed in thinking, killed with words. He is already 'dead meat' before he is 'slaughtered'. The opponent is never seen in a 'neutral' way. To call him 'opponent', 'enemy', 'guerrilla fighter', 'activist', 'terrorist', etc. is already a particular construction – often a lethal one. The framing is part of the fighting.

But do 'targets' in drone fighting always appear as 'targets', as 'enemies', as 'people-to-be-killed'? Contemporary surveillance technology as used by drone crews, in combination with information gathered by (other) intelligence services and their technologies, enable the drone fighters to get much closer to the persons they are supposed to follow and perhaps kill. Today, the drone crew sees particular people on the ground and what they are doing. They see 'people', 'persons', 'human beings'. Colonel Brenton, who flies a Reaper drone in Afghanistan, told a New York Times journalist that he and his team often watch people and their family for weeks:

> "I see mothers with children, I see fathers with children, I see fathers with mothers, I see kids playing soccer" (Brenton quoted in Bumiller 2012)

This does not render it easier to kill, on the contrary, it becomes harder. This is due to the technology: the cameras "bring war straight into the pilot's face" (Bumiller 2012). The technology supports what we may call an 'epistemic' bridge and a 'moral bridge': it does not only mediate remote killing; it is also at the same time a condition of possibility for bridging the physical and moral distance initially created by the drone system. How does this work?

A drone crew is not always busy with fighting and killing. Most of the time, they watch people, they watch (potential) targets. But as the term 'target' already indicates, what they see is never epistemically or morally neutral. There is always already *interpretation*. The technological practice makes possible the active interpretation and – given the longer timeframe of days or weeks – the construction of *narratives*. Because the cameras enable such 'close' observation, the crews do not only see people but also people with *lives.* Combining what they see through the camera with other information (also brought to them via contemporary information and communication technologies), they make up stories about the people they monitor. But this does not happen 'afterwards', after they get 'information'. Framing already takes place when they observe the people. They do not see 'data' but 'enemies' or indeed people of flesh and blood. At the moment when they see something or someone 'on the ground', they have already interpreted it or him/her. And because they can see "details as fine as individual faces" (Brooks 2012), one kind of framing is more likely to happen and it is no longer easy to kill. The crew members watch people similar to themselves. They see people who have families, people who "wake up in the morning, do their work, go to sleep at night' (an Air Forcemajor quoted in Bumiller 2012). Moreover, in contrast to old-style bombing, the crew now sees the consequences of a strike for the people. They see the suffering of people. A CIA drone operator told a journalist:

> "'I dropped bombs, hit my target load, but had no idea who I hit. [With drones], I can look at their faces… see these guys playing with their kinds and wives… After the strike, I see the bodies being carried out of the house. I see the women weeping and in positions ofmourning. That's not PlayStation; that's real."
> (drone operator quoted in Brooks 2012)

Thus, whereas there is a process of de-personalisation and indeed moral distancing made possible by the remote surveillance and remote fighting technology, there is also a process of re-personalization and indeed *humanization* of the 'target'. The 'target' turns into a human being, a particular person. This creates a moral bridge between drone fighter and target, which makes it more difficult to fire a missile. But this humanization and moral bridging should not be understood as a kind of 'built-in' psychological response (i.e. an empathic response) to stimuli, to the data of the camera. The construction of knowledge, the shaping of the experience, is an active epistemic process that involves a hermeneutic exercise involving different stories. Feelings of empathy or sympathy may occur, of course, but they are linked to this interpretative and narrative work. What the crew sees is interpreted in the context of a larger narrative about the person and perhaps also about oneself, and at any time this narrative can also be revised on the basis of what one sees. For example, it is likely that the drone operator has a story about the target such as 'This is a father of four children and soon he will be alone since the rest of the family will go out to the market' and about himself, for example 'I am not the kind of person that kills women and children'. This is a contextual, situated perception and understanding; what the drone operator sees and experiences

is not 'camera data' but lives, people, persons that are not only 'identifiable' but also have identities.

Moreover, because of the interpretative and narrative possibilities supported by the new surveillance technologies, it is also likely that the drone operator has to deal with two conflicting, morally relevant narratives: one that concerns the life of the potential 'target' that turned out a human being like oneself, and one that concerns the story of a professional military officer trying to do what she considers to be her duty (and what others tell her that is her duty), trying to obey order, trying to justify the killing, etc. There may be even a third story line, one that concerns the private life of the crew member. When the pilot goes home, there is another life waiting, with other expectations and other appearances and meanings. Thus, the crew members find themselves in an epistemic web they at the same time actively construct, and with which they have to cope. They have to try to weave together the different lines. They have to act and take responsibility for their action, but they also have to cope with moral-epistemic frictions. There are different stories and there are different and dynamic appearances: the 'target' that becomes a 'kid', the control room that becomes a living room, the professional that becomes a father, etc. There are different 'worlds'. Sometimes 'faces' appear and at other times there is only a 'target'.

These hermeneutic processes and dynamics are not only present in drone surveillance and drone fighting. We can also find them in other surveillance practices.

## Zooming out: Surveillance in public places, distance, and interpretation

Interpretation and narrative are also relevant to ethics of surveillance in general, especially if we keep in mind the issue of moral distance. Consider first the case of 'traditional' surveillance in public places, that is, surveillance without the use of video surveillance – let alone 'smart' video surveillance that would recognize faces or behavioural patterns. Usually security personnel or policy officers would walk around in, say, a shopping street, an airport or a train station, and try to spot 'suspect' behaviour. Because of the task they perform, they already produce moral and social distance between them and the people around them. In defining themselves as standing outside the sociality of the public space, they are no longer 'fellow travellers'. Of course public spaces are also about watching others and being seen by others, and with Sartre we could say that the gaze of the other can make us into an 'object' (see also Patton 2000,183-184) rather than a 'fellow', but even if this happens there is a certain kind of symmetry, whereas with surveillance this symmetry is broken. There is a gap, a distance, between the spectator and the 'crowd'. Moreover, from the point of view of the surveillance officer, the appearance from people in the crowd can always change from 'traveller' or 'customer' or 'man' or 'woman' to 'suspect', 'target', 'terrorist', etc. Let me suggest that the way this works is again through interpretation and narration. The epistemic background of the surveillance is formed by stories: known stories about a 'terrorist' who entered a train and blew it up, on the one hand, and a story about the particular individual that is being watched at a given time ('he is carrying a suitcase which could contain a bomb, now he takes the stairs, he seems a little nervous', etc.). The latter story has to be actively (but not necessarily consciously) constructed by the security or policy officer. Does what this person is doing and *how* (s)he is doing it fit into a story of a criminal, terrorist, etc.? If the spectator achieves a hermeneutic integration between these two stories, then it is time for *alarm* and action. However, in non-automated surveillance, there is still a lot of room for proximity – both in a physical and in a social and moral sense. In case of

doubt (and humans *can* doubt), the security officer can get closer or 'even' *talk* to the 'suspect' or 'potential terrorist', and in the course of the interaction the status of the 'suspect' may change into 'fellow human being' again. (Verbal communication helps here: once you talk to someone, that chances are high that that person is no longer is an 'object' that is subject to your gaze; he becomes a *subject*.) If this is the case, it means that the interpretation changes and that the story is re-written, so to speak. Now the 'suspect' becomes again 'a woman making her way to the train' or the 'terrorist' becomes 'a man with a present for his wife'. Again this hermeneutic play is highly morally significant: it changes the moral status of the person being watched (from 'bad' to 'good', from 'terrorist' to 'innocent citizen' etc.) but it also changes an entire *scenario*, it changes the (potential) actions of security people and police and it changes what happens and what will happen to the other people in the public space.

With automated surveillance technology, however, the situation is different. In case of half-automated surveillance, there is still a human person watching screens with images delivered by cameras. This already increases the physical and social distance, and limits the possibilities for interpretative work, since the person who watches the screen cannot be in the social space at the same time. When one watches the screen, it is not possible to be *part* of the story – a *common* story – and to link one's own story to the stories of others. It is no longer possible to write a story *together*, to arrive at a shared understanding. The removal of the surveillance-subject from the social space is now definitive. Of course, the operator can decide to go in the social space or send someone in – then there is a different situation. But if and in so far as the operator's experience is mediated by the screens, he or she remains a *spectator* and has a less rich understanding of what is going on. Moreover, the spectator can still see 'a man going to work' rather than a 'terrorist', there is still a range of possible interpretations and stories. But the construction of the story as a *realistic* story is hindered by the distance. It becomes more likely that the faces and bodies on the screen become only that – faces and bodies. There is no longer a person, no longer a face in the Levinasian sense of the world; there is a 'target'. This distance is even further increased in the case of automated surveillance, where computer algorithms are used to discern 'suspect' behavioural patterns. In the extreme case, if surveillance were to become fully automated, this would mean a disruption of interpretation and narration, since during that process, there would be no *human* surveillance. In interpretation and narration there is always room for what I called 'hermeneutic play'. The 'status' of a particular person in the crowd is not calculated in terms of probabilities but is constructed by a meaning-giving human subject. Automated surveillance relies on statistics and meanings *fixed* by the programmers. The computer cannot use the hermeneutic richness of stories (histories and present, on-going stories). At that point, the space of meanings is limited and closed. This is why we tend to use semi-automated surveillance, which lets the hermeneutic process continue after its disruption by automation: first the cameras and the computers 'do their job', then it is up to humans to do the interpretative work. But since a selection has already been made by the computer instead of a person present in (and part of) the social space, the condition of possibility for a full understanding of the situation has already been lost. The point is not that we have less information; we always have to select. The point is about the way the selection is made and about who or what made the selection: not a human person present and interacting in the social space of the public place, not even a human person watching screens.

Perhaps this is also exactly what is still problematic in the case of drone surveillance (in general and in military contexts), in spite of the hermeneutic possibilities created by the new technolo-

gies. It seems plausible that, as I have argued in the previous section, interpretation and narrative can bridge the moral gap between drone operators and the people they spy on and perhaps kill. Yet this bridging is always only partial since the hermeneutic work is still hindered by the physical distance. There is still a qualitative difference between on the one hand the knowledge gained by someone who walks around 'on the ground', in the local place, in the country, someone who interacts and talks to people or at least *could* do so, and the knowledge gained by someone who sits in a drone cockpit at a military base thousands of miles away. The qualitative difference that is morally relevant lies in the restriction of hermeneutic resources that comes with *not being there* and *not being with* the people. A shared physical-social and physical-communicative space is lacking. The spheres of sociality do not overlap and hence the appearances and stories are still too poor in meaning. Of course given what I said in the first section about the psychology of fighting, a cynic may retort that people who want to kill do not *want* to close the moral gap, do not *want* to blur the distinction between 'us' and 'the enemy', do not *want* to humanize their target. I concede this point. But we should also keep in mind that military professionals do not generally kill because they enjoy killing. They – or those who command them – kill or order to kill if they think that they have good reasons for doing so. Whether or not there are good reasons in a particular case, and whether or not there can be good reasons at all to kill *anyone*, requires judgment, moral judgment. Exercising that moral judgment and responsibility requires, among other things, taking all measures to make sure that, if one decides to kill at all, one knows what one is doing and to whom one is doing it. On the basis of the discussion offered in this paper, we can conclude that contemporary surveillance technology may assist a drone operator in fulfilling this moral-epistemic duty in so far as it supports interpretation and the construction of narrative, but that this is still morally and epistemologically inferior to conditions that make the transfiguration from 'target' to 'human being', from 'militant' to 'father', from 'suspect' to 'fellow traveller', from 'terrorist' to 'someone who is also trying to get back to her children', from object to subject not only *possible* but also more *likely* to occur. It seems to me that there is a general moral and political duty to create such conditions, and to prevent the emergence of situations in which such a moral metamorphosis becomes impossible, situations where 'targets' can no longer appear *other*-wise and killing or other violent action becomes the only option.

This is what fully automated surveillance (and of course also with fully automated killing based on it) would also do: it would reduce the appearances and the options since it would destroy interpretation and remove the possibility of common stories. It also strikes me that in automated surveillance there is no room for hermeneutic play, there is also no room moral ambiguity. The status is zero or one, 'enemy' or 'we', 'terrorist' or 'innocent person', but there is no room for different meanings. A particular 'target' is either 'a terrorist' or 'an innocent person', but *there is no place for doubt.* But certainty is the enemy of mature moral reflection. If situations and the status of people are (pre-)defined by a machine, by those who programmed the machine, and by those who defined the rules used in the programming, then we can no longer interpret and no longer discuss our interpretation. Then talking is replaced by following rules. This is a great moral danger – inside and outside surveillance contexts. In fact, in ethics itself and indeed in approaches to ethics there is a clear tension between on the one hand ethics by *regulation*, understood as the design of rules and laws to govern conduct, and on the other hand a kind of ethics that seeks to keep an open space for interpretation, discussion, and communication. I have no room to further discuss this issue, but my remarks on automated surveillance technology suggest that we can evaluate particular tech-

nologies and practices by investigating if and how they contribute to regulatory-technological closure or rather help to keep the ethical space open.

## Conclusion

In this paper I have reflected on the relation between teletechnologies and moral distance by discussing the cases of drone fighting and surveillance in public places. I have argued that the physical distance created by drone technology indeed seems to make killing easier, but that this effect is mitigated by the moral proximity made possible by contemporary surveillance, at least in so far as it supports interpretative and narrative moral-epistemic work that lets appear the 'target' as a person with a face, with family, with a life. Of course as we know when it comes to action the "family" or "person" narrative does not usually prevail over other narratives, for example a narrative of "duty"; but at least the technology makes it possible that the former narrative can be constructed. Discussing surveillance in public places, I have also argued that the moral distance in surveillance and drone fighting can only partly be bridged by remote, technology-mediated interpretation and narration given the lack of shared sociality (being-present-with-others) and communication, which limits the interpretative possibilities and, in the case of automated surveillance, threatens the possibility of interpretation as such – including the moral ambiguity and the open ethical space that comes with it. I conclude that we need more reflection and research on how technologies could create the conditions under which moralmetamorphosis and interpretative freedom is not only possible but also probable.

To end let me say more about what kind of research is needed for this purpose. Next to further conceptual work on the relations between technologies, distance, epistemology and morality, which would need to engage for example with literature on "teletechnologies" and on "telepistemology" in philosophy of technology (e.g., Goldberg 2000), we also need to study the technologies and technological practices in more detail and we need empirical work that includes for example interviewing drone teams and operators of surveillance systems. This may enable us to more fully disclose various narrative spaces (e.g. military narratives of "duty" and narratives about "fathers, mothers, and children") and to say more about the relation between specific features of the technological artefacts and the phenomenology and hermeneutics of remote fighting. Moreover, the issue concerning the relation between technologies, distance, and morality is not unique to drones and surveillance devices, but is relevant to many "digital" or "electronic" technologies as "teletechnologies". We need to explore this problem in several domains and also think about it at different levels of analysis and generality. We need both "zooming in" and "zooming out" to take this further.

## Acknowledgment

I thank the anonymous reviewers for their comments, which helped me to prepare a corrected version of this paper and to expand my conclusion with suggestions for further research.

## References

Arkin, R.C. 2008. Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative/Reactive Robot Architecture. Proceedings of the 3rd ACM/IEEE International Conference on Human-Robot Interaction.

Asaro, P.M. 2008. How just could a robot war be? In P.Brey, A. Briggle, & K. Waelbers (eds.),Current Issues in Computing and Philosophy (pp. 50-64). Amsterdam: Ios Press.

Bumiller, E. 2012. A Day Job Waiting for a Kill Shot a World Away. *The New York Times*. Retrieved from http://www.nytimes.com/2012/07/30/us/drone-pilots-waiting-for-a-kill-shot-7000-miles-away.html?pagewanted=all

Brooks, R. 2012. What's *Not* Wrong With Drones? *Foreign Policy*. Retrieved fromhttp://www.foreignpolicy.com/articles/2012/09/05/whats_not_wrong_with_drones

Goldberg, K. (ed.) 2000. The Robot in the Garden: Telerobotics and Telepistemology in the Age of *the Internet*. Cambridge, MA: MIT Press.

Grossman, D. 1995. On Killing: The Psychological Cost of Learning to Kill in War and Society. NewYork/Boston/London: Little, Brown & Company, revised edition 2009.

Grossman, D. 2001. On Killing. II: The Psychological Cost of Learning to Kill. *Int J Emerg MentHealth* 3(3): 137-144.

Levinas, E. 1961.*Totality and Infinity*. Pittsburgh, Pennsylvania: Duquesne University Press,1969.

Lin, P., Bekey, G., and K. Abney. 2008. Autonomous Military Robotics: Risk, Ethics, and Design. Report for the US Department of Navy, Office of Naval Research.

Patton, J.W. 2000. Protecting Privacy in Public? Surveillance Technologies and the Value of Public Spaces. Ethics and Information Technology 2: 181-187.

Singer, P.W. 2009. Military Robots and the Laws of War. *The New Atlantis: A Journal of Technology & Society*, Winter issue: 28-47.

Sparrow, R. 2007. Killer Robots. *Journal of Applied Philosophy* 24(1): 62-77.

Sparrow, R. 2009. Building a Better WarBot: Ethical Issues in the Design of Unmanned Systemsfor Military Applications. *Science and Engineering Ethics* 15: 169-187.

Sullins, J. 2010. RoboWarfare: Can Robots Be More Ethical Than Humans On The Battlefield? Ethics and Information Technology 12(3): 263-275.

Sharkey, N. 2012. Killing Made Easy: From Joysticks to Politics. In Lin, P., Abney, K., and G.A.

Bekey, Robot Ethics: The Ethical and Social Implications of Robotics (pp. 111-128). Cambridge, MA: MIT Press.

Valdes, R. 2012. How the Predator UAV Works. *HowStuffWorks.* Retrieved from http://science.howstuffworks.com/predator4.htm/printable

# Trust and technology in collaborative consumption. Why it is not just about you and me

Esther Keymolen
Erasmus University Rotterdam
Faculty of Philosophy
✉keymolen@fwb.eur.nl

**Abstract:** Trust relations online cannot be analyzed as mere interpersonal interactions because of the new complexity mediating technology brings forth. Based on the work of the German philosopher Helmuth Plessner (1975), I will argue that *distance* is constitutive of men's life form and that the endeavour to bridge this ontological gap, for example by producing technology, is an important driving force in human action. Human beings are *artificial by nature* (Plessner 1975). They have to mould their own world and create a balance they are deprived of by nature.. Artefacts, when they enter the domain of culture, gain their own momentum, they possess a kind of objectivity that stands apart from their creators (de Mul 2003, 261).Nonetheless, technology *par excellence* holds an *utopian -and therefore misleading- promise* of not just bridging this ontological distance but of *overcoming* it (de Mul 2001). Online users are enabled to collaborate in a way that resembles interaction based on reputation and face-to-face contacts in small communities. Botsman (2012) claims that: "trust will become the currency of the new economy". I will make a case that *trust through technology* as Botsman describes it will not lead to *interpersonal trust* as we know it from direct interaction, but will result in what I call *interpersonal system trust,* with an active role for technology in building and shaping these trust relations. In view of the fact that technology can bridge but cannot overcome distance, bringing along new complexity, it is not enough to simply *translate cues of interpersonal trust* to an online environment. In analyzing trust online, one has to take into account the specific workings of the online technology, its *mediation* (Verbeek 2011b), to see if and how measures have to be taken to ensure trustworthy online interaction. I will suggest that at least four aspects of internet technology need to be taken into account when analyzing online trust: *context, code, company,* and *country*.

**Keywords**: Trust, Plessner, Luhmann, Internet, Collaborative Consumption

## Introduction

Nowadays trying to imagine a world without Internet is almost as difficult as trying to imagine a world without electricity or the printing press. Nonetheless, it was only 24 years ago that the Netherlands was connected to the web; in those days a network mostly used by academics[1]. Within a sweeping two decades, 63,2% of the European population and 78,6% of the population in North America have access to the Internet. Looking at the period 2000-2012, this is a growth of respectively 393,4% and 153,3% (internetworldstats 2012). Although all new technologies to a certain extent are welcomed as the ultimate problem solvers, in the case of the Internet this is indisputably the case.

The advantages the world wide web has brought us seemed countless. Mainly in the 1990's and the beginning of the new millennium, the internet has been characterized as a technology that would break down physical boundaries, make time differences irrelevant, and facilitate direct interaction without intermediaries. It would open up a space for people to experiment with their identity,

[1] http://www.nuentoen.nl/fotos/252998/1988-nederland-aangesloten-op-internet.html

giving them the opportunity to become who they want to be, not constrained by the physical limits the offline world imposes on them. “All they see are your words” Turkle writes (1995, 184).
Moreover, the way in which the Internet itself has been designed seems to embed the core values of a deliberative democracy in action. It is developed to be *open* to every computer and network, the protocol is *minimalistic* without stringent conditions to connect, and all connected applications are handled in the same manner (Goldsmith and Wu 2008, 23). As a result, Internet would enable self-governance and bring like-minded people together (see Morozov 2011; Rheingold 1993). In short, the earth would become ‘flat’(Friedman 2005). Deibert et al. (2012, 8) refer to this optimistic take on the development of the Internet as the phase of “*The Open Commons”*. And although according to Deibert et al., (2012) already in 2000 this optimistic phase had to move over for a more critical phase called *Access Denied*, followed by a third phase in 2005 called *Access Controlled* and a fourth one in 2010 *called Access Contested*, they also acknowledge that up until today the idea of an Open Internet remains very attractive (Deibert et al 2012, 9). Although there is a flow of reports, books and articles on cyber crime (InformationWarfareMonitor 2009), techno-regulation (Zittrain 2008; Lessig 2006; Goldsmith and Wu 2008; Wu 2011), and on the impact of censuring measures on human rights in cyberspace (Morozov 2011; Deibert et al. 2010; Deibert et al. 2012; Deibert 2008), the belief in a free and open internet that facilitates community building and bottom-up activities remains strong.

Grounding their idea of *collaborative consumption* on the concept of an *Open Internet*, Rachel Botsman and Roo Rogers endorse this *commons perspective*. They claim that, enabled by the internet, a new economy will arise built on the key values: “**critical mass, idling capacity, belief in the commons** and **trust between strangers”** (Botsman and Rogers 2010, xvi). They focus on websites such as *Airbnb* -a platform for people who want to rent their spare room and travellers who want to find accommodation- and peer-to-peer lending websites such as *Zopa* and *Lending club*, to show how *access* to certain goods becomes more important than *owning* them. Botsman and Rogers find in the Internet the possibility to overcome distances and bring people together to collaborate in an ‘old-fashioned’ way. Based on *interpersonal trust*, people will be able to collaborate on online platforms in a way that resembles their familiar, face-to-face interaction in small communities. They state that:

> “Online exchanges mimic the close ties once formed through face-to-face exchanges in villages, but on a much larger and unconfined scale. In other words, technology is reinventing old forms of trust”(Botsman and Rogers 2010, xiii).

