HUMAN RIGHTS AND DIGITAL TECHNOLOGY

Digital Tightrope

Susan Perry
Claudia Roda

Human Rights and Digital Technology

Susan Perry • Claudia Roda

Human Rights and Digital Technology

Digital Tightrope

palgrave
macmillan

Susan Perry
American University of Paris
Paris, France

Claudia Roda
American University of Paris
Paris, France

ISBN 978-1-137-58804-3 ISBN 978-1-137-58805-0 (eBook)
DOI 10.1057/978-1-137-58805-0

Library of Congress Control Number: 2016957155

Printed on acid-free paper

This Palgrave Macmillan imprint is published by Springer Nature
The registered company is Macmillan Publishers Ltd.
The registered company address is: The Campus, 4 Crinan Street, London, N1 9XW, United Kingdom

For Andrew and Gilbert

Relevant International Human Rights and Humanitarian Declarations and Treaties

Universal Declaration of Human Rights. (New York, 1948)
International Convention on the Elimination of All Forms of Racial Discrimination. (New York, 1965)
International Covenant on Economic, Social and Cultural Rights. (New York, 1966)
International Covenant on Civil and Political Rights. (New York, 1966)
Convention on the Elimination of all forms of Discrimination Against Women. (New York, 1979)
Convention Against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment. (New York, 1984)
Convention on the Rights of the Child. (New York, 1989)
Rome Statute of the International Criminal Court. (Rome, 1998)
Convention on the Rights of Persons with Disabilities. (New York, 2006)

Preface and Acknowledgments

The scholarly collaboration that led to this book began nearly twenty years ago in the analogue age. When we first met in the 1990s, one was publishing her work on artificial intelligence, while the other was learning to send her first emails. One was well into her career as a human rights defender, while the other's only experience with the law had been to file for a marriage licence. In short, neither knew much about the other's disciplinary expertise.

Cross-disciplinary collaboration requires clarity, intellectual flexibility and a good sense of humour. Our early conversations stretched across a multitude of subjects. As our interest in interdisciplinary work grew, we developed the friendly habit of patiently explaining the technicalities of our discipline(s) to one another, a habit we have put to good use in writing this book. Our experience reinforced what we had already suspected: designing sustainable and just solutions for our digital world requires unabashed navigation across disciplinary boundaries. The negotiation of alternative approaches also demands a broad view and willingness to compromise. Our understanding of these trade-offs forms the core of this book.

The awarding of a European Commission grant to work on privacyby-design methodologies in 2013 gave us the means to move forward with our scholarly collaboration. Under the auspices of Project PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research at: http://pripareproject.eu), we designed a mixed curriculum on human rights and digital technology (with a focus on privacy) and were able to test-drive our course with students at The American University of Paris. We began to co-publish on a range of technology-related issues and

to exchange ideas with colleagues from across Europe, as we collaborated to develop privacy methodologies adapted to the digital age. Our book is far richer thanks to input from our students and colleagues, and we would like to thank them here.

Students in our team-taught course, Human Rights and Digital Technology, learned with us as we experimented with a curriculum that mixed law and science. Our PRIPARE colleagues Antonio Kung (Trialog and AUP), Frank Kargl (University of Ulm) and David Wright (Trilateral) joined us in the classroom for individual lectures on their areas of expertise; our exchanges with them have been particularly enriching for us and for our students. Our gratitude also goes to José María del Álamo (Universidad Politécnica de Madrid), Fanny Coudert (KU Leuven), Alberto Crespo Garcia (ATOS), Hisain Elshaafi (WIT), Christophe Jouvray (Trialog), Henning Kopp (University of Ulm), Inga Kroener (Trilateral), Yod Samuel Martín (UPM), Daniel Le Métayer (Inria), Nicolás Notario McDonnell (ATOS), Carmela Troncoso (Gradiant), Pagona Tsormpatzoudi (KU Leuvan), and the many others we cannot mention here, for their insightful input, organizational skills and warm hospitality.

Our student researchers Jed Carty, Alyssa Evans, Rachel Fallon, Anna Wiersma and Zona Zaric provided steady support, as did our professorial colleagues Kerstin Carlson, Kathleen Chevalier, Waddick Doyle, Philip Golub, Julie Newton, Claudio Piani, and Georgi Stojanov. We deeply appreciate their enthusiasm and scholarly feedback. Julie Thomas' comments on a late draft of the book were especially precious and we are sincerely grateful for her suggestions.

Finally, Christina Brian and her editorial team at Palgrave have championed this book from the earliest stages. We thank Christina warmly for her support throughout. Christian van den Anker generously provided invaluable input in the latter stages of this work. Last, but not least, our families have been very patient as this book has taken form. We dedicate our work to them.

Susan Perry
Claudia Roda
Paris, France

Contents

CHAPTER 1

Introduction: A Question of Balance

This book explores the application of a human rights framework to the roll-out and use of digital technologies. Such an innovative connection between two distinct disciplines—law and technology—allows us to understand more fully the dense, multidimensional nature of the digital revolution and how we are going to live with it. When we speak of digital technology, our focus is often prohibitively narrow; taking our cues from scientific research models, we examine the parts rather than the whole, inadvertently isolating hardware from software, the technological frameworks from their actual use, or the costs of the digital revolution from the benefits. The existing body of international human rights treaty law requires a balancing of fundamental rights and freedoms,[1] an exercise which, when applied to technology, encourages us to evaluate and prioritize in a more ethical fashion the ways in which we use the machines that surround us. We define technology both as science and in its original sense, *tekhnologia*, meaning the study of art, skill and craft. We acknowledge that human rights serves both a moral and legal purpose, one in which the normative development of individual and collective rights is often contested despite the broad, enabling language of many of the international and domestic legal texts.[2] Thus, while it is somewhat risky to predict the outcome of any revolution, our application of a multidisciplinary approach allows us to highlight several of the most challenging aspects of the digital transition and to engage in thoughtful reflection on how to find balance between technological advances and citizens' rights.

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_1

In many respects, human beings have become virtual tightrope walkers, poised between two remarkable acquisitions of the post-Cold War period: the simultaneous expansion of the international human rights framework and the network of information technologies. Although these processes began long before the fall of the Berlin Wall, the promulgation of binding treaty law for the implementation of human rights has continued apace since the end of the Cold War, alongside the proliferation of multiple channels of communication offered by the growth of information technology during an intensified period of globalization. This dual paradigm has created new tensions between individual citizens and their states. Certain philosophers refer to this as the 'Great Transition', a time of fast-track social change.[3] We support the notion that digital technology reinforces shifting political, social, and economic patterns. In what is rapidly becoming a society of multiple loyalties (Hedley Bull's prescient 'neo-medievalism'[4]), human beings experience governance in a highly personalized manner. The middle ground of the nation state, once the recipient of individual loyalty, has given way to an interdependent, globalized economy and weak, but expanding systems of world governance; these evolving economic and political systems are underpinned by ambitious municipalities, feisty civil society organizations, powerful transnational corporations, and extended virtual networks.[5] The human rights framework on a national and international level interacts with digitally driven networks to provide citizens with leverage to safeguard their rights. In fact, 83 per cent of users surveyed by the Internet Society believe that Internet access should be considered a basic human right.[6] And yet, as digital technology users learn to intervene in governance in myriad innovative ways, governments and companies are using the same technology to interfere with human lives on a brand new scale. It is the dense, contested nature of this interaction that creates the potential for greater democracy or abject tyranny.

Digital technology is complex and, generally speaking, extremely stable within a given design parameter. Nonetheless, if we apply C.S. Holling's resilience theory from the field of ecology,[7] our sophisticated machines are often surprisingly fragile outside of the parameters for which they were designed, leading to a host of unintended, potentially serious consequences. As science and business join forces to make critical decisions in the roll-out of new technologies, they do so well in advance of regulatory frameworks and often with little regard for the diverse consequences of their hardware and software choices. The flattening, transformative power of information technology heralded by pundits may well be a lure,[8]

an illusion that promises a neat and simple response to the intricacies of contemporary life and, more particularly, the unintended consequences of our technology. Only if we view the world as a round, knotty interaction of humans and machines, of digital causes and effects, can we nurture democratic values in an age of digital revolution.

This book will examine the interaction of key scientific and legal issues that illustrate the tough decisions citizens and societies must make in order to harness the potential of digital technology. Each chapter presents the scientific choices made by researchers and companies responsible for a particular component of the digital revolution—base transceiver stations, Internet surveillance and censorship software, the Internet of Things, and massive open online courses—and analyses different ways to extend existing law to include these technologies. We have chosen to emphasize specific human rights that are both enhanced and violated through use of digital technology; these include an individual's right to privacy, health, and education, to freedom of expression and freedom from discrimination. Because the impact of technology extends well beyond the individual to society as a whole, we also examine the consequences of technology with respect to collective rights, such as public health, a pollution-free environment, ownership of the global commons or human-robotic interaction. Throughout this book, we demonstrate that the law to regulate digital technology with respect to the individual is already in place, the fruit of centuries of public debate and conflict that course through the constitutional and international treaty law of the twentieth century. We argue that the law need only be fine-tuned to protect the individual from the potentially negative consequences of the digital revolution. Even though some fine-tuning has already occurred, such as the Chilean Tower Law on electromagnetic pollution or the Chinese government's inclusion of data software protection as intellectual property, this book will show that the application of individual human rights protection to digital technology is still in its infancy. We also insist that human rights protection takes into account the impact of digital hardware and software on a range of collective rights, a newly developing area of human rights law that we believe is critical to our ability to harness technology for the greater common good. The separation of hardware infrastructure from software systems, or the citizen from the collective only serves to slow down implementation of existing human rights protections. The examples presented in this book aim to foster an in-depth analysis of the costs and benefits of key components of the digital revolution, and demonstrate the remarkable resilience

of people everywhere as they learn to use and adapt digital technology to their own needs; they do so often in the face of extraordinary political or commercial pressures to extend control over users and their communities.

1.1 Historical Overview

Determining the precise balance between a particular technology and the application of international legal obligations allows us to reflect on how we intend to walk the digital tightrope in the years to come. Before laying out the architecture of this book, we present an overview of the beginnings of the digital revolution and a brief summary of the international human rights framework.

Technology: The impetus of our current information and communications revolution is driven by three main trends that have guided technology development: (1) increased device ubiquity, (2) improved information storage and management, and (3) widespread connectivity. While the world's first stored computer-program was arguably the early nineteenth century Jacquard textile loom in France,[9] computers have progressed in the last fifty years from highly specialized and prohibitively expensive machines to general purpose, consumer market devices. The first computers that were developed in the mid-1930s served many people at once and usually functioned according to a time-sharing paradigm.[10] The invention of the integrated circuit in 1958, which enabled a single semiconductor to pack-in the essential components of a computer, led to the miniaturization of devices that, in turn, made possible the creation of personal computers in the 1970s. From that point onward, an increasingly large number of people had access to dedicated computing facilities, as the technological infrastructure moved from a configuration where several people shared one computer, to another in which each user had his or her own personal device (Box 1.1).

Parallel to component miniaturization, other technical developments enabled the connection of devices into a set of networks that allowed users both to share resources and to communicate in an increasingly sophisticated manner. Communication through telephone lines was already commonplace by the 1940s and many inhabited areas of the world had some form of connection through either telephone or telegraph. But, as networking through computers became increasingly available in the 1960s, these devices presented a major advantage: computers are able to represent various types of information in a single, digitized format.[11] Digital representation also enabled the transmission of data in a homogenous

manner. Thus, text, images, sound and numbers could all be treated in a similar fashion and stored in a virtual package for easy retrieval or transmission.[12] In the early 1980s, however, communication networks were still scattered amongst networking systems that could not interact. Although the foundations for the Internet were laid as early as the 1960s when researchers first proposed 'packet-switching' as an efficient and robust manner to transmit information over unreliable links, it was only in 1977 that the first few computers were connected using the TCP/IP Internet protocol.[13] Industry, governments, and researchers all agreed that it was necessary to establish a widely accepted standard for interoperable networks that defined how computers should be connected and how they should communicate information, but there was no agreement on the technical requirements. A tipping point was reached thanks to plentiful US government funding, first through ARPANET (Advanced Research Projects Agency Network) and later through the NSFNET (National Science Foundation Network). American academic networks quickly joined, along with British academic networks through JANET (Joint Academic Network). By the mid-1980s, these diverse systems all joined in an inter-net (a connection of networks), with thousands of connected hosts whose communication through the TCP/IP protocol was facilitated by the introduction of domain name servers.[14]

If the success of the Internet was in large part due to the financial support it received from the US government and the fact that important universities and research centres were enthusiastic proponents, another factor that certainly contributed to create widespread support was its innovative management. The Internet permitted bottom-up management procedures that not only allowed for development of the technology, but more importantly established a 'Net culture' that contributed to user demand for a participatory and open collaborative structure. As integrated circuits grew smaller, lighter, cheaper and consumed less energy, processing power and functionality improved exponentially; circuits could be employed in a variety of devices, replacing the mechanical controls of common equipment. Today, each user interacts with many differently-sized devices capable of specialized services: switching lights on and off, taking notes, playing music or making phone calls. From the configuration of one computer typically serving many people in the first half of the twentieth century, we have moved to one computer for each user (the personal computer of the second half of the twentieth century), and finally to the many devices that serve each individual in the current configuration.

International human rights law: According to historians, our contemporary understanding of human rights encompasses three 'interlocking qualities': rights must be *natural* (inherent in all human beings), *equal* (the same for everyone) and *universal* (applicable everywhere).[15] Like the foundations for digital technology, the origins of human rights may be traced to the seventeenth and eighteenth centuries, and the writings of jurists such as Grotius, Montesquieu and Beccaria, philosophers such as Rousseau and Kant, and even novelists.[16] Theory became practice through several key documents that frame our idea of fundamental rights and freedoms: the 1775 American Declaration of Independence, the 1789 Declaration of the Rights of Man and the Citizen,[17] and the Universal Declaration of Human Rights (UDHR), promulgated by the United Nations (UN) General Assembly in 1948 at the close of the Second World War.

The UDHR was just that—a declaration that was non-binding for signatories, but served as the founding document of the UN, expressing the highest standards for human values.[18] Assumptions with respect to the Declaration's universality quickly became problematic, as did principles having to do with *natural* and *equal* rights. With the onset of the Cold War, the USA and its supporters pushed for the rapid promulgation of a binding treaty law on civil and political rights, in keeping with the Enlightenment tradition of individual liberties, while the Soviet Union and its supporters privileged an agreement on economic, social and cultural rights, more closely aligned with socialism and the reluctance of authoritarian governments to permit political pluralism. Certain practitioners call this the debate on *freedom* versus *bread* rights.[19] The UDHR was thus split in two: the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights, both of which entered into force in 1976. These covenants were subsequently joined by sister treaties that extended human rights protection to vulnerable individuals and groups—to women, children, migrants, and the disabled and to those subject to racism or torture. These instruments intersected with an abundant body of humanitarian law, such as the Laws of War and the Geneva Conventions, the Genocide Convention, the Refugee Convention and, more recently, the Rome Statute, which set up the International Criminal Court, the first permanent tribunal to hold individual violators accountable to humanitarian law and related human rights. Enforcement of humanitarian and human rights law through an international criminal court has only just begun; because the court works closely with national governments based on the principle of complementarity

and is mandated to deal exclusively with leaders responsible for the most heinous violations—those that 'shock the conscience of humanity'[20]— few defendants have made it into the dock at The Hague since the first arrest warrants were issued in 2005.

Today, the vast number of daily human rights infringements are subject to the relatively weak enforcement mechanisms of the UN treaty body monitoring system or to the highly varied efficiency of domestic courts worldwide. Consequently, as digital technology has improved access to a wealth of information through extraordinarily wide-reaching Internet search engines and innovative software, citizens have turned to digital cameras, email, social media and mobile phones to communicate knowledge of human rights and rights violations to one another. The speed of this individual and collective empowerment has been nothing short of stunning. Citizens worldwide have taken full ownership of the human rights paradigm and transformed it. Freedom and bread rights have been extended to include collective rights, initially a rubric focused on the rights of indigenous peoples that now embraces environmental and peace rights for groups of vulnerable citizens, the stateless, or any collective entity that claims to represent the voiceless. This book will explore these seminal normative developments. Such advances, when coupled with the recent trend to impose penal liability on individuals who commit violations in the name of a business (an area traditionally beyond the ambit of international human rights law), create powerful new understandings of what constitutes a human rights violation and who is responsible. We suggest that the marriage of digital technology and the extended human rights paradigm embodies a potent force for the twenty-first century.