In this paper, I will explain how such a strong belief in the Internet as a technology to bring people together is linked to the *life form* of human beings who are depending on technology to mould their life. Based on the work of the German philosopher Helmuth Plessner, I will argue that technology can partly and temporarily bridge interpersonal distance but can never overcome it. Consequently, the *commons perspective* as nowadays formulated by advocates of Collective Collaboration is *misleadingly utopian*. Technology always brings with it new complexities that need to be dealt with. Moreover, I will argue that trust online is not the same as interpersonal off-line trust. While I agree with Botsman and Rogers that trust online is essential for interpersonal interaction and that a lot of the complexity inherent in human interaction can be dealt with through the act of trust, the online context is not a neutral environment bringing back “old forms of trust” (Botsman and Rogers 2010, xiii). Rather, to build a familiar world in which trustworthy online interactions can thrive, one has to

take into account the specific workings deriving from the co-shaping interaction of user and Internet technology. I will introduce the concept of *interpersonal system trust* to emphasize the new form trust online takes because of the mediating aspects of the online platform. I will suggest that when analyzing trust online at least four aspects of the workings of the Internet have to be taken into account: *context, company, country* and *code*. If we find the core values of the Open Commons perspective worthwhile, a different, less utopian perspective on the influence of the online environment on trustworthy online interactions has to be developed.

## Trust versus power online

### *Internet in its early days*

To fully understand the rise of an online movement like collaborative consumption, we have to go back to the late 1980s and early 1990, when the Internet was not mainly concerned with online Christmas shopping, being on Twitter or making use of social network sites to start a revolution. Largely free from commercial or governmental meddlesomeness, people participated in online communities; they 'met' in chatrooms, played online games, and posted messages to 'bulletin boards'. This online world was perceived as being separate from the real world, also referred to as "meatspace", in which people were freed of physical constraints and governmental regulation (Goldsmith and Wu 2008). The Internet was a place where people could experiment with their identity (Turkle 1984), find like-minded people (Rheingold 1993) and hope to form the "first truly liberated communities in human history" (Goldsmith and Wu 2008, 16).

On a technical level, this *openness* seemed ingrained in the structure of the Internet. The TCP/IP protocol that makes the online world go around enables an open and global network in which all kinds of data flow. The protocol is indifferent to the nature of the content that travels through the networks or the devices that are plugged in, as long as they all apply the basic rules the protocol sets (Wu 2011; Zittrain 2008). Goldsmith and Wu (2008, 23) describe how the engineers who developed this protocol "…built strains of American libertarianism, and even 1960 idealism, into this universal language of the Internet." They developed a global network, which reflected distrust for "centralized control" (Wu 2008, 23). The Internet is probably the first information-related innovation that resulted in a technology almost everybody can access, making use of a multitude of devices on a neutral net (Zittrain 2008; Wu 2011).

Supporters of this Open Internet perspective - also referred to as the Open or Digital Commons - include engineers, hacker groups, p2p communities, online entrepreneurs, and all kinds of political activists[2]. Obviously, this is not a homogeneous group of users, but what they nonetheless have in common is their belief in *self-regulation* (and as a consequence their dislike of governmental regulation) and *in bottom-up participation* and *problem solving*.

[2] These Open Internet adherers are not necessarily academics or people who are interested in publicizing or engaging in academic debate. Nonetheless their activities on and visions of the Internet are of great importance because they co-shape the evolution of the online world. Therefore, to attend to their ideas and activities, one has to take into account non-academic sources such as blogs, online discussions, video's, etc.

## *Collaborative Consumption*

The advocates of Collaborative Consumption can also be characterized as belonging to this mixed group of *netizens* that endorse the Open Internet perspective. They strongly believe that, through the Internet, interpersonal relations can be built, which will support a new economic model based on *sharing*. Instead of *owning* a car, you *share* one, you no longer *buy* clothes but *swap* them, and instead of going to the bank to beg for a loan, you turn to *peer-to-peer* lending sites to look for individual investors. Where the 20th century was defined by *hyper-consumerism* based on *owning*; *Collaborative Consumption* or a *Shared Economy* based on *access* will characterize the 21st century.
As we have seen, Collaborative Consumption stands in the – in Internet terms - 'long tradition' of approaching the Internet as a technology to empower people. That it is a trend unlikely to fade away soon is supported by the fact that, besides Botsman and Rogers, a lot of other key-authors, like Tapscott (2006), Chesbrough (2006), Benkler (2006), and Bauwens (2012), write about similar developments online. Moreover, there is a growing attention for this phenomenon in international media. The Economist, for example, sees as one of the important trends in 2013 the "ownerless economy expand" (Malnight and Keys 2012). And already in 2011, TIME magazine viewed Collaborative Consumption as one of the "10 ideas that will change the world" (Walsh 2011).

## *Four principles of Collaborative Consumption*

Botsman and Rogers (2010) identify four basic principles that lie at the heart of this new movement: *critical mass, idling capacity, belief in the commons,* and *trust between strangers*.

*Critical mass* stands for the required *momentum* to make a collaborative consumption initiative successful. For example, if I want to rent an electric saw, but I have to drive an hour to get one, this tempers my will to participate. An initiative needs enough participants – how many exactly depends on the kind of initiative - to make it attractive.

*Idling capacity* refers to the core assumption that there is a large offer of things and services, which by redistribution can be made useful elsewhere with the Internet as a distributor *par excellence*.

With *the belief in the commons,* Botsman and Rogers refer back to the well-known article of Garrett Hardin (1968) "The Tragedy of the Commons" in which the latter describes how people who self-govern a piece of land that no one owns, will eventually take too much, damaging all participants. However, the advocates of Collaborative Consumption assert the opposite. They claim that, especially on the Internet, it is possible to provide value to the community and at the same time enable social value to expand for oneself. A digital common can become a reality.

With *trust between strangers* we touch the central principle of collaborative consumption. On online peer-to-peer platforms, the traditional role of the middleman who enables third-party trust ceases to exist. Based on rating-systems, known from websites such as eBay, trust between strangers can be enabled.

## *The concept of trust in Collaborative Consumption*

Although these four principles are all very important and lie at the heart of the movement, I will chiefly focus on the last principle, namely: trust, which probably is the most challenging one to accomplish (Brodwin 2012). Recent research also indicates that issues of trust influence the decision of potential users to participate. The biggest barrier to participate is the "… concern that a lent item

would be lost/stolen (30 percent), followed by worries about trusting the network (23 percent) and privacy concerns (14 percent) (Bauwens et al. 2012, 135)."

First of all, trust as described by Botsman and Rogers (2010) has a *direct nature*. It is something that happens between persons, also referred to as *interpersonal trust*. On the Internet, people who develop and maintain platforms for collaborative consumption are mainly "curators" and "ambassadors", earning money by creating "the right tools and environment for familiarity and trust to be built" (Botsman and Rogers 2010, 92). In the end, it is *up to the users* to establish this trust.

One of the important tools to establish trust is the *online rating system*. People can reward each other's trustworthiness by giving a good review or grade. Mother of all online rating systems is eBay. This online second-hand marketplace already introduced its peer-to-peer monitoring device in 1996. Because of its rating system, traders can build up a reputation of a trustworthy buyer or seller, enabling new interactions. Axelrod (1984) refers to this process as "the shadow of the future". If someone wants to establish a durable relation or wants to participate in a community for a longer period of time, it is necessary to act in a reliable way to convince people of his or her good intentions and as a result make interaction possible. Botsman and Rogers (2010, 218-219) speak of "reputation capital". It is a currency that claims: "You can trust me" and in the view of Botsman and Rogers it will become one of the pillars of the new economy.

All in all, Botsman and Rogers envisage a new way of doing business, even a new way of community-building online, which leans heavily on the possibilities the Internet provides to connect like-minded people. Essential to the success of this new *Shared Economy* is the building of trust, which mainly takes place on an interpersonal level. By leaving out the middleman, Botsman and Rogers link together an 'old-fashioned' way of doing business with a new technological platform.

While I agree with Botsman and Rogers that Collaborative Consumption is starting to become an important movement, even bringing about a shift in the way we set up our economic system, I am critical of their perspective on trust and more specifically of their focus on direct interaction supposedly made possible by the internet. With their rather *utopian approach* they run the risk of losing sight of what is happening outside of the commons, which may be of great importance to their movement. Moreover, their approach on trust could even be weakening their groundswell. To substantiate my critique I will build my argument based on two lines of reasoning: first, an *empirical* one and second, a more elaborated, *philosophical* one. Together these arguments will form the basis for an alternative way of conceptualizing trust: *interpersonal system trust*.

## *Controlled space*

Despite the success and attractiveness of the *Open Internet perspective*, inspiring movements like Collaborative Consumption, different authors have unmasked this intrinsic openness as being a myth (Deibert 2008; Deibert et al. 2010; Deibert et al. 2012; Lessig 2006; Zittrain 2008; Goldsmith and Wu 2008; Rheingold 1993; Morozov 2011). From 2000 onwards, governments and other online stakeholders came to think about ways to manage and control Internet traffic[3]. Governments are monitoring online interactions and information flows, companies are making use of real-time

[3] Of course a distinction can and has to be made between the motives of governments, companies, or criminals to act and intervene online. Nonetheless, for the point I want to make- that interpersonal trust is not an accurate level to analyze interaction online- it is sufficient to show that these different actors with their own specific motives can be found online and that they do influence and shape interpersonal online interaction.

targeting and profile their users to personalize their services, cybercriminals are attacking banks and other institutions. All these different online actors are working hard to turn the Internet into a filtered and controlled environment (Hildebrandt and Gutwirth 2008; Keymolen 2013). While users are under the impression that they can anonymously surf the Internet and that nobody is really interested in their online activities (Benoist 2008, 168), almost 80% of the most frequently-visited websites use tracking technology to gather information on their visitors (Angwin 2010). Authoritarian states as well as democratic states participate in *techno-regulation*[4], often "…delegating censorship and surveillance to private companies…" (Deibert et al. 2012, 12). All in all, the Internet has become a *digital panopticum*. To quote Deibert et al. (2012, 7):

> "While we celebrate the ways in which ICTs, whether digital or not, are useful to those who would bring democracy about around the world, it is equally important to realize that the same tools can be useful to those who would harm other people. Nearly all the problems that arise in offline space find their way into the online environment and in turn give rise to control strategies and contestation over them."

To illustrate this shift from an open to a controlled online space, we have to return to the example of eBay. Perhaps this flagship of the Open Internet is not that "open" after all. Goldsmith and Wu (2008) convincingly show that when eBay became big, methods like rating systems and self-policing were not sufficient to keep the community free of all too damaging attacks from frauds. Unfortunately, cybercriminals simply do not seem to be deeply impressed by reputational damage. In 1999, only 3 years after the rating system was set in place, eBay recruited its own investigators to actively locate cyber thieves and frauds. Working together with law enforcement, these corporate investigators' main goal is to regulate eBay. While it is true that for the vast majority of eBay-users the "robust system of community norms" is sufficient to establish trustworthy interactions, the self-organisation of eBay is nonetheless grounded in "the rule of law and government coercion" (Goldsmith and Wu 2008, 139).

What these studies on control and regulation online show is that the *commons* are not built in a vacuum but in an online environment in which free access to the online world becomes more and more contested (Deibert et al. 2012; Morozov 2011). It is not so much that on an interpersonal level people cannot cooperate based on trust, but that trust can easily be shattered by *external* influences.

Goldsmith and Wu (2008) focus on governmental regulation to deal with these problems. They state that although too aggressive or severe laws can smother the activities in the commons, the question still stands whether "the greatest dangers for the future of the internet come not when governments overreact, but when they don't react at all (Goldsmith and Wu 2008, 145)?"An author like Zittrain (2008) focuses on the "generative" quality of the device or platform itself. Is it possible for users to alter it or write their own code? In his view, the possibility of tinkering with technology is of the utmost importance to keep innovation going. If one wants to keep the Internet open, the devices and applications that flow in this network should be open as well. Lessig (2006) also repeatedly argues that the Internet is not a free and open space but that through code – the way in which the online environment is designed - behaviour online can be regulated and that it is not only gov-

[4] With techno-regulation I refer to the definition of Leenes who states that techno-regulation is the "deliberate employment of technology to regulate human behaviour (Leenes 2010, 21)" cited in Leenes (2011, 149). In his view, states as well as non-states can participate in techno-regulation.

ernments that are regulators online, but commercial parties that are doing it as well (and perhaps even better). All in all it becomes clear that the commons can be threatened in such a pervasive way that self-regulation is no longer sufficient. In other words:

> "The core elements of an open commons have now become the touchstones for a set of constitutive principles to be shored up and defended, as opposed to assumed away as invincible. Perhaps ironically, what were once assumed to be the immutable laws of powerful technological environments are now potentially fragile species in a threatened ecosystem" (Deibert et al. 2012, 8).

## Plessner and Luhmann

Besides the empirical analysis which points to the failure of the Collaborative Consumption movement in taking into account broader tendencies of online power struggles, from a more conceptual-philosophical point of view some objections can also be made against their view on trust and technology.

For Botsman and Rogers, trust and technology, and more specifically trust and the Internet, are intrinsically linked to each other. Online technology is the enabler of trustworthy interactions. Because the Internet makes it possible to interact in a direct manner with other people, new trustworthy relationships can be established online with a spinoff in the offline world. In other domains we also see this kind of connection, for example in the domain of e-commerce where trust is identified as a necessary condition for e-commerce to flourish (Harrison McKnight et al. 2002; McKnight and Chervany 2002; McKnight et al. 2002). After all, if intended buyers do not trust the online shop, they will not order, hence the shop has to close its virtual doors. In the domain of e-government trust and technology also form a well-known couple. In the development of online platforms to facilitate a new, more interactive relationship between government and citizens the question arises regarding how citizens can be persuaded to trust their e-government and to approach it through online channels (Welch 2005; Welch 2003; Prins 2011; Keymolen et al. 2012; Warkentin et al. 2002).

## *It takes two to tango*

This common connection between trust and technology in a diversity of research domains seems to indicate the presence of an underlying association. From a philosophical anthropology perspective, this association can be best explained by the fact that trust and technology are both *strategies* human beings employ to deal with the same question, namely: *'how to act in a world that is overwhelmingly complex?"*.

To elaborate trust and technology as two ways of coping with complexity, I will bring together the work of two German scholars who, contrary to trust and technology, are *not* often connected, namely: Helmuth Plessner and Niklas Luhmann. The former is a philosopher and one of the founding fathers of Philosophical Anthropology. The latter is a sociologist, known for his system theory approach.

At the beginning of his career, Luhmann (1979) wrote the insightful book *Trust* (*Vertrauen*) that, up until today, is very influential in all kinds of trust-research. His fundamental idea that trust functions as a way to *reduce complexity* inherent in human life, is widely acknowledged as the starting point for a modern analysis of trust (Taddeo 2009; Seligman 1997; Möllering 2006). Although later on in his career he frequently distanced himself from philosophical anthropology (Hahn 2004; Fischer 2006), looking at his early work on trust it becomes clear that a substantial part of

his analysis is influenced by concepts and ideas deriving from phenomenology and philosophical anthropology. Above all, in several notes he explicitly and approvingly mentions the work of Helmuth Plessner.

In *Die Stufen des Organischen und der Mensch*, Plessner [1928] (1975)[5] poses the very fundamental and ambitious question: "what is the nature of the preconditions that make human life possible?"Or, in other words, "what is the human *a priori*?" Central to this is the concept of *positionality*, which refers to the differentiated way all living nature - whether it concerns a plant, animal or human being - upholds its own boundaries. To interact with the environment, a living thing has to cross this boundary. The different ways in which this *boundary traffic* is organised, makes it possible to distinguish between an *open* (plants), *closed* (animals) and *eccentric* (human beings) positionality. Moreover, because a living thing has its boundary as part of itself, there is a *cut, an in-between, a distance* or *hiatus* between living things and their environment. *Interaction with the environment therefore always entails the bridging of this hiatus.*

## *It's a complex world after all*

Luhmann and Plessner both acknowledge that while all living systems have to deal with their complex environment, this complexity for human beings is overwhelming -radical even- because they are, unlike animals or plants, *aware* of this complexity and therefore also "…of the possibility of selecting their environment" (Luhmann 1979, 6). They are aware of the *world's contingency*. They know that their life and the world they inhabit could have been different. Where Luhmann takes this awareness as his unquestioned starting point for his analysis of trust, for Plessner this human awareness is one of the central themes of his research. Plessner (1975, 293) writes that a human being"is body, is in its body (as inner life…) and outside the body as the point of view from which it is both (body and inner life)"(translation by Grene 1966, 274). Because human beings can take a position *outside of their centre of experience,* they can also *have a relation towards it*. Consequently, human beings are not only defined by a distance towards their environment –a distance or hiatus they share with all living nature-, they are also defined by a distance towards their centre of experience. This new, *second distance* - or *second mediation* as De Mul (2013) calls it -is the defining element of their eccentric positionality and enables reflexivity.

On an interpersonal level, the act of trust can be seen as a strategy to cope with this complex world. Luhmann emphasizes that trust does not take away this complexity; it only reduces it to a bearable level. Trust enables human beings to bridge the informational gaps they encounter on a daily basis (Möllering 2006; Luhmann 1979; Keymolen 2008). In the end, we are never completely sure about what tomorrow brings nor can we foresee all the actions of our fellow-human beings. Trust is to act 'as if' the future is certain(Möllering 2006; Luhmann 1979; Keymolen 2008). It is "a blending of knowledge and ignorance" (Luhmann 1979, 25). It makes it possible for human beings to act despite irresolvable uncertainties. By the act of trust "certain dangers which cannot be removed but which should not disrupt action are neutralized"(Luhmann 1979, 24). It is a move to indifference (Luhmann 1979, 25).

---

5 Given the scope of this article, it is not my intention to present the reader with a full description of Plessner's anthropological philosophy or reconstruct in detail his main argument. However, I will make use of some of his concepts and ideas concerning the role of artefacts in human life to analyze the role of the internet.

On an instrumental level, using technology is a way of bridging the distance human beings experience in their relation towards the world, their fellow human beings, and themselves. Because of their eccentric positionality, human beings can be everywhere and nowhere. With an existence that is literally "based on nothing" (translation by Grene 1966, 274), they are homeless by constitution. Therefore, they can only lead the life they build up first (Plessner 1975, 310). Without technology, or in a broader sense without culture, human beings would be lost. By producing artefacts, they are able to build and shape their life. Consequently, technology is not just a tool or a simple aid to make our lives easier but an ontic necessity (Plessner 1975; also see de Mul 2003). Human beings are artificial by nature (Plessner 1975).

Notwithstanding the ontological interlocking of human beings and technology, Plessner emphasizes that by producing artefacts only a *temporary* equilibrium can be reached. Artefacts, when they enter the domain of culture, gain their own momentum. They have their "own weight" which makes them stands apart from the people who created them. As a result, artefacts always initiate unintended consequences. They are not neutral instruments sticking to the rules set by their designers and users. In other words, where artefacts are set in place to reduce complexity, *new complexity* instigated by these artefacts arises. Luhmann (1979, 15-16) also remarks:

> "So it is not to be expected that scientific and technological development will bring events under control, substituting mastery over things for trust as a social mechanism and thus making it unnecessary. Instead, one should expect trust to be increasingly in demand as a means of enduring the complexity of the future which technology will generate."

Moreover, Luhmann describes a transition from interpersonal to *system trust*. Living in a globalized world, we have to interact with people and organisations we do not really know very well. From the bus driver to the online shop, from the civil servant to the hospital; all these relations cannot be based on interpersonal trust, simply because cues that instigate trust like a *shared history* or *common friends*, cannot be provided. To ensure these interactions can still take place, we develop *system trust*. For Luhmann, system trust entails two things:"trust in the effectiveness of certain opportunities for communication as a safety valve, should it become necessary, and trust in the general functioning of the system, which enormously increases the effectiveness of these opportunities" (Luhmann 1979, 56). In other words, we do not really have to trust the bus driver as long as we can trust the system he presents: namely the bus company. We trust that the company has checked if he has a drivers licence and is capable of doing his job. Moreover, we trust that if something would go wrong, we can turn to the company to solve the problem. Although Luhmann illustrates his approach of system trust with examples originating from the banking system and political power, it is not far-fetched to extend his view of system trust to the online commons. Online also, people who want to participate in collaborative consumption are depending on the facilitating website. Without a well-developed, operating interface interaction would be impossible. The way this interface is designed and how the rules are set, sorts and shapes the interaction.

## *Critique*

Based on this short presentation of the work of Plessner and Luhmann, my first point of critique will address the *conceptualization of technology* in the work of Botsman and Rogers. The way Botsman and Rogers characterize the Internet as a straightforward enabler of trustworthy interaction seems to lack an important aspect regarding the working of technology. As technology always

initiates new, unforeseen consequences and complexity, originators of Collaborative Consumption initiatives should keep an eye open for the "own weight" of the technology. However, Botsman and Rogers approach the Internet as a neutral service-hatch, enabling people to connect and interact. They do not consider the ways in which this online environment is shaping the building of trust itself. Their rather *instrumental view* on technology makes them blind to the *unintended consequences* of this technology-in-use. In the worst case this blind spot can result in the collapse of online initiatives in the domain of Collaborative Consumption.

This *instrumental view of technology* is closely connected with my second point of critique concerning the focus of Botsman and Rogers on *interpersonal trust*. Their assumption that the Internet is a neutral instrument leads them to conclude that it can function as facilitator of interpersonal trust without any shaping influence on the trust relation it apparently enables. They describe websites with rating systems and reputation schemes, which enable a *transfer* of face-to-face cues for trust such as a *shared history* or *common friends*, to the online context. Or as Botsman and Rogers(2010, xiii) formulate it*:* "… technology is reinventing old forms of trust". This assumption grounds the intention of the Collaborative Consumption movement to cut out the middleman "who polices that trade" and replace him with companies "creating platforms that facilitate self-managed exchanges and contributions", leaving it up to the participants to establish trustworthy interactions (Botsman and Rogers 2010, 92).

However, when we analyse Collaborative Consumption initiatives from a system trust perspective as Luhmann formulates it, the website itself also becomes an object of trust. Because it is through the online system that interpersonal trust is established, the system itself becomes part of this interaction. The system counts. Trust between strangers is not established in a vacuum but in a meaningful context, which influences actors in their willingness to place their trust. It shapes the interaction in unforeseen ways. In other words, companies or other initiators behind the collaborative consumption communities cannot withdraw themselves from the interactions taking place even if they want to.

Moreover, taking into account the fact that technology-in-use is accompanied by side effects, which are not necessarily all for the good, backing away is probably not even a desirable option. Although in most cases participants will solve problems on their own, when they do reach a deadlock they should be able to turn to a third party - the system - to help solve their problem and safeguard trust. Perhaps contra-intuitively, trust is not so much gained by providing a stable online environment, but by successfully intervening in exactly those cases where complexity and uncertainty become acute. It is in these latter cases that trust can be put to the test and participants can find out if their trust is justified (Luhmann 1988).

All in all, this instrumental view of technology resulting in a rather incomplete perspective on interpersonal trust can be partly traced back to the *utopian* and therefore misleading belief in technology as a means to *not only bridge but* also *overcome* the hiatus that defines human beings. Because of this hiatus, the way human beings perceive the world and interact in the world is of a broken, indirect nature. They need a detour via artefacts to establish a meaningful relation with their environment. Due to this mediation, human beings are still able to experience their *indirect* relations to the environment in a *direct* manner. Plessner speaks of *meditated immediacy*; characterizing these relations as both direct and indirect. Nonetheless, human beings have the tendency to dismiss the aspect of indirectness and act as if their interactions are simply of a *direct* and stable nature. They try to set aside the triviality (*Nichtigkeit*) of their existence and flee to a *utopian world*

–Plessner speaks of a *utopian standpoint* in which they can find a final ground, a *definitivum* that provides them with a predictable environment. While Plessner describes how this desire to find a final ground leads human beings to the *domain of religion*, nowadays this domain has to move over in favour of the *domain of technology.* As de Mul (2001 20 translation by author) notes: "in the secular world,… the Internet functions as the 'holy grail'. It is a resource that promises us attributes which up until now belonged to God: omniscience, omnipresence, and omnipotence". As Plessner remarks that it is not easy to be an atheist, it is also not easy to be a non-instrumentalist. After all, it implies one has to be prepared to take on the difficult task to live in an open and unstable, even sometimes capricious, online world.

## Interpersonal system trust

If interpersonal trust online, trust between you and me, is not just about you and me, but is influenced and shaped by the medium that facilitates this interaction, a new level of analysis is needed. Bringing together the main issues coming forth from the empirical findings and the conceptual findings presented in this paper, I would like to propose the concept of *interpersonal system trust* to open up a new perspective on the workings of Collaborative Consumption.

This new concept is needed because it is not enough to just replace interpersonal trust with Luhmann's system trust. First of all, it would do no justice to the justified observation of Botsman and Rogers that interpersonal trust is an important and even necessary basis for online interaction. Moreover, where Luhmann focuses on systems, which stand somewhat apart from the people who use it, making these systems only controllable by a handful of experts, the *online platform as a system* has another configuration. While we have to expound our point of view on what users can and cannot do, when looking at the initiatives of the Collaborative Consumption movement, it nonetheless becomes clear that there is a lot of resilience and knowledge in these online communities. It must be possible for these users to actively take into account the workings of the system influencing the development of trust.

In the concept of interpersonal system trust, the *interpersonal aspect* stands for the experience participants of Collaborative Consumption initiatives have when interacting online. Although their interaction is in effect indirect, they experience it in a direct manner, through the use of artefacts or, more specifically, the website or online platform. As long as the technology works, or as Heidegger (2010) would say as long as the artefact is 'at hand', the online world functions as a background of which users are not really aware. This interpersonal aspect is what Botsman and Rogers pinpoint when they talk about trust. They focus on trust building between strangers, assuming that the platform, which enables this interaction, is functioning as a neutral facilitator.

However, by adding the *system element* to the concept of interpersonal trust, one also has to take into account the *mediating function*[6] of the system itself when analyzing the development of trust between participants. What does this system 'add' to the interaction? How does it invite users to act in a certain manner? And how are the users shaping the system? These questions of mediation lead to a more profound analysis of trust in which the online context, provided by the system, is placed at the heart of the interpersonal interaction.

---

6 In the domain of the philosophy of technology, P.P. Verbeek has extensively written about the mediation of technology. See Verbeek (2010, 2000, 2011c; Verbeek 2011a)

## *Context, code, company, and country*

Given the nature and scope of this paper, I cannot provide a full description of all the aspects of the system – in our case an online platform or website in the domain of Collaborative Consumption - that have to be taken into account in order to analyze interpersonal system trust. Nonetheless, influenced by the works of Zittrain (2008), Lessig (2006), Deibert et al. (2008, 2010, 2012) Goldsmith and Wu (2008), Wu (2011), Morozov (2011) (see paragraph 2.5 *Controlled space*), some initial guidelines regarding the influence of systems on online trust can be put forward. I will limit myself to the following four c's of interest: *context, code, company* and *country.*

The influence of the *online context* on interpersonal trust seems to be the most obvious one. The way in which a website is designed pre-sorts the options users have in order to shape their online interactions and as a result the way trust is established –is there an option to post a photo? Can a user write a review? Is there a possibility to check someone's reputation? -. These elements of context neatly fit the view of Botsman and Rogers (2010) who see it as the role of the "curators" of the Collaborative Consumption initiatives to create an environment in which trust online can thrive. It is up to the users to take on these tools to develop an online reputation and 'materialize' their interactions, making them visible to the whole community. However, this user-level perspective on the way trust is established strongly depends on the way the online environment has been built.

This brings us to the second aspect of the system which influences trust, namely: *code*. As the Internet is functioning as the most important infrastructure for Collaborative Consumption, it is important to evaluate the techniques employed to build, use, and maintain the platforms that populate this network. In this respect there are some important choices to be made by the Collaborative Consumption movement. From the perspective of interpersonal trust it is probably beneficial to choose a platform with a closed design that is easily manageable and steady-in-use; a so-called 'walled garden'. It is simply more convenient to control and manage a closed device or platform than an open one. However, from an ideological point of view this option would conflict with the core values of the Collaborative Consumption movement, which stands for openness, participation, and belief in the commons. To keep the online environment *open* and the interactions *trustworthy*, participants themselves should be attentive to personal safety measures such as updated firewalls and strong passwords. In addition, they should be willing to review their interactions and give feedback to the community to make the reputation scheme and the building up of trust online work.

Then again, what users can do to protect their personal information depends on another aspect of the system, namely, the *company* –or curator- which owns the website or platform. Does this company share personal information with third parties? What is its business model? Does it make use of profiling or data-mining?- . Taking into account the company as part of the interpersonal trust relation requires critical self-reflection on the part of the Collaborative Consumption movement. Are the interests of the company or curator in line with the interests of the users or are there possible points of conflict, which may influence the trust invested in the collaborative project? In particular, in the Collaborative Consumption movement, users should not only be able to have full access to their own data, but should also be informed about the specific workings of the platform and perhaps even have the power to alter these workings. However, on this level also interdependency can be detected.

This brings us to the final aspect, namely, *country*, which refers to the way in which the company is willing to interact with governments to regulate the online environment. The relation company-government can take on different forms. Is the company safeguarding the community by proactively monitoring the platform to catch frauds and other malicious users, like eBay is doingnow? Or is the online platform used by the government as a regulatory means, providing officials with information on suspected movements online?Up until now Collaborative Consumption counts on self-regulation, but as the eBay example illustrates, when the stakes get high, this might not be enough. A minimal basis of top-down regulation can strengthen the development of bottom-up trust, which is one of the core aspects of the movement. In addition, if participants of the Collaborative Consumption movement want to keep the character of their community open and free, preserving the commons, they should not ignore the 'offline' government but actively lobby and apply to their representatives. To ensure that the online commons are not smothered by over-aggressive legislation, the Collaborative Consumption movement should remain alert to new political developments and sit around the table with policy-makers.

## Conclusion

All in all, it becomes clear that the development of interpersonal trust in Collaborative Consumption is much more stratified and richer when one takes into account the workings of the system in this process. Exploring *interpersonal system trust* not only opens up a more comprehensive perspective on 'how trust works' in relation to the medium at hand, it also reveals some urgent questions concerning the way in which the Collaborative Consumption movement manages its platforms and how it can relate in a meaningful way to the system itself. Where Collaborative Consumption focuses on the way individuals can share resources and services online, based on trust, I argue in this paper that the development of *trust online isnot just about you and me*, but about you, me and the system that brings us together. Only when users are aware of the workings of technology and the mutual shaping effects technology-in-use has, can trust thrive online.

## References

Angwin, J. (2010). The web's new gold mine: your secrets. *The Wall Street Journal*.

Axelrod, R. (1984). *The Evolution of Cooperation* New York: Basic Books.

Bauwens, M., Mendoza, N., & Iacomella, F. (2012). A Synthetic Overview of the Collaborative Economy. Orange Labs, P2P Foundation.

Benkler, Y. (2006). The wealth of networks : how social production transforms markets and freedom New Haven Conn.: Yale University Press.

Benoist, E. (2008). Collecting Data for the Profiling of Web Users. In M. Hildebrandt, & S. Gutwirth (Eds.), *Profiling the European Citizen. Cross-Disciplinary Perspectives* (pp. 169-184): Springer Netherlands.

Botsman, B. (2012). The currency of the new economy is trust. In Ted (Ed.), http://www.ted.com/talks/rachel_botsman_the_currency_of_the_new_economy_is_trust.html.

Botsman, R., & Rogers, R. (2010). *What's mine is yours : the rise of collaborative consumption* (1st ed.) New York: Harper Business.

Brodwin, D. (2012). The Rise of the Collaborative Consumption Economy. http://www.usnews.com/opinion/blogs/economic-intelligence/2012/08/09/how-collaborative-consumption-reinvigorates-our-economy. Accessed December 4th 2012.

Chesbrough, H. W., Vanhaverbeke, W., & West, J. (2006). *Open innovation : researching a new paradigm* Oxford: Oxford University Press.

de Mul, J. (2001). Afstand in filosofisch perspectief. In V. J. J. M. Bekkers, & B. Foederer (Eds.), *ICT, afstand en compliance. Internet en Openbaar bestuur* (pp. 17-23). Den Haag: Belastingsdienst.

de Mul, J. (2003). Digitally mediated (dis)embodiement. Plessner's concept of excentric positionality explained for cyborgs. *Information, Communication & Society, 6*(2), 247-266.

Deibert, R. (2008). *Access denied : the practice and policy of global Internet filtering* (The information revolution and global politics)Cambridge, Mass.: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2012). *Access contested : security, identity, and resistance in Asian cyberspace information revolution and global politics* (Information revolution and global politics) Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R., Zittrain, J., & OpenNet Initiative. (2010). *Access controlled : the shaping of power, rights, and rule in cyberspace* (Information revolution and global politics) Cambridge, Mass.: MIT Press.

Fischer, J. (2006). Philosophische anthropologie - ein wirkungsvoller denkansatz in der deutschen soziologie nach 1945/Philosophical anthropology - an important approach in post-war german sociology. *Zeitschrift Für Soziologie, 35*(5), 322-347.

Friedman, T. L. (2005). *The world is flat : a brief history of the twenty-first century* (1st ed.)New York: Farrar, Straus and Giroux.

Goldsmith, J. L., & Wu, T. (2008). *Who controls the Internet? : illusions of a borderless world* New York: Oxford University Press.

Grene, M. (1966). Positionality in the Philosophy of Helmuth Plessner. *The Review of Metaphysics, 20*(2), 250-277.

Hahn, A. (2004). Der Mensch in der deutschen Systemtheorie. In U.B. et al (Ed.), *Vernunft-Entwicklung-Leben. Schlüsselbegriffe der Moderne. Festschrift für Wolfgang Eßbach* (pp. 279-291). München: Fink.

Hardin, G. (1968). The Tragedy of the Commons. *Science, 162*(5364), 1243-1248.

Harrison McKnight, D., Choudhury, V., & Kacmar, C. (2002). The impact of initial consumer trust on intentions to transact with a web site: a trust building model. *The Journal of Strategic Information Systems, 11*(3), 297-323.

Heidegger, M., Stambaugh, J., & Schmidt, D. J. (2010). *Being and time* (SUNY series in contemporary continental philosophy)Albany: State University of New York Press.

Hildebrandt, M., & Gutwirth, S. (2008). Profiling the European citizen : cross-disciplinary perspectives New York: Springer.

InformationWarfareMonitor (2009). Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor Reports*. Toronto.

internetworldstats (2012). http://www.internetworldstats.com/stats.htm. Accessed 12-13 2012.

Keymolen, E. (2008). Vol Vertrouwen. Over online (on)zekerheid en de brug van het vertrouwend handelen.Master thesis. Erasmus University Rotterdam, Rotterdam.

Keymolen, E. (2013). A Moral Bubble. The influence of online personalization on moral repositioning (forthcoming).

Keymolen, E. L. O., Prins, J.E.J, Raab, C. (2012). Trust and ICT: New Challenges for Public Administration In v. d. Donk, W., Thaens, M. (Ed.), *The Coming of Age of ICT in Public Administration* (pp. 21-35). Amsterdam: IOS Press.

Leenes, R. E. (2010). Harde lessen: Apologie van technologie als reguleringsinstrument Tilburg: Universiteit van Tilburg.

Leenes, R. E. (2011). Framing techno-regulation: an exploration of state and non-state regulation by technology. *Legisprudence, 5*(2), 143-169.

Lessig, L. (2006). *Code : version 2.0* ([2nd ed.)New York: Basic Books.

Luhmann, N. (1979). *Trust and Power. Two works by Niklas Luhmann* (H. Davis, Trans.)New York: John Wiley & sons Ltd.

Luhmann, N. (1988). Familiarity, Confidence, Trust: Problems and Alternatives. In D. Gambetta (Ed.), *Trust: Making and Breaking Cooperative Relations* (pp. 94-107): Blackwell Publishers.

Malnight, T., & Keys, T. (2012). A top ten for business leaders. http://www.economist.com/blogs/theworldin2013/2012/11/global-trends-2013?fsrc=nlw%7Cnewe%7C11-26-2012%7C4248303%7C109444847%7CEU. Accessed 12-13 2012.

McKnight, D. H., & Chervany, N. L. (2002). What trust means in e-commerce customer relationships: An interdisciplinary conceptual typology. *International Journal of Electronic Commerce, 6*, 35-60.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information systems research, 13*(3), 334-359.

Möllering, G. (2006). *Trust, Reason, Routine, Reflexivity* Amsterdam: Elsevier.

Morozov, E. (2011). *The net delusion : the dark side of internet freedom* (1st ed.) New York: Public Affairs.

Plessner, H. (1975). *Die Stufen des Organischen und der Mensch; Einleitung in die philosophische Anthropologie* (2., um Vorwort, Nachtrag und Register erweiterte Aufl. ed.) Berlin,: De Gruyter.

Plessner, H. (2003). *Die Frage nach der Conditio humana* (Gesammelte Schriften VIII).1961 Frankfurt am Mein: Suhrkamp.

Power, A., & Kirwan, G. (2012). Trust, Ethics and Legal Aspects of Social Computing. *Proceedings of AISB/IACAP World Congress 2012*, 98-103.

Prins, C., D. Broeders, H. Griffioen, A.-G. Keizer, E. Keymolen (2011). *iGovernment* Amsterdam: AUP.

Rheingold, H. (1993). The virtual community : homesteading on the electronic frontier Reading, Mass.: Addison-Wesley Pub. Co.

Seligman, A. B. (1997). *The Problem of Trust* Princeton: Princeton University Press.

Taddeo, M. (2009). Defining Trust and E-Trust: From Old Theories to New Problems. (pp. 23-35): IGI Global.

Tapscott, D., & Williams, A. D. (2006). *Wikinomics : how mass collaboration changes everything* New York: Portfolio.

Turkle, S. (1984). *The second self: computers and the human spirit* New York: Simon and Schuster.

Turkle, S. (1995). Life on the screen: identity in the age of the Internet New York: Simon & Schuster.

Verbeek, P.-P. (2000). *De Daadkracht der Dingen* Amsterdam: Boom.

Verbeek, P.-P. (2010). Accompanying Technology: Philosophy of Technology after the Ethical Turn. *Techné, 14*(1), 49-54.

Verbeek, P.-P. (2011a). De grens van de mens : over techniek, ethiek en de menselijke natuur Rotterdam: Lemniscaat.

Verbeek, P.-P. (2011b). *Moralizing technology : understanding and designing the morality of things* Chicago ; London: The University of Chicago Press.

Verbeek, P.-P. (2011c). Subject to technology: on autonomic computing and human autonomy. In M. Hildebrandt, A. Rouvroy (Ed.), *Law, Human Agency and Autonomic Computing* (pp. 27-45). New York: Routledge.

Walsh, B. (2011). Today's Smart Choice: Don't Own. Share. http://www.collaborativeconsumption.com/buzz-and-press/Today%20s%20Smart%20Choice%3A%20Don%20t%20Own.%20Share%20-%2010%20Ideas%20That%20Will%20Change%20the%20World%20-%20TIME.pdf. Accessed 4th of December 2012.

Warkentin, M., Gefen, D., Pavlou, P. A., & Rose, G. M. (2002). Encouraging citizen adoption of e-government by building trust. *Electronic Markets, 12*(3), 157-162.

Welch, E., Hinnant, C. & Jae Moon (2005). Linking Citizen Satisfaction with E-Government and Trust in Government. *Journal of Public Administration Research and Theory, 15*(3), 371-391.

Welch, E. C. H. (2003). Internet Use, Transparency, and Interactivity Effects on Trust in Government. *hicss, 5* (36th Annual Hawaii International Conference on System Sciences), 144a.

Wu, T. (2011). The master switch : the rise and fall of information empires (1st ed.)New York: Alfred A. Knopf.

Zittrain, J. (2008). *The future of the Internet and how to stop it* New Haven [Conn.]: Yale University Press.

# Should I trust my gut feelings or keep them at a distance? A prospective analysis of point-of-care diagnostics practice

Federica Lucivero
University of Tilburg
Tilburg Institute for Law Technology, and Society (TILT)
✉f.lucivero@tilburguniversity.edu

Lucie Dalibert
University of Twente
Department of Philosophy
✉l.dalibert@utwente.nl

**Abstract** Point-of-care devices can be expected to change current medical practices, create new ones and raise crucial questions concerning responsibilities in healthcare. In this paper we explore the issue of point-of-care devices and trust. More specifically, we draw attention on a dimension of 'trust' which is closely related to point of care devices, namely the potential tension in future users of emerging point-of-care devices between trusting their experience of a symptom and trusting the technology. We will take a case study approach in which we focus our attention on an emerging case of point-of-care diagnostics: the Nanopil. After introducing this case, we introduce the concept of mediation, as elaborated by Verbeek on the basis of Ihde and Latour's work. This concept provides a good analytical tool to address the question of how a point of care diagnostics, like the Nanopil, creates new meanings and practices. Our analysis shows how the Nanopil is a hybrid of proximity and detachment from the user. We conclude with some final considerations explaining why this type of analysis of such a close-and-yet-distant relationship with the user is important in the innovation process.

**Keywords** point-of-care diagnostics, trust, mediation, body, philosophy of technology

## Introduction

In the media, technology developers' discourses and academic research, it is increasingly pointed out that 'early diagnostics' is a solution for the problems currently faced by Western healthcare systems of reducing treatment costs (Leifer 2003; Banerjee and Wittenberg 2009; Hogg et al. 2005). By detecting diseases at an early stage of development, therapeutic treatments are expected to be more effective and healthcare costs effectively reduced. Another type of innovation in healthcare that responds to a similar need is telemedicine. By creating a system in which the medical personnel enter peoples' homes in a virtual way, through the use of online portals, web-based platform and smart sensors, costs of care personnel can be reduced and the efficiency of the system increased (Mosis et al. 2007; Noel et al. 2004; Voight 2012). Interestingly, so-called 'Point-of-care' diagnostic tests address the aim of reducing healthcare costs by clustering both expectations of early diagnostics and telemedicine. Commonly defined as 'the analysis of clinical specimens as close as possible to the patient'[1], these devices allow patients to perform by themselves the test for early screening of health conditions from the comfort of their home.

These innovations can be expected to change the current distribution of roles within healthcare. First, as Gerard de Vries remarks, we are assisting to a change from clinical, complaints-induced medicine to a non-complaints-bund, health risk and prevention-oriented predictive medicine (de Vries 2005). Predictive medicine is based on new knowledge assumptions and intro-

[1] MacGraw-Hill Concise Dictionary of Modern Medicine 2002

duces new practices: sickness and health are redefined here in terms of health risks and the practice is oriented towards prevention rather than cure.

> The shift towards predictive medicine includes a reorientation of goals (from cure to prevention), the emergence of a statistical style of medical reasoning and of concepts of health and disease that replace the old dichotomy between health and disease by a continuum, i.e. a new medical epistemology. The shift also includes changes in the relations between doctors and their patients and in the social organization of the healthcare system at large. Medical practice moves to new spaces and involves an array of new actors. Predictive medicine requires co-operation of clinicians with a large number of non-clinical professionals, inside and outside the traditional medical field: epidemiologists, geneticists, but also psychologists, health educators, and social workers […] Medical action thus moves from consultation-room-based contacts induced by an individual's complaint, to interactions in a complex network of institutions. Individual who may not have asked for this are invited for diagnosis and risk assessment and are addressed by health education's targeted campaigns (de Vries 2005, 159)

Second, point-of-care devices, not only introduce a predictive medicine paradigm in the relationships that people have with their health conditions, they are also used as do-it-yourself, or self-tests. This specific aspect of point-of-care devices also influences healthcare practices. This has been pointed out, for example by Annemarie Mol, who analyzes the case of a monitoring device for blood sugar measurement (Mol 2000). When this device was introduced in the routine of diabetic patients, it did not simply fulfill a function of measuring the level of sugar in the blood, but it created a practice of self-monitoring. This new practice not only implied different actions, behaviors and routines, but also new standards of normality and different relations between a patient and their own body.

Therefore, point of care devices can be expected to change current medical practices, create new ones and raise crucial questions concerning responsibilities in healthcare. Some scholars have pointed out how this shift in responsibilities brought about by innovations in medicine raises questions concerning users trust in this services (Vedder and Vantsiouri 2013). Using the example of remote monitoring and treatment system, as vital sign monitoring for elderly or chronic patients, the authors examine the users' trust (as a pre-condition of acceptance) in these technologies. The dimensions of trust that are analyzed concern the trust in the fact that a system will be in place to protect sensitive data and liability for the misuse or damage caused by the system.

In this paper we will explore the issue of point-of-care devices and trust. More specifically, we will draw attention to a dimension of 'trust' which is closely related to point of care devices, namely the potential tension future users of emerging point-of-care devices may experience between trusting their experience of a symptom and trusting the technology. In order to do this, we will take a case study approach in which we will focus our attention on an emerging case of point-of-care diagnostics: the Nanopil[2]. After introducing the case, we will introduce the concept of mediation, as elaborated by Verbeek on the basis of Ihde and Latour's work. This concept provides a good analytical tool to address the question of how a point of care diagnostics, like the Nanopil, creates new meanings and practices. Our analysis will show how the Nanopil is a hybrid of proximity and detachment from the user. We will conclude with some final considerations explaining why this type

[2] Since expectations on the 'Nanopil' have mainly circulated in a Dutch context, we will keep the Dutch form 'Nanopil' rather than the English 'Nanopill'. Some English reviews of the project circulate on the web, but they are mainly quotations of press releases from the University of Twente. In the text, we will also refer to the Nanopil with the acronym 'NP'.

of analysis of such a close-and-yet-distant relationship with the user is important in the innovation process.

## A case-study of point-of-care diagnostics: the Nanopil

Between 2009 and 2011 in the Netherlands, television, several national newspapers, magazines, and a children's book presented images of the Nanopil (NP). The NP was presented as an ingestible capsule that contains a miniaturized chip that is able to perform an in vivo analysis of intestinal fluid, detect the presence of biomarkers for colorectal cancer, and communicate the result to the outside via radiosignalling. Although the development of such a complex pill may appear futuristic, Professor van den Berg remarked at the time that there was already a so-called "Camera pill" (PillCam), which could take pictures of the interior of the gastro-intestinal channel and send these to the outside of the body (2009). Professor Pinedo, the oncologist who conceived of the Nanopil idea, anticipated (in 2009) that in 5 to 10 years doctors would be able to use the pill in hospital settings (Melchior 2009).

Albert van den Berg (2009), professor of Miniaturized Systems for (Bio)Chemical Analysis at the University of Twente (the Netherlands) leads the research group that is currently investigating the feasibility of such a device. As he points out, on the occasion of the annual ceremony commemorating the founding of the University of Twente,

> Colonic cancer is one of the most common cancers in people over the age of 50. The Dutch Health Board has already advised endoscopic or colonoscopic screening for people in this age group. But this is a painful and uncomfortable experience. Moreover, it presents a logistical nightmare and nothing is found in 95% of cases. What we need is a simple first-line test. The only alternative at present is a faeces test, but eventually, a nano-pill [sic] will provide a much more patient-friendly alternative.[3]

Prof van den Berg explains that the available methods for detecting colorectal cancer are painful and expensive, like in the case of endoscopic investigations. When simple screening tests are available, like the Fecal Occult Blood Test (FOBT), they are not user friendly. The FOBT is uncomfortable because it requires the screenee to collect a stool sample and to send it to the laboratory to check for blood traces: this is 'not the best hobby' as the oncologist remarks in an interview, or, as a scientist exclaims, it is 'a medieval practice!'. The NP proposes a 'technological' solution to this discomfort. The promise is therefore to provide the users (both the screenee and the general practitioner) with a means to effectively monitor bowel condition in an easy and comfortable manner. The NP offers a way for people to monitor their health and to detect abnormal statuses at a very early stage since it tests for the molecular causes of cancer and it is a clean, non-medieval, modern way of testing and receiving results.