Nonetheless, at the very same moment that citizen empowerment has accelerated via digital technology, the reach of governments and the private sector has also extended deep into the personal life of the average citizen. This book will examine individual, state and corporate human rights violations in the digital arena. We argue that such violations include government overreach in the case of online surveillance, censorship and the discreet rental of public airspace for ever-increasing broadband emissions, along with corporate creep in the sale of personal and aggregated data (Big Data), steadily higher levels of electromagnetic wave pollution and questions around nascent issues such as robotization. We suggest that while technological advances do not require new human rights, the UN treaty body committees tasked with upholding binding treaty law and domestic governments should accelerate discussion of the extension of the human

rights framework to digital technology. Finally, we insist that education at all levels should not only alert the citizen to the safe use of technology, but provide a venue for training the next generation—those who have grown up with ubiquitous technology—to think and debate about how we wish to live with the digital revolution.

1.2 Five Critical Issues

Given the range of questions that arise from our use of digital technology, we have selected issues that best illustrate the complex challenge of balancing rights amongst different individuals and groups within a community or polity. We examine questions of health, privacy, censorship, control of one's environment and learning, as well as the diverse costs and benefits to democratic governance, in the context of information technology systems and binding human rights treaty law. We start off each chapter with a straightforward lay explanation of the hard science necessary to make different aspects of digital technology work, before turning to a concise explanation of the legal issues that the science raises. We then situate scientific choice and international law within a variety of geographic settings, ranging from the municipal (Paris), the national (China), and the comparative (Europe and the USA), to more familiar settings such as our homes and classrooms. Each chapter makes a series of recommendations in an effort to enlarge the debate and improve our prospects of harnessing digital technology for the greater common good.

Chapter 2 of this book begins with the most critical issue of all—the protection of future digital technology users. Mobile phones, tablets and intelligent machines are designed to function either through wired cables or, increasingly, through wireless wave frequencies. Researchers and commercial telecommunications laboratories have developed and continue to evolve electromagnetic field (EMF) transmissions for wireless communication of digital information. Our fascination with wireless technology—the sleek design of smartphones and tablets, the dizzying range of applications and available information, the ability to be connected at all times—has blinded us to the potential costs of the hardware necessary to make the technology function. As of this writing, there are over five million mobile phone towers worldwide, serving nearly all of the global population. This 'invisible' infrastructure constitutes one of the largest experiments with human biology and environmental capacity to date, and yet scientists are

still debating how to measure its impact and how to evaluate the long-term consequences of electromagnetic wave exposure on the human organism.

Human rights law provides us with a necessary counterpoint in analysing the under-regulated use of wireless technology. Our case study for this chapter is the city of Paris, which has *voluntary* electromagnetic emissions limits and a proliferation of mobile phone towers. The protection of children constitutes a high threshold norm in international human rights law, obliging those states that have ratified the Convention on the Rights of the Child (all but a handful of states have ratified the Convention) to provide 'the highest attainable standards' of protection for children's health. Citing the principle of precaution, we argue for national legislation to safeguard children from prolonged exposure to mobile phone towers via a coherent, planned permit strategy that privileges (1) shared mobile tower infrastructure amongst telecom companies, (2) consultation with residents before installation, and (3) 'white' zones to protect schools and health facilities from overexposure to electromagnetic fields. This does not mean that electromagnetic wave emissions have to be so low that our mobile phones will no longer function, but rather that we find a balance. If we are to deliver on the promise of digital technology to enhance democratic dialogue and facilitate human lifestyles, then we have to make sure that the hardware is safe to use—particularly for the generations to come.

Chapter 3 explores challenges posed by the vast trove of user information stored in digital technology systems. While digital record-keeping may facilitate the protection of human rights in some cases—such as the tracking of child pornography—the inappropriate or non-consensual use of information constitutes a critical threat to the more positive aspects of the digital revolution. As users, governments and private businesses across the globe conflate protection of privacy (a human right) with security threats, we lose sight of the important distinction between human rights violations and criminal activity. This chapter compares European and US approaches to privacy protection, positing that a balance between privacy and security can be achieved through the coupling of appropriate regulatory frameworks and 'privacy-by-design', which provides the consumers of digital technology with choices over how their data is to be used.

The chapter begins with a detailed explanation of the technical means governments and corporations employ to collect our personal online data. The European Union has been a pioneer in promulgating a strict privacy protection regulation that makes personal data security the responsibility of the online service provider, rather than the consumer. And yet, certain

countries with a tradition of strong privacy laws, such as the USA, have collaborated with technology businesses to spy on citizens, thereby violating a host of human rights. PRISM, along with other surveillance programs exposed by the celebrated whistle-blower Edward Snowden, demonstrate the current failure to find a balance between preserving a citizen's privacy and providing states (as well as public and private organizations) with enough information so they can protect all citizens and supply efficient services. We suggest that individual control of personal data is a seminal rights issue that outweighs government or business security concerns in the vast majority of circumstances and we advocate for the incorporation of human rights protection into the design of the actual software itself.

Chapter 4 traces the extension of online surveillance to actual censorship of the Internet. With 3.2 billion users worldwide, the Internet is both a universal crossroads for information exchange and a set of separate compartments divided by language, regulation and policing systems. As indicated in Chapter 3, Internet use involves a range of human rights protections and violations, the most controversial of which may be the question of government censorship. The very premise of the Internet is open access, freedom to innovate, and unfettered collaboration across borders. Online censorship thus strikes a particular chord with users, the majority of whom adhere to remarkably high expectations concerning the Internet as a tool for free expression and information access; users everywhere reckon it is the duty of national governments, as the guarantors of human rights, to protect fundamental liberties, fairness, and justice online.[21]

The power to control access and content lies with national governments and corporate servers. The first example in this chapter analyses the Chinese government's extensive efforts to control Internet use and subject matter through the building of a 'Great Firewall', designed with the help of Western companies and now exported as a model of digital censorship. And yet, despite cutting-edge software design and active policing by tens of thousands of human censors,[22] we suggest that China's state-led censorship policy will prove impossible to implement in the long run. Instead, we propose that the Internet has become an arena for the renegotiation of human rights values in Chinese society, and that the social consequences of this renegotiation are changing the power relations between citizens and state. The second example in this chapter explores hate speech censorship in Europe, pointing to the difficulties in guaranteeing freedom of speech in a climate of ongoing terrorist attacks. Many European countries have adopted broad executive powers enabling their governments

to proscribe material that threatens the state. Despite the very different censorship targets, we argue that efforts at proscription in Europe are just as ineffective as those in China. In fact, we note that the creation of dissident online cultures may be enhanced by state censorship. When combined with the crossover between virtual and physical worlds and the high due process expectations for most users, Internet censorship can lead to an increasingly proactive relationship between citizens and state that resists political categorization or control.

Chapter 5 begins with a milestone: since 2008, more machines than humans have been connected online in a web of shared information that ranges from saving lives to virtual medical diagnoses, from e-voting to selecting a shade of lipstick at one's favourite department store. With little or no public debate, the technology sector and researchers have joined forces to move human society in the direction of a digitized lifestyle—the Internet of Things—claiming that this brave new world will provide a better life for all. We argue that this vision requires a more balanced analysis. We present three scenarios that describe the transformation of our daily lives and the human home, as we know it. This chapter provides an explanation of the technology required for such a transformation, and the hardware and software infrastructure necessary to make interconnected objects function. We argue that the Internet of Things will be problematic in the home unless several factors are urgently addressed: (1) the steadily rising use of electromagnetic frequencies for the wireless transmission of information, and the potential long-term impact on human health, (2) the cost of data storage systems that make exorbitant demands on energy consumption, and (3) vulnerability to technological malfunction in the home. While the lack of coordinated communication systems between machines is a scientific and policy conundrum that could be solved by replacing digital diversity with global uniformity, we caution that such a meta-communications system, while useful, may expose our homes to digital viruses, hacking and service breakdowns, raising additional issues of human control and autonomy.

Substantive public and private investment in research is necessary to explore other means of data transmission (li-fi, or light fidelity, for example), alternative modes of data storage and the promotion of built-in technological diversity to spawn a culture of digital resilience, rather than one-size-fits-all communication between machines. This chapter also explores the great promise that the Internet of Things holds for the realization of human rights for marginalized members of society, particularly

the elderly, the disabled and the disenfranchised. But, we ask what will a fully digitized world look like? What happens to those who choose (or are forced) to live off the grid? Will machines, like people, have rights and responsibilities? How will we experience human autonomy in a world where machines play an increasingly important role?

Chapter 6 investigates the interaction between digital technology and human rights through the design of university curricula. As educators, we examine the question whether online education will replace traditional universities or expand their reach to the farthest corners of the globe. In response to MOOCs (massive open online course), we point to new ways of learning that can encourage technology designers and users across disciplines to reflect on the highly varied impact of digital technology on human society. We present a blended learning curriculum that creates a real-time platform for a global discussion on the integration of human rights into our design and use of digital technology.

This chapter begins with an exploration of e-learning and human attention in digital environments, a subject that one of the authors of this book has explored more fully elsewhere.[23] We suggest that the capacity to learn as we know it may be reshaped more than we realize in a digitized world. We note that education is a seminal human right, one that provides citizens with the ability to access, analyse and apply the body of human rights treaty law to their daily lives. We explore the potential impact of online education on universities everywhere, suggesting that teachers will come to play a determining role in the design of digital curricula and the framing of digital knowledge, and that universities are ideally suited as physical spaces for this endeavour. Finally, we close the chapter with an experiment, a semester-long course in which our own students worked with us to build a curriculum that integrates human rights concerns into the construction of privacy-by-design information materials. By transforming the physical classroom into a laboratory for interdisciplinary reflection and shared knowledge, teachers worldwide may contribute to blended learning at its digital beginnings.

We conclude in Chapter 7 with a reflection on the possibilities inherent in the combination of collective or group rights and low-tech machines and systems that use recycled materials in their construction and little energy to function, leaving a smaller environmental footprint with fewer rights violations. The current model for technology development is based on a dated paradigm of cheap energy and corporate externalization of health and pollution costs to the consumer, a model which does little to reverse accelerated destruction of the environment.[24] Each of the digital

systems discussed in the preceding chapters—wireless communication, massive online surveillance and censorship, and individualized interconnected objects—require the extraction of increasingly rare minerals and ever larger amounts of energy to function. Not only may the sourcing and mining of these resources involve human rights violations, but there is simply not enough lithium on the planet, for example, for the hundreds of millions of electric driverless vehicles to come, nor enough platinum to render their hydrogen equivalents fully operational.[25] The idea of using energy-guzzling technology to create energy-saving solutions, an idea much in vogue in Europe and the USA, is clearly a contradiction. In fact, the paradigm focus on individualized objects, rather than collective low energy systems, may render digital technology too expensive for long-term human use. Given the gravity posed by global warming and the destruction of our environment, we agree with scholar Christien van den Anker that 'ecological sustainability is not solely a human rights issue'.[26] We suggest thoughtful consideration of initiatives, such as 'ecology by design', an analysis of end-to-end impacts that would precede development of every digitized object, or UN oversight of extractable resources, as means to encourage a more sustainable use of new technologies. Climate change and questions of environmental sustainability are likely to trigger a shift in our understanding of human rights from the individual to the collective. As we apply individual rights to groups, vocal insistence on equally sustainable technologies may intensify. If we intend to apply the international human rights treaty law in place to a host of new and exciting developments in the course of the 'Great Transition' that aptly describes the digital revolution, then we must do so in a coherent and systematic fashion, encouraging innovation and dignity for all.

Box 1.1 Computer history

History of the Computer

The first mechanical adding machine was developed in 1642 by B1aise Pascal. In the following two centuries, mechanical and steam operated calculating machines of various complexity were developed. Charles Babbage designed an analytical machine for the first time in 1835. Hollerith's Electric Tabulating System, the first successful electrical calculator, was used for the processing of US census data in 1890. Following the success of his machine, Hollerith

(continued)

Box 1.1 (*continued*)
established in 1896 the company that became IBM in 1917. The birth of digital computers was marked by several events including Zuse's memory capable of storing programs as bits sequences in 1936, Shannon's application of Boolean logic to switching circuits in 1937, and Aiken's digital calculating machine which performed simultaneous arithmetic operations in 1937. The concept of a 'multipurpose' machine, capable of solving symbolic logic problems by reducing them to a sequence of simple operations was initiated by Alan Turing; his 1936 paper *On Computable Numbers* introduced the Turing Machine. Large programmable machines were subsequently developed for war applications (breaking secret codes or determining ballistic calculations, for example). The one machine that best demonstrated the strength of digital computers was the ENIAC (Electronic Numerical Integrator and Computer), developed from 1943–1946. It was enormous by current standards, but could perform 5000 additions or 400 multiplications per second. The many improvements in computer technology, architecture, design and software which followed include: von Neumann work on the logic design of computers; Goldstine's invention of flowcharts (1946); Bell Labs' development of the transistor (1947); the magnetic drum memory (1948); Shannon's studies on communication processes; Hamming's method for correcting errors in blocks of data (1948); Mauchly's Short Order Code, considered the first high level programming language (1949); and Turing's studies on artificial intelligence (1950). In 1951, the predecessors of today's structured programming, microprogramming, and compiler concepts were developed. The first mass-produced computer was the IBM 650 (about 1000 sold) in 1953. The first commercial application of the computer was the payroll program designed for General Electric's UNIVAC in 1955. In 1956 the keyboard was used for the first time to supply input to a computer. IBM's 1957 Fortran (FORmula TRANslator) compiler is still in use in many scientific labs. The first scanned picture was displayed by a computer in 1957. Bell Laboratories developed technology for the transmission of binary data on the telephone line in 1958. The 1958 invention of the integrated circuit is credited to two engineers who worked

(continued)

Box 1.1 (*continued*)

independently: Jack Kilby of Texas Instruments and Robert Noyce, the founder of Intel. In the same year, John McCarthy at MIT invented Lisp (List Processing) for artificial intelligence applications. In 1960, Paul Baran at Rand Corp. developed the packet-switching mechanism, the basis for the Internet. In the same year the COBOL compiler opened up many new possibilities for the business application of computers, and Rosenblatt's Perceptron learned by trial and error to implement a neural network. DEC's PDP-l was the first commercial computer with a monitor and a keyboard. The first departments of computer science were established by Purdue and Stanford Universities in 1962—just in time for students to play the first video game, *Spacewar*, created by an MIT graduate student. DEC's PDP-8 was the first mass-produced mini-computer (1964). In 1973, experimental personal computers were created by Alan Kay and by researchers at Xerox Parc … and the rest is recent history (so to speak!).

Sources: (Association for Computing Machinery, 2000; Institute of Electrical and Electronics Engineers, 1984 and 1996)

Notes

1. Freedom of expression for one individual, for example, may violate another person's right to freedom from discrimination.
2. Risse, T., Ropp, S. and Sikkink, K., eds. (2013) *The Persistent Power of Human Rights: From Commitment to Compliance* (Cambridge: Cambridge University Press).
3. Balandier, G. (2015) *Recherche du politique perdu* (Paris: Fayard).
4. Bull, H. (1977) *The Anarchical Society: A Study of Order in World Politics,* 3rd ed. (New York: Columbia University Press); Kobrin, S. (1998) 'Back to the Future: neo-medievalism and the post-modern digital world economy', *Journal of International Affairs*, Vol. 51, No. 2, pp. 361–386; Arend, A.C. (1999). *Legal Rules and International Society* (Oxford: Oxford University Press).
5. Katz, B., and Bradley, J. (2013). *The Metropolitan Revolution: How Cities and Metros Are Fixing Our Broken Politics and Fragile Economy* (Washington, DC: Brookings Institution Press).