> Albert van den Berg clearly imagines the use of this pill: a population screening program in which, for example, every three years all people aged over 50 are invited to swallow a nanopil. In the event of a positive result, a colon examination will follow. "*I heard from the medical specialists that in this way the number of examinations, surgeries and deaths from colon cancer will decrease sharply. After all, the sooner something is found, the easier it is to treat the tumor*." (Melchior 2009)

The promises of the NP emphasize cost-effectiveness, the increased chance of saving human lives, the increased autonomy of the user, and a decrease in discomfort as valuable expected out-

[3] A Pill with a Lab Inside http://www.azonano.com/news.asp?newsID=15039Posted December 8th, 2009.

comes of the introduction of the device in the colorectal cancer screening and diagnostic practice. The NP is expected to change the current screening practice by involving the patient in a self-monitoring practice and the medical practitioner in a monitoring system that is computer based and beyond the traditional laboratory or doctor's room. Within this context, how can we expect actors' roles and responsibilities to be altered? How can we expect trust relationships within these practices to be altered by this type of innovation in healthcare? Before addressing the question of how a point-of-care device like the Nanopil can be expected to alter users' roles and responsibilities, we will introduce some conceptual and methodological tools that inspire our approach to the question.

## Conceptual tools and methodological remarks

In order to explain how artifacts influence and determine human epistemologies and practices, Peter-Paul Verbeek explores the concept of 'mediation' within the post-phenomenological tradition, drawing on Don Ihde's work (1990). Technologies 'mediate' our relationship with the world by providing a representation of the world that has to be interpreted. The thermometer is a good example of this type of so-called 'hermeneutic' mediation: such a device stands in between the world and our understanding of it. Indeed, when using a thermometer we do not perceive or experience the temperature directly, but we can 'read' it. A more complex example concerns imaging instruments introduced into the obstetrician's room (Verbeek 2011). By allowing parents to see the fetus with greater precision, these technologies alter the way the world presents itself to the future parents. The images of the fetus invite parents to perceive, experience and understand the world in a different way than a non-technologically-mediated perception would allow. These new ways of perceiving and experiencing involve 'opening' up the world in a different way and changing the universe of meaning; for example, by being able to see the fetus and its human resemblance, prospective patients may attach a new meaning to it. Re-articulation of meanings and interpretations of reality also affect the values attached to aspects of that reality. For example, being able to see the human figure in a fetus might influence the importance that parents attribute to it or the moral status that they ascribe to it.

Building on Bruno Latour's and Madeleine Akrich's'script theory' (Akrich 1992; Latour 1992; Akrish and Latour 1992), Verbeek emphasizes a second type of technological 'mediation' that he refers to as 'pragmatic'. For example, the cumbersome shape and weight of some hotel key-chains encourages the users to return the room key to the reception before leaving the hotel (Akrich and Latour 1992). The key-chain contains a 'program of action' inscribed in it (Latour 1992): a non-written instruction of how it should be used and by whom: "*technical objects define a framework of action together with the actors and the space in which they are supposed to act*" (Akrich 1992: 208). In this space, roles and responsibilities are allocated to actors in a way that re-designs the previous practice. For example, the alarm system integrated in modern cars is activated when the seat belt is not buckled. In this way, the design of modern car invite drivers to wear a seat belts: the respect of the rule of safety on the road is not left to the driver's moral reasoning alone, but it is distributed between the human and the non-human actor. This artifact's design mediates human actions in the world in such a way that some actions will be allowed and others forbidden. In this sense, the artifact prescribes, obliges, permits, prohibits and disciplines users' behavior. This is what Akrich defines as the "moral" content of objects (*ibidem:* 219). The moral connotation of this relation emerges in the delegation of moral actions to the technology.

If the relationships between humans and technologies are so rich, we should reconsider the 'instrumentalist' expectations that a new and emerging technology like the Nanopil simply offers a tool for more effective and comfortable screening. These expectations hide a metaphor of linearity according to which technology is a direct means to a(n) (un)desirable end. However, one can expect that, in addition to comprising a tool with which to improve the current state of affairs, these new technologies create *new* meanings and practices in different areas of life (Geels and Smits 2002). In this paper, we take this perspective and we explore the mediating potential of the Nanopil.

In so doing, we will take methodological inspiration by Annemarie Mol's philosophical narratives or 'empirical philosophy' stories (Mol 2000). As she remarks in relation to her work on blood sugar measurement devices, her stories are assembled based on empirical fieldwork(observations, interviews and reviews of professional literature), but they are not told for empirical purposes. Instead of offering a collection of empirical data or patients' experience for generalization purposes, Mol aims at doing theoretical work of a 'heuristic' kind. This means that she uses stories, gathered in concrete times and places, to "*develop or strengthen in their readers the so urgently needed open eye and keen sensitivity for the kinds of effects diagnostic techniques may have when they are put to use*" (Mol 2000, 10).

Telling 'empirical' stories about technologies that are still emerging is arduous since the stories will be intrinsically fictional. The Nanopil is not there yet and every story about its role in changing practices cannot be grounded on empirical observations. In the case of emerging objects, we cannot de-scribe the program of action or prescription as we would do in the case of existing objects, like the previously mentioned car and key-chain, by observing the objects, their interactions with users and the intentions of designers[4]. However, as de Laat points out we can reconstruct the 'fictive script' of these emerging objects, that is the expected involved actors, their tasks and relationships (de Laat 1996 and 2000). Such reconstruction is based on funding proposals, public oral communications, patents and interviews with actors involved in the development of the emerging technology at stake (scientists/engineers, policy makers, funding institutions, venture capitalists, policy makers, etc).

Therefore, our stories, although based on fieldwork (see Lucivero 2012), are mostly explorations of expectations surrounding the Nanopil and thick illustrations of their 'fictive scripts'. These explorations aim at 'thickening' the discourses about the use of the NP as a tool for more efficient and effective screening by fleshing out the details and concrete practices in which this device is expected to change. In the following, we first tell a story about current screening practices, then, we tell two stories of how the NP, as it is currently conceived, will mediate screening practices. That is, after we have explored current expectations of how responsibilities and tasks will be allocated to the NP user, we will explore the expectations of how the Nanopil-mediated screening practice will alter the users' perceptions of the world and themselves. These stories lead us to reflect on how emerging point-of-care devices raise new compelling issues related to trust.

[4] A methodological guidance and examples on how to conduct 'script analysis' is sketched in (Akrich 1992).

## Nanopil's scripts

### *The practice of screening*

The importance of monitoring oneself is not an emerging practice. In fact, it is quite rooted in our society; the idea that our body manifests some signs that inform us about our health condition is not new to us. Our grandmothers learned it from their mothers and they are still worried when our cheeks look rather pale or when there are white stains on our nails. Our grandmothers also know that if there is blood in their stool matter, there is something wrong going on in their body and they should contact the doctor. The practice of observing abnormal signs appearing on our body involves noticing something that should not be present. This practice can involve routine self-checking and relates to some feeling of repugnance on the realization of signs of decay on our body: we see pimples, blood, cuts, leakages or crusts, we sense bumps or nodes or we feel pain or tingling.

This routine self-checking differs however from systematic and scientifically informed self-monitoring. When women are instructed to palpate their breasts as routine self-monitoring for breast cancer, they are taught how to *look for* eventual nodes. Nodes do not appear on the body; rather women are asked to search for indications that something might be wrong with their health. The presence of blood in the stool, a change in bowel habits, diarrhea, constipation or a feeling that the bowel does not empty completely, abdominal discomfort, smaller stools than usual, and constant fatigue are symptoms of colorectal cancer[5], symptoms that a GP might ask patients to investigate in a daily practice of self-monitoring.

Tests like the Fecal Occult Blood Test (FOBT) are similar to breast palpation in the sense that the users are asked to interact with their body (or a product of it). However, these tests differ: while the subject of breast palpation can experience the problem herself by sensing a node under her fingertips, the subject of the FOBT does not have direct experience of the problem. Her interaction with her body (or its product) ends with the act of collecting the sample. Subsequently, the responsibility of monitoring is transferred to the lab and eventually to the GP who communicates the result. In this practice of monitoring, the subject is detached from the experience of her health condition.

### *The Nanopil: Allocating tasks and re-distributing responsibilities*

The discourses about the Nanopil are underpinned by a rhetoric of 'comfort', emphasizing the desirability of a test that is acceptable, easy and patient-friendly. By being able to test yourself in the comfort of your own home, whenever you want, and by freeing the user from being dependent on laboratories for results, the NP is expected to fulfill this promise. Furthermore, this device is presented as a clean modern test that saves the user from the unpleasant task of sampling her feces.

In fact, these ideas are inscribed in the NP's design. The miniaturization of the analyzing platform and its integration into a capsule allows the user to ingest it. The manual collection of samples becomes superfluous, since the pill gathers the sample and analyzes it from within. In this sense, the pill takes care of the whole monitoring process. The screenees are left with information on their mobile phones rather than having to involve themselves in an active and unpleasant prac-

[5] See http://www.testsymptomsathome.com/mtl01_colon_facts.asp.

tice. The screenees do not have to move and touch their body as in breast or testicular cancer self-screening; they are relieved from the task of peering at their skin to map new and abnormal moles; and they do not have to bend over the toilet to collect feces samples. The technology is expected to liberate people from the discomfort of monitoring, the distaste of dealing with their body, and the embarrassment of describing repugnant signs and symptoms to their GP. The pill liberates users from this awkward link with their diseased body.

Indeed, the practice of self-monitoring requires the screenee to perform some tasks. In contrast to the FOBT, the Nanopil does not require the user to interact with her stool matter, to sample it and send it to the lab. However, the user is invited, or even directed to perform other tasks, like ingesting a laxative before taking the pill. This task is inscribed in an artifact, since one of the main conditions for the pill to work is the ingestion of a laxative to clear up the bowel and to allow the pill to traverse it. Moreover, depending on the interface chosen to communicate results to the user, the user is either required to put on a belt and receive a text on her mobile phone or to look at the color of the stool. Such a test requires strong self-discipline and clashes with some standards of well-being and user-friendliness that the user might have.

### *The Nanopil: Changing meanings and self-perception*

The NP also 'mediates' in the same way a thermometer would do. Reading off the pill is like reading off a thermometer in the sense that the device tells something about ourselves without resulting in a direct sensation. The idea that the pill will be better than other available screening devices (excluding the colonoscopy) is grounded on the promise of molecular diagnostics. The developments of molecular biology in the last twenty years have shown that the presence of diseases can be best detected at a molecular level long before perceivable symptoms appear (Demidov 2003, Poste 2001).

Such scientific knowledge is mobilized by the Nanopil developers to justify why traditional self-monitoring, such as 'peering into the toilet', is not enough to detect early disease stages: there are some phenomena that cannot be observed by the naked-eye. A currently available screening device such as the FOBT detects the presence of blood in the feces that is hidden ('occult') to human beings, but visible when a sample of stool matter is analyzed in the lab. The NP brings this observation to a new level of molecular investigation. By detecting molecular markers in the intestinal liquor, the NP seeks a different type of 'sign' than the FOBT does. The latter detects the presence of blood in the feces. This could be interpreted as a sign of the presence of a tumor that causes the intestinal walls to bleed. The FOBT provides information about a disease in a stage that might be already advanced. Furthermore, the presence of occult blood in the stool could also be a sign of something else, for example the inflammation of anal veins (hemorrhoids). Finally, the absence of blood does not necessarily indicate the absence of a tumor: indeed, the tumor might be growing but not bleeding.

The NP provides information that differs from that of the FOBT; it provides information about a cancer that does not yet exist, but has the molecular triggering conditions that can lead to its development. In fact, the pill detects an abnormal status before any (visible or occult) symptom occurs. By analyzing the molecular mechanisms that underlie the disease, the pill enables detection of the disease at a much earlier stage, when it is still invisible. In this way, a therapeutic or surgical intervention can take place at an even earlier stage, increasing the chances of survival and reducing health care costs.

In the logic of these expectations and discourses, molecular knowledge is considered to be superior, because it is more accurate than the behavioral knowledge; it offers a means of returning to the subcellular, molecular level[6], a level that is expected to be more informative. Our visible body is less informative than our invisible cells according to molecular medicine. It contains less information about ourselves, or it gives us information at a stage at which we cannot intervene with the same efficiency. It looks like the pill knows you best, better than you know yourself even.

The Nanopil can be expected to contribute to a change in the way we self-monitor our health, in addition to the way in which we relate to our body. It has an impact on our practices of being ill, being healthy, and being concerned about our health. In this sense, the practice of self-monitoring introduced by the Nanopil affects several dimensions of our beliefs and perceptions on our personal identity and relations to others.

## Exploring the scripts: point-of-care devices mediating trust

As in the case of the blood sugar measurer used by diabetic people, also we can expect that the NP will not simply improve a current practice, but will create a new practice. As we showed, the users have to perform some tasks like clearing their bowel with a laxative, wearing a belt to detect the NP signal, having their mobile phone or other receiving device at hand. Within these expectations about the easiness and lack of burden of point-of-care devices, the tasks that have to be performed by the users are neglected. As Nelly Oudshoorn has remarked in the case of telemedicine, the users remain with some 'invisible work' to do (Star 1991; Oudshoorn 2011). With new tasks, new responsibilities also come. For example, adequate performance of the preparatory tasks prior to ingestion of the capsule becomes the user's responsibility rather than the responsibility of the medical personnel or the device itself. Within this new practice, responsibilities are re-distributed among actors and technologies. Indeed the adequacy of the sample collection is a shared responsibility of the pill manufacturer together with the pill user. While the screenee become more autonomous because free to perform the test at any location and time, more responsibilities for the good performance of such a test are allocated to them.

Furthermore, in mediating the screening practice of checking what is wrong with our body, the Nanopil creates some distance with one's body, or rather, it puts the un-hygienic body at distance, at bay. Following Martha Nussbaum's considerations (Nussbaum 2004 and Nussbaum 2010), we can say that there is a 'rhetoric of disgust' promoted by NP developers and inscribed in its design. The NP is expected to free screenees from the burden of interacting with their own diseased body and free them from the unpleasant ('medieval') task of relating with its secretions and abnormalities. As such, this device not only relies on and conveys a very specific idea of the body, but also enacts it. The body conceived in the Nanopil's script is hygienic, a whole entity that does not leak and whose boundaries stop at the skin. As Nussbaum remarks referring to the empirical work of psychologist Paul Rozin, the emotion of disgust '*concerns the borders of the body'* and it is related to the idea of 'contamination': '*the disgusted person feels defiled by the object, thinking that it has somehow entered the self*' (Nussbaum 2010, 14). The primary objects of disgusts are '*feces, blood, semen, urine, nasal discharges, menstrual discharges, corpses, decaying meat*' (ibidem, 15) are reminders of human animality, mortality and decay to which people express aversion. As

[6] A similar remark is made by Nordmann (2007)on the assumptions behind the idea of efficiency of nanomedicine.

Nussbaum points out, the identification of some actors – and practices, as we would add[7] – as disgusting implicitly contrasts them with those actors – and practices – that are 'normal' or 'pure'. So, disgust is an emotion that underpins the stigmatization of some actors or practices and classifies them as less valuable and only worthy to be taken at distance. The rhetoric of disgust that characterizes the expectations surrounding the NP stigmatizes the practice of collecting samples of feces and checking for blood in the stool. The bleeding body and its secretions are identified as disgusting and therefore kept at a distance. When it enters into close proximity with the user – it is ingested – the NP simultaneously creates some distance, as the user gets detached from his or her body, or aspects thereof (e.g., feces).

The Nanopil is presented as a more efficient way of self-monitoring that transcends our physical body; in this way, while still burdened by some practical responsibility towards ourselves, we are relieved of what we can refer to as 'epistemic responsibility' (Code 1987). We are not responsible for the resulting information regarding our health condition because the device is responsible of the collection, processing, and understanding of information. The screenees' responsibility lies in following the steps to make the pill work effectively, but they have no responsibility of materially collect and understand the signs in their body. The screenees' capability of understanding their bodies is in fact undermined by the molecular knowledge provided by the pill. Thus, on one hand, the pill is presented as desirable within a 'monitoring' discourse in which health monitoring is presented as a moral responsibility towards ourselves and society at large. On the other hand, trust in the pill builds on a molecular trend that indirectly implies the incompetence of the user to effectively monitor her body.

Within the framework of technical mediation, the notion of trust takes on a renewed meaning. As Asle Kiran and Peter-Paul Verbeek (2010) have argued, trust in relation to technology has generally been conceived as oscillating between reliance and suspicion. One relies upon a technological artifact to achieve a certain task, e.g. the NP to detect the presence of the disease based on molecular information, and thereby trusts the technology, or else, one is wary of the risks the technological artifact generates and distrusts the technology, e.g. the fear of either a dysfunction in the NP that renders the screened information unreliable or the NP's environmental impact once it is ingested and excreted from the body, into the toilet. Yet, such conceptions of trust are informed by an understanding of technology as being situated in an external relation to humans. In this external relation, technologies are viewed as neutral and transparent instruments used to reach predetermined (by humans) goals. However, as previously showed, technologies mediate our perceptions and actions. Technologies are not external to human beings, but constitute what it means to be human. That is, as technological artifacts *mediate* our existence, they *constitute* us. Therefore,

> [i]nstead of suspicion and reliance, here we encounter a third manifestation of trust, which could be indicated as *confidence*. From this manifestation of trust, human beings deliberately and actively trust themselves to technology. Rather than being risky or useful, technology is approached here as *trustworthy*. … [I]t comes down to taking responsibility for the ways in which one's existence is impacted by technology.
>
> (Kiran and Verbeek 2010: 424).

[7] Nussbaum's argument aims at showing the roots and fallacies of ethical arguments justifying popular stigmatization of some social groups (like homosexuals) and unequal policies towards them. We think that her reflection on the emotion of disgust can also be applied to the stigmatization of some social practices.

In fact, entering into a(n intimate) relation with a technology implies re-configuring oneself. If the NP is ingested and excreted, interacting with the device requires the users to engage in some invisible work. By performing such tasks, the body is put at a distance: users know if something is wrong because the device will show them, however they do not experience, perceive or feel any of that wrongness. As it enters into close proximity with the body, the NP is not a mere instrument screening for molecular makers, but rather mediates and constitutes one's existence. As it puts the body at a distance, or more precisely, puts the fleshy, carnal body at a distance, it enacts a very hygienic body. Proximity and distance fold into one another. Trust is pivotal here. Trust, however, is not a matter of not, or no longer, being suspicious of the technological device and finally relying on it. Rather, as the NP enters into close proximity with one's body, as the relation between oneself and the technology becomes intimate, trust in the NP becomes a matter of 'trusting ourselves to' the technology: '*technologies help to constitute us as subjects, and…we can actively involved in these processes of mediation and subject constitution*' (Kiran and Verbeek 2010, 425). There, as the body becomes intimate with technology and the technology 'enfleshed' (made flesh), trusting oneself to technology implies entering into a renewed relation with one's body, enacting, even, a different body. Trusting the NP is not a one-sided and exclusive relation, however. Trusting oneself to the NP does not mean handing over oneself to the technological device and dismissing or downplaying other 'sources' of trust. Rather, interacting with – and trusting – the technological device can be expected to give new meaning, as well as renewed actuality, to one's gut feelings for instance. Indeed, by getting aware of the mediating role of the NP with respect to our practices of self-monitoring and to the way we conceive of ourselves and of our body, we can become active and get involved in these mediating instances. As the NP promotes a 'rhetoric of disgust' and enacts a hygienic body, we might become ever more sensitive – if only revolted – to our bleeding, secreting, decaying body and come to develop a renewed trust in our gut feelings. In their intimate interaction, the NP and the body constitute each other, and trusting our gut feelings becomes intertwined with trusting ourselves to technology.

## Conclusions

As we recomposed the fictive scripts embedded in the Nanopil, we were able to shed light on the mediating role of this point-of-care device. If point-of-care devices are expected to render health care cheaper and more effective through the increasing availability and generalization of early diagnostics, it can also be assumed that they will create new practices, involving new roles and responsibilities. The NP, and point-of-care devices in general, are not mere instruments but rather instances of technological mediation.

By mediating our practices of self-monitoring, these technological devices can be expected to reconfigure the conceptions we have of ourselves. While it is promoted as simplifying self-monitoring, the NP can also be expected to necessitate some invisible work. Furthermore, as it is informed by a rhetoric of disgust, when it enters in close proximity with one embodied self, the point-of-care device enacts a hygienic body while putting the leaking and decaying body at bay. Trust is also reconfigured. Trust is central when using a point-of-care device such as the NP. Trust is nevertheless not merely relying on the device and the information it provides, but rather trusting oneself to it. Point-of-care devices as they mediate our existence also constitute us as embodied subjects. Trusting ourselves to technologies does not mean passively abandoning ourselves to

them but becoming active agents in the ways in which point of care devices reshape ourselves. While trusting oneself to the NP might mean taking distance with one's leaky, fleshy and decaying body and enacting a hygienic body, it might also mean entering into a renewed relation – proximity – with one's 'disgusting' body and trusting one's gut feeling.

These aspects, which are generally neglected in the assessment of point-of-care devices, are pivotal if we are to understand what is at stake with these technologies. These aspects are important in the context of governance of the innovation process. Indeed, this type of reflection can guide technology developers in making design choices. In the case of the NP for example, technology developers are currently debating two alternative ways of conveying the results of the pill's sample analysis outside the human body (Lucivero 2012). Currently NP developers believe that the most effective and efficient design choice is to send the test result by radiosignalling to an external receiver that could also communicate with the screenee's doctor. The NP developers believe that the radiosignalling is a better technical solution than the one initially proposed by the NP inventors, that is the release of a colored dye within the intestine in the case of positive result. In this scenario, if the screenees witnessed colored stool after the ingestion of the pill, they would know that something was wrong and should contact the doctor. Our considerations about the change in the trust relationship between the screenees, their bodies the device and their disease suggest that it is important for the screenee to remain "in touch" with their bodies and to be responsible of understanding symptoms. This brings the dye-coloring solution back to the table for discussion.

When point-of-care devices are introduced, but also when their design changes, new practices and relations of trust come to existence. These are hidden in the current rhetoric and discourses surrounding point of care devices. Yet, identifying them and accounting for them is necessary not only for the successful introduction and use of a technology, but also for the kinds of selves we are to become.

## References

Akrich, M. (1992). The description of technological objects.In ( W. Bijker & J. Law 1992).

Akrich, M. & Latour B. (1992).A Summary of a Convenient Vocabulary for the Semiotics of Human and Nonhuman Assemblies.In (W. Bijker and J. Law 1992).

Banerjee, S., & Wittenberg, R. (2009). Clinical and cost effectiveness of services for early diagnosis and intervention in dementia. *International Journal of Geriatric Psychiatry*, *24*(7), 748–754.

Berg, A. van den(2009). De kunst van het kleine,in Brinskma and van den Berg, *De kunst van de wetenschap, Redevoeringen 48ste Dies Natalis*, Universiteit Twente.