6. Internet Society (2012). 'Global Internet User Survey 2012', *ISOC.*
7. Holling, C.S. (1973). 'Resilience and stability of ecological systems', *Annual Review of Ecology and Systematics,* Vol. 4, pp. 1–24.
8. Friedman, T. (2005). *The World is Flat* (New York: Farrar, Strauss and Giroux).
9. Essinger, J. (2004). *Jacquard's Web: How a hand-loom led to the birth of the information age* (Oxford: Oxford University Press).
10. Time-sharing meant that computing time was shared amongst the needs of all the users. One would typically give one's software program to an operator, who would return the computed results a few hours, or even days later; alternatively, one could connect to the mainframe computer through an available terminal, launch a series of calculations and come back to see the results.
11. A digital quantity is something that can be organised into separate, detectable units. Information, as we normally think of it, is an analogue quantity, because we cannot easily identify units of information. A good example that highlights the difference between analogue and digital quantities is time. Time is continuous and therefore intrinsically analogue; we are able to quantify time by looking at the numbers on our watch, which organise time into digital units. Because analogue watches let us approximate the position of the arms of the watch to the nearest number mark, we are likely to say that it is 'about' 6 o'clock, or 'about' quarter past 6. With a digital watch, time is digitised for us; rather than approximate time to the nearest mark, we read a precise number on the watch screen. There is nothing in between 6:00 and 6:01. It is either one or the other. Thus, a digital quantity is described by discrete units.
12. The first *integrated software packages* of the 1990s were a clear demonstration of the enormous potential of this common representation, combining spreadsheet capabilities with text processing and graphing.
13. Packet-switching is a network communication method that organises information that needs to be transmitted over the network in chunks (packets). By doing so, network communication can be made more efficient (because the use of communication channels is optimised) and robust. Paul Baran is considered by many as the inventor of packet-switching.
14. Domain name servers enable the use of easy-to-remember domain names or identifiers (such as, http://www.someuniversity.edu) rather than IP numbers (for example, 123.456.789.10).
15. Hunt, L. (2007). *Inventing Human Rights: A History* (New York: WW Norton & Company), p. 20.
16. Hunt (2007). *Inventing Human Rights*, pp. 35–69.
17. Those of women followed with the *Declaration of the Rights of Women and the Female Citizen*, drafted by Olympe de Gouges in 1791 and ignored by the French *Assemblée Nationale*. Madame de Gouge was guillotined for her political initiative in 1792.

18. Universal Declaration of Human Rights. (1948). G.A. Res. 217 A(III), adopted by U.N. Doc. A/810 (December 10).
19. Public Lecture by Justice Albie Sachs on the Constitutional Court of South Africa at Oxford University, July 2005.
20. Rome Statute of the International Criminal Court, U.N. Doc 2187 U.N.T.S. 90, *entered into force* July 1, 2002.
21. Internet Society (2012). 'Global Internet User Survey 2012', *ISOC*.
22. King, G., Pan, J., and Roberts, M. (2013). 'How Censorship in China Allows Government Criticism but Silences Collective Expression', *American Political Science Review*, Vol. 107, No. 2, pp. 326–343.
23. Roda, C. (2011). Human attention in digital environments. Cambridge: Cambridge University Press.
24. Perry, S. (2016). 'L'envers de l'utopie numérique', *Panorama des Idées*, No. 7, pp. 15–16.
25. Bihouix, P. (2015). *L'Age des low-tech* (Paris: Seuil).
26. We thank Christien van den Anker for her thoughtful comments on our draft introduction.

Bibliography

Arend, A. C. (1999). *Legal rules and international society*. Oxford: Oxford University Press.

Association for Computing Machinery. (2000). ACM timeline of computing. *ACM*. Retrieved March 30, 2016, from http://www.acm.org (home page).

Balandier, G. (2015). *Recherche du politique perdu*. Paris: Fayard.

Bihouix, P. (2015). *L'Age des low-tech*. Paris: Seuil.

Bull, H. (1977). *The anarchical society: A study of order in world politics* (3rd ed.). New York: Columbia University Press.

Essinger, J. (2004). *Jacquard's Web: How a hand-loom led to the birth of the information age*. Oxford: Oxford University Press.

Friedman, T. (2005). *The world is flat*. New York: Farrar, Strauss and Giroux.

Holling, C. S. (1973). Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics, 4*, 1–24.

Hunt, L. (2007). *Inventing human rights: A history*. New York: W.W Norton & Company.

Institute of Electrical and Electronics Engineers. (1984). A century of electricals, an exhibit by the IEEE history centre. Retrieved March 30, 2016, from https://www.ieee.org (home page).

Institute of Electrical and Electronics Engineers. (1996). Timeline of computing history. *IEEE Computer Society*. Retrieved March 30, 2016, from https://www.computer.org (home page).

Internet Society. (2012). Global internet user survey 2012. *ISOC*. Retrieved March 30, 2016, from http://www.internetsociety.org (home page).

Katz, B., & Bradley, J. (2013). *The metropolitan revolution: How cities and metros are fixing our broken politics and fragile economy*. Washington, DC: Brookings Institution Press.

King, G., Pan, J., & Roberts, M. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review, 107*(2), 326–343.

Kobrin, S. (1998). Back to the future: Neo-medievalism and the post-modern digital world economy. *Journal of International Affairs, 51*(2), 361–386.

Perry, S. (2016). L'envers de l'utopie numérique. *Panorama des Idées, 7*, 15–16.

Risse, T., Ropp, S., & Sikkink, K. (Eds.). (2013). *The persistent power of human rights: From commitment to compliance*. Cambridge: Cambridge University Press.

Roda, C. (2011). *Human attention in digital environments*. Cambridge: Cambridge University Press.

Rome Statute of the International Criminal Court, U.N. Doc 2187 U.N.T.S. 90, *entered into force*, July 1, 2002.

Sachs, A. (2005, July). *Constitutional court of South Africa*. Public Lecture. Oxford University.

Turing, A. M. (1936). On computable numbers: With an application to the Entscheidungsproblem. Series 2. *Proceedings of the London Mathematical Society, 42*(1), 230–265.

Turing, A. M. (1950). Computing machinery and intelligence. *Mind, 59*(236), 433–460.

United Nations General Assembly. (1948). Universal Declaration of Human Rights, General Assembly Resolution 217A(III), adopted by the U.N. Doc. A/810, 10 December.

CHAPTER 2

The Great Debate on Wireless Technology

As the progress of mobile phone technology accelerates worldwide, the regulatory framework necessary for its safe and extended use has been slow to develop. The hardware delivery of wireless phone technology poses new challenges to our understanding of human rights. This chapter analyses the relationship between scientific knowledge and regulation concerning the health effects of increasing electromagnetic field emissions from mobile phone towers (base transceiver stations). From a conservationist perspective, no other example of industrial impact on the natural environment has achieved such extended penetration so quickly. This presents an ethical conundrum: stakeholders are faced with the difficult choice between waiting for a comprehensive, long-term assessment of health impacts from electromagnetic exposure and immediate application of the precautionary principle. By exploring examples of interaction between citizens, governments, and international bodies, we first analyse the challenges faced by regulators in the presence of uncertain scientific knowledge and standards of measurement. We then highlight the inadequacy of current parameters. Lastly, we expand the debate on how we may use a human rights framework to protect vulnerable populations from digital pollution. We conclude that, because scientific knowledge on the health

This chapter appeared in an earlier form as: Roda, C., Perry, S. (2014). Mobile Phone Infrastructure Regulation in Europe: Scientific Challenges and Human Rights Protection. *Environmental Science and Policy*, 37, 204–214. Reproduced by permission.

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_2

effects of wireless technology delivery is incomplete, a precautionary approach is better suited to State obligations under international human rights law.

We begin our book with the most ubiquitous form of digital technology: mobile phones and the infrastructure that makes them work. This whirring, ringing prop of everyday life has achieved a 97 per cent penetration worldwide within two decades,[1] with individual use ranging from moderate interaction to outright addiction. By 2016, there were nearly as many mobile phone subscriptions as people on the planet.[2] Any study of mobile phones must take into account the wireless technology that allows them to function, specifically the use of electromagnetic wave frequencies to transmit information from one user to another. A good deal of scientific literature has attempted to determine whether exposure to electromagnetic field emissions (EMF) during mobile phone use is dangerous to human health.[3] Yet, while the public remains focused on the likely dangers of the device itself,[4] the rapidly growing infrastructure necessary to make mobile phones work is interfering with human physiology as 'the antennas of broadcast stations are the most powerful continuous sources of RF (radio frequency) energy intentionally radiated into free space'.[5] From a conservationist perspective, no other example of industrial impact on the natural environment has achieved such extended penetration so quickly.

Base transceiver stations (BTS)—equipment normally connected to elevated structures that relay electromagnetic signals between mobile devices and a network—emit electromagnetic energy.[6] It is the under-regulated emission of electromagnetic wave frequencies to seven billion mobile phone users worldwide that promotes certain well-established human rights, while violating others. This chapter will examine the difficult balance that must be achieved by governments, mobile phone operators, and consumers in order to provide wireless services to citizens without endangering their health or time-honoured democratic procedures. Currently, most national governments require full bandwidth coverage for consumers; the European Union (EU) requires maximal coverage by member states,[7] much like the US Federal Communications Commission, which is tasked with the promotion of broadband availability for all Americans.[8] Virtually no robust legislation exists to protect consumers from the possible effects of prolonged electromagnetic wave exposure via BTS. Most governments do not require public hearings concerning the placement and number of BTS, even though such hearings are mandatory for many other potential sources of environmental pollution. In 2011, the International Agency for Research on Cancer (IARC), a specialized agency of the World

Health Organization (WHO), classified radio frequency EMF as Group 2B: possibly carcinogenic to humans.[9] *The Lancet Oncology* reported that the IARC committee mainly focused on the impact of two types of exposure on humans: (1) the use of personal devices, and (2) occupational sources.[10] A third type of exposure, due to *environmental* sources such as BTS, was not included because the committee found 'the available evidence insufficient for any conclusion'.[11] This is of obvious concern because a large part of the population is exposed to the compound effect of radiation from mobile phone towers, handsets radio transmitters, WLAN (wireless local area network), Wi-Fi, portable computers, and other devices. More importantly, children are at higher risk according to many studies.[12]

Ironically, the promise of digital technology to deliver unhindered access to information, thereby reinforcing the socio-political foundations for democracy and human rights, is belied by the lack of semantic transparency in the public debate surrounding BTS installation and the potential dangers of radio frequency EMF exposure in general. The question 'are mobile phones or BTS installations dangerous to human health?' cannot yet be answered with complete precision, despite the fact that we are more than twenty years into the digital revolution and most of the world's population uses a mobile phone. The confusion surrounding the functioning of the technology and its impact on human beings has been to the advantage of the telecom companies; the longer the consumer remains uninformed or unable to understand the difficult choices inherent in the digital revolution, the greater the opportunity for profit.[13]

We argue that the socio-political foundations for democracy rest not only on unhindered access to information, but also on the intelligent use of that information to estimate risk and to protect populations from harm. As scientific research on the possible health effects of exposure to radio frequency EMF sources continues, this chapter contributes to existing scholarship by (1) explaining the current biological research on the impact of EMF on the living environment and the difficulty in establishing EMF protection standards due to a complex, controversial risk assessment procedure and measurement paradigm, (2) evaluating the extent of the resulting inadequacies in national regulatory systems in the USA and Europe, and (3) expanding the human rights construct to 'protect, respect and remedy' vulnerable populations by including regulation of radio frequency EMF exposure within a 'due diligence' environmental pollution framework.[14] From a theoretical standpoint, the regulator's dilemma encompasses a choice between the principle of

precaution and long-term risk assessment. This chapter affirms that, due to the lack of scientific consensus and contradictory standards of measurement, the international human rights treaty system guaranteeing the protection of vulnerable populations obliges states to adopt a precautionary approach in the short and medium term, until a majority of peer-reviewed scientific publications establish the danger, or safety, of electromagnetic wave emissions.

The advancement of human rights is facilitated by digital technology, in much the same way that the promise of digital technology is based on the premise of a better quality of life for all. This chapter explores the response of local citizens' action groups in framing the human rights violations caused by wireless technology in their cities—a response that uses digital technology to organize while, at the same time, calls on the telecom industry to account for an impressive spate of corporate lobbying that rivals that of the tobacco industry.[15] We argue that human rights and digital technology can be mutually enhancing only within a framework of comprehensive information and intelligent regulation to protect the citizen-consumer.

2.1 The Regulator's Dilemma

Regulators may draw upon two bodies of theoretical knowledge in formulating a viable policy strategy to protect vulnerable populations from the potential health risks associated with radio frequency EMF exposure. One set of theories underpins risk assessment as developed primarily in the fields of economic, financial, and behavioural theory. The second set of theories draws on the German concept of *Vorsorge*,[16] an expansion of nineteenth century British law and its evolution into an obligatory due diligence framework for governments and the private sector.[17] In terms of practical application, regulators may either wait until a full assessment has been carried out to determine if populations are at risk or take preventative action, under the banner of due diligence.

In their work on prospect theory,[18] Amos Tversky and Daniel Kahneman demonstrated that human beings are hardly rational when it comes to risk assessment. Although the theoretical implications of Tversky and Kahneman's work are complex, one particularly relevant aspect for the regulator is that the majority of respondents in one of their studies found that the certain death of 400 people is less acceptable than the two-in-three chance that 600 will die, despite the fact that the statistical risk is nearly identical.[19] Thus, in the event of a possible danger to their own health, even informed citizens may not make a rational decision or choose the best option

for their own protection. Richard Thaler and Cass Sunstein have theorized a form of 'choice architecture' in which policymakers nudge irrational citizens towards behaviour that is in their (or the government's) best interest.[20] The danger of choice architecture is a form of paternalism, described by Suzanne Mettler as part of a broader trend towards the 'submerged state'.[21] Mettler contends that a functioning democracy requires citizens to participate in thoughtful public policy debate in a meaningful way.[22] We would add that, despite evidence of irrationality in decision-making, citizens should be given the chance to debate the necessity for protective legislation when there is evidence of a risk to public health (however incomplete), rather than wait for a full risk assessment to be concluded.

The precautionary principle requires states to act before harm occurs. While there is great academic debate on the difference between the US doctrine of 'due diligence' versus the European principle of precaution,[23] democratic states in general recognize the need to anticipate widespread harm to citizens caused by industry or government and the obligation to take policy action to prevent or mitigate that harm. The economist Christian Gollier has attempted to address human irrationality in risk assessment by integrating risk evaluation and due diligence into a coherent paradigm that allows regulators to know when and how to act. Gollier presents what he calls a 'reasonable interpretation' of the precautionary principle.[24] When the basic scientific data relating to a problem requiring a decision are uncertain, he suggests that the 'learn then act' principle should be applied—but only when a careful cost-benefit analysis establishes that current and future preventative actions are *close* substitutes for one another. In all other circumstances, there is a clear benefit in acting to prevent long-term risk. In the case of EMF exposure from BTS, preventative action would require application of the ALARA (as low as reasonably achievable) principle to curb BTS emissions, an action that resembles reduction in exposure to tobacco smoke: the earlier the reduction to exposure occurs, the fewer potential health problems. Thus, current and future preventative actions are not close substitutes in the case of BTS emissions. Gollier's normative paradigm would suggest application of the precautionary principle in these circumstances. This approach is reinforced by scholarship on the Dutch government's vigilant response to the lower electromagnetic frequencies generated by electric pylons.[25]

Environmental history points to the importance of acting sooner rather than later to protect vulnerable populations and ecosystems from air and

water pollution. The 1972 Oslo Convention on dumping waste at sea and the 1974 Paris Convention on land-based sources of marine pollution were early attempts to protect the marine environment. It took another twenty years for Europe to ramp up regulation through the 1992 OSPAR[26] Convention on protection of the marine environment in the North-East Atlantic, an initiative reinforced by the promulgation of REACH[27] in 2006. Asbestos is another striking example of the lag-time between knowledge of the danger, first recognized by courts in the 1970s that led to protection of workers in 1983, and an outright European ban on its use in 2005.[28] In both cases, one to two generations of citizens were put at risk before definitive legislative action was taken. Hence, from a theoretical point of view, the regulator's dilemma may well be resolved: history tells us that sooner is better than later.

2.2 Contested Science and Technology

From an empirical standpoint, however, three questions underlie the debate about the safe use of mobile phones and BTS. Do EMF emissions generated by mobile phone technology affect human health? If so, what constitutes appropriate safety standards? And finally, who is responsible for BTS installation, implementation, and monitoring? We now turn to the functioning of electromagnetic wave frequencies and explore the controversies associated with the first two questions. The third question is examined in the latter part of this chapter.

Wireless technology functions via electromagnetic waves of a certain frequency range which are generated by a source that introduces information in the form of changes to the waves. A receiver capable of interpreting the information then picks up the waves. Electromagnetic waves are propagating Electromagnetic Fields EMF, and their strength is measured in terms of their electric and magnetic *fields*. We distinguish electromagnetic waves according to their wavelength, constituted by the distance between two crests (Fig. 2.1).