Bijker, W.E. and Law J. (eds.) (1992). Shaping Technology, Building Society: Studies in Sociotechnical Change. Cambridge, Mass, MIT Press.

Code, L. (1987). *Epistemic responsibility*, Hanover, N.H.: Published for Brown University Press by University Press of New England.

Demidov, V. V. (2003). DNA diagnostics in the fifty-year retrospect. *Expert review of molecular diagnostics*, *3*(2), 121–4.

Geels, F.W. & Smits, W.A. (2000). Failed technology futures: pitfalls and lessons from a historical survey. *Futures*, 32(9-10), 867-885.

Hogg, W., Baskerville, N., & Lemelin, J. (2005). Cost savings associated with improving appropriate and reducing inappropriate preventive care: cost-consequences analysis. *BMC Health Services Research*, *5*(1), 20.

Ihde, D. (1990). *Technology and the Lifeworld: From Garden to Earth*. Bloomington and Minneapolis: Indiana University Press

Kiran, A.H. & Verbeek P.P. (2010). Trusting Our Selves to Technology.In *Knowledge, Technology & Policy* 23(3): 409-427.

Laat, B. de (1996). Scripts for the future : technology foresight, strategic evaluation and socio-technical networks: the confrontation of script-based scenarios, Thesis (Ph.D.) – Universiteit van Amsterdam.

Laat, B. de (2000). Scripts for the Future: Using Innovation Studies to Design Foresight Tools. In-*Contested futures: a sociology of prospective techno-science*, eds. Brown, N., Rappert, B. & Webster, A.Aldershot: Ashgate.

Latour, B. (1992). Where are the Missing Masses? Sociology of a Few Mundane Artefacts. In (Bijker and Law 1992): 225-258.

Leifer, B. P. (2003). Early Diagnosis of Alzheimer's Disease: Clinical and Economic Benefits. *Journal of the American Geriatrics Society*, *51*(5s2), S281–S288.

Lucivero, F. (2012). Too good to be true? Appraising expectations for ethical technology assessment. Universiteit Twente. Enschede

Melchior M. (2009). Doctoren met nanotechnologie. *Medisch Contact*. 64 nr 49: 2032-2035.

Mol, A. (2000). What Diagnostic Devices Do: The Case of Blood Sugar Measurement. *Theoretical Medicine and Bioethics*, *21*(1), 9-22.

Mosis, G., Colkesen, E. B., Ferket, B. S., Mathijssen, J. J., Peters, R. J. G., Kraaijenhagen, R. A., Van Kalken, C. K., et al. (2007). A Holistic Approach for Prevention and Early Diagnostics: Personal Health Management with Web-based Personal Health Records, In: Kuhn, Klaus A (Editor); Warren, James R (Editor); Leong, Tze-Yun (Editor). *Medinfo 2007: Proceedings of the 12th World Congress on Health (Medical) Informatics; Building Sustainable Health Systems*. Amsterdam

Noel, H., Vogel, D., Erdos, J., Cornwall, D., & Levin, F. (2004). Home telehealth reduces healthcare costs. *Telemedicine journal and e-health : the official journal of the American Telemedicine Association*, *10*(2), 170–183.

Nordmann, A. (2007). Knots and strands: an argument for productive disillusionment. *The Journal of medicine and philosophy*, *32*(3), 217-36.

Nussbaum, M. C. (2004).*Hiding from humanity: disgust, shame, and the law.* Princeton: Princeton University Press.

Nussbaum, M. C. (2010).*From disgust to humanity : sexual orientation and constitutional law*. New York, NY [etc.]: Oxford University Press.

Oudshoorn, N. (2001).*Telecare Technologies and the Transformation of Healthcare.* Basingstoke [England]; New York: Palgrave Macmillan.

Poste, G. (2001). Molecular diagnostics: a powerful new component of the healthcare value chain. *Expert review of molecular diagnostics*, *1*(1), 1–5.

Star, S.L., (1991). Invisible Work and Silenced Dialogues in Knowledge Representation. In I. Eriksson, B. Kitchenham and K. Tijdens (eds.) *Women, Work and Computerization,* Amsterdam: North Holland: 81-92.

Vedder A. and Vantsiouri P. (2013). Responsibility and Trust in E–Health Services, forthcoming.

Verbeek, P. (2005). *What things do: Philosophical reflections on technology, agency, and design.*University Park, Pa. Pennsylvania State University Press.

Verbeek, P.-P. (2011). Moralizing technology : understanding and designing the morality of things, Chicago; London: The University of Chicago Press.

Voight J. (2012), Telemedicine: A Prescription For Lower Health-Care Costs? available at http://www.cnbc.com/id/47989411/Telemedicine_A_Prescription_For_Lower_Health_Care_Costs.

Vries, G. de (2005). Pragmatism for medical ethics inKeulartz, J., M.Schermer, M.Korthals, T.Swierstra (Eds.) (2002). Pragmatist Ethics for a Technological Culture. Deventer: Kluwer Academic Publishers.

# Will technology innovation save the health system?

Anton Vedder
Tilburg University
Tilburg Institute for Law, Technology, and Society
✉anton.vedder@tilburguniversity.edu

**Abstract** Many experts and policy makers in relevant fields consider health care technologies to be promising responses to the problems created by demographic changes – increasing demand because of ageing and decreasing supply because of diminishing labor potential. Technology might indeed offer promising solutions for sustaining health care systems at the current level of provisions. The ways in which technologies can change traditional care practices should, however, not be overlooked if they are to be used effectively and efficiently. In this paper, I will focus on possible effects of e-health care applications on the organization of care, the care provider-patient relationship and the status and roles of the care providers and patients in general. Normative issues involved are related to privacy, (professional) autonomy and responsibility of both patients and care providers. Dealing with these issues is a necessary condition for the adoption of the technologies involved.

**Keywords** care, technology adoption, legitimacy, trust, ethics.

## Introduction

Experts in health economy and demography warn already for some time against the consequences of the demographic changes taking place in Western Europe for health care (Tjalsma 2007; Schillmeier, Domènech 2010). The gradually increasing demand for care due to ageing and the menace of decreasing supply of care solutions because of the simultaneously diminishing labor potential is causing a lot of trouble to policy makers and governments. Technology might offer important instruments for sustaining health care systems at the current level of provisions. It would be wise, however, to anticipate the, sometimes, drastic ways in which technologies can change traditional care practices, if the new technologies are to be used effectively and with maximum efficiency. In this chapter, I will focus on possible effects of e-health care applications on the care provider-patient relationship and the status and roles of the care providers and patients in general that might easily raise normative issues related to privacy, (professional) autonomy and responsibility of both patients and care providers. Dealing with these issues either in their design or by providing additional regulatory arrangements is a necessary condition for the adoption of the technologies involved.

Although the focus of this chapter will be on the aforementioned normative issues, it is nonetheless important to start with a general observation with regard to the discussion on sustainable health care. It is often unclear, from which perspective assessments about sustainability are made. Are they about quality improvement, cost reduction, reduction of labor? Since these criteria are relative by their very nature, what are the exact terms of comparison? Are they being compared to existing traditional modalities and practices of care, which they are to replace? Are they about relevant ways of cutting costs for insurance companies? Or are they about reducing costs and labor in the overall care system? Getting clear about these questions is the number one priority in the debate on the usefulness of new technologies in health care. At this point, it should be noted that advocates of the use of technology for raising the sustainability of health care usually refer to applica-

tions that are used for not too complicated purposes of care, prevention and diagnostics, e.g., relatively simple measurements and treatments in which the user-patient or someone close often plays an important role supported by the technology.[1] Medical-technological highlights such as applications of neurotechnology, magnetic resonance imaging, telesurgery and genetic engineering are considered to be quality improvers, rather than cost savers. This, often latent, restriction to applications for relatively simple and basic purposes, should not make us think that quality enhancement is by its very nature always in the way of efficiency, let alone efficacy. As it will be elaborated below, professionals and patients-users tend to adopt efficient and effective applications, when their use is an improvement in the perspectives of both parties. Such improvement should be visible when compared to the relevant traditional practice that the application should in the long run replace even if the application serves relatively simple purposes.

## Use of technology before care becomes necessary

From the point of view of the sustainability of health care it is not only of importance to think about cost-saving and efficiency-enhancing technological alternatives to existing care practices. It is equally important to think about technologies that can help prevent or delay the demand for care. Games for memory training, e-coaching systems for fitness exercises, slimming or sleep training et cetera might all have beneficial effects on people's mental and physical health and reduce or delay the consumption of care. The advantage of technological applications for well-being is that the technologies enable people to practice self-management for preventive purposes in a pleasant way. Technically supported games, sports coaching, diet help often are agreeable because they are easy to combine and to be associated with leisure activities. They also make it possible for people to take responsibility for their own health in a pleasant way, instead of being merely motivated by moral obligations towards oneself and towards society or by threats of exclusion from services when not living up to the responsibilities. Technology can help people choose positively in favour of healthy resources and activities.

## Motivation of professionals

In almost all e-health applications, medical and care professionals are involved, who will all have to be motivated, or at least not be discouraged, to continue working with the applications involved. Substantial motivation will be derived from the efficiency and effectiveness of the application, and in any case from the beneficial effects on the care for the patients and their health. Here a few aspects deserve special attention.

Efficacy requires at least that the application is in all respects reliable. Most applications, however, will largely hinge on interactivity: the patient-user provides certain information (e.g., about his blood pressure, temperature, heart rate, results of an exercise) and then gets feedback, new instructions or action taken in their direction. The provision of such data and information is either done by the persons themselves, or gathered and passed on automatically by sensors and other measuring equipment. For the professional who receives the data and information, and ultimately decides on the basis of them, it is essential that such data and information are correct. The me-

[1] For a discussion of the delimitations of the scope of relevant health care technologies, compare (Pols 2012).

chanical and electronic acquisition and processing must in no respect be flawed. Where people enter the data themselves, it is important that they do it correctly and that the data actually comes from and relates to the patient-user whom the professional envisages virtually. Although it may seem to be simple and obvious, in practice it takes quite a lot of effort both technically (in terms of security and authentication techniques) and motivation-wise with regard to the patient-users and their environment, to ensure that the professionals can rely on the data and the information provided to them.

Another issue relevant for the motivation are their liabilities and responsibilities. Are these sufficiently mapped out and clearly and realistically distributed among the different actors involved? Can the professional make realistic estimations whether the risks of his or her involvement in the system are acceptable and whether he or she will take responsibilities for it? Of course, many professionals are primarily interested in the effectiveness of an application for the well-being of the patient and far less eager to make all kinds of risk assessments with regard to themselves. However, there need not be many "medical errors" attributed to professionals that eventually derive for instance from incorrect information or data, before a system will drop from grace.

## Motivation of patient-users

Acceptance by the patient-users is quintessential when care technology is to repay the high expectations. Acceptance by patient-users presupposes in turn different things.

First of all, it is necessary that the professionals involved accept and support the application. Without their blessing, the patient-users will not trust the application. A further important prerequisite for trust in technology in general is that an application does what it should do: it must be effective. That also goes for healthcare applications. For applications for which there exists in fact a traditional alternative, there should be added value. People should at least in some way or another be seduced to use the new application instead of the traditional alternative. A radical way to accomplish this is simply shutting down the traditional supply. Often this will be practically impossible or undesirable. In these cases, the technology application should have additional benefits, e.g. a higher grade of effectiveness and ease of use or, for instance, options for the patient-user to participate in a community of like-minded people or people with the same problem, or easier access to other facilities that the patient-user may also need sooner or later (for instance through an e-health portal).

In addition to the additional effectiveness and attractiveness, the patient-user – just like the professional – will need to be surethat the facility will not carry with it any unexpected surprises. Also for the patients-users there should be clarity about the responsibilities and the liabilities involved, just as the distribution of the responsibilities and liabilities among the various stakeholders should be reasonable. But especially relevant for the patient-users are privacy issues.

Many care technology applications have an impact on the privacy of the user-patients. Privacy is nowadays often conceived of in terms of informational privacy and data protection. With regard to e-health this notion of privacy is absolutely relevant. Privacy is however more than the right to protection of personal data. Privacy in this wider meaning is also relevant to e-health. Privacy also has to do with the value we assign to being able to have discretionary power over the personal domain. This domain is partly spatially delineated - think of one’s own body and one’s own home - but also extends to less tangible things like personal correspondence, conversations, friendships,

intimate relationships and decisions about these matters. We could call this the personal autonomy dimension of privacy. Interestingly, many e-health applications can impact privacy both as to its meaning in terms of data protection as to its meaning in terms of autonomy in the personal sphere.

New care technologies often rely heavily on the collection and processing of data and information on the patients concerned. Therefore it is wise to include (informational) privacy protective measures already from the outset in the design of the relevant technologies and throughout the process. It should also be made clear to new users in what ways exactly personal data will be protected. This, however, is not completely certain as research has not conclusively shown that confidence in a technological application really increases when the makers explicitly show and explain what they did on a technological level to protect user privacy. What research has nonetheless shown is that user confidence disappears as soon as privacy incidents occur. Preventing them from happening is therefore of utmost importance (Kool et al 2011).

At the same time many e-health applications affect the privacy of patients in the sense of personal autonomy. The applications have the advantage of enabling the patients to receive treatment and care outside the institution, in the home. The patients can remain independent and stay in an environment that is familiar to them. This seems a gain from the perspective of privacy as autonomy in the personal domain. At the same time, however, by doing exercises and receiving treatment, the medical institution enters the home in a way. The customary demarcations of the public and the private sphere run the risk of getting blurred. Of course one could say that the use of the application at home is always better than getting care or treatment or doing exercises in an institution or in the offices of a counselor. However, a risk of erosion of privacy from within is not completely to be excluded.

## Medicalization

The idea of “healthcare at home” evokes memories of the debate that took place during the last decades of the twentieth century on the phenomenon then referred to as medicalization. Medicalization is the exaggerated attention paid to (one’s own) health and a convulsive effort to stay healthy with whatever medical means, even if this would mean going against the deficiencies and limitations that naturally come along with life and the human predicament in general.

Assigning an important role to technology in the struggle to keep the health care system sustainable may, if no additional measures are taken, easily result in medicalization. People will gradually receive more care and treatment facilities at home. Many of these presuppose an active role of the patient as well as discipline and new routines. More importantly, as already pointed out above, since technology will not only be used for treatment and care but also for well-being in combination with prevention purposes, people will be made aware of health risks and responsibilities for their own health already from an early age in order to delay health care consumption as long as possible. The introduction of technology to make the health care system more robust, therefore, seems to carry with it all the ingredients to deliver a new medicalization. In addition to the question whether it is in all respects desirable that people can become preoccupied with their own fitness and health, this raises the question whether this might not even create additional demand for care. Accompanying measures to counteract these possible effects are in any case required.

## After all

Not every technological innovation contributes automatically to the sustainability of the health care system at its current level of quality. Obviously it is difficult to establish specific criteria when it comes to assessing the degree to which a new technology will contribute to the sustainability of the healthcare system. Much depends on the exact perspective chosen: patient-consumers, workers, insurers, etc. In this chapter, we have in a sense complicated the issue of assessing the efficacy and efficiency of e-health technologies even further. We have explored the possible impact of the use of e-health applications on the respective roles of patients and care providers and on the care provider-patient relationship. We established that these changes may raise various normative problems that ought to be anticipated in a satisfactory manner or altogether avoided in order to pave the way to adoption of the technologies. Early onset observation and anticipation of these problems is thus an important precondition for the introduction of efficiency and efficacy raising new technologies in health care. The assessment of the degree to which e-health technologies contribute to the sustainability of healthcare should therefore not be confined to the individual and isolated technologies. Their possible impact on the traditional care practice and the degree to which possibly arising normative problems can be dealt with in the design or in accompanying regulation in a satisfying manner should be included in the assessment.

## References

Kool, L., A. Vedder, F. Fleurke, B. van Schoonhoven, M. van Lieshout (2011). Trusted Technology. TNO-report 35598. Delft: TNO. [http://www.rijksoverheid.nl/onderwerpen/digitale-overheid/documenten-en-publicaties/rapporten/2011/12/05/trusted-technology-een-onderzoek-naar-de-toepassingsvoorwaarden-voor-privacy-by-design-in-de-elektronische-dienstverlening-van-de-overheid.html].

Schillmeier, M. and M. Domènech (eds.) (2010). *New Technologies and Emerging Spaces of Care*. Farnham: Ashgate.

Tjalsma, D. (2007).Remote control! Toekomst en betekenis van telemedicine voor de zorggebruiker. Utrecht: NPCF

Pols, J. (2012).*Care at a distance*. Amsterdam: Amsterdam University Press.

# PART IV: MANAGING ACCESS TO TECHNOLOGY

# Robot.txt: balancing interests of content producers and content users

M.H.M. Schellekens
Tilburg University
Tilburg Institue for Law, Technology, and Society
✉m.h.m.schellekens@tilburguniversity.edu

**Abstract** Access to websites by robots is a contentious issue.Access contributes to positive network effects. Innovators can build new innovative services on the data that can be made available through bot-access to servers. But a site owner may also have legitimate interests in not allowing access by robots. These interests may focus on the hardware, such as use of bandwidth, the data stored thereon, such as time critical information, or on the relation of the proprietor and the aggregator (the former may be perceived to endorse the latter's activities). The proprietor can de facto regulate access by bots through robots.txt protocols. Should the law vindicate this protocol? Two legal actions to vindicate a prohibition of access are described: the criminal act of unauthorised access as found in art. 2 Convention on Cybercrime of the Council of Europe and the U.S. civil action of trespass to chattels. Do these actions provide an adequate framework to regulate these questions? Based on the characteristics of the problem at hand, a number of desirable characteristics for an ideal form of regulation are identified. It is found that both types of action are lacking. An action loosely based on the structure of the fair use exception in US copyright law is found to provide a better context for addressing these disputes.

**Keywords**robots.txt protocol, unauthorised access, trespass to chattels, regulation

## Introduction

Internet robots – also known as web crawlers, spiders or simply as (ro)bots - roam the net. They are the backbone of useful services such as search engines, auction aggregators, news aggregators, review aggregators or information gatherers for crime fighting or security. At the same time the proprietors of the computer systems visited by the Internet robots sometimes have an interest in refusing or limiting access to robots. Robots may take up too much bandwidth or they may collect information that is too time-sensitive to be reused. Services offered on the basis of information collected by a robot, may compete with the website from which the data are gathered. Or an aggregation site deprives the source site from visitors that otherwise would have spent time browsing on the source site. Or the owner of a source site may not want to be associated with or seen to be endorsing the activities of the aggregator. If conflicts arise about access by a robot, the visited website may have a strong claim for refusing robot access based on the possession or propriety of the computer. However, the party sending the robot offers services that are usually beneficial to society. A tension exists between the interests of those that offer primary services and the interests of those that build on the primary services. This raises the question how the law should deal with such tensions.More specifically, the central problem addressed in this article is: should the law vindicate the exclusion of robots by proprietors of computers connected to the Internet? More specifically the article will examine the role of the robot exclusion protocol.

In the US, proprietors of computers seeking legal vindication of the restrictions they impose on third parties have the action of trespass to chattels at their disposal. Courts have grappled with the question of what restrictions they want to allow proprietors to set. Similar questions arise in the

context of the Convention on Cybercrime (Wong 2007 127).[1] In its second article, the Convention describes the offense of unauthorised access. Here, the question arises what constitutes access without right. Can the proprietor elaborate his own prohibitions, which then will be vindicated by criminal law?

In order to answer these questions the following topics will be addressed. First, it will be investigated how robots seek access to a computer and how such behaviour can be prohibited by proprietors of the computers that are visited by robots. Secondly, it will be described how to deal with access by robots to a computer system. What constitutes access without right and could give rise to a criminal sanction? Thirdly, case law that has developed in the US about trespass to chattels in the context of cyberspace will be described. Subsequently, it will be evaluated what prohibitions by proprietors should be vindicated by the law, where it concerns access by robots. Finally, it is assessed how the approach could best be implemented in the law. In doing so both academic literature and the approaches found in both the US and the Cybercrime Convention will be combined.

## Imposing restrictions in practice

Most Internet sites and attached databases are freely accessible and searchable. Nonetheless, website owners sometimes do not want robots (also known as bots, spiders or webcrawlers) to access (certain parts of) their website. A reason may be that the robot usurps too much computer time or that some information is not suitable for inclusion in a search-engine, e.g., because it is very temporal and transient. Other reasons may be related to diminished goodwill: inclusion of a harvested website in an aggregator site may be perceived as an implied endorsement of the aggregator's site by the owner of the harvested site. Yet other reasons may be that the harvested site may not compare favourably with other harvested websites mentioned or otherwise represented on the aggregator site. The owner of the harvested website may prefer that the visitors of his website have a unique experience, controlled by him. It may also be that the owner of a website for copyright reasons does not want to see the contents of his website replicated elsewhere.

In brief, the owner of a website may have several reasons to deny access. These reasons may focus on the computer system (claim to capacity), the data on the system (copyright) or the relation between the proprietor and the party seeking robotic access (endorsement).

There are a number of ways in which the proprietor of a system can prohibit access by robots: technical measures, notifications or use of the robot exclusion protocol.

### *Technical measures and notification*

A proprietor of computer connected to the Internet can choose to create factual barriers for robots. The computer or parts of it may be protected with a username and a password. Access is only allowed to those who have obtained a username and password. However, this is a very elaborate way to prohibit access if the only goal is to exclude robots. A simpler way of creating a technical barrier may be to block IP addresses of the computers from which the robots come that are known to access the system. The advantage of this way of creating a technical barrier is that it can be ap-

[1] Council of Europe – ETS no. 185 – Convention on Cybercrime, available at: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm.

plied ad hoc: as soon as it is noticed that a robot lays too large a claim on the system's resources it can be blocked. A drawback is that the barrier is relatively easy to evade. The robot only needs to be sent from another IP-address or through a proxy-server to have access again.

Apart from these more technical means to prohibit access, a proprietor of a system may also send a notification to the natural or legal person using the robot indicating that he does not allow its robot to visit his system or website. The proprietor can even do so off line, for example with a letter addressed to such persons. In many cases, this may prove to be sufficient to stop robots being directed at the system. A drawback is that a notification can only be sent if the user of the robot is known. The robot itself may not identify its 'master'.

### *The robots.txt protocol*

Perhaps the most harmonious way to exclude robots is use of the so-called robots exclusion protocol.[2] This is a protocol attached to the root of a website, telling robots what pages should not be accessed. It could be likened to a sign saying "no trespass" or "no access" as used in the brick-and-mortar world. But the robots protocol is more specific. The file containing the prohibitions (robots.txt) has two fields named 'User-agent:' and 'Disallow:'. The latter indicates what pages are off-bounds. Although this allows for some specification of what is accessible and what not, the method of indicating may be unwieldy if pages belong to different 'owners' (Berghel 1997, 21). Research has shown a significant number of incorrect uses of the Robots Exclusion Protocol (Sun, Zhuang & Lee Giles 2007, 1124). The former field (user-agent) specifies to what robots the prohibition applies. The specification of the addressees of the 'sign' is something not readily encountered in the real world. By the way, it is possible to specify that the prohibitions apply to any robot (viz. by specifying an '*' behind 'User-agent: ').