Electromagnetic waves of varying frequencies interact with the body in different ways, depending on the amount of energy associated with the wave. Gamma rays and X-rays have frequencies (and energies) high enough to knock an electron off its atom and break the bonds between molecules; this phenomenon is called ionizing radiation. Fields at lower frequencies produce non-ionizing radiation. All electrical devices, power supply networks, and telecommunications technology generate EMF in frequencies lower than those of ionizing radiation (unless they are purposely

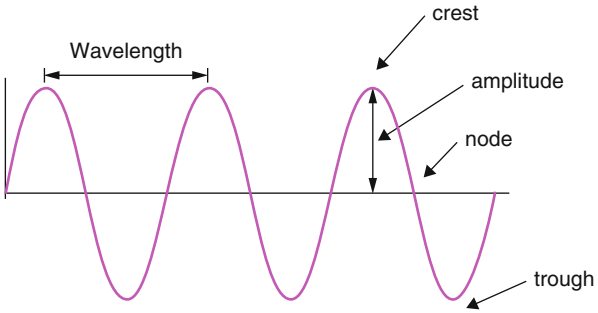

Fig. 2.1 Electromagnetic wave frequencies

designed to do otherwise). Therefore, everyone is exposed to multiple EMF radiation in the non-ionizing frequency range. For example, power grids and electrical devices are a source of extremely low frequency (ELF) fields, while wireless devices and mobile phone towers are a source of radio frequency (RF) radiations. These exposures induce currents within the human body and cause two types of effects: either thermal or non-thermal. The WHO has explained that 'the strength of these currents depends on the intensity of the magnetic field. If sufficiently large, these currents could cause stimulation of nerves and muscles or affect other biological processes'.[29]

2.3 Measuring the Biological Impact of EMF

Both the telecom industry and the public sector have multiple peer-reviewed scientific studies to determine whether prolonged exposure to electromagnetic waves poses a danger to human health. Biologists concede a wide range of opinion on the subject. Numerous scientific studies report that exposure to EMF has an impact on human tissues and cell development,[30]and yet experts do not agree on how much exposure may lead to health risks for adults or children, while some research results seem to contradict one another.[31] One trend is clear: the number of peer-reviewed scientific studies that link EMF exposure to health risks has expanded rapidly and is appearing in extremely well-respected journals.[32]

Effects have been reported on the reproductive system,[33] on foetal and neonatal development,[34] on increased risk of childhood leukaemia, adult brain tumours and acoustic neuromas,[35] on breast cancer,[36] and

on neurodegenerative diseases.[37] EMF exposure has been linked to sleep disturbance,[38] as well as headaches, memory changes, and depressive symptoms.[39] Numerous effects on plants and animals have also been reported.[40] Although more studies account for effects on human health due to mobile phone use rather than proximity to BTS radiation, scientists indicate that 'the two kinds of radiation are very similar and effects produced by mobile phones at certain distances, can be extrapolated to represent effects from base station antennas, of the same type of radiation, at about 100 times longer distances'.[41]

Scientific studies may focus on exposure to EMF with specific characteristics, such as frequency range, source position relative to the subject, or emission duration. However, as demonstrated by Martin Blank and Reba Goodman, the same biological impact may occur across the range of the electromagnetic spectrum:

> While low energy EMF interacts with DNA to induce the stress response, increasing EMF energy in the RF range can lead to breaks in DNA strands …. The intensity of EMF interactions with DNA leads to greater effects on DNA as the energy increases with frequency.[42]

The effects of simultaneous exposure to several EMFs could also be additive. The same authors explain that DNA has the structural characteristics of fractal antennae and therefore the same wide-frequency range of interaction with EMF. This would 'contribute to greater reactivity of DNA with EMF in the environment, and the DNA damage could account for increases in cancer epidemiology'.[43]

In addition to the nature of EMF exposure, the characteristics of the exposed subject (such as age, gender, or general health) have an impact on the possible health consequences of radiation. Particularly relevant to our argument are studies about the age-related differences in tissue response to EMF exposure and the impact on children.[44] A research team led by Andreas Christ suggests that, 'in general and on average, children suffer a higher exposure of their brain regions than adults. This higher exposure is due to differences in anatomical proportions'.[45] In a study where clinical and growth pattern data were collected for up to 13 years from 733 children whose mothers carried a magnetic field (MF) measuring meter during pregnancy, De-Kun Li and colleagues conclude that 'maternal exposure to high MF during pregnancy may be a new and previously unknown factor contributing to the world-wide epidemic of childhood obesity/

overweight'.[46] Even those scientists who believe there is no causal effect between mobile phone use and health problems for the general population have called for further studies and suggest caution with respect to childhood exposure to EMF[47] (Box 2.1).

Blake Levitt and Henry Lai conducted an extensive literature review of studies related to the biological effects from exposure to EMF radiated by BTS and other RF antennae. They reported that children are impacted

Box 2.1 Protection measures
Protection measures include:

1. Reducing exposure to EMF
2. Prohibiting specific 'windows' of exposure
3. Establishing age limits for the use of wireless communication devices
4. Barring installations from sensitive areas such as schools and hospitals
5. Requiring maximization of wired rather than wireless networks
6. Establishing procedures for citizens to request accurate exposure *measurements.*

differently than adults by electromagnetic wave emissions from mobile phones and BTS:

> Children absorb energy differently than adults because of differences in their anatomies and tissue composition…For instance, radiation from a cell phone penetrates deeper into the heads of children…The same can be presumed for proximity to towers, even though exposure will be lower from towers under most circumstances than from cell phones. This is because of the distance from the source. The transmitter is placed directly against the head during cell phone use whereas proximity to a cell tower will be an ambient exposure at a distance.[48]

Determining the risks of ambient exposure at a distance highlights a key issue in the regulatory framework discussed in greater detail below. In mobile phone communication, BTS distribute a signal, received by a landline, and send it to a receiver (a mobile phone) within a certain

area using the available frequency spectrum (bandwidth). The broader the available bandwidth, the more information can be transmitted in a given unit of time. This means that increasing download speed boosts emission levels.[49] Accessing an online movie or playing an online game, for example, requires more bandwidth than accessing a web site with still images and text. Users employ their smartphones to access services requiring high data transmission rates and they expect their connection to be maintained in a variety of locations, including indoors and on public transport. Consequently, as demands for bandwidth and connectivity coverage have increased, telecom companies have responded by augmenting the number of BTS to partition each sector into smaller coverage areas so that the available bandwidth is reused, capacity is increased, and more people can be served at the same time within the original sector.

As the number of BTS increase, more people are living in closer proximity to a mobile phone tower than ever before. The only way to reduce the biological impact of exposure to EMFs is either to reduce the number of towers or their transmission power. This means that either fewer customers will be served at the same time, which could be a problem in densely populated cities, or that these same customers will be served, but with a lower data transmission rate. A lower data rate may imply, for example, that access to websites and emails is available, but video download is not. Consequently, the application of the ALARA principle regarding health risks needs to be weighed against the benefits of accessibility required by the Digital Agenda for Europe or the US Federal Communications Commission. Regulators will need to evaluate, on the one hand, which technologies are safe to use for delivering the desired accessibility and, on the other hand, what sort of information or services should be made available to citizens. In order to determine which measures to implement, regulators need accurate and comprehensible information allowing them to weigh the trade-offs between large data services availability and the protection of human health. According to Gollier's risk assessment paradigm discussed above, when the health risk cannot be determined with sufficient certainty, the precautionary principle should be applied.

2.4 Setting Standards

In order to establish regulations and recommendations, several national and international bodies have used guidelines made available by the International Commission on Non-Ionizing Radiation Protection (ICNIRP). The Institute of Electrical and Electronics Engineers (IEEE) also provides similar recommendations.[50] According to the ICNIRP, there are two safety categories: (1) basic restrictions on 'exposure to time-varying electric, magnetic, and electromagnetic fields' and (2) reference levels 'provided for practical exposure assessment purposes…Compliance with the reference level will ensure compliance with the relevant basic restriction.'[51]

In Table 2.1 below, which only covers the frequency range typical of a mobile phone tower, we provide basic restrictions for human exposure that are expressed in terms of specific absorption rate (SAR), and power density (S). SAR, which defines the rate of energy absorption per unit mass (how much energy the body absorbs), is expressed in Watts per kilogram (W/kg), and is not directly measurable. Power density represents the rate of energy flow through a given surface area of the body and is measured in Watts per square metre (W/m^2). For practical purposes however, the values used to establish regulations are those in the reference levels column of Table 2.1. Emission limits for electric field strength are indicated in Volts per metre (V/m).

There is a good deal of controversy over the reliability of the ICNIRP guidelines (as well as other, less referenced, guidelines), which are questioned on several grounds:

1. There is a likely conflict of interest between the ICNIRP and the telecom industry, an issue that has been raised in a report to the Council of Europe that eventually led to the adoption of Resolution 1815 (discussed below) that advised precaution.[52]
2. It has been argued that ICNIRP's reference levels do not actually ensure that corresponding basic restrictions are met. The electric field strength reference level for expressing EMF radiation exposure limits may misrepresent the SAR basic restrictions.[53]
3. The measures used to define basic restrictions are contested. Some scientists argue that both SAR and power density measures have several limitations, including the fact that 'the existing standardized phantom is not optimal for SAR measurements of large base station

Table 2.1 Guidelines for the frequency range of BTS

Frequency	*Basic restrictions (ICNIRP, 1998)*	*Reference levels*[a] *(ICNIRP, 1998)*				
		Frequency range	*Electric field strength (V/m)*	*Magnetic field strength*		*Electrom. field strength power density (W/m^2)*
				H-field (A/m)	*B-field (μT)*	
100 kHz –10 GHz	Restrictions on specific energy absorption rate (SAR) prevent whole-body heat stress and excessive localized tissue heating 0.08 W/kg	3–150 kHz	87	5	6.25	
		0.15–1 MHz	87	0.73/f	0.92/f	
		1–10 MHz	$87/f^{½}$	0.73/f	0.92/f	
		10–400 MHz	28	0.073	0.092	2
		400–2000 MHz[b]	$1.375f^{½}$	$0.0037f^{½}$	$0.0046f^{½}$	f/200
		2–300 GHz	61	0.16	0.20	10
10–300 GHz	Restrictions on power density (S) prevent excessive heating in body tissue 10 W/m^2	Same as 2–300 GHz range above				

[a]The limits reported are those for public exposure; different (higher) limits are specified for occupational exposure

[b]If calculated, the E-field strength level ranges between 27.5 and 61.5 V/m (sqrt(400) × 1.375 = 27.5 and sqrt(2000) × 1.375 = 61.49)

antennas',[54] that current SAR recommendations do not take into account 'the smaller size and greater physiological vulnerability and increased absorption to the heads of children and females',[55] and that SAR needs to be integrated with other measures in order to be a useful tool for the evaluation of health risks associated with EMF exposure.[56]

4. Most contentiously, the ICNIRP guidelines do not offer protection against the non-thermal effects of EMF, particularly with respect to prolonged exposure.[57] In fact, current restrictions are based only on short-term thermal health effects, because the ICNIRP committee concluded in 2009, before the impact of third and fourth generation technology could be measured: 'Whilst it is in principle impossible to disprove the possible existence of non-thermal interactions, the plausibility of various non-thermal mechanisms that have been proposed is very low.'[58]

The fundamental question of what constitutes sufficient evidence for setting restrictions is still open. While certain experts deem the epidemiological studies on long-term EMF exposure inconclusive on the basis of their potentially biased results or an unconvincing demonstration of risk, other scientists argue that studies of this type should be considered more carefully.[59] The latter indicate that current standards for risk assessment are inappropriate;[60] these scientists suggest that long-term effects on citizens' health are due to a heightening of exposure to several EMF sources over time, a phenomenon normally more difficult to measure than acute effects.[61]

We are facing a conflict of epistemic cultures of non-knowledge, one where some scientists place a higher value on more controlled experiments, but disregard 'contextual factors or persisting real-world uncertainties'[62] (such as exposure to multiple EMFs and its long-term effects), while others attempt to address the complexity and context of the problem, but at the cost of scientific reproducibility and predictability. Regulatory bodies that are tasked with appropriate protective policy for radio frequency EMF exposure are in a difficult position; research aimed at assessing its potential danger has so far produced mixed results (especially for long-term exposure). Moreover, controversy is not limited to the magnitude of values that would limit health hazards, but also extends to the definition of what should actually be measured. The difficulty in establishing measurement standards, as well as the scarcity of long-term impact studies

of EMF on the living environment, may explain why the WHO has only recently recognized the danger related to radio frequency fields and maintains a classification of 'possibly' carcinogenic to humans.[63] And yet, issues remain, such as which policy framework should be applied when evidence of risk is inconclusive, and whether the burden of proof should be on demonstrating risk or on demonstrating the safety of the technology (a standard regularly applied to medical products).

In the next part of this chapter, we examine how the USA and Europe have addressed the former issue, albeit with non-binding norms, and how a local citizens' group has responded to the dearth of protective legislation. We then demonstrate how the issue of protection can be resolved on the basis of state compliance with binding international human rights law.

2.5 Legislative Dearth in the USA and Europe

In this section we discuss the reluctance of the USA and the national governments of Europe to impose threshold restrictions on mobile phone tower emissions for fear of hindering economic growth and slowing down preparations for the Internet of Things, the hyper-connectivity of household objects and machines discussed in detail in Chapter 5. The US government has no recommended or obligatory federal exposure limits for EMF emissions from mobile phone towers.[64] Congress first attempted to mitigate the impact of electromagnetic waves on human health in 1993 with two bills, the Children's Electromagnetic Field Risk Reduction Act[65] and the Electromagnetic Labelling Act,[66] the first of which languished in the House Subcommittee on Elementary, Secondary and Vocational Education and the second in the House Subcommittee on Energy and Power. In 2012, Congress considered a far more effective bill designed to protect vulnerable populations from radio frequency EMF exposure. The Cell Phone Right to Know Act required:

> The Director of the National Institute of Environmental Health Sciences and the Administrator of the Environmental Protection Agency (EPA) to: (1) conduct or support a comprehensive research program to determine whether exposure to electromagnetic fields from mobile communication devices causes adverse biological effects in humans, including vulnerable subpopulations such as children, pregnant women, those with compromised immune systems and hypersensitivity reactions, men and women of reproductive age, and the elderly, and (2) disseminate research results to the general public ….[67]

The bill also directed 'the EPA to promulgate regulations establishing maximum exposure level goals and maximum exposure levels for exposure to electromagnetic fields generated by mobile communication devices.'[68] A concerted lobbying effort by the American telecom industry prevented this bill from becoming law.[69] Nonetheless, the attempt to remove standard setting from the ambit of the Federal Communications Commission or the Department of Commerce and place it in the hands of the EPA's Office of Air and Radiation was an important initiative.

Despite the lack of federal guidelines in the USA, six states have set limits and several more states have 'prudent avoidance' policies. Grassroots organizations from California to Connecticut[70] have demanded more protective regulation from the federal or state governments. Responses have often been contradictory, since public officials are guided by the conflicting needs of protecting citizens' health, responding to the commercial logic of the telecom companies (frequently major employers within their jurisdictions), and meeting the obligations of information accessibility or infrastructure deployment required by law. In many instances, citizens have filed complaints against the telecom industry in an effort to prevent BTS installation. While in most cases the legal framework for robust protection from EMF pollution is too weak to provide effective remedy, jurisprudence has advanced citizen protection in some instances, as will be discussed later in the chapter.