The robots exclusion protocol has no formal status; it is not explicitly recognised in statutes or international conventions as a binding instruction to (managers of) robots. It is also not a formal standard, i.e. a standard brought about by one of the formal standard setting institutes. The protocol is based on a consensus reached on 30 June 1994 on the robots mailing list (robots-request@nexor.co.uk), between the majority of robot authors and other people with an interest in robots. The document specifying the protocol has been open for discussion on the Technical World Wide Web mailing list (www-talk@info.cern.ch). It mainly derives its value from the fact that the protocol is adhered to by large search engines, such as Google. Research has shown that about 45% of government, newspaper and university websites use the protocol (Sun, Zhuang & Lee Giles 2007, 1124).

Hereinafter, two regulations under which a robots.txt protocol may be relevant are introduced.

## Robots and criminal law

For the analysis under criminal law, the Convention on Cybercrime is taken as a starting point. It is an international convention brought about under supervision of the Council of Europe and all Member States of the EU are also party to the Convention on Cybercrime (hereinafter: CoC).

---

2 http://www.robotstxt.org/orig.html

> Article 2 Convention on Cybercrime – Illegal access
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

This article raises a number of issues: 1. access to what?, 2. what is infringement of security measures? and 3. when does a robot enter 'without right'?

### *Access to what?*

Is art.2 CoC applicable to access to data, i.e. access to the file in which the data are contained? Art. 2 concerns access to a computer system or a part of it. A computer system is any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data (art.1(a) CoC). Section 46 of the Explanatory Report mentions a number of examples:[3] "Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). From the example 'stored data of the system installed', can be deduced that also content files stored on a computer can be seen as part of a computer; hence accessing them is covered by art. 2 CoC. In the 'Disallow:'-field of robots.txt both a file or a directory may be inserted. A file would typically be a HTML-file. Also an exclusion of a file in robots.txt may give rise to a criminal offense pursuant to art. 2 CoC, if a robot entered the excluded file. Provisions in national Criminal codes sometimes do explicitly criminalise illegal access to data. This is the case in countries such as: Bulgaria ("access to the resources of a computer"), Croatia ("access to computer data or programs") and the United Kingdom ("access to computer material") (Picotti & Salvadori 2008, 11-14). Other countries are true to art 2 CoC and criminalise illegal access to a system. These countries include Belgium (art. 550bis Penal Code) and The Netherlands (art. 138ab CC). Some countries do not criminalise access at all and only address the illegal use of data obtained after accessing a system. An example is the Czech Republic.

### *Infringement of security measures*

From article 2 it can be derived that illegal access may be a crime, even if no security measures have been infringed; whether this is so, depends on the way in which this provision has been implemented by the states that are party to the convention. In states where security measures are required, the mere ignoring of the robots.txt file does not give rise to illegal access in a criminal sense. The robots.txt file is a mere text file and does not physically prevent a robot from entering the site. The states requiring infringement of security measures include: Austria, Italy, Germany, Lithuania, Cyprus, Estonia and Rumania (Picotti & Salvadori 2008, 11-14). Other states do not require the infringement of a security measure. These states include: Belgium (Art. 550bis Penal Code), Bulgaria (Art. 319a New, SG 92/02), and The Netherlands (art. 138ab Sr).

---

3 Explanatory report to the Convention on Cybercrime ETS 185, available at: http://conventions.coe.int/treaty/en/reports/html/185.htm .

### *Robot 'without right'?*

Does access by a robot in spite of a robots exclusion protocol requesting not to do so constitute access without right? The explanatory memorandum of the convention states the following when discussing the term 'without right' in general (i.e. not specifically relating to art. 2 CoC):

> 38. [ … ] The expression 'without right' derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their domestic law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law. [ … ] Furthermore, legitimate and common activities inherent in the design of networks, or legitimate and common operating or commercial practices should not be criminalised. [ … ]

The explanatory memorandum at 47 and 48 discusses the meaning of without right in the specific context of art. 2 (illegal access):

> 47. The act must also be committed 'without right'. In addition to the explanation given above on this expression, it means that there is no criminalisation of the access authorised by the owner or other right holder of the system or part of it (such as for the purpose of authorised testing or protection of the computer system concerned). Moreover, there is no criminalisation for accessing a computer system that permits free and open access by the public, as such access is "with right."
>
> 48. The application of specific technical tools may result in an access under Article 2, such as the access of a web page, directly or through hypertext links, including deep-links or the application of 'cookies' or 'bots' to locate and retrieve information on behalf of communication. The application of such tools per se is not 'without right'. The maintenance of a public web site implies consent by the web site-owner that it can be accessed by any other web-user. The application of standard tools provided for in the commonly applied communication protocols and programs, is not in itself 'without right', in particular where the rightholder of the accessed system can be considered to have accepted its application, e.g. in the case of 'cookies' by not rejecting the initial instalment or not removing it.

Whether access is without right is strongly dependent on the context. Access by a tool is without right if the rights holder cannot be considered to have accepted its application.[4] A robots.txt file forbidding access to whole or part of the system is but one indication that the rights holder does not accept access to the specified areas by a robot. Somebody 'manually' visiting a website is not addressed by the robots.txt protocol and his access is not illegal.

In the American case of Register.com Inc. v. Verio Inc.[5] the use of a search robot was found to constitute unauthorized access because Register.com did not consent to Verio's use of the robot and Verio was on notice of this fact. In the same vein, is the well-known decision in eBay Inc. v. Bidder's Edge Inc. 100 F Supp 2d 1058, 1070 (ND Cal 2000). Hence, according to US law the owner of a computer system can legally withhold authorisation to (managers of) robots to enter their system, while allowing 'manual access' to the public. This does however not answer the question whether robots.txt is an adequate means for conferring the declaration of the rights holder: is it sufficiently clear and conspicuous? With respect to clarity, the robots.txt file specifies what access the rights holder wants to forbid. An explanation of the instructions used is given on the robotstxt.org website. However the robots.txt protocol is somewhat limited in its vocabulary. The compli-

---

4 Compare Clough 2010, 70.

5 126 F Supp 2d 238, 238-49 (SD NY 2000).

ance with a robots.txt file also raises questions. Respect for the instructions in the robots.txt file does require that the robot is programmed to look up the robots.txt file before entering a website and to act in conformity with the prohibitions specified in it. If a robot is not programmed to look for the file it simply enters the site or computer system without ever having seen the file. So basically, the user or programmer of a robot must anticipate that the robot can come across robots.txt files by inserting adequate code into the robot (viz. code that instructs the robot to look for possible robots.txt-files etc.). The question is whether every robot-programmer should take the robots.txt protocol in account when programming a robot. The robots-website has a list of 300+ robots that respect the protocol.6 Large search engines, such as Google respect the protocol. Robots.txt has a certain de facto compliance with a large number of robots. As we saw above US law has accepted that the wishes of the proprietor should be complied with. However, the protocol lacks aformal status. In the US cases, the proprietors next to using the protocol, also directly addressed the managers of the robots.

## Bots trespassing to chattels?

In the US, owners of computers connected to the Internet finding the access and use by third parties unacceptable have sued for trespass to chattels. The Second Restatement of Torts defines trespass to chattels as intentionally dispossessing another of the chattel or using or intermeddling with a chattel in the possession of another.[7] A chattel is a movable property. Not each trespass is actionable. A trespass, even if not actionable, may be relevant for the relationship between the parties. The possessor is for example allowed to use reasonable force to protect his chattel. Trespass to chattels is actionable under the following conditions:[8]

One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,

(a) he dispossesses the other of the chattel, or

(b) the chattel is impaired as to its condition, quality, or value, or

(c) the possessor is deprived of the use of the chattel for a substantial time, or

(d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.

An intermeddling with a chattel possessed by another is thus only actionable if it has caused damage to the possessor. The action of trespass to chattels has led a quiet life for a long time. It has been given a new leash of life with its application to electronic communications and especially in the context of cyberspace. The key precedent case is Thrifty Tel. Inc v. Bezenek.[9][10]In this case, the

---

6 http://www.robotstxt.org/db.html.

7 Section 217 Restatement (2nd) of Torts.

8 Section 218 Restatement (2nd) of Torts.

9 Thrifty-Tel, Inc. v. Bezenek, 46 Cal.App.4th 1559.

10 A number of cases mention the 'robots.txt'-protocol, but do not decide anything of interest to the topic of this article. These cases include:

- In Re Complaint of Judicial Misconduct, 575 F.3d 279 (2009), J.C. No. 03-08-90050, United States Court of Appeals, Third Circuit, June 5, 2009, available at: www.leagle.com .
- In Re Hydroxycut Marketing and Sales Practices Litigation, United States District Court Southern District of California, CASE NO. 09md2087BTM (CAB),

California Appeals Court found that the use of a telephone service with the help of authorisation codes that were obtained by hacking constituted a trespass to chattels. This conclusion was reached in spite of the fact that there was no mechanical intermeddling with thrifty Tel's telephone exchange system: mere electronic signals constituted the interference. This decision opened the road to apply the action in the context of cyberspace.A bot is nothing more than a program that is sent to a computerin the form of electronic signals. Application of trespass to chattels thus became likely after this ruling, as was later confirmed in eBay v. Bidder's Edge (see below).

In CompuServe v. Cyberpromotions, the latter party sent unsolicited e-mails to customers of ISP CompuServe. CompuServe notified Cyberpromotions that it forbade the latter's use of its system for bulk e-mail. Nevertheless, Cyberpromotions continued. The Ohio District Court found trespass to chattels in that Cyberpromotions exceeded CompuServe's consent to use its system for e-mail purposes. It found damage in the following way:[11]

To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

---

- Netbula, LLC and Dongxiao Yue v. Chordiant Software, Inc., Steven R. Springsteel, and Derek P. Witte, No. C08-00019 JW (HRL), United States District Court for the Northern District of California, San Jose Division, available at: http://www.american-justice.org/upload/page/123/69/docket-187-order-on-IA-motion.pdf (order to disable a robot.txt [SIC] file in the context of discovery; the argument is no so much that access would be a breach, but more that access is easier with the file disabled).
- Gordon Roy Parker v. YAHOO!, Inc., et al., No. 07-2757, United States District Court for the Eastern District of Pennsylvania, available at: http://docs.justia.com/cases/federal/district-courts/pennsylvania/paedce/2:2007cv02757/231543/23/0.pdf?ts=1224870836 (not using a robots.txt protocol is instrumental in finding an implicit license barring a finding of direct copyright infringement).
- Blake A. Field vs. GOOGLE Inc., NO. CV-S-04-0413-RCJ-LRL, United States District Court District of Nevada, available at: http://docs.justia.com/cases/federal/district-courts/nevada/nvdce/2:2004cv00413/18321/64/0.pdf?ts=1187988878. The court finds inter alia:
  - The Internet industry has widely recognized the robots.txt file as a standard for controlling automated access to Web pages since 1994.
  - Estoppel: Second, Field remained silent regarding his unstated desire not to have "Cached" links provided to his Web site, and he intended for Google to rely on this silence. Field could have informed Google not to provide "Cached" links by using a "no archive" meta-tag or by employing certain commands in robots.txt file. Instead, Field chose to remain silent knowing that Google would automatically interpret that silence as permission to display "Cached" links.
  - Second Fair Use Factor: Moreover, Field added a "robots.txt" file to his site to ensure that all search engines would include his Web site in their search listings.
  - Fourth Fair Use Factor: Notwithstanding Google's long-standing display of "Cached" links and the well-known industry standard protocols for instructing search engines not to display them, the owners of literally billions of Web pages choose to permit such links to be displayed.
  - Fifth Fair Use Factor: Google honors industry-standard protocols that site owners use to instruct search engines not to provide "Cached" links for the pages of their sites. See, e.g., Brougher Decl. 18-22. Google also provides an explanation on its Web site of how to deploy these industry-standard instructions, and provides an automated mechanism for promptly removing "Cached" links from Google's search results if the links ever appear.
- Kelly v. Arriba Soft Corp., Case No. SA CV 99-560 GLT[JW], United States District Court for the Central District of California, Southern Division
  - Only mentioned in a footnote: The parties argue at length about the possibility of blocking the Ditto crawler from a Web site by use of a "robots.txt" file or other methods. Defendant posted instructions on its Web site for blocking the Ditto crawler in March, after Plaintiff's images had already been indexed. Plaintiff's Web sites have never used any of these blocking methods.

[11] CompuServe, Inc. v. Cyber Promotions, Inc. 962 F. Supp. 1015 (S.D. Oh. 1997).

This case was not about bots, but in relevant aspects the case exhibits important similarities. From a distance, through electronic signals part of the capacity of a computer was claimed for a use that was more intensive than the computer proprietor may have catered for. This is alike those cases where a bot grazes through a website, absorbing relevant capacity of the system it is visiting. Whether the absorption of capacity is so intensive that the proprietor of the computer could claim damage as required for trespass to chattels may be a contentious issue, as we will see hereinafter in the eBay v. Bidder's Edge case. Nevertheless, it is striking that in CompuServe v. Cyberpromotions the value of the chattel is assessed as the value for the possessor, not as value on the market. In the case of eBay v. Bidder's Edge, the action of trespass to chattels has been applied to Internet robots accessing the servers of online auctioneer eBay and consuming processor time.[12] Bidder's Edge (hereinafter: BE) was an auction aggregation site that scraped the sites of online auctioneers in order to give a comprehensive overview of objects that were up for auction on the Internet. Bidder's Edge's bots also visited eBay's website. eBay notified Bidder's Edge that it forbade BE's bots from entering its website and server and it tried to block the IP addresses from which BE operated. This did however not stop BE from having its bots enter eBay's system, whereupon eBay sued for trespass to chattels. The most contentious issue proved to be the issue of damage. The court found as follows:

> Even if, as BE argues, its searches use only a small amount of eBay's computer system capacity, BE has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes. The law recognizes no such right to use another's personal property. Accordingly, BE's actions appear to have caused injury to eBay and appear likely to continue to cause injury to eBay. If the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers. If preliminary injunctive relief were denied, and other aggregators began to crawl the eBay site, there appears to be little doubt that the load on eBay's computer system would qualify as a substantial impairment of condition or value.

The court apparently was not sure that BE's actions in themselves were enough of an impairment of the value or condition of eBay's system to warrant a finding of trespass to chattels. Therefore, it saw itself forced into a slippery slope argumentation. In my view, it is not completely clear whether such a slippery slope in fact was a risk that eBay was exposed to. The court did not adduce any evidence for the likelihood of this slippery slope and later referred to it as a possibility. This does not take away that eventually, the court enjoined Biddder's Edge from accessing eBay's computer system or network using a bot.

Another important limitation of trespass to chattels is that the damage should affect the possession or value of the chattel. If the 'trespass' gives rise to other kinds of damage the action will fail. The issue of 'other types of damage' was reason to deny a finding of trespass to chattels in Intel v. Hamidi. In this case, a disgruntled ex-employee of Intel – Hamidi – approached current employees of Intel with his e-mails. Hamidi sent many mails and those e-mails distracted current employees of Intel to whom they were directed. Intel notified Hamidi to stop, but Hamidi disregarded the notification. Intel sued for trespass to chattels, but it did not prevail at the California Supreme Court: [13]

---

[12] eBay v. Bidder's Edge, 100 F.Supp.2d 1058 (N.D. Cal. 2000)

[13] Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003).

> Intel's claim fails not because e-mail transmitted through the Internet enjoys unique immunity, but because the trespass to chattels tort … may not, in California, be proved without evidence of an injury to the plaintiff's personal property or legal interest therein. … In the present case, the claimed injury is located in the disruption or distraction caused to recipients by the contents of the e-mail message an injury entirely separate from, and not directly affecting, the possession or value of personal property.

Intel v. Hamidi was not a case concerning bots. But the requirement that damage concerns the chattel is a general requirement. Intel v. Hamidi does not give reason to believe that the way in which the damage was caused (by man or by machine?) would be material to the issue of the type of damage caused. The issue of what type of damage occurs is however relevant to the ability to act against bots on the basis of 'trespass to chattels'. As indicated in the introduction, there are various reasons for disallowing bots access to a computer system. Some of them concern the computer itself (bandwidth), whereas other reasons do not relate to the computer at all (e.g. endorsement). So the action of trespass to chattels would be useful only in a limited subset of cases.
Trespass to chattels can be found where the chattel is a computer system and the trespass is committed electronically from a distance with the help of a network. The most contentious issue is the element of damage.[14] Under what circumstances is there damage of a type and substantiality that is sufficient to warrant a finding of trespass to chattels? The claim that robots lay on the capacity of the computer system may not be substantial enough to cause an impairment of the functioning of the system. The pain is often in other types of damage, such as distraction of employees or damage by free riding competitors. But that type of damage is not relevant under the action of trespass to chattels.

## Evaluation of access by Internet robots

The paper deals with computer systems that – even though private property - are opened up for the public. Contents stored on the computer system are thus made accessible/available to the public. The issue is under what conditions access, searching copying and downloading of content from such open sources should be allowed if it is performed by using a special technology: the (ro)bot. This question is not triggered because the mentioned actions are intrinsically objectionable if performed by a robot. On the contrary, in themselves such robot actions are not morally reprehensible at all. Only under additional circumstances, there may be arguments to disallow such actions. These arguments concern the proprietor and may be private arguments of the proprietor of the computer or the arguments may relate to public policy. Above we saw that private arguments may have to do with the computer system that the robot enters, they may have to do with the data that are harvested or they may have to do with the relation between the proprietor and an aggregator. But there is also general interest in disallowing robot actions. The Internet is a network of computers. Connection of computers to the Internet gives rise to network effects. The same holds for the addition of new data or information to the internet. With every computer and website added to the Internet the utility of the Internet rises for everybody already connected to the Internet. The person adding a new computer or website to the Internet thus provides society with a positive externality

[14] There is a case in which a claim to trespass to chattels was denied because it was pre-empted by federal law. See Diokno (2007).

(Short 2004, 86). As classical economic theory predicts positive externalities run the risk of being underproduced (Liebowitz & Margolis 1994, 134). In the absence of property rights, the person deciding to connect his computer to the Internet does not reap all the benefits of his decision to connect. eBay would for example have been unable to capture the benefit Bidder's Edge enjoyed from scraping its server. A property right in the computer system allows internalisation of the positive social effects. If the underproduction, predicted by this argumentation, becomes reality there are policy reasons to make connection of a computer to the network attractive, for example by giving the proprietor ample room to determine the conditions under which third parties are allowed to access and use the networked computer.

Obviously, questions about robotic activities as discussed here are not solely revolving around the interests of the proprietor. The aggregators may have respectable interests in gaining robotic access to the system as well. Private interests concern e.g. services that can be offered on the basis of data freely available on the internet. There are also public policy reasons to support the aggregator in this. Society as a whole may benefit from the new services. Moreover, it can be questioned to what extent the lesson from the classical economic theory about externalities should be determinative for the access we want to allow to networked computers (Liebowitz & Margolis 1994, 140). At present, no company, organisation or even private person can afford to stay away from the Internet. Every company or organisation needs to have a website or other presence on the Internet. In other words, there is enough exogenous stimulation for connecting up to the Internet. The expectation that connection of a computer to the Internet, being an externality, is underproduced may not hold or only be true to a limited extent. If Internet presence is indeed 'socially mandatory' measures by which a proprietor restricts the access and use that third parties have of his computer may actually diminish network effects. Aggregators offer for example services for which a potential demand under consumers exists. Disallowing aggregators' access may have the effect that desirable services cannot be offered because rights holders acting in their individual interest block them. Hence, there could be a policy reason to be reticent with legal vindication of restrictions on the use that third parties can make of a connected computer or the data it contains.

Intermediate conclusion: the law should cater for both the interests of the proprietor of a connected system and the aggregator. The question is whether the law should give preference to one interest over the other at all. Hereinafter, the specification of a regulatory intervention is further circumscribed.

This paper does not concern content that is behind lock and barrel, in the sense that it is physically impossible to access the content. After all, a robots.txt protocol can be ignored. This is a circumstance different from and to be distinguished from the fact that the computer system is opened up for the public. The latter concerns the abstract decision about who to allow into the computer. The former concerns the technology by which the abstract decision is enforced or to say it differently, how compliance is ensured.

This paper is also not concerned with the situation in which the data available from the computer system are protected by copyright. In such a situation, the resolution of the dispute tends to be dominated by copyright considerations and is the robots.txt protocol reduced to a minor circumstance under which a possible copyright infringement takes place.

### *The nature and the extent of the problem*

That the law should be receptive to interests of both sides, as stated above, does of course not take away that the interests are not identical and that their divergence may develop into a dispute. However, a difference of interest does not necessarily mean that there is a clash between the interests and values of some party and those of another party. The difference in interest may merely amount to a coordination problem, i.e. there is a problem for which a solution exists that hurts none of the parties. Finding the solution only requires coordination between the parties. Sometimes a technical aid can help provide the needed coordination. This seems to be predominantly the case with problems relating to the computer system and those relating to information. Examples are robots.txt protocols specifying a measure of intensity with which robots may use the computer, e.g. there must a specified number of hours or minutes between consecutive robotic searches of a server. Another example is provided by metatags that specify on data (as opposed to server) level what information may be indexed or copied. In other cases coordination may require some sort of agreement between parties. An agreement could be reached between the parties for example on how the harvesting party will present the harvested data, with a view to avoid that the public makes an inference of endorsement by the 'proprietor' of the data.

### *Intermediate conclusion*

In many instances, coordination may bring a solution that is acceptable for both parties. Regulation should give ample room for finding a solution through coordination. The law should set parties up to first try and see whether the conflict can be resolved by coordination. In fact, coordination may be the best way to resolve the majority of cases. The ideal solution is one that is self-establishing. If you have to resort to court the solution is too cumbersome

## Specification of an ideal legal regime

So given a situation that is specified as above, what would be an ideal way to regulate robotic access to connected computer systems?

An approach whereby the property argument is decisive appears to be a bad fit. The cases that we discuss do not involve the object of property (the computer system) being taken away. It merely concerns the modalities of use of the property in a situation where the proprietor has made it – completely or partly - available for public use. Complete discretion on the basis of property also appears to make the positions of the parties uneven. The proprietor is in strong position and can enforce a simple solution that is favourable for him, without bothering too much about the interests of the weaker party. Why would he incur the transaction costs of negotiation for a more balanced solution? In other words, transaction costs prevent coordination from taking place.

Specific legal rules governing undesirable uses of such public property could come some way. Such rules however do exhibit certain shortcomings when put to this use. Above we saw that the types of situation in which the need for such a rule is triggered are diverse. Relevant interests may concern the computer itself, the data stored on it or it may concern the relation between the proprietor and a third party. Devising specific rules for each and every situation may lead to a strong expansion of the body of rules. The question is whether such formalisation would be an adequate answer to the issues at hand. The rules may be too rigid for many situations that can develop in an online environment. Further formalisation may lead to less coordination and more en-

trenchment of legal positions. If the rules were an exact fit for situations such may not be a problem, but given the dynamics of the internet, new situations would probably soon develop for which the rules are not an adequate fit.

Given that proprietor has made the object available and that coordination is an important element in resolution, an approach based on specific rules appears to be inadequate. Also an approach whereby the property argument is decisive appears to be inadequate.

There is a need for an open norm that is flexible, can be tailored to the situation at hand, does as little as possible create a presumption in favour of one party or the other, allows for legal development and has ample room for a balancing of interests.

In this balancing exercise, a proportionality test and perhaps a subsidiarity test are relevant. A proportionality test basically compares the benefits and harms of the litigious non-compliance with robots.txt. It does not compare scenarios with each other but just concentrates on the merits of one scenario. Its individual steps comprise:

- What are the benefits of the litigious non-compliance with robots.txt? What weight can be accorded to them?
- What harm does non-compliance cause? What weight should be accorded to that?
- What is the result of comparing the benefits and harms and their respective weights?