As mobile phone technology progressed, requiring ever more powerful antennae, the Council of Europe responded in 2011 with Resolution 1815, a set of non-binding norms defining an emissions limit of 0.6 V/m for wireless devices, along with recommendations to reduce 'threshold values for relay antennae in accordance with the ALARA principle and install systems for comprehensive and continuous monitoring of all antennae'.[71] Resolution 1815 also articulated strategies for better protection of children. But, Council of Europe resolutions, unlike directives promulgated by the EU, do not have the power of law. The Council must thus rely on its 47 members to regulate electromagnetic emission levels at the national or municipal level. At the national level, moving from recommendations on standards of measurement to legislation is a slow process.[72] Throughout Europe, several states have adopted more restrictive norms on BTS emissions than those fixed by the EU in 1999 at 41–61 V/m, restrictions which were based on thermal considerations as dictated by the controversial ICNIRP guidelines discussed above.[73] EU members Belgium, Bulgaria, Greece, Italy, Lithuania, Luxembourg, Poland, and Slovenia

have adopted more restrictive limits in 'residential areas' and 'sensitive locations'. This is also the case with Switzerland and Liechtenstein. Several cities, such as Paris and Salzburg, have promulgated voluntary charters or resolutions in an effort to lower radio frequency EMF emissions locally; because cities often rent municipal property to the telecom companies for BTS installations, they have more leverage than citizens' action groups.[74]

2.6 Grassroots Activism in Paris

The case of Paris clearly illustrates competing policy demands, particularly in heavily populated urban areas. France is one of two countries worldwide (along with Chile) that has promulgated national legislation recognizing the potential danger of radio frequency EMF pollution. France's Green Party twice introduced protective legislation before the French parliament, and each time the text was met with a concerted lobbying effort designed to table the proposed bill to an inappropriate committee or to water down the protective clauses.[75] The resulting *Loi Abeille*, promulgated in January 2015, was named after parliamentarian Laurence Abeille who proposed the bill and worked for its passage. The *Loi Abeille* is a compromise between industrial and environmentalist concerns. While the bill calls for 'sobriety, transparency, information and consultation' in all matters pertaining to electromagnetic wave emissions and acknowledges electro sensitivity as a medical condition, the law sets no emission thresholds.[76] In fact, as of this writing, the law has not yet benefited from implementation *décrets*, which means that the Prime Minister's office may be unwilling to put this law into practice. Consequently, French cities and towns must set voluntary emissions standards through a process of negotiation with the telecom industry.

Paris has been considered a leader in calling for extremely low levels of electromagnetic wave emission from BTS, with a ten-year norm of 2 V/m from 2003 to 2011.[77] This Charter of Voluntary Compliance was suspended in autumn 2011 as the city moved to decrease emissions in accordance with the Council of Europe Resolution 1815 cited above, while the operators hoped to increase emission levels to accommodate the arrival of fourth generation (4G) wireless technology.[78] In October 2012, despite the determined opposition of local NGOs and the Green Party, the Mayor's Office ceded to the demands of the telecom companies, and raised emission limits to 5–7 V/m.[79] A 2013 report from the French

government indicated that citizen exposure to EMF was expected to rise 50 per cent due to 4G emissions from BTS.[80]

France currently has four telecom companies that compete for installation sites on Parisian rooftops. The city was home to more than 3000 BTS in 2015, once of the densest distributions of antennae on the planet.[81] Zoning regulations are extremely strict and focus on aesthetics, or what the French call *l'aspect*.[82] Thus, mobile phone towers are virtually invisible, hidden by camouflage structures resembling chimneys or brick walls. Equally invisible is the type of public information sharing that citizens have come to expect for the installation of high-impact structures, such as wind farms or power plants.[83] Public property rights allow building cooperatives to approve rooftop installations in exchange for an annual fee, without prior consultation with their neighbours, many of whom live on the upper floors in surrounding buildings and will be exposed to stronger wave frequencies than those who actually approved the installation. Once the project has been endorsed by a homeowners' cooperative, the *Agence nationale des fréquences* (ANFR) must vet the level of emissions and the technical capacity of the BTS, while the aesthetic aspect is scrutinized by another national agency, the *Monuments Nationaux de France*. When approved at the national level, the project is then examined at the municipal level, where a Preliminary Declaration is filed with the *Département d'urbanisme*. Only once the Preliminary Declaration has been approved, does the first indication of a BTS installation appear in the public domain. A small white sign posted on the building door informs passers-by that a construction project will take place, in this case the installation of a new BTS on the roof. In several instances, especially when the white sign has appeared near schools or day-care centres, citizens have mobilized to insist on the removal of the installation to a different location. The fact remains, however, that the state safeguards the aesthetic beauty of Paris and obliges the telecom companies to provide maximal coverage to consumers, while providing insufficient regulation to protect children from the potentially harmful effects of electromagnetic exposure from BTS.

The *rue Lobineau* is a small street in the heart of Paris, unremarkable except for the hundreds of children coming in and out of the day-care centre, play school, music conservatory, and handicapped housing on the first floor of the *Marché St. Germain* on a weekly basis. When the small white sign first appeared at number 5, neighbours were surprised that a telecom company would consider installing mobile phone towers right across the

street from infants and toddlers. Assuming that a quick letter to the Mayor would set things right, citizens were disconcerted to discover that there was no binding regulation whatsoever in 2012 to protect children from the potentially harmful effects of close-range exposure to electromagnetic waves. When a second set of small signs appeared announcing that cars would be towed away in order to facilitate the installation of two towers by crane, neighbours formed a citizens' action group, the *Collectif rue Lobineau*, and physically occupied the street to block the arrival of the trucks. Mothers, children, and one of the authors of this book faced down bailiffs and chatted with local and national media for weeks, unaware that behind the scenes municipal officials were inexorably giving way to the idea of tripling recommended emission thresholds to accommodate the arrival of 4G technology.[84]

2.7 Expanding the Regulatory Framework

International human rights law constitutes a possible means to address the current regulatory impasse in Europe and the USA. The painstaking work after the end of the Second World War to build an edifice of binding international treaties, ranging from the international bill of human rights to more specific protection for women, children and minorities, culminated with the entry into force of the Convention on the Rights of the Child in November 1989. Recent international instruments, such as the OECD Guidelines for Multinational Enterprises or the Ruggie Report, oblige state parties to 'protect, respect and remedy' human rights violations by businesses against individuals or groups, bringing corporations into the international human rights paradigm through state compliance with binding treaty law. Certain scholars contest the viability of international human rights law, insisting that the maximum flexibility afforded by the language of the human rights treaties renders them unenforceable.[85] This may be true. Nonetheless, we contend that the protection of children continues to constitute a high threshold norm in law in nearly all countries, thanks in part to the influence of the international human rights framework. Consequently, the safeguarding of children should be pursued through the application of existing domestic legal protections to the roll-out of digital technology. (Box 2.2).

Box 2.2 Committee on the rights of the child
General Comment No. 16 (2013) on State obligations regarding the impact of the business sector on children's rights.

'4. Remedies and reparations

'States have an obligation to provide effective remedies and reparations for violations of the rights of the child, including by third parties such as business enterprises.

'…for example, if children are identified as victims of environmental pollution, immediate steps should be taken by all relevant parties to prevent further damage to the health and development of children and repair any damage done.'

In this section, we argue that (1) because protection of children is a high threshold norm in human rights law, and (2) the binding language of the Convention on the Rights of the Child obliges state parties to provide a higher standard of protection for children than for adults, any widespread or systematic form of environmental pollution that poses a long-term threat to a child's rights to life, development or health may constitute an international human rights violation. Thus, when EMF exposure is too high, the state must legislate to implement the 'protect, respect and remedy' framework. Even states that have signed, but not ratified the Convention on the Rights of the Child, such as the USA, may be bound under the Vienna Convention on the Law of Treaties to uphold the treaty.[86] The Committee's General Comments are intended as guidelines for state parties in interpreting implementation of the treaty in their national jurisdictions.

Articles 3, 6 and 24 of the UN Convention of the Rights of the Child constitute a legally binding responsibility on the part of state parties to protect children from verified and potential threats to health and safety. We have argued, in a submission to the UN Committee on the Rights of the Child, that electromagnetic pollution poses a potential threat to the 'highest attainable standards of health' for children, as articulated in article 24 of the Convention on the Rights of the Child.[87] As noted above, scientists from both industry and university research laboratories recognize that children's physiology places them at greater risk from electromagnetic

pollution due to mobile phones and BTS, which should trigger stricter legal thresholds and precautions under articles 2 and 3 of the Convention. Regular testing of emission limits by an independent body of experts, with 'appropriate sanctions' for widespread or systematic pollution under article 32, coupled with regular monitoring of both voluntary and legally binding compliance by the telecom industry, constitutes a minimum level of protection as required by the Convention.[88] Thus, according to the treaty, decisions on where to place BTS and on what constitutes safe levels of EMF exposure for children should be made by competent health specialists. These specialists should be guided by national legislation that requires public consultation, articulates prudent thresholds and sets the lowest emissions possible in proximity to day-care and schools. The principle of precaution should function as a guiding standard when determining how to evaluate environmental risk with respect to children.

The question of accountability is further complicated by the problem of multiple sources of environmental pollution, a reality which means that a business may bear no legal responsibility as a corporate entity because the impact is cumulative. The rapid increase in all sorts of environmental pollutants, ranging from diesel particle emissions to multiple sources of EMF, renders it difficult to isolate the precise cause of a particular cancer or disease. However, what if radio frequency EMF exposure constitutes one environmental pollutant too many for the infants and toddlers exposed to a disputed installation? While the main difficulty in legislating to protect has to do with the science—both the complex measurement paradigm for EMF emissions and the ongoing biological research into EMF impacts on the living environment—theory and practice suggest that the lack of agreement on scientific knowledge can best be addressed through the principle of precaution. Moreover, the Convention on the Rights of the Child, ratified by nearly all nations, together with Council of Europe Resolution 1815 oblige member states to protect the most vulnerable from this relatively new form of environmental pollution.

After a decade of debate, this is precisely the strategy that was adopted in Chile. Chilean congressional representatives promulgated a far-reaching bill in 2012 to 'manage and streamline the deployment and use of cellular antennas support infrastructure' in urban areas, including measures to protect vulnerable persons and empower citizens to permit or deny an installation in their locality.[89] The so-called Tower Law is the most extensive example of national regulation to date, and may pave the way for an eventual international treaty to organize mobile phone technology

in much the same way that the international conventions of 1926, 1949 and 1968 systematized road traffic safety.[90] What is most interesting in this decisive piece of legislation is the focus on vulnerable populations and the promotion of civic engagement through concrete measures designed to remove control of BTS installation from the telecom companies. This has created a framework for dialogue and compensation that is sorely missing in the legislative landscape of most national governments. As self-proclaimed leaders in BTS streamlining and management, the Chileans have chosen to focus on the technology hardware, rather than electro sensitivity, the illness linked to intolerance of electromagnetic waves. The most egregious violation of human rights is in fact caused by the hardware because, without a protective legislative framework, a BTS installation directly impacts children whether or not they use a mobile phone. This infringes upon the responsibility to protect children guaranteed by international treaty law. Moreover, installation usually proceeds without any civic engagement whatsoever, amplifying the democratic deficit that occurs when governments or institutions fall short of fulfilling citizen consultation, one of the essential tenets of democracy.

While we argue that all states are obliged to regulate business compliance with the Convention on the Rights of the Child on a national level, we recognize the effectiveness of corporate lobbying and the subsequent reluctance of states to promulgate emissions thresholds that might impact the breakneck development of the technology sector. This presents an opportunity for national judicial systems to interpret whether radio frequency EMF constitutes a new form of environmental pollution and whether the absence of consultation for BTS installations is a violation of democratic principles. Given the slow pace of regulation worldwide, courts have begun to produce judicial interpretation of the principle of precaution and state obligations under national and international law with respect to electromagnetic pollution. The great debate in international law between binding versus voluntary human rights standards for businesses has created a regulatory void that certain courts have been called upon to fill.[91] Despite argument concerning a plaintiff-friendly regime in Europe versus a defendant-friendly regime in the USA,[92] we note that the main problem seems to be the difficulty in applying existing law to the competing interests engendered by the digital revolution.

In the case of France, the principle of precaution inscribed in the Constitution in 2005 is supposed to function as a guiding standard when determining how to evaluate environmental risk, especially with respect to

the most vulnerable members of society, such as children. France presents a good example, however, of the complexities of judicial interpretation of the precautionary principle. As demonstrated below, lower courts initially decided in favour of citizen protection from EMF pollution, only to have their rulings reversed by higher tribunals. With the passage of the *Loi Abeille* in 2015, lower courts have again ruled in favour of citizen protection in a new series of rulings on electro sensitivity. It is not entirely clear why the judicial system is divided on the issue of wireless technology, but France's unusual system of three jurisdictions (civil, criminal and administrative) may also lend itself to discordant jurisprudence among these three jurisdictions.

In October 2011, the Council of State (*Conseil d'Etat*), the highest court overseeing French administrative matters, handed down a decision that circumscribed the role of mayors in determining whether a BTS installation was appropriate in their commune or municipality. Instead, the Council indicated that responsibility for BTS installation was firmly in the hands of the *Autorité de regulation des communications électroniques et des postes* and the ANFR, two national bodies that regulate the emission of electromagnetic waves and the placement of mobile phone towers, with a mandate to assure full coverage throughout France. Activist organizations immediately pointed out that agencies tasked with a full coverage mandate would be less likely to adopt a precautionary approach, which in turn poses a challenge to the Constitution.[93] Another controversial ruling occurred in May 2012 when the French Jurisdictional Court (*Tribunal des Conflits*), a hybrid super-court that is called upon to decide whether France's civil or administrative courts have jurisdiction in the event of a dispute, overturned a seminal appeals decision.[94] The industry claimant insisted that the authority to dismantle BTS was under the jurisdiction of the administrative, rather than the civil court system; the plaintiff's suit to the hybrid court rightly emphasized the lack of pertinent national legislation on this issue. The Tribunal rendered an odd decision, declaring that a civil court was competent to determine financial damages for health risks incurred due to exposure to emissions from a mobile phone tower, whereas only an administrative court could order the dismantling of the tower, concluding that it is the administrative court that has policing jurisdiction in this domain under French law.[95] By diminishing the force of the principle of precaution through these two decisions—the first of which removes the power to protect from the elected official closest to

those citizens most impacted by an installation, and the second of which provides the administrative court with the power to adjudicate what is essentially a civil matter—the French judicial system rendered jurisprudence that appears to contradict the nation's binding treaty obligations concerning children.

With the promulgation of the *Loi Abeille* in January 2015, the courts were presented with the opportunity to interpret new legislation couched in broad language. The Tribunal for Disability Litigation of Toulouse (*Tribunal du contentieux de l'incapacité de Toulouse*) recognized electro sensitivity as a handicap for a limited period of three years, but with the possibility of renewal if the condition persists. The National Court for Disability in Amiens upheld the lower body's decision, awarding a former journalist 800 euros per month in disability allocations in what may be a precedent-setting decision. Certain organizations claimed that up to 70,000 electro sensitive citizens who live in France would be affected by the ruling.[96] Although these numbers may be exaggerated, the ruling could result in annual costs of over 600 million euros if the French government were required by the courts to award disability allocations to these potential claimants.

More importantly, these latter examples of French jurisprudence demonstrate a narrow reading of the law, one that benefits the plaintiff suffering from electro sensitivity due to EMF pollution, but provides no protection whatsoever in terms of the general population. If we return to Gollier's 'reasonable' interpretation of the precautionary principle, discussed at the beginning of this chapter, there is a clear benefit to the state in acting to prevent long-term risk—a careful cost-benefit analysis shows that current and future preventative actions are not close substitutes for one another, and that it may be very expensive to wait until the numbers of electro sensitive plaintiffs increases. Instead, our earlier recommendations of reducing exposure to EMF, requiring maximization of wired rather than wireless networks, and creating 'white zones' with little to no EMF pollution would represent substantive efforts to enact the principle of precaution.

In conclusion, this chapter has explored the challenges posed by the promulgation of EMF emission regulation and argued that the difficulties are due to a lack of scientific knowledge on long-term impact, along with a contested understanding of what constitutes appropriate assessment of risk. We have demonstrated how inadequate regulation of BTS

emissions has generated contradictory policies and jurisprudence at the national and local level, and has failed to reassure citizens that their health and the health of their children is sufficiently protected. In light of this situation we have posited that the human rights framework to 'protect, respect and remedy' vulnerable populations from corporate violations of international law should apply to US and European regulation on EMF exposure. In particular, we have explained how the dearth of legislation to regulate the installation of BTS in close proximity to children's facilities and schools constitutes a human rights concern according to the language of the Convention on the Rights of the Child, a treaty that has been ratified by nearly all states.

If we wish to stay digitally connected, there are currently no technical solutions available to modify the latent danger posed by the hardware necessary for mobile phone delivery. Thus, we must turn to civic choices in order to protect vulnerable populations from the increasing power of BTS emissions. In the case of the automobile, we have decided as a society that it is not necessary to travel at 200 kilometres per hour on the highway in order to reach our destination. By imposing speed limits, we 'arrive alive', to quote a popular public education campaign. Much the same is true for mobile phone use. If, as many independent scientists have demonstrated, exposure to low level electromagnetic frequencies has a verifiable impact on health and may lead to serious illness in some cases, how many people are we willing to sacrifice for our technological comfort? Surely children, who are biologically more vulnerable and who have no say in the matter, warrant a higher level of protection than adults.