In addition, a subsidiarity test may be needed. Even if the litigious non-compliance with robots.txt is proportional, this does not necessarily mean that the best or optimal solution has been found. It may for example be possible to coordinate as described above. Subsidiarity allows for a comparison of scenarios, including scenarios involving coordination.

### *How do the described regimes fare?*

Given the outline of ideal regulation as described in the previous section, how do the two regimes described above fare? Compared to the benchmark set above, an action based on trespass to chattels exhibits some shortcomings. The action only allows taking the direct property interest in the computer into account, not (or only to a lesser extent) other interests of the proprietor, such as interests in the data stored on the computer or interests of the proprietor concerning the relation with third parties. In eBay v. Bidder's Edge, this property interest is accorded much and perhaps too much weight. The benefits accrued by the aggregator and the public at large can hardly be taken into account. Taking these interests into account would require creative interpretation. For example, if there is a large benefit in allowing access a court may be more reticent in finding harm done to the proprietor. This may go some way in accommodating the interests of the aggregator or the public at large, but remains a somewhat twisted and forced solution, with its own limitations. A court is not completely at liberty in the determination of the harm done to the proprietor. It will have to come up with a reasonable assessment of the harm done.

How does art. 2 CoC and the national criminal provisions based on it fare? The element 'without right' allows for many circumstances to be taken into account. However, circumstances indicating consent to or forbidding access probably play a greater role than other circumstances. On the one hand, the specifications of a robot.txt protocol may make clear that certain robots are not welcome. On the other hand, the robots.txt protocol may not be seen by a robot and it lacks an official status. This may in combination with the fact that the server has been opened up to the public and access by robot is a fairly usual action in a computer network lead to the conclusion that there is no access 'without right'. So circumstances relating to consent or a bar allow for different out-

comes. Flexibility in deciding is however somewhat hampered, because in the long run, the case law will have to settle on the issue of the status of the robots.txt protocol. It is also not completely clear whether other circumstances (the aggregator offers a service of great value to society, while the proprietor is hardly affected in his interests) can overrule a robots.txt protocol clearly denying access to the robot of the aggregator. Also, it is not clear that art. 2 CoC or provisions based on it allow for coordination. It is rather likely that a criminal prosecution troubles the relation between parties so much that a coming together in order to coordinate is no longer very likely.

Intermediate conclusion: both regimes described above exhibit important shortcomings when tested against the ideas we developed above about an ideal regime for regulating robotic access to open computers.

### *What kind of regime would be ideal?*

The shortcomings of the existing regimes can be summarised by saying that they only to a limited extent allow taking all the relevant circumstances or factors into account. Also there seems to be bias in which some circumstances are more self-evident to consider than other circumstances. Those other circumstances only in a cumbersome way can be drawn into the equation. One may argue that a certain bias is inevitable because the property in the computer system places the proprietor in a relatively strong position. That is the necessary consequence of the importance the law attaches to property. However, it seems to me that there is something to gain. A property based system that allows for adequate consideration of various circumstances has been seen before.
More concretely, I think of the (formal structure of the) fair use exception in US copyright. Under the fair use exception somebody may use a copyrighted work in a way that is relevant under the exclusive rights of the holder of the pertinent copyright. Nevertheless, this use may take place without permission of the rightholder if it constitutes a fair use. In order to establish whether there is a fair use a number of specified factors is evaluated. The factors considered are: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for non-profit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work. Of course, these very same factors cannot be used for the issues discussed in this paper. But the first factor clearly shows that values and interests of others than the copyright holder are explicitly considered. The other three factors seem to focus on the harm done to the proprietor or the lack of it. Different aspects of the harm done are elicited and harm seems to be slightly more prominent present in the test than the benefits of the potential fair use. All in all, the fair use test appears to be a proportionality test that allows for all interests to be taken into account. The subsidiarity element is not explicitly present. It is only the course of action of the party appealing to the fair use exception that is considered. An investigation in the presence of less burdening alternatives is not demanded by the fair use exception.

Given the outline we made above for a regulation addressing robotic access disputes, a rule comparable to the fair use test would form a promising candidate. It would be flexible enough to allow for the different interests and values to be taken into account. However, it may be argued that this flexibility has a downside. There would be a certain risk that outcomes are not predictable at first: how will courts weigh the different factors? The question however is whether uncertainty about court decisions actually is a risk. The uncertainty has a positive effect in that it will force parties to reflect upon the strength of their arguments instead of reflection on the strength of their

rights. The self-assessment may make parties willing to solve problems amicably and to look for alternatives that by way of coordination are acceptable to both parties.

Would it be possible to have a test based on factors for the disputes discussed in this article? Obviously, other factors are needed than those used for the fair use test. I wonder whether the steps identified above would do: What are the benefits of the litigious non-compliance with robots.txt? What weight can be accorded to them? What harm does non-compliance cause? What weight should be accorded to that? What is the result of comparing the benefits and harms and their respective weights? These factors are superficially less specific than these used in the fair use test. The question however is whether the difference is that big in practice. Moreover, I think that the disputes addressed by them are also less uniform and therefore the factor should also be a little less specific.

A second issue is the subsidiarity test. The fair use test does not include subsidiarity. I doubt whether subsidiarity should be included explicitly. The reason is that it is not up to a court or other arbiter to come up with alternatives. Where the possibility of an alternative seems real a court may have procedural means to invite parties to try and find an amicable compromise. If parties do not arrive at such a compromise and such result is attributable to the unreasonable attitude of one of the parties the court may find against this party, thus increasing the pressure on this party to revisit the possibility of coordination. As said above, the focus on real arguments anyway guides parties towards coordination, even before a court or arbiter is in sight. So, subsidiarity is important but may be difficult to incorporate explicitly in a test. Furthermore, there are other more implicit means to stimulate coordination.

Finally, does such a test fit a legal system such as the US legal system? This is a question that will not be explored here in depth. What can be said is that the test is based on the fair use test that is long since part of US law; the pre-existing common law was codified in 1976. So the test is not antithetical to US law. The only question would be where to put such a test in legalisation if at all. Perhaps such a test could start life as an instrument of common law and be incorporated in statutes once it has matured. Such would be much the same way that the fair use test developed. This test also once started life as a construct of common law.

## Conclusion

Access to websites by robots is a contentious issue. Access contributes to positive network effects. Innovators can build new innovative services on the data that can be made available through bot-access to servers. But a site owner may also have legitimate interests in not allowing access by robots. These interests may focus on the hardware, such as use of bandwidth, the data stored thereon, such as time critical information, or on the relation of the proprietor and the aggregator (the former may be perceived to endorse the latter's activities). The proprietor can de facto regulate access by bots through robots.txt protocols. Should the law vindicate this protocol? Two legal actions to vindicate a prohibition of access were described: the criminal act of unauthorised access as found in art. 2 Convention on Cybercrime of the Council of Europe and the US civil action of trespass to chattels. The question was asked whether these actions provided an adequate framework to judge these questions. Based on the characteristics of the problem at hand, a number of desirable characteristics for an ideal form of regulation were identified. It was found that both types

of action were lacking. An action loosely based on the structure of the fair use exception in US copyright law was found to provide a better context for addressing these disputes.

## References

Berghel, H. (1997). Cyberspace 2000: Dealing with Information Overload, *CACM* Feb. 1997, Vol. 40, No.2, 19-24.

Burk, D.L. (2000). The Trouble with Trespass, 4 *J. Small & Emerging Bus. L.* 27.

Clough, J. (2010). *Principles of Cybercrime*, Cambridge University Press.

Xavier P. Diokno, Case Summary Healthcare Advocates, Inc., v. Harding, Earley, Follmer & Frailey 497 F. SUPP. 2D 627 (E.D. PA. 2007), 18 DePaul J. Art, Tech. & Intell. Prop. L. 221.

Liebowitz, S.J. and Margolis, S.E. (1994). Network Externality: An Uncommon Tragedy, *Journal of Economic Perspectives*, Volume 8, Number 2, Spring 1994, 133-150.

Picotti L. and Salvadori I. (2008). National Legislation Implementing the Convention on Cybercrime – Comparative analysis and good practices, www.coe.int/cybercrime.

Sharkey, C.M. (2009). Trespass Torts and Self-Help for an Electronic Age, 44 *Tulsa L. Rev*. 677.

Short, J.M.H. (2004). An Economic Analysis of the Law surrounding Data Aggregation in Cyberspace, 56 *Me. L. Rev.* 61.

Spencer, S. (2009). *A Deeper Look At Robots.txt*, available at: http://searchengineland.com/a-deeper-look-at-robotstxt-17573.

Sun, Y., Zhuang, Z. & Lee Giles, C. (2007). *A large-scale study of robots.txt*, Proceeding WWW '07, Proceedings of the 16th international conference on World Wide Web, ACM New York, 1123-1124, available at: http://dl.acm.org/citation.cfm?id=1242726 .

Wong, M.W.S. (2007). Cyber-trespass and “unauthorised access” as legal mechanisms of access control: lessons from the US experience, *International Journal of Law & Information Technology* 2007, 15(1), 90-128.

# Credential Design in Attribute-Based Identity Management

Gergely Alpár[1]
Radboud University Nijmegen, ICIS Digital Security and TNO Security, The Netherlands
✉ gergely@cs.ru.nl

Bart Jacobs
Radboud University Nijmegen, ICIS Digital Security, The Netherlands
✉ bart@cs.ru.nl

**Abstract** Attribute-based credentials are cryptographically secured carriers of properties that hold for a particular individual. They are the basic building blocks of many upcoming privacy-enhancing technologies and user-centric identity management systems. There are a number of limitations and requirements besides security and privacy, such as usability and efficiency, that have to be taken into account when designing specific credentials in practice. This paper elaborates several realistic on-line and off-line use cases in attribute-based identity management; moreover, it identifies and analyses some of the design issues that require a decision or solution. It provides the most important credential design principles and also shows how setting up an attribute-based credential system formalises identity relationships in society.

**Keywords** attribute-based credential, smart card, pilot, identity management, identity card

## Introduction

Authorisation requires authentication: before letting someone do or use something, it must be clear that this person is actually allowed to do so. Traditionally, authentication is understood as proof of identity, for instance, by means of a password or an identity document. But precisely identifying people, using uniquely identifying numbers and names – such as a social security number (SSN), credit card or bank account number – is often overkill. In many situations it suffices to know some attribute (property) of a person in order to authorise a transaction. If a hairdresser offers a cheap haircut to students, it is not necessary, or even desirable, that the hairdresser learns a (uniquely identifying) student number as part of the proof of 'studentship'. Similarly, buying an alcoholic drink only requires a proof that the buyer is above a certain age limit (16, 18, or 21). Attribute-based authentication aims to provide a mechanism for precisely doing this: allowing transactions on the basis of those attributes, which are required for the transaction. The main advantages are:

- it is privacy-friendly, in the sense that it is based on the idea of data minimisation and that it provides unlinkability among user transactions;
- it offers protection against identity fraud: if one's identity is not involved in a transaction, it cannot be stolen;
- it provides a new, more flexible approach in identity management and authentication, in particular, an approach that is based on attributes instead of unique identities.

[1] Supported by the research program Sentinels as project 'Mobile IDM' (10522).

Attribute-based authentication is not new. Attribute certificates [10] were defined in the X.509 stack over a decade ago. They enable authentication that does not require identification; *e.g.*, role-based access or proof of membership. However, they are (1) linkable (each transaction is linked to the same public key) and (2) transferable (delegateable). Attributes in the context of attribute-based credentials and in this paper are different; they provide security, unlinkability, and untransferability simultaneously (see details about security and privacy properties in the next section). Cryptographic techniques that enable secure and privacy-friendly attribute-based authentication have also been around for more than a decade; see [4, 7, 8, 14]. But what is new is that the latest generation of smart cards is powerful enough to perform the required (non-trivial) cryptographic operations in an adequately efficient manner. Hence only now we see efforts to actually deploy attributes in practice. This paper is based on the experiences in one such deployment in the course of a pilot project, namely the IRMA project[2] in The Netherlands. It relies on the Idemix technology [13] and uses personal smart cards as carriers of credentials and attributes—see the next section for more details. Getting attribute technology up-and-running brings us into largely unexplored territory that poses a multitude of technical and organisational challenges. But it also leads to new (research) questions and forces us to think deeper and more systematically about the technology and its implications. As its main contribution, the current paper explores these matters. It concentrates on the issues that arise regarding the organisation of *multiple* attributes and of the dependencies between them, and on the decisions that need to be made to make these cryptographic techniques and their implementation practical while preserving their advanced properties. Many other interesting topics are out of scope, like the underlying cryptography [7, 8], the smart card technicalities, or a detailed security analysis.

To the best of our knowledge, there are two other pilot projects in the context of attribute-based credentials. Both of them – a Swedish and a Greek pilot – are carried out by the EU-sponsored ABC4Trust project [6]. The Swedish pilot [3] gives anonymous access for elementary school pupils to on-line resources (*e.g.*, chat room), while the Greek pilot [1] enables university students to evaluate lectures anonymously. In both cases eligibility and privacy are of primary importance. Although our pilot uses the same underlying technology, the objective of our research is more general as we investigate a *broad variety* of attributes and applications. The kinds of challenges investigated in this paper are absent in the ABC4Trust pilots since each of these focuses on a single context.

One may view an individual's identity as the collection of all attributes that hold for him/her. We can imagine that using a personal smart card, people manage dozens of attributes for various authentication goals, determined by the organisations that they interact with. Given that there are many dependencies between all these attributes, the question of how to organise them in a logical/coherent and intuitive manner is non-trivial and not free from politics (information is power). This is the main topic of this paper. We make the various issues explicit that we came across in the context of our pilot project and explain the choices we have made. This is certainly relevant beyond this particular project.

[2] See http://irmacard.org, where IRMA is an abbreviation for: I Reveal My Attributes.

## Technical Background

Technically, digital credentials, containing attributes, form a coherent unit. In our discussion, however, attributes play a more important role conceptually. We can simplify it and say that credentials are issued and attributes are shown. In this section we describe some abstract technical details of the technology, the participants, and our implementation.

**Attributes –** In the current context, an attribute is some property of or a piece of data about a person that some party (most often some authority) attested to. We briefly elaborate.

Some attributes are identifying and some are non-identifying, i.e., some attributes hold for a single individual (in a particular context) whereas other attributes hold for many people. For instance, the attribute 'male' is in general not identifying, but the attribute 'bank account is …' identifies the (sole) holder of the account. The phrase 'anonymous credential system' is often used in the literature for systems like U-Prove and Idemix, but in the current context attributes need not be anonymous (non-identifying).

What is important is that for a particular individual, an attribute either holds or not, at a particular point in time. So, for instance, the attribute 'under 18' may hold now for my son, but may no longer hold next year: the validity of personal attributes is time-dependent.

In this context it is assumed that there is some authority that can decide whether attribute A holds for person P at time t, and that this authority is willing to provide this attribute to P with its digital signature. For instance, my bank can digitally sign the statement what my bank account is at this moment, and provide the result in a credential to me. In some cases it is obvious for a given attribute which authority is in the best position to issue it in a credential: my bank is most authoritative when it comes to my bank account. But in other cases there may be multiple authorities. An example might be my address attribute, which can be provided either by the municipal authorities or, for example, by the postal service. We return to this matter later on.

Part of such a digital signature on an attribute is usually an expiration date. The expiration date may be necessary because the attribute may no longer hold after some time (like for 'under 18'). But expiration may also be used to limit the usage period of an attribute. For instance, the signature on the attribute containing my home address may expire after a year in order to ensure that it is reasonably fresh (and thus accurate).

**Credentials –** A credential, in the context of this paper, is a cryptographic container for attributes. It is digitally signed by a trusted party, the issuer (see more details below). This digital signature provides certainty about the validity of the attributes within the credential and also about the fact that they have not been changed since issuance. Furthermore, credentials hide the attributes; so, seeing a credential, one cannot deduce any information about the attribute values in it. The structure of a credential (i.e. the semantics and types of attributes in it), unlike its content, is public. This enables a card-holder and a verifier to select the appropriate credential(s) for a certain scenario (see example scenarios in Section 'use cases').

Anonymous credentials were already proposed over 25 years ago by David Chaum [9]. They enable individuals to authenticate without identification and to perform unlinkable actions. Stefan Brands [4] suggested practical and efficient cryptographic protocols for implementing digital credentials that include multiple attributes. Recently, this notion was renamed

to attribute-based credentials (ABCs). An ABC may contain several attributes that can be shown independently of one another. Brands' protocols belong now to Microsoft and is incorporated in their U-Prove technology [5, 12] and replace Microsoft's earlier Windows CardSpace approach. Jan Camenisch and Anna Lysyanskaya [7, 8] proposed another technology for attribute-based credentials, using zero-knowledge proofs. These schemes are now collected in IBM's Idemix [13]. ABC4Trust [6] aims to create a common architecture for these technologies.

Our pilot project uses an efficient smart card implementation of Idemix; but conceptually it could also use the U-Prove technology. A smart card may contain dozens of credentials, each with multiple attributes. In a particular attribute-based authentication proof, any subset of attributes in a single credential may be revealed, without revealing the remaining attributes. This is called selective disclosure. Also, several attributes from different credentials may be revealed, like 'over 21' and 'Student'.

Within the context of this project at most four attributes are grouped together in a credential, see Figure 1. The number four is chosen pragmatically, mainly for implementation reasons, but other reasons turn out to support this choice. On the one hand, having many attributes in one credential means that if only one attribute is revealed, all the others remain hidden. Hiding more attributes requires more time, and thus reduces the performance. On the other hand, the number four seems to be reasonable to form a coherent set of attributes, issued jointly by a single authority.

All credentials are required to contain two additional basic attributes. First, an expiry date has to be determined at issuance, and it is included as an attribute applying to the whole credential. When the credential is verified, the expiry date can be revealed to confirm validity. Second, each user has a master secret key, stored in the smart card's secure storage, which is also incorporated – technically, like an attribute –, in all credentials.

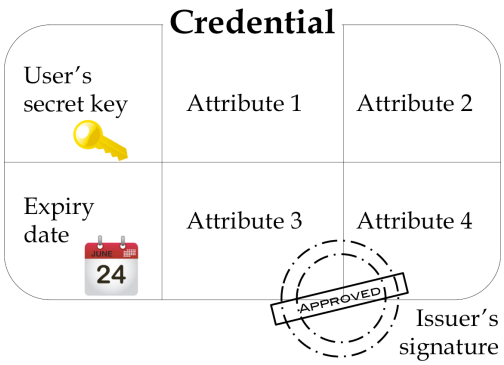



**Figure 1:** The structure of an attribute-based credential with two reserved and four 'free' attributes.

**Roles –** In attribute-based identity management we distinguish the following roles.

1. **Users** are people who own a smart card that holds valid attributes; validity means that the attributes on the card are valid for the card-holder (and are not expired).

2. **Issuers** are the authorities that sign credentials with attributes and provide them to Users. For instance, citizen registration authorities are the obvious issuers of 'over 18'

attributes (and of many other attributes as well) and banks are authoritative issuers of bank account number attributes.

3. **Verifiers** (also called **relying parties**) are the parties that verify a subset of the available attributes on a card in order to authorise a transaction. An example verifier is a website that wants to verify the attribute 'over 18' before it allows me to view a certain video online.

4. The **scheme manager** is an independent, non-profit organisation that sets the rules for the different parties (users, issuers and verifiers) and is responsible for the software and smart card management. Of course, these roles can be split up and assigned to different organisations, but that is not so relevant for the current discussion.

**Security and privacy properties –** Attribute-based credentials are assumed to provide the following security properties. (1) The issuer's digital signature ensures authenticity: the credential originates from the issuer, and this issuer assures that the attributes hold for the person. (2) This signature also guarantees integrity: the attributes contained in the credential have not been changed since they have been issued. (3) A credential is non-transferable as it is bound to the card of the person involved in the issuing protocol.

Furthermore, an attribute-based credential protects the privacy of its owner by the following cryptographic properties. (a) A credential hides its content, so it does not reveal the attributes that it contains. (b) Issuer unlinkability assures that any information gathered during issuing cannot be used to link the credential when it is shown. (c) Multi-show unlinkability guarantees that when a credential is shown multiple times, these sessions cannot be linked. The privacy of users is protected by both of these unlinkability properties even if the credential issuer and all verifiers collude.

**Implementation used in this pilot –** In this paper we rely on technical assumptions from the pilot project that we are working on. We make these assumptions explicit.

1. The smart cards are MULTOS cards[3], because they provide relatively easy access to cryptographic primitives. The cards communicate via a wireless interface. Preferably, card readers are used that have a (secure) PIN pad. In the (near) future, widely employed card readers will probably be NFC enabled smart phones and tablets.

2. Attributes are stored on smart cards in credentials; each credential can store up to four attributes, which are collectively issued (and signed) by one issuer. Hence, one design criterion for the contents of credentials is that all the attributes involved should fall under the responsibility of a single issuer.

3. Selective disclosure is an essential functionality. The verification of one or more attributes from the same credential can be done rather efficiently, taking on average in the order of one se-

[3] http://www.multos.com

cond[4]. Verification of multiple attributes from multiple credentials is also possible (within one session), but then the verification times add up, proportional to the number of credentials.

4. Issuing takes place per credential (and not per attribute) and is rather slow: in the order of 3 to 4 seconds. Typically, issuing is done either during a physical session (e.g., at the town hall) or online at a device that the user trusts (e.g., a personal tablet or a home PC).

   As a result, attributes are appropriate for rather static scenarios, and not for dynamic scenarios, such as an electronic purse, where the monetary value on the card is stored as an attribute: spending money would involve both verification (of the old amount, before paying) and re-issuing (the new amount, after paying). This is simply too slow with the current smart card technology.

5. Users have a 'card management' environment at their PC or other device, in which they have read/delete/update access to all the data on the card. Within this environment they can see dependencies (in tree-form, like in Figure 2) and inspect access logs. Furthermore, users can delete credentials or initiate to update them.

6. The whole process in relation to attributes and credentials takes place using open standards (and to a large extent even via open source software). This means that, in principle, every organisation or individual can use the same card for their own purpose, by issuing and verifying their own attributes. However, the scheme manager controls access to the cards (see also in Section 'Problems and decisions'). This happens by special certificates that terminals need to have before cards are willing to communicate with them. The role of the scheme manager enforces a certain level of consistency among issuers and verifiers and (thereby) protects the cardholders.

## Use Cases

This section gives an informal description of some of the use cases that we foresee for attribute-based authentication. As the current discussion considers attributes of a wide variety, we let attributes be non-identifying as well as identifying. We do not address however the problem of attribute semantics or anonymity sets in different scopes. While ABCs were originally devised for anonymous applications, we are convinced that they provide many more usage and application opportunities with (partly) identifying attributes. The use cases described shortly below form the basis for some further discussion of issues analysed in Section 'Problems and decisions'.

**Age bounds –**The attribute that is most needed now is probably the minimal-age attribute, like 'over 18'. It will be useful for many online and offline transactions, such as buying/playing (violent) games, alcoholic drinks, cigarettes, (certain) movies or books, online gambling, etc.

[4] This one second is good enough for verifications online or offline, say in a shop, but too slow for entrance control like in public transport; in such cases the required maximal transaction time is typically 0.3 second.

Analogously, one may form maximal-age attributes, like ‘under 15’. They may be used to regulate access to certain chat rooms, which are set up exclusively for minors.