This does not mean that electromagnetic wave emissions have to be so low that the telecom companies are no longer able to operate, but rather that we find a balance. If we are to deliver on the promise of digital technology to enhance democratic dialogue and facilitate human lifestyles, then we have to make sure it is environmentally safe to use—particularly for the generations to come. In the next chapter, we move to the virtual world of the Internet in order to examine the impact of surveillance, both public and private, on our use of digital technology. As the technology of surveillance improves, our ability to protect our privacy and respond to this substantive threat to one of our fundamental freedoms diminishes. We argue for privacy-by-design initiatives to protect all users from non-consensual use of their personal data in a digital environment.

Notes

1. International Telecommunication Union (2016) 'The World in 2015: ICT Facts and Figures', http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx, date accessed, 10 March 2016.
2. International Telecommunication Union (2016), The World in 2015.
3. See Roda & Perry (2014) 'Mobile Phone Infrastructure in Europe'. Also note that human rights activists, legal scholars and journalists have denounced in chorus the violations provoked by the mining of minerals such as coltan, a dense silicate necessary for the functioning of analogue and digital mobile phones. Perry, S. (2015). L'Illusion Pixel. Paris: Lemieux Éditeur; Essick, K. (2001) 'Guns, Money and Cell Phones', *The Industry Standard Magazine*; Hayes, K., and Burge, R. (2003) 'Coltan Mining in the Democratic Republic of Congo: How tantalum-using industries can commit to the reconstruction of the DRC'; Montague, D. (2002) 'Stolen Goods: Coltan and Conflict in the Democratic Republic of the Congo', *SAIS Review,* Vol. 22, No. 1, Winter-Spring.
4. See, for example, Davis, D. (2010) *Disconnect: The Truth about Cell Phone Radiation, What the Industry Has Done to Hide it, and How to Protect Your Family*. While no US government agency as of this writing had acknowledged health risks from EMF exposure, the US Federal Communications Commission has suggested steps to avoid excessive wireless phone use, and the US Food and Drug Administration has provided precautionary suggestions for children and mobile phone use.
5. International Commission on Non-Ionising Radiation Protection (2009b) 'Guidelines for Limiting Exposure to Time-varying Electric, Magnetic, and Electromagnetic Fields (up to 300 GHz)', *Health Physics,* Vol. 97, No. 3, p. 11.
6. BTS typically support antennas, one or more sets of transmitter/receivers, transceivers, digital signal processors, control electronics, a GPS receiver for timing, primary and backup electrical power sources, and covering or shelter.
7. The Digital Agenda for Europe required all member states to devise, and make operational by 2012, national broadband plans which would enable the EU to meet the broadband targets for Europe by 2020.
8. FCC (2014) 'Statement of Commissioner Ajit Pai Approving in Part and Concurring in Part', http://www.fcc.gov/article/fcc-14-113a3, date accessed 6 August 2014. Under 47 U.S.C. § 1302(b), the Commission inquiry must 'determine whether advanced telecommunications capability is being deployed to all Americans in a reasonable and timely fashion', with a negative determination requiring 'immediate [Commission] action to accelerate deployment of such capability by removing barriers to

infrastructure investment and by promoting competition in the telecommunications market.'

9. International Agency for Research on Cancer (2011) 'IARC Classifies Radiofrequency Electromagnetic Fields as Possibly Carcinogenic to Humans', World Health Organization, Press release No. 208.
10. Baan, R., et al. (2011) 'Carcinogenicity of Radiofrequency Electromagnetic Fields', *The Lancet Oncology,* Vol. 12, pp. 624–626.
11. Baan, R., et al., Carcinogenicity of Radiofrequency Electromagnetic Fields, p. 625.
12. For example, Blank, M., and Goodman, R. (2009) 'Electromagnetic Fields Stress Living Cells', *Pathophysiology,* Vol. 16, pp. 71–78; Christ, A., et al. (2010) 'Age-dependent tissue-specific exposure of cell phone users', *Physics in Medicine and Biology,* Vol. 55, p. 1767; Divan, H.A., et al. (2008) 'Prenatal and Postnatal Exposure to Cell Phone Use and Behavioral Problems in Children', *Epidemiology',* Vol. 19, pp. 523–529; Divan, et al. (2012) 'Cell Phone Use and Behavioural Problems in Young Children', *Journal of Epidemiology and Community Health,* Vol. 66, pp. 524–529. ICNIRP (2009) 'Guides for Limiting Exposure'; Sudan, M., et al. (2012) 'Prenatal and Postnatal Cell Phone Exposures and Headaches in Children', *The Open Pediatric Medicine Journal*, Vol. 6, pp. 46–52.
13. One researcher has suggested that telecommunications companies have achieved an untouchable status with respect to health regulators in today's economy, similar to that of major banks with respect to financial regulators. See Eileen O'Conner's 'Statement to European Commission Stakeholder Dialogue Group', Brussels, 20 February 2013.
14. Recent international instruments discussed below, such as the *OECD Guidelines for Multinational Enterprises* or the Ruggie Report, promulgated by the UN Human Rights Council, oblige state parties to 'protect, respect and remedy' human rights violations by businesses against individuals or groups, bringing corporations into the UN human rights paradigm through state compliance with binding treaty law.
15. Brandt, A. (2007) *The Cigarette Century: The Rise, Fall, and Deadly Persistence of the Product That Defined America*; Kluger, R. (1996) *Ashes to Ashes: America's Hundred-Year Cigarette War, the Public Health, and the Unabashed Triumph of Philip Morris*; Knopf, A., and Glantz, S. (1996) *The Cigarette Papers*; Proctor, R. (2012) *Golden Holocaust: Origins of the Cigarette Catastrophe and the Case for Abolition*.
16. 'Foresight' in German, an idea developed in the 1930s by German social scientists.
17. Heaven v. Pender (1883) 11 QBD 503, Court of Appeal, UK, introduced the 'duty of care', a wider duty to be responsible in tort to those who might be injured if 'ordinary care and skill' were not exercised.

18. Prospect theory is a probabilistic theory modeling the choices of people in situations in which decisions are madeunder risk with knowledge of the probabilities of the outcomes. In particular, the authors propose this theory as analternative to expected utility theory to account for facts such as the underweighting of outcomes that are merelyprobable in comparison with outcomes that are obtained with certainty.
19. Tversky, A. and Kahneman, D. (1981) 'The Framing of Decisions and the Psychology of Choice', *Science*, *New Series*, Vol. 211, No. 4481, p. 453.
20. Thaler, R. and Sunstein, C. (2008) *Nudge: Improving Decisions about Health, Wealth, and Happiness.*
21. Mettler, S. (2010) 'Reconstituting the Submerged State: The Challenges of Social Policy Reform in the Obama Era', *Perspectives on Politics,* Vol. 8, No. 3, pp. 803–824.
22. Mettler, Reconstituting the Submerged State, p. 803.
23. Sunstein, C. (2005) *Laws of Fear: Beyond the Precautionary Principle* (Cambridge : Cambridge University Press).
24. Gollier, C. (2001) 'Should we beware of the Precautionary Principle?' *Economic Policy*, Vol. 16, No. 10, pp. 301–328.
25. de Jong, A., et al. (2012) 'Assumptions in Quantitative Analyses of Health Risks of Overhead Power Lines', *Environmental Science & Policy,* Vol. 16, No. 10, pp. 114–121.
26. The OSPAR Commission is a collaboration between the EU and 15 Governments to protect the marineenvironment of the North-East Atlantic. The name originates from the Oslo and Paris Conventions ("OS" for Osloand "PAR" for Paris).
27. REACH is a European Union regulation adopted to improve the protection of human health and the environmentfrom the risks posed by chemicals. See https://echa.europa.eu/regulations/reach
28. See Council of European Communities (1983) 'Council Directive 83/447/EEC On the protection of workers from the risks related to exposure to asbestos at work', European Commission, https://ec.europa.eu (home page), date accessed 13 March 2016; and European Parliament (2003) Directive 2003/18/EC, http://www.europarl.europa.eu (home page), date accessed 10 March 2016.
29. World Health Organization (2012) Electromagnetic Fields: Current Standards.
30. Reviews are provided in: Bioinitiative Report 2012; Bioinitiative Working Group Comments 2014; Kostoff, R.N., and Lau, C.G.Y. (2013) 'Combined biological and health effects of electromagnetic fields and other agents in the published literature', *Technological Forecasting and Social Change,* Volume 80, No. 7, pp. 1331–1349; Levitt, B., and Lai, H. (2010) 'Biological effects from exposure to electromagnetic radiation

emitted by cell tower base stations and other antenna arrays', *Environmental Review,* Vol. 18, pp. 369–395.

31. See: Consales, et al. (2012) 'Electromagnetic fields, oxidative stress, and neurodegeneration', *International Journal of Cell Biology,* Vol. 2012, pp. 1–16; Feychting, M., and Forssen, U. (2006) 'Electromagnetic fields and female breast cancer', *Cancer Causes Control,* Vol. 17, No. 4, pp. 553–558; Gaestel, M. (2010) 'Biological monitoring of non-thermal effects of mobile phone radiation: recent approaches and challenges', *Biological reviews of the Cambridge Philosophical Society,* Vol. 85, No. 3, pp. 489–500; Merhi, Z.O. (2012) 'Challenging cell phone impact on reproduction: a review', *Journal of assisted Reproduction and Genetics*, Vol. 29, No. 4, pp. 293–297; Sommer, C., et al. (2009) 'Induced pluripotent stem cell generation using a single lentiviral stem cell cassette', *Stem Cells,* Vol. 27, No. 3, pp. 543–549.
32. See, for example, Foliart, D.E., et al. (2006) 'Magnetic Field Exposure and Long-term Survival among Children with Leukaemia', *Br J Cancer,* Vol. 94, No. 1, pp. 161–164; Lowenthal, R.M., et al. (2007) 'Residential exposure to electric power transmission lines and risk of lymphoproliferative and myeloproliferative disorders: a case-control study', *Internal Medicine Journal*, Vol. 37, No. 9, pp. 614–619 for ELF effects; Aldad, T., et al. (2012) 'Fetal Radiofrequency Radiation Exposure From 800–1900 Mhz-Rated Cellular Telephones Affects Neurodevelopment and Behavior in Mice', *Nature Scientific Reports,* 2, Article No. 312; Aslan, A., et al. (2013) 'Effect of 900MHz electromagnetic fields emitted from cellular phones on fracture healing: an experimental study on rats', *Acta orthopaedica et traumatologica turcica,* Vol. 47, No. 4, pp. 273–280; Christ, A., et al. (2010) 'Age-dependent tissue-specific exposure of cell phone users'; Gutschi, T., et al. (2011) 'Impact of cell phone use on men's semen parameters', *Andrologia,* Vol. 43, No. 5, pp. 312–316; Hardell, L., et al. (2005) 'Case-control study on cellular and cordless telephones and the risk for acoustic neuroma or meningioma in patients diagnosed 2000–2003', *Neuroepidemiology,* Vol. 25, No. 3, pp. 120–128; Hardell, L., et al. (2013) 'Use of mobile phones and cordless phones is associated with increased risk for glioma and acoustic neuroma', *Pathophysiology,* Vol. 20, pp. 85–110; Panagopoulos, D.J., and Margaritis, L.H. (2010) 'The effect of exposure duration on the biological activity of mobile telephony radiation', *Mutation Research,* Vol. 699, No. 1–2, pp. 17–22 for RF effects caused by the use of wireless devices; and Abdel-Rassoul, G., et al. (2007) 'Neurobehavioral effects among inhabitants around mobile phone base stations', *Neurotoxicology,* Vol. 28, pp. 434–440; Khurana, V.G., et al. (2010) 'Epidemiological evidence for a health risk from mobile phone base stations', *International Journal of Occupational and Environmental Health,*

Vol. 16, pp. 263–267; Levitt and Lai (2010) 'Biological effects from exposure to electromagnetic radiation'; Otitoloju, A.A., et al. (2010) 'Preliminary study on the induction of sperm head abnormalities in mice, Mus musculus, exposed to radiofrequency radiations from global system for mobile communication base stations', *Bulletin of Environmental Contamination and Toxicology,* Vol. 84, No. 1, pp. 51–54., and Shahbazi-Gahrouei, D., et al. (2014) 'Health effects of living near mobile phone base transceiver station (BTS) antennae: a report from Isfahan, Iran', *Electromagnetic Biology and Medicine,* Vol. 33, pp. 206–201 for RF effects caused by exposure to BTS stations.

33. Agarwal, A., et al. (2009) 'Effects of radiofrequency electromagnetic waves (RF-EMW) from cellular phones on human ejaculated semen: an in vitro pilot study', *Fertility and Sterility,* Vol. 92, No. 4, pp. 1318–1325; La Vignera, S., et al. (2012) 'Effects of the exposure to mobile phones on male reproduction: a review of the literature.', *Journal of Andrology,* Vol. 33, No. 3, pp. 350–356; Otitoloju, A., et al. (2010) 'Preliminary study on the induction of sperm head abnormalities in mice'; Panagopoulos and Margaritis (2010) 'The effect of exposure duration on the biological activity of mobile telephony radiation'.
34. Aldad, T., et al. (2012) 'Fetal Radiofrequency Radiation Exposure F'; Divan et al. (2008) 'Prenatal and Postnatal Exposure'; Li, D.K., et al. (2012) 'A Prospective Study of In-utero Exposure to Magnetic Fields and the Risk of Childhood Obesity', *Nature Scientific Reports* 2, Article 540.
35. Hardell et al. (2005) 'Case-control study on cellular and cordless telephones'; Hardell, et al. (2013) 'Use of mobile phones and cordless phones'; Kheifets, L., et al. (2010) 'Pooled analysis of recent studies on magnetic fields and childhood leukaemia', *British Journal of Cancer,* Vol. 103, No. 7, p. 1128; Levis, A.G., et al. (2011) 'Mobile phones and head tumours. The discrepancies in cause-effect relationships in the epidemiological studies—how do they arise?' *Environmental Health: a Global Access Science Source,* Vol. 10, No. 1, p. 59.
36. Chen, Q., et al. (2013) 'A Meta-Analysis on the Relationship between Exposure to ELF-EMFs and the Risk of Female Breast Cancer', *PLoS One,* Vol. 8, No. 7; Erren, T.C. (2001) 'A meta-analysis of epidemiologic studies of electric and magnetic fields and breast cancer in women and men', *Bioelectromagnetics,* Suppl 5, pp. 105–119.
37. Hug, K., et al. (2006) 'Magnetic field exposure and neurodegenerative diseases-recent epidemiological studies', *Sozial und Praventivmedizin,* Vol. 51, No. 4, pp. 210–220.
38. Abelin, T., et al. (2005) 'Sleep Disturbances in the Vicinity of the Shortwave Broadcast Transmitter Schwarzenburg', *Somnologie,* Vol. 9, No. 4, pp. 203–209; Shahbazi-Gahrouei, D., et al. (2014) 'Health effects of liv-

ing near mobile phone base transceiver station (BTS) antennae: a report from Isfahan, Iran', *Electromagnetic Biology and Medicine,* Vol. 33, No. 3, pp. 206–201.

39. Abdel-Rassoul, G., et al. (2007) 'Neurobehavioral Effects'; Hagström, M., et al. (2013) 'Electromagnetic hypersensitive Finns: Symptoms, perceived sources and treatments, a questionnaire study', *Pathophysiology,* Vol. 20, No. 2, pp. 117–122.
40. Cucurachi, S., et al. (2013) 'A review of the ecological effects of radiofrequency electromagnetic fields (RF-EMF)', *Environment International*, Vol. 51, pp. 116–140.
41. Panagopoulos, D.J. (2011) 'Analyzing the Health Impacts of Modern Telecommunications Microwaves', *Advances in Medicine and Biology,* Vol. 17, p. 11.
42. Blank and Goodman (2009) 'Electromagnetic Fields Stress Living Cells', pp. 71, 76.
43. Blank and Goodman (2011) 'DNA is a fractal antenna in electromagnetic fields', *International Journal of Radiation Biology,* Vol. 87, pp. 409–415.
44. See, for example, Byun, Y.H., et al. (2013) 'Mobile phone use, blood lead levels, and attention deficit hyperactivity symptoms in children: a longitudinal study', *PLoS One*, Vol. 8, No. 3, e59742; Davis, D.L., et al. (2013) 'Swedish review strengthens grounds for concluding that radiation from cellular and cordless phones is a probable human carcinogen', *Pathophysiology,* Vol. 20, No. 2, 123–129; Divan, et al. (2012) 'Cell Phone Use and Behavioural Problems in Young Children'; Hardell, L., et al. (2013) 'Use of mobile phones and cordless phones is associated with increased risk for glioma and acoustic neuroma'; Peyman, et al. (2009) 'Variation of the dielectric properties of tissues with age: the effect on the values of SAR in children when exposed to walkie-talkie devices', *Physics in Medicine and Biology*, Vol. 54, No. 2, pp. 227–241; Sudan, M., et al. (2012) 'Prenatal and Postnatal Cell Phone Exposures and Headaches in Children'; Wiart, J. et al. (2008) 'Analysis of RF exposure in the head tissues of children and adults', *Physics in Medicine and Biology*, Vol. 53, No. 13, pp. 3681–3695.
45. Christ, et al. (2010) 'Age-dependent tissue-specific exposure of cell phone users', p. 1780.
46. Li, et al. (2012) 'A Prospective Study of In-utero Exposure to Magnetic Fields and the Risk of Childhood Obesity, p. 1.
47. See, for example, Aydin, D., et al. (2011) 'Mobile Phone Use and Brain Tumors in Children and Adolescents: A Multicenter Case-Control Study', *Journal of the National Cancer Institute,* Vol. 103, No. 16, pp. 1264–1276; Scientific Committee on Emerging and Newly Identified Health Risks (2015) 'Potential Health Effects of Exposure to Electromagnetic Fields', European Commission; Valentini, E., et al. (2010) 'Systematic review and

meta-analysis of psychomotor effects of mobile phone electromagnetic fields', *Occupational and Environmental Medicine,* Vol. 67, No. 10, pp. 708–716.

48. Levitt and Lai (2010) 'Biological effects from exposure to electromagnetic radiation emitted by cell tower base stations and other antenna arrays', p. 373.
49. As the download speed increases, the number of bits per second increases. Since the energy per bit must remain the same in order to maintain the same quality of service, there is a higher energy level per second, which is an increase in radiated power.
50. Institute of Electrical and Electronics Engineers Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 (1999, 2005).
51. International Commission on Non-Ionising Radiation Protection (1998) 'Guidelines for Limiting Exposure to Time-varying Electric, Magnetic, and Electromagnetic Fields (up to 300 GHz)', *Health Physics*, Vol. 74, No. 4, pp. 494–522.
52. In his report to the Council of Europe, Rapporteur Jean Huss states 'it is most curious, to say the least, that the applicable official threshold values for limiting the health impact of extremely low frequency electromagnetic fields and high frequency waves were drawn up and proposed to international political institutions (WHO, European Commission, governments) by the ICNIRP, an organization whose origin and structure are none too clear and which is furthermore suspected of having rather close links with the industries whose expansion is shaped by recommendations for maximum threshold values for the different frequencies of electromagnetic fields'. (Huss, J. (2011) Section B Explanatory Memorandum by Mr. Huss, Rapporteur, point 29).
53. Georgiou, C.D. (2010) 'Oxidative stress-induced biological damage by low-level EMFs: mechanism of free radical pair electron spin polarization and biochemical amplification,' *European Journal of Oncology*, Vol. 5, pp. 63–113.
54. Hansson, B., et al. (2011) 'Analysis of the effect of mobile phone base station antenna loading on localized SAR and its consequences for measurements', *Bioelectromagnetics,* Vol. 32, No. 8, pp. 664.
55. Han, Y., et al. (2010) 'Comparative assessment of models of electromagnetic absorption of the head for children and adults indicates the need for policy changes', *European Journal of Oncology,* Vol. 5, p. 103.
56. Belyaev, I.Y. (2010) 'Dependence of non-thermal biological effects of microwaves on physical and biological variables: implications for reproducibility and safety standards', *European Journal of Oncology,* Vol. 5, pp. 187–217; Fragopoulou, et al. (2010) 'Scientific panel on electromag-

netic field health risks: consensus points, recommendations, and rationales', *Reviews on Environmental Health,* Vol. 25, No. 4, pp. 307–317.

57. See, for example, Belyaev (2010) 'Dependence of non-thermal biological effects of microwaves', Bioinitiative Working Group Comments 2014; Bioinitiative Report 2007, 2012; Blackman, C. (2009) 'Cell phone radiation: Evidence from ELF and RF studies supporting more inclusive risk identification and assessment', *Pathophysiology*, Vol. 16, No. 2–3, pp. 205–216.
58. International Commission on Non-Ionising Radiation Protection (2009a), pp. 102 and 273.
59. Axelson, O. (2004) 'Negative and non-positive epidemiological studies', *International Journal of Occupational Medicine and Environmental Health,* Vol. 17, No. 1, pp. 115–121; Blair, A., et al. (2007) 'Methodological issues regarding confounding and exposure misclassification in epidemiological studies of occupational exposures', *American Journal of Industrial Medicine,* Vol. 50, No. 3, pp. 199–207; Georgiou (2010) 'Oxidative stress-induced biological damage'.
60. Bioinitiative Working Group Comments (2014); Bioinitiative Report (2007, 2012); Fragopoulou (2010) 'Scientific panel on electromagnetic field health risks'.
61. Belyaev (2010) 'Dependence of non-thermal biological effects of microwaves'; Kostoff and Lau (2013) 'Combined biological and health effects of electromagnetic fields'.
62. Böschen, S., et al. (2010) 'Scientific Nonknowledge and Its Political Dynamics: The Cases of Agri-Biotechnology and Mobile Phoning', *Science, Technology & Human Values,* Vol. 35, p. 792.
63. International Agency for Research on Cancer (2011) IARC Classifies Radiofrequency Electromagnetic Fields as Possibly Carcinogenic to Humans', *World Health Organization,* Press release No. 208.
64. The Federal Communications Commission set the SAR threshold limit for public exposure from cellular telephones at 1.6 watts per kilogram (1.6 W/kg), compared to the threshold of 2.0 W/kg recommended by the Council of Europe. See discussion above regarding the viability of SAR measurements.
65. House of Representatives (1993) Children's Electromagnetic Field Risk Reduction Act, 103rd Congress, 1st Session, H.R. 1494.
66. House of Representatives (1993) Electromagnetic Labeling Act, 103rd Congress, 1st Session, H.R. 1665.
67. House of Representatives (2012) Cell Phone Right to Know Act, 112th Congress, 2nd Session, H.R. 6358.
68. House of Representatives (2012) Cell Phone Right to Know Act.

69. Crawford, S. (2013) *Captive Audience: The Telecom Industry and Monopoly Power in the New Gilded Age* (New Haven: Yale University Press).
70. A simple (cabled) Internet search will reveal dozens of newly formed citizens' action groups every month on both sides of the country. On installation of smart meters in California, see: Stop Smart Meters, (2014) 'Some PG&E Customers Getting Fees Reversed as CPUC Endlessly Delays Smart Meter "Opt Out" Decision', http://stopsmartmeters.org (home page), date accessed 15 August 2014. On protest against towers in rural Connecticut, see: Smith, A. (2014) 'Westporters Rally Against Cellphone Tower Proposed for Residential Area', http://westport.dailyvoice.com (home page), date accessed 15 August 2014.
71. Parliamentary Assembly, Council of Europe (2011) 'Resolution 1815 On the potential dangers of electromagnetic fields and their effect on the environment', Section 8.4.3.
72. The authors of one of the major studies that prompted the IARC carcinogenic classification recently remarked that the measure 'does not seem to have had any significant impact on governments' perceptions of their responsibilities to protect public health from this widespread source of radiation' Hardell, et al. (2013) 'Use of mobile phones and cordless phones associated with increased risk for glioma and acoustic neuroma', p. 85.
73. EU limits are set at 41 V/m for GSM 900; 58 V/m for GSM 1800; and 61 V/m for UMTS. These norms were calculated on the basis of thermal effects of electromagnetic waves on the human organism, based on the assumption that excessive heat posed the greatest danger to the human cell.
74. Up to one third of mobile phone tower installations in Paris, for example, are on city property that is rented to the telecom companies. Interview with Mao Peninou, *Maire adjoint* for the City of Paris, chief negotiator for the 2012 Charter, March 2012.
75. One of the authors of this chapter has been active in drafting protective legislation for the French parliament. See *Proposition de Loi relative à la sobriété à la transparence et à la concertation en matière aux ondes électromagnétiques*, Sponsored by Laurence Abeille, *Assemblée Nationale*, 31 January 2013 and 22 January 2014; Loi no. 2015-136 du 9 février 2015.
76. Loi Abeille, 2015 and Abeille, L. (2015) Exposition aux ondes électromagnétiques: deuxième lecture, Assemblée nationale, XIVe législature, Session ordinaire de 2014-2015, Compte rendu intégral, Première séance du jeudi 29 janvier 2015, p. 5, http://www.assemblee-nationale.fr (home page), date accessed 13 March 2016.
77. Ville de Paris (2003) *Charte relative aux antennes relais de téléphonie mobile, Au sens de l'article 1 du décret n° 2002-775 du 3 mai 2002.*

78. Maussion, C. (2011) '4G: la suspension des antennes irrite Besson', *Liberation,* 19 October.
79. Ville de Paris (2012) *Charte relative à la téléphonie mobile, Au sens de l'article 1 du décret n° 2002-775 du 3 mai 2002.*
80. According to the report, the average simulated exposure for the cities under study was increased by approximately 50 per cent with the addition of 4G (LTE) antennas. For example, in the 14th arrondissement of Paris, the simulated ground exposure levels rose from approximately 0.6 V/m to 0.9 V/m (Direction Générale de la Prévention des Risques du Ministère de l'Ecologie, du Développement Durable et de l'Energie et al. (2013) Diminution de l'exposition aux ondes électromagnétique émises par les antennes-relais de téléphonie mobile, p. 95, author's translation)
81. Agence Nationale des Fréquences (2016b) Cartoradio, http://www.cartoradio.fr/cartoradio/web/, date accessed 13 March 2016.
82. Historic zoning is especially strict. See Art. R111-21, amended by decree no. 2007–18 of 5 January 2007, Code de l'Urbanisme.
83. Commissariat Générale au Développement Durable 2009, 73/1 and 84/1.
84. Brigaudeau, C. (2012) 'Ils disent non à l'antenne-relais', *Le Parisien*, 20 February.
85. See Posner, E. (2014) *The Twilight of Human Rights Law*.
86. U.S. Ambassador to the United Nations, Madeleine Albright, signed the Convention on the Rights of the Child on 16 February 1995. The USA also signed the Vienna Convention on the Law of Treaties on 24 April 1970.
87. Perry, et al. (2012) 'Submission to the United Nations Committee on the Rights of the Child'.
88. Perry, et al. (2012) 'Submission to the United Nations Committee on the Rights of the Child'.
89. Ministerio de Vivienda y Urbanismo, Gobierno de Chile, 11 June 2012, Authors' translation.
90. See: 1926 Paris Convention on Motor Traffic, 1949 Geneva Convention on Road Traffic, and 1968 Vienna Convention on Road Traffic.
91. See, for example, Norms on the Responsibilities of Transnational Corporations and other Business Enterprises with respect to Human Rights Panel discussion at the 60th session of the UN Commission on Human Rights, 25 March 2004, Geneva. Scholar David Weissbrodt has noted that the norms were never adopted as binding treaty law, but instead were incorporated into the UN Global Compact, a strictly voluntary reporting mechanism on corporate compliance with human rights law.
92. Smith, E. F. (2010) 'Right to Remedies and the Inconvenience of Forum Non Conveniens: Opening U.S. Courts to Victims of Corporate Human

Rights Abuses', *Columbia Journal of Law and Social Problems,* Vol. 44, No. 145, Winter.

93. The most active organisations on this issue in France are Robin des Toits and PRIARTEM at: http://www.robindestoits.fr and http://www.priartem.fr.
94. Cour d'Appel de Versailles, (8/09/2010) SAS Adia c/ comité d'entreprise de la Société Adia, 14ème chambre, Arret N°:324.
95. Tribunal des Conflits (14/05/2012) C3848, Publié au recueil Lebon.
96. Agence France-Presse (2015) 'L'électrosensibilité reconnue comme handicap par la justice', *Le Figaro*, http://sante.lefigaro.fr (home page), date accessed 26 August 2015.

Bibliography

Abdel-Rassoul G., El-Fateh O., Salem M., Michael A., Farahat F., El-Batanouny M., Salem E. (2007). Neurobehavioral effects among inhabitants around mobile phone base stations. *Neurotoxicology, 28*(2), 434–440.

Abeille, L. (2015). *Exposition aux ondes électromagnétiques: deuxième lecture*, Assemblée nationale, XIVe législature, Session ordinaire de 2014–2015, Compte rendu intégral, Première séance du jeudi 29 janvier 2015, p. 5. Retrieved March 13, 2016, from http://www.assemblee-nationale.fr (home page).

Abelin, T., Altpeter, E., & Röösli, M. (2005). Sleep disturbances in the vicinity of the short-wave broadcast transmitter Schwarzenburg. *Somnologie, 9*(4), 203–209.

Agarwal A., Desai N., Makker K., Varghese A., Mouradi R., Sabanegh E., Sharma R. (2009). Effects of radiofrequency electromagnetic waves (RF-EMW) from cellular phones on human ejaculated semen: An in-vitro pilot study. *Fertility and Sterility, 92*(4), 1318–1325.

Agence France-Presse. (2015). L'électrosensibilité reconnue comme handicap par la justice. *Le Figaro.* Retrieved August 26, 2015, from http://sante.lefigaro.fr (home page).

Agence Nationale des Fréquences. (2016). *Cartoradio.* Retrieved March 13, 2016, from http://www.cartoradio.fr/cartoradio/web/.

Aldad T., Gan G., Gao X., Taylor H. (2012). Fetal radiofrequency radiation exposure from 800–1900 Mhz-rated cellular telephones affects neurodevelopment and behavior in mice. *Nature Scientific Reports,* 2. Article 312.

Aslan A., Atay T., Gulle K., Kırdemir V., Ozden A., Comlekci S., Aydogan N. (2013). Effect of 900 MHz electromagnetic fields emitted from cellular phones on fracture healing: An experimental study on rats. *Acta orthopaedica et traumatologica turcica, 47*(4), 273–280.

Axelson, O. (2004). Negative and non-positive epidemiological studies. *International Journal of Occupational Medicine and Environmental Health, 17*(1), 115–121.

Aydin, D., et al. (2011). Mobile phone use and brain tumors in children and adolescents: A multicenter case-control study. *Journal of the National Cancer Institute, 103*(16), 1264–1276.

Baan R., Grosse Y., Lauby-Secretan B., El Ghissassi F., Bouvard V., Benbrahim-Tallaa L., et al. on Behalf of the WHO International Agency for Research on Cancer Monograph Working Group. (2011). Carcinogenicity of radiofrequency electromagnetic fields. *The Lancet Oncology, 12*, 624–626.

Belyaev, I. Y. (2010). Dependence of non-thermal biological effects of microwaves on physical and biological variables: Implications for reproducibility and safety standards. *European Journal of Oncology, 5*, 187–217.

Bioinitiative Report. (2007). A rationale for a biologically-based public exposure standard for electromagnetic fields (ELF and RF). Retrieved July 12, 2012, from http://www.bioinitiative.org (home page).

Bioinitiative Report. (2012). A rationale for biologically-based public exposure standards for electromagnetic radiation. Retrieved August 15, 2014, from http://www.bioinitiative.org (home page).

Bioinitiative Working Group Comments. (2014). Comments on 2014 SCENIRH preliminary opinion on potential health effects of EMF. Retrieved August 15, 2014, from http://www.bioinitiative.org (home page).

Blackman, C. (2009). Cell phone radiation: Evidence from ELF and RF studies supporting more inclusive risk identification and assessment. *Pathophysiology, 16*, 205–216.

Blair A., Stewart P., Lubin J., Forastiere F. (2007). Methodological issues regarding confounding and exposure misclassification in epidemiological studies of occupational exposures. *American Journal of Industrial Medicine, 50*, 199–207.