Within the Idemix context there are ‘interval proofs’ which make it possible to derive these minimal- and maximal-age attributes from the date of birth. Such proofs are computationally rather expensive and are (currently) not included in this project. Instead, minimal-age and maximal-age credentials are foreseen consisting of the form:

| minimal junior |
|---|
| $\geq 12$ |
| $\geq 16$ |
| $\geq 18$ |
| $\geq 21$ |

| minimal senior |
|---|
| $\geq 60$ |
| $\geq 65$ |
| $\geq 70$ |
| $\geq 75$ |

| maximal junior |
|---|
| $< 12$ |
| $< 16$ |
| $< 18$ |
| $< 21$ |

The most authoritative issuers for such credentials are local or national authorities, using their citizen registration database.

**Citizen Identity** Your identity as citizen may be organised in three credentials:

| name |
|---|
| family name |
| first name |
| full first names |
| initials |

| identity |
|---|
| social security nr. |
| date of birth |
| place of birth |
| gender |

| address |
|---|
| country |
| city |
| street + number |
| postal code |

As before, public authorities are the most authoritative source to issue such credentials. Recall that each of these attributes can be used separately in authentication. But also combinations of these (and other) attributes are possible.

**Loyalty Cards and Pseudonyms –**Shops, or other commercial organisations such as airlines, like to build a relationship with their customers using loyalty cards, giving them selected benefits when they have accumulated enough loyalty points. Applying such cards, these shops can keep track of who purchases what and this allows them to build up detailed profiles of their customers. In practice, each chain of shops issues its own (virtual) loyalty card. This is no longer needed with an open card, since each chain can add its own loyalty credential to it.

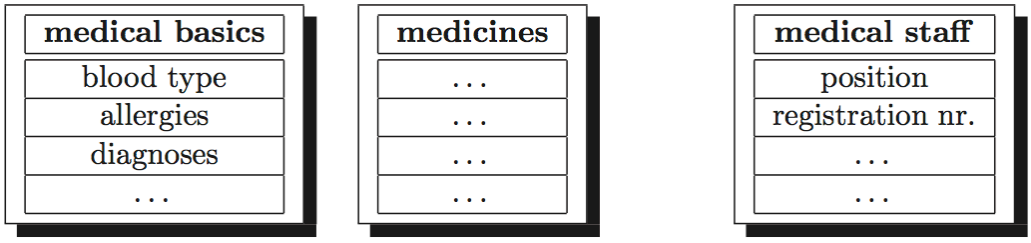
| shop X loyalty |
|---|
| customer number |
| customer status |
| ... |
| ... |

The customer number in the credential acts as a key for a database entry in the back office that contains the actual purchase history of the customer (cardholder). On the basis of this history, a customer may reach a certain status, like bronze/silver/gold. In each shopping situation the customer may be offered the option to buy anonymously, using only the status attribute to get certain benefits, or to buy non-anonymously using also the customer number. Only in the latter case, the purchase is added to the personal history (in the back office) and contributes to the status build-up. The remaining two attributes, written as ‘…’, are left open and can be used for other customer relationship management (CRM) purposes. They can also be left empty (blank).

A cardholder may use his/her card with this credential offline, in a 'brick and mortar' shop. But it can also be used online, to purchase something, or to access an overview of the cardholder's purchase history and, possibly, to update the status attributes. For these purposes, the loyalty number attribute is sufficient as authentication. Of course name & gender are nice to have for communication purposes, but they need not be the real ones. An address credential may be required in case of delivery. It can be verified per transaction, and need not be stored centrally.

Such customer numbers in credentials may thus be used as pseudonyms, one for each commercial relationship (with shops X, Y, Z, etc.). There is a potential privacy risk when many commercial organisations decide to cooperate and use one number for all of them. In this way they can profile customers across different organisations, a bit like it is done now via third party cookies or device fingerprinting. Such broad commercial use of a single pseudonym, possibly at a national level, may be forbidden by the scheme manager and/or by the relevant data protection authority.

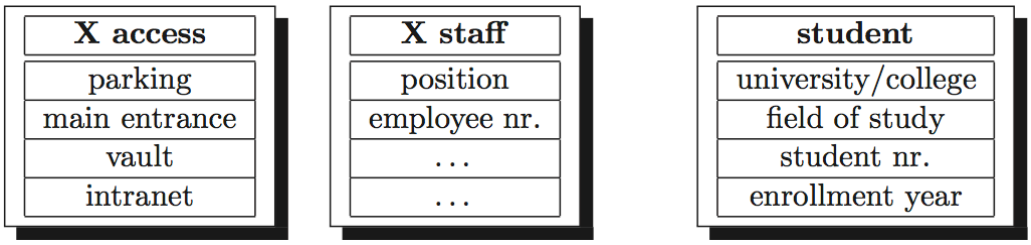
**Medical information –** In a medical context one can envisage attributes for patients and for medical staff. Patients can carry for instance credentials with attributes containing essential personal medical information in a micro-dossier, see the first two credentials below. Medical staff can use credentials that describe their medical role and access rights to patient files, as suggested in:




The first two credentials may be issued by health authorities (hospitals, or even general practitioners). They are useful in medical emergency situations, like after an accident. The last credential falls under the responsibility of health staff registration authorities. The 'position' attribute typically determines access right to medical records, such as: doctors may both read and write, but nurses may only read. For accountability, the registration number should be used in each such transaction in order to monitor who accesses which file.

At this stage, it becomes clear that designing the content of credentials is not entirely trivial, and requires knowledge of the relevant domain of use. Another thing to note is that the names of the cardholder are not included in these credentials. For now it suffices to say that the name occurs in a Name credential, so there is no need to repeat it. But this 'overlap' matter will be discussed further below.

**Access control and role/claim-based access control –** Within one company/organisation X, a credential can be designed for specific access rights, roles, positions, etc., as suggested in:




**Issuing a mobile phone number credential** So far we have concentrated mostly on the contents of credentials. We now look at how the issuing of credentials might work. Suppose you wish to obtain a credential containing your mobile phone number. The obvious issuer is your mobile network operator (MNO). The issuing procedure might work via the following steps.

1. You go to the website of the MNO, using https, and prove using your IRMA card your name and date of birth.
2. The MNO looks in its database if there is a contract with this name and date of birth[5]; if not, it aborts; if so, it sends a one-time code over SMS to the (mobile) phone number associated with this contract.
3. Upon receiving this one-time code, you feed it back into the website (within the same https session).
4. The MNO now issues the credential containing your phone number, possibly together with some other attributes, to your card.

What is interesting about this protocol is that it involves authentication that uses both existing credentials and an out-of-band channel. The use of existing credentials leads to dependencies among credentials, as described in the next Section.

**Festival ticket –** We conclude this list of use cases with a non-standard application of attributes, in order to suggest the great variety and breadth of possible usage scenarios. If you wish to get a ticket online for a pop concert or other festivals, you often need to fill out long forms requiring personal information. The main purpose – apart from profiling – seems to be to prevent transfer of tickets. One may also provide such a ticket in electronic form, after payment, as a credential for the festival at hand, containing for instance: the festival name & date, a ticket number, any additional pre-paid consumptions, etc. Upon entering the festival terrain, the presence of a valid ticket on a card can be checked (and consumption vouchers can be handed over). The next day the ticket/credential is unusable, and can be removed from the card (by the card owner).

[5] In many countries, before obtaining a mobile phone subscription, a copy of an identity document must be handed over; this practice is assumed to be the case here.

## An Example Credential Tree

As we saw in Figure 1, credentials are containers of attributes signed by an authoritative issuer. An issuing procedure requires some sort of authentication to prove that a specific card is entitled to hold a credential. This authentication can include the verification of already existing credentials on the card. On the one hand, so-called root credentials do not rely on other credentials on the card. They require only out-of-band authentication. Dependent credentials, on the other hand, are issued only after verifying at least one other existing credential on the card. Technically, it is essential that the verification and the issuance happen in the same secure session.

Figure 2 shows a dependency graph, a possible arrangement of digital credentials logically residing on a card in the IRMA project. In this example, there are two root credentials. An Academia credential represents the cardholder's identity in the national education system. A Citizen root credential can be used by a broader audience in a broader context. These root credentials can be issued after a personal, face-to-face identification accompanied by a physical identity document authentication.

A Student credential, for instance, relies only on the Academia root. After a student proves that he or she has such a root credential with the appropriate attributes of Organisation and unique student identifier (SID), the organisation can look up all relevant personal data in its database and issue the Student credential. Note that this issuing procedure requires identification since a Student credential is bound to a specific person. A university's Library credential can be issued similarly relying on an already existing Student credential. It can depend on policies, defined by the Scheme manager, which attributes a particular issuer is eligible to verify in relation to issuing a particular type of credential.

Issuance therefore often requires verification of credentials on the card, not only an out-of-band authentication. The simplest case is when only one credential is verified. But authentication can include multiple credentials residing in different parts of the dependency graph. Business scenarios, involving legal obligations, often require credentials from the citizen 'tree'—not only from the one that provides discount for the customer. A festival, for instance, may offer cheaper tickets for students (academia) while requiring certain minimum age (citizen) to give a voucher for alcoholic drinks.

We foresee that the scheme manager decides in a contract with each Issuer what the dependencies and (out-of-bound) authentication methods are (required for issuing). These matters will then be made public, so that others (esp. Verifiers) know what they can/cannot rely on.

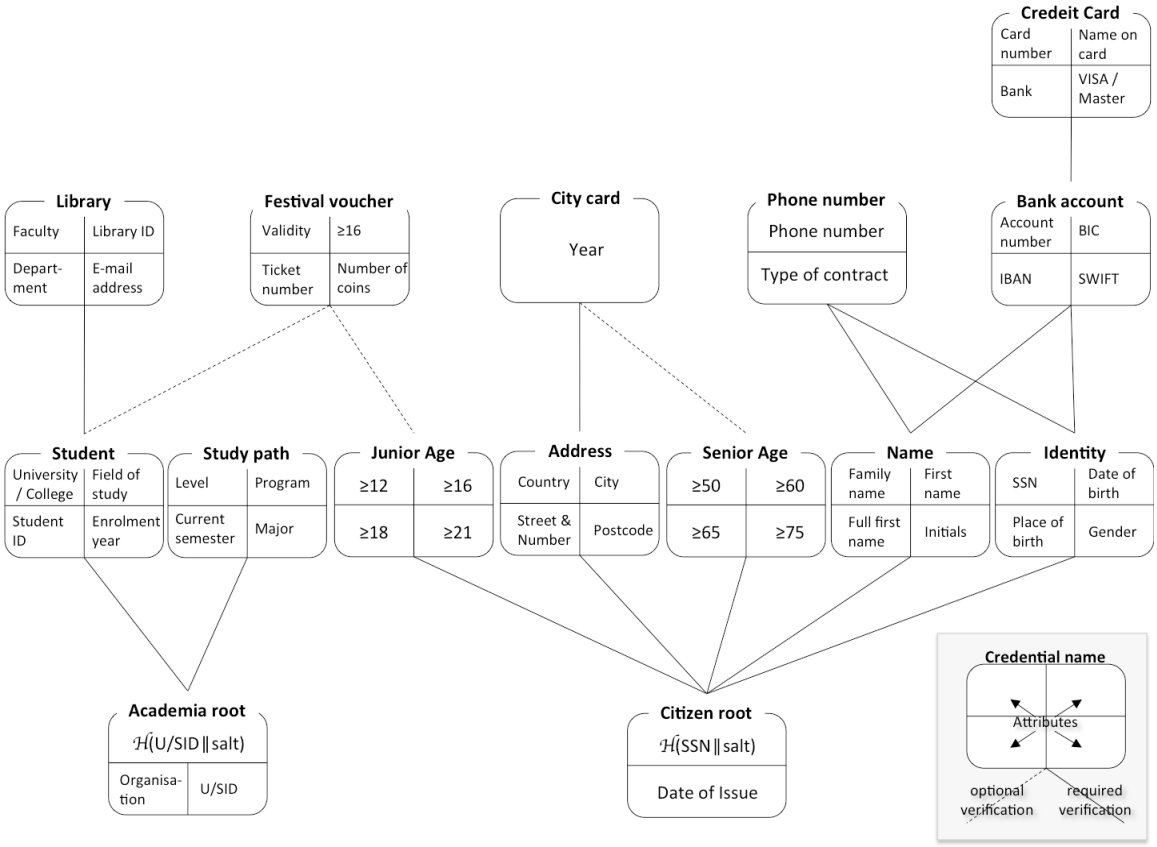



**Figure 2:** An example for credentials and dependencies.

## Problems and Decisions

This section discusses several issues that we came across in setting up the IRMA pilot project. Although we recognise the importance of cost and liability in deploying a new technology, these considerations are out of scope in this study. In the decisions we took the main motivations were: simplicity of the set-up, intuitiveness of usage, protection of privacy, and security.

**Outside of a card –** In online usage the outside of a card is irrelevant for the issuer or the verifier. The only practical requirement is that the card owner should recognise his/her own card (to prevent confusion). In offline scenarios, however, the verifier should be able to check that the person presenting a card is the cardholder. This is done via two mechanisms:

- on the front of the card there is a picture of the cardholder—and nothing else;
- the verification of many attributes is only possible after a PIN is entered; as a result, if someone else wishes to use your card, you should also give your PIN. This works as hindrance.

At the back of a card there is (general) information about how lost cards can be returned. Additionally, there is a card-specific number. It can be used to look up the owner of a lost-and-returned card. The card number is a dangerous addition that could make it possible to trace cards. Therefore, the card number is used only externally, and not internally, in the chip.

**Restricting relying parties –** One serious challenge is how to make sure that a verifier (relying party) does what it promises: if a web shop says it only needs to see my 'over 18' attribute, how do I know that it does not read all other attributes as well? There are several possible approaches.

1. A purely **legal** one: let verifiers sign a contract with the scheme manager in which they commit themselves to behave as they promise.
2. Add a posteriori **monitoring**: make sure that the card logs all transactions, and take (legal) action if a verifier reads too much.
3. Add a priori **technical restrictions**: verifiers obtain a certificate from the scheme manager that will be checked by the card and that contains the attributes that the verifier may read; the card is programmed in such a way that it only reveals the attributes that are listed in the certificate.

The first two options provide no protection against rogue verifiers, operating outside the span of control of the scheme manager. The last solution is therefore the most secure one, but also the most inflexible and complicated one, since it requires an elaborate certificate management policy. It is the preferred solution within the IRMA project (although it is not yet implemented).

With this third solution in place, protecting card reading by a PIN is less urgent – increasing user convenience. For instance, it is not wise to protect medical emergency data by a PIN, since the cardholder may not be able to provide it when needed most. But by providing only to medical emergency services a certificate to read the medical data, the privacy risks are reduced.

An alternative solution is to use designated proofs [2] in which the prover can control which verifier can receive particular attributes. Selective disclosure (see in Section 'Technical background') enables to restrict which attributes are revealed, while designation enables to restrict which verifiers can receive those attributes. When this technique is applied, verifiers are required to have secret keys for being able to compute those attributes. As this technology entails an additional infrastructure for designation keys (or certificates) and is still in its infancy, we do not use it at this stage of the IRMA project.

**PIN use and card management –** In general, access to a card can be protected by a PIN. This is used to ensure:

- **confidentiality**: to prevent unauthorised reading of private data, for instance, after a card loss; the use of certificates (as discussed above) restricts this risk to some extent, but does not remove it;
- **user consent**: to make sure that a card is only used when the cardholder agrees;
- **authentication**: the card is only usable by the card owner; in particular, someone else who obtains/finds a card cannot use it.

It is clear that the addition of new credentials to a card should be protected by a PIN, to guarantee consent & authentication. But when should revealing of attributes be protected by a PIN? You may think of the fairly innocuous 'over 18' attribute. But it should not be possibly that my little nephew temporarily borrows my card to do/obtain 'over 18' stuff online. Hence the age credential should be PIN-protected. Attributes that give access to a parking or open an entrance are typically not PIN-protected, except for high-security facilities.

If some credentials require PIN-protection and others do not, the question arises: who decides about this? Of course it can be left to the card reader or the user to set PIN-protection, but probably following some general policy is better. This policy should be set in general terms by the scheme manager, and elaborated in detail with each credential issuer.

**Card hand-over –** A User obtains a card during a face-to-face protocol, called card hand-over. It involves verification of the (external) photo, PIN setting by the new card owner, and issuance of a number of root credentials. In the database of the scheme manager an entry will be maintained involving the external card number, contact details of the card owner, and a timestamp recording the hand-over.

**Expiry and revocation –** In the current stage of the pilot project revocation will not be implemented although in a large-scale project this functionality is essential. Recent developments [11] show that privacy-friendly revocation techniques are reaching performance figures that make addition of revocation possible at some later stage in the project. Expiry data in credentials, see Figure 1, put some limit on the usability of credentials after a card loss. Additionally, some identifying attributes, containing for instance a registration number, can be blacklisted on the basis of their content.

**Attribute duplication in the tree? –** In the credential examples in Section 'Use cases', we have seen that a cardholder's name occurs in the Name credential (obviously!), but not in a medical staff or employee credential. This may look unexpected at first. In principle, there could be multiple name attributes, issued by different parties (like local authorities, or Facebook; see below). Similarly, multiple accounts at different banks or different phone numbers can be issued in separate credentials. It is the role of the scheme manager to decide which organisations are authoritative about a type of credential. Verifiers can then decide which issuer they wish to trust for having attested to certain attributes. However, we propose as few attributes to be issued by multiple issuers as possible for simplicity and efficiency. In fact, so far we are excluding any duplication of attributes (same content, different issuers).

**Facebook – root credential or not? –** In what follows, we take Facebook as example in considerations that apply to many other, similar organisations. If you sign up for Facebook, you choose the name that you like (within certain technical/decency limits). Facebook has a Real Name Policy, but it has no way of checking that the name you provide is your real one. Many people like to use a pseudonym on Facebook and currently this is possible.

Now suppose Facebook wishes to join the project at hand and use smart card based credentials for authentication. The credential only needs to contain Facebook's user ID. An

interesting question is: should this be a root credential or not?[6] This technical question has wide societal relevance.

1. Facebook probably does not want to have a root credential: it likes to first verify the (real) name on the card (and probably more attributes), before issuing its own credential. In this way Facebook can enforce its Real Name Policy.
2. People who don't wish to use their real name on Facebook expect Facebook's credential to be root, not depending on any other.

There will be many other organisations like Facebook who are interested in issuing and using their own credentials if they can be based on other (reliable) attributes: probably Skype, but possibly also your favourite book store chain. Should the scheme manager allow this, and on which grounds? These decisions are political in nature, and they involve the identity fabric of our society and also considerable commercial interest. For this reason, we firmly believe that the scheme manager should be set-up and run as an independent non-profit and potentially distributed organisation.

**Omitted functionalities –** In this project, we deployed an efficient implementation of the basics of Idemix. This attribute-based credential technology provides several advanced features that we did not include in this pilot for usability and/or for efficiency reasons. Nevertheless, future use cases and developments may require these functionalities.

- Construction of logical AND / OR zero-knowledge proofs. Proofs about attributes, provided by the card for a verifier, can be combined into one proof by the conjunction (AND) and disjunction (OR) operations.
- Combined proofs using users' master keys. A master secret key must be generated and stored on a card and never leave it. This key, used in each credential, can then be used to construct a single proof about attributes in different credentials on that card. Applying a similar method, this key can be used to bind verification of existing credentials and issuing of a new one on the card. Although this feature provides high security assurance, we chose to use for the time being independent proofs within a previously established single secure session.
- Inequality and interval proofs about attributes. Using inequality and interval proofs, a user can demonstrate properties of attributes (see an example at the Age credential in Section 'use cases'). Furthermore, an identifier attribute can be demonstrated to be on a membership list without disclosing the identifier.

[6] Within the pilot phase Facebook is not involved, but a similar issue has come up; we decided in favour of a root credential, thus preventing dependencies and verifications of other attributes.

In spite of these omitted functionalities all privacy and security properties (see in Section 'Technical background') of the Idemix system are incorporated.

## Conclusion

In this paper we described the relevance and challenges of credential design in attribute-based identity management. Several use cases demonstrated the breadth of possible applications on a smart card that supports attribute-based credentials. The main reason for this diversity is that attributes, issued by the most authoritative organisations, can be disclosed independently. Therefore, verifiers learn all relevant information to authenticate and authorise users but nothing more, thus contributing to data minimisation.

**Recommendations** We conclude the paper with six principles for credential design in the context of attribute-based credentials.

1. Attributes in one credential form a coherent set.
2. Each attribute in one credential falls under the responsibility of a single most authoritative issuer.
3. Attribute duplication (same content, multiple issuers) is avoided.
4. Verifiers can read only a limited, predefined set of attributes.
5. Credential dependencies are public.
6. An independent non-profit scheme manager should decide about such dependencies.

## References

[1] Joerg Abendroth, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Ahmad Sabouri, Eva Schlehahn, Yannis Stamatiou, and Harald Zwingelberg (2012). D7.1 Application Description for Students.Technical report, ABC4Trust.

[2] Gergely Alpár, Lejla Batina, and Wouter Lueks (2012). Designated Attribute-Based Proofs for RFID Applications. In RFID Security and Privacy – RFIDsec 2012. LNCS.

[3] Souheil Bcheri, Norbert Goetze, Monika Orski, and Harald Zwingelberg (2012). D6.1 Application Description for the School Deployment.Technical report, ABC4Trust.

[4] Stefan A. Brands (2012). Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge, MA, USA.

[5] James Brown, Phil Stradling, and Craig H. Wittenberg (2011). U-Prove CTP R2 Whitepaper.Technical report, Microsoft Corporation, February 2011.

[6] Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Kai Rannenberg, and Harald Zwingelberg (2011). D2.1 Architecture for Attribute-based Credential Technologies.Technical report, ABC4Trust.

[7] Jan Camenisch and Anna Lysyanskaya (2001). An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In Birgit Pfitzmann, editor, Advances in Cryptology — EUROCRYPT 2001, volume 2045 of LNCS, pages 93–118. Springer Berlin / Heidelberg.

[8] Jan Camenisch and Anna Lysyanskaya (2003). A Signature Scheme with Efficient Protocols. In Stelvio Cimato, Giuseppe Persiano, and Clemente Galdi, editors, Security in Communication Networks, volume 2576 of LNCS, pages 268–289. Springer Berlin / Heidelberg.

[9] David Chaum (1985). Security without identification: transaction systems to make big brother obsolete. Communications of the ACM, 28:1030–1044, October 1985.

[10] S. Farrell and R. Housley (2002). RFC 3281: An Internet Attribute Certificate Profile for Authorization, April 2002.

[11] Jorn Lapon, Markulf Kohlweiss, Bart De Decker, and Vincent Naessens (2011). Analysis of Revocation Strategies for Anonymous Idemix Credentials. In Bart De Decker, Jorn Lapon, Vincent Naessens, and Andreas Uhl, editors, Communications and Multimedia Security, volume 7025 of Lecture Notes in Computer Science, pages 3–17. Springer Berlin / Heidelberg.

[12] Christian Paquin (2011). U-Prove Cryptographic Specification v1.1.Technical report, Microsoft Corporation, February 2011.

[13] IBM Research Zürich Security Team (2012).Specification of the Identity Mixer cryptographic library, version 2.3.4.Technical report, IBM Research, Zürich, February 2012.

[14] Eric Verheul (2001). Self-Blindable Credential Certificates from the Weil Pairing. In Colin Boyd, editor, Advances in Cryptology — ASIACRYPT 2001, volume 2248 of Lecture Notes in Computer Science, pages 533–551. Springer Berlin / Heidelberg.