Blank, M., & Goodman, R. (2009). Electromagnetic fields stress living cells. *Pathophysiology, 16*, 71–78.

Blank, M., & Goodman, R. (2011). DNA is a fractal antenna in electromagnetic fields. *International Journal of Radiation Biology, 87*, 409–415.

Böschen, S., Böschen, S., Kastenhofe K., Rust I., Soentgen J., Wehling P. (2010). Scientific non knowledge and its political dynamics: The cases of agri-biotechnology and mobile phoning. *Science, Technology & Human Values, 35*, 783–811.

Brandt, A. (2007). *The cigarette century: The rise, fall, and deadly persistence of the product that defined America*. New York: Basic Books.

Brigaudeau, C. (2012, February 20). Ils disent non à l'antenne-relais. *Le Parisien*.

Byun, Y. H., Ha , M., Kwon, H., Hong, Y., Leem, J., Sakong, J., et al. (2013). Mobile phone use, blood lead levels, and attention deficit hyperactivity symptoms in children: A longitudinal study. *PLoS One*, *8*(3), e59742.

Chen, Q., et al. (2013). A meta-analysis on the relationship between exposure to ELF-EMFs and the risk of female breast cancer. *PLoS One*, 8(7), e69272.

Christ, A., Gosselin M., Christopoulou M., Kühn S., Kuster N. (2010). Age-dependent tissue-specific exposure of cell phone users. *Physics in Medicine and Biology, 55*, 1767.

Code de l'Urbanisme. (2012). Art. R111-21, Légifrance. Retrieved March 6, 2016, from https://www.legifrance.gouv.fr (home page).

Commissariat Générale au Développement Durable. (2009). Annual report to parliament on implementing France's environmental roundtable commitments. Ministère de l'Ecologie, de l'Energie, du Développement durable et de la Mer.

Committee on the Rights of the Child. (2013). General comment no. 16 on state obligations regarding the impact of the business sector on children's rights. United Nations Convention on the Rights of the Child.

Consales, C., Merla, C., Marino, C., Benassi, B., (2012). Electromagnetic fields, oxidative stress, and neurodegeneration. *International Journal of Cell Biology, 2012*, 1–16.

Council of European Communities. (1983). Council directive 83/447/EEC on the protection of workers from the risks related to exposure to asbestos at work. European Commission. Retrieved March 13, 2016, from https://ec.europa.eu (home page).

Cour d'Appel de Versailles. (8/09/2010). SAS Adia c/ comité d'entreprise de la Société Adia, 14ème chambre, Arret No. 324.

Crawford, S. (2013). *Captive audience: The telecom industry and monopoly power in the new gilded age*. New Haven, CT: Yale University Press.

Cucurachi, S., Tamis, W., Vijver, M., Peijnenburg, W., Bolte, J., de Snoo, G. (2013). A review of the ecological effects of radiofrequency electromagnetic fields (RF-EMF). *Environment International, 51*, 116–140.

Davis, D. (2010). *Disconnect: The truth about cell phone radiation, what the industry has done to hide it, and how to protect your family*. New York: Dutton Adult.

Davis, D., Kesari S., Soskolne, C., Miller, A., Stein Y. (2013). Swedish review strengthens grounds for concluding that radiation from cellular and cordless phones is a probable human carcinogen. *Pathophysiology, 20*(2), 123–129.

Direction Générale de la Prévention des Risques du Ministère de l'Ecologie, du Développement Durable et de l'Energie et al. (2013). *Diminution de l'exposition aux ondes électromagnétique émises par les antennes-relais de téléphonie mobile,* Rapport de Synthèse des Experimentations du COPIC. Retrieved September 10, 2013, from http://www.developpementdurable.gouv.fr/document138630

Divan, H. A., Kheifets, L., Obel, C., Olsen, J. (2008). Prenatal and postnatal exposure to cell phone use and behavioral problems in children. *Epidemiology, 19*, 523–529.

Divan, H., Kheifets, L., Obel, C., Olsen, J. (2012). Cell phone use and behavioral problems in young children. Journal of Epidemiology and Community Health, 66, 524–529.

Erren, T. C. (2001). A meta-analysis of epidemiologic studies of electric and magnetic fields and breast cancer in women and men. *Bioelectromagnetics, 22*(Suppl. 5), S105–S119.

Essick, K. (2001). Guns, money and cell phones. *The Industry Standard Magazine*. Retrieved March 13, 2016, from http://www.globalissues.org/article/442/guns-money-and-cell-phones

European Parliament. (2003). Directive 2003/18/EC. Retrieved March 10, 2016, from http://www.europarl.europa.eu (home page).

Feychting, M., & Forssen, U. (2006). Electromagnetic fields and female breast cancer. *Cancer Causes Control, 17*(4), 553–558.

Foliart, D. E., Pollock, B. H., Mezei, G ., Iriye,R ., Silva, J, M., Ebi, K. L.,et al. (2006). Magnetic field exposure and long-term survival among children with leukaemia. *British Journal of Cancer, 94*(1), 161–164.

Fragopoulou, Grigoriev, Y., Johansson, O., Margaritis, L.H., Morgan, L., Richter, E., Sage, C. (2010). Scientific panel on electromagnetic field health risks: Consensus points, recommendations, and rationales. *Reviews on Environmental Health, 25*(4), 307–317.

Gaestel, M. (2010). Biological monitoring of non-thermal effects of mobile phone radiation: Recent approaches and challenges. *Biological Reviews of the Cambridge Philosophical Society, 85*(3), 489–500.

Geneva Convention on Road Traffic. (1949). United Nations treaty collections. Retrieved March 6, 2016, from https://treaties.un.org (home page).

Georgiou, C. D. (2010). Oxidative stress-induced biological damage by low-level EMFs: Mechanism of free radical pair electron spin polarization and biochemical amplification. *European Journal of Oncology, 5*, 63–113.

Gollier, C. (2001). Should we beware of the precautionary principle? *Economic Policy, 16*(33), 301–328.

Gutschi, T., Mohamad Al-Ali, B., Shamloul, R., Pummer, K., Trummer, H. (2011). Impact of cell phone use on men's semen parameters. *Andrologia, 43*(5), 312–316.

Hagström, M., Auranen, J., & Ekman, R. (2013). Electromagnetic hypersensitive Finns: Symptoms, perceived sources and treatments, a questionnaire study. *Pathophysiology, 20*(2), 117–122.

Han, Y., Gandhi, O. P., DeSalles, A., Herberman, R. B., Davis, D. L. (2010). Comparative assessment of models of electromagnetic absorption of the head for children and adults indicates the need for policy changes. *European Journal of Oncology, 5*, 103.

Hansson, B., Thors, B., & Törnevik, C. (2011). Analysis of the effect of mobile phone base station antenna loading on localized SAR and its consequences for measurements. *Bioelectromagnetics, 32*(8), 664–672.

Hardell, L., Carlberg, M., & Hansson Mild, K. (2005). Case-control study on cellular and cordless telephones and the risk for acoustic neuroma or meningioma in patients diagnosed 2000–2003. *Neuroepidemiology, 25*(3), 120–128.

Hardell, L., Carlberg, M., & Hansson Mild, K. (2013). Use of mobile phones and cordless phones is associated with increased risk for glioma and acoustic neuroma. *Pathophysiology, 20*(2), 85–110.

Hayes, K., & Burge, R. (2003). *Coltan mining in the Democratic Republic of Congo: How tantalum-using industries can commit to the reconstruction of the DRC*. Cambridge: Fauna & Flora International, NHBS.

Heaven v. Pender. (1883). Trading as West India Graving Dock Company, 11 QBD 503, Court of Appeal, United Kingdom.

House of Representatives. (1993a). Children's electromagnetic field risk reduction Act, 1st Session, 103rd Congress, H.R. 1494, The Library of Congress. Retrieved March 13, 2016, from https://www.loc.gov (home page).

House of Representatives. (1993b). Electromagnetic Labeling Act, 103rd Congress, 1st Session, H.R. 1665, The Library of Congress. Retrieved March 13, 2016, from https://www.loc.gov (home page).

House of Representatives. (2012). Cell Phone Right to Know Act, 112th Congress, 2nd Session, H.R. 6358, Library of Congress. Retrieved March 13, 2016, from https://www.loc.gov (home page).

Hug, K., Roosli, M., & Rapp, R. (2006). Magnetic field exposure and neurodegenerative diseases—recent epidemiological studies. *Sozial und Praventivmedizin, 51*(4), 210–220.

Huss, Jean. (2011). Document 12608: The potential dangers of electromagnetic fields and their effect on the environment. Committee on the Environment, Agriculture and Local and Regional Affairs, Council of Europe. Retrieved March 12, 2016, from http://www.coe.int (home page).

Institute of Electrical and Electronics Engineers. (1999). C95.1–1999 IEEE Standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz. Retrieved March 13, 2016, from https://www.ieee.org (home page).

Institute of Electrical and Electronics Engineers. (2005). C95.1–2005—IEEE standard for safety levels with respect to human exposure to radio frequency electromagnetic fields, 3 kHz to 300 GHz. Retrieved March 13, 2016, from https://www.ieee.org

International Agency for Research on Cancer. (2011). *IARC classifies radiofrequency electromagnetic fields as possibly carcinogenic to humans*. Lyon, France: World Health Organization. Press release No. 208.

International Commission on Non-Ionising Radiation Protection. (1998). Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). *Health Physics, 4*(4), 494–522.

International Commission on Non-Ionising Radiation Protection. (2009a). Exposure to high frequency electromagnetic fields, biological effects and health consequences (100 kHz–300 GHz). INCPR. Retrieved March 13, 2016, from http://www.icnirp.org (home page).

International Commission on Non-Ionising Radiation Protection. (2009b). Guidelines for limiting exposure to time-varying electric, magnetic, and electromagnetic fields (up to 300 GHz). *Health Physics, 97*(3), 11.

International Telecommunication Union. (2016). The world in 2015: ICT facts and figures. Retrieved March 5, 2016, from http://www.itu.int (home page).

de Jong, A., Wardekker, J. A., & van der Sluijs, J. P. (2012). Assumptions in quantitative analyses of health risks of overhead power lines. *Environmental Science & Policy, 16*(10), 114–121.

Kheifets, L., Ahlbom, A., Crespi, C. M., Draper, G., Hagihara, J., Lowenthal, R. M.,et al. (2010). Pooled analysis of recent studies on magnetic fields and childhood leukaemia. *British Journal of Cancer, 103*(7), 1128–1135.

Khurana, V. G., Hardell, L., Everaert, J., Bortkiewicz, A., Carlberg, M., Ahonen, M. (2010). Epidemiological evidence for a health risk from mobile phone base stations. *International Journal of Occupational and Environmental Health, 16*(3), 263–267.

Kluger, R. (1996). *Ashes to ashes: America's hundred-year cigarette war, the public health, and the unabashed triumph of Philip Morris.* New York: Vintage.

Knopf, A., & Glantz, S. (1996). *The cigarette papers.* Berkeley: University of California Press.

Kostoff, R. N., & Lau, C. G. Y. (2013). Combined biological and health effects of electromagnetic fields and other agents in the published literature. *Technological Forecasting and Social Change, 80*(7), 1331–1349.

La Vignera, S., Condorelli, R. A., Vicari, E., D'Agata, R., Calogero, A. E. (2012). Effects of the exposure to mobile phones on male reproduction: A review of the literature. *Journal of Andrology, 33*(3), 350–356.

Levis, A. G., Minicuci, N., Ricci, P., Gennaro, V., Garbisa, S. (2011). Mobile phones and head tumours. The discrepancies in cause-effect relationships in the epidemiological studies—How do they arise? *Environmental Health: A Global Access Science Source, 10*, 59.

Levitt, B., & Lai, H. (2010). Biological effects from exposure to electromagnetic radiation emitted by cell tower base stations and other antenna arrays. *Environmental Review, 18*(1), 369–395.

Li, D. K., Ferber, J. R., Odouli, R., Quesenberry, Jr C. P. (2012). A prospective study of in-utero exposure to magnetic fields and the risk of childhood obesity. *Nature Scientific Reports 2.* Article 540.

Loi no. 2015-136 du 9 février 2015 relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques (*Loi Abeille*), JORF no 0034 du 10 février 2015, page 2346, texte no 1.

Lowenthal, R. M., Tuck, D. M., & Bray, I. C. (2007). Residential exposure to electric power transmission lines and risk of lymphoproliferative and myeloproliferative disorders: A case-control study. *Internal Medicine Journal, 37*(9), 614–619.

Maussion, C. (2011, October 19). 4G: la suspension des antennes irrite Besson. *Liberation*.

Merhi, Z. O. (2012). Challenging cell phone impact on reproduction: A review. *Journal of Assisted Reproduction and Genetics, 29*(4), 293–297.

Mettler, S. (2010). Reconstituting the submerged state: The challenges of social policy reform in the Obama era. *Perspectives on Politics, 8*(3), 803–824.

Ministerio de Vivienda y Urbanismo Gobierno de Chile. (2012). Entra en vigencia ley que regula instalación de torres para antenas celulares con nuevas facultades para municipios y mayor protección de la salud. Retrieved October 30, 2013, from http://www.minvu.cl/opensite_det_20120611132909.aspx

Montague, D. (2002, Winter–Spring). Stolen goods: Coltan and conflict in the Democratic Republic of the Congo. *SAIS Review*, *22*(1), 103–118.

O'Connor, E. (2013, February 20). *Statement to European Commission stakeholder dialogue group.* Brussels: EM Radiation Research Trust, European Commission.

Otitoloju, A. A., Obe, I. A., Adewale, O. A., Otubanjo, O. A., Osunkalu, V. O. (2010). Preliminary study on the induction of sperm head abnormalities in mice, Mus musculus, exposed to radiofrequency radiations from global system for mobile communication base stations. *Bulletin of Environmental Contamination and Toxicology, 84*(1), 51–54.

Panagopoulos, D. J. (2011). Analyzing the health impacts of modern telecommunications microwaves. *Advances in Medicine and Biology, 17*, 1–54.

Panagopoulos, D. J., & Margaritis, L. H. (2010). The effect of exposure duration on the biological activity of mobile telephony radiation. *Mutation Research, 699*(1–2), 17–22.

Parliamentary Assembly. (2011). Resolution 1815: On the potential dangers of electromagnetic fields and their effect on the environment. Council of Europe. Retrieved March 12, 2016, from http://www.coe.int (home page).

Perry, S. (2015). *L'Illusion Pixel.* Paris: Lemieux Éditeur.

Perry, S., Roda, C., & Carlson, K. (2012). Submission to the United Nations committee on the rights of the child. In preparation for the general comment on the rights of the child and the business sector, Committee on the Rights of the Child. Retrieved March 19, 2013, from http://www2.ohchr.org/english/bodies/crc/callsubmissionsCRC_BusinessSector.htm

Peyman, Gabriel, C., Grant, E. H., Vermeeren, G., Martens, L. (2009). Variation of the dielectric properties of tissues with age: The effect on the values of SAR in children when exposed to walkie-talkie devices. *Physics in Medicine and Biology, 54*(2), 227–241.

Posner, E. (2014). *The twilight of human rights law*. Oxford: Oxford University Press.

Proctor, R. (2012). *Golden holocaust: Origins of the cigarette catastrophe and the case for abolition*. Berkeley: University of California Press.

Roda, C., & Perry, S. (2014). Mobile phone infrastructure regulation in Europe: Scientific challenges and human rights protection. *Environmental Science and Policy, 37*, 204–214.

Ruggie, J. (2011). United Nations guiding principles on business and human rights. Office of the High Commissioner for Human Rights. Retrieved March 10, 2016, from http://www.ohchr.org (home page).

Scientific Committee on Emerging and Newly Identified Health Risks. (2015). Potential health effects of exposure to electromagnetic fields. European Commission. Retrieved March 6, 2016, from http://ec.europa.eu (home page).

Shahbazi-Gahrouei, D., Karbalae, M., Moradi, H. A., Baradaran-Ghahfarokhi, M. (2014). Health effects of living near mobile phone base transceiver station (BTS) antennae: A report from Isfahan, Iran. *Electromagnetic Biology and Medicine, 33*(3), 206–201.

Smith, A. (2014). Westporters rally against cellphone tower proposed for residential area. Retrieved August 15, 2014, from http://westport.dailyvoice.com (home page).

Smith, E. F. (2010, Winter). Right to remedies and the inconvenience of *Forum Non Conveniens*: Opening U.S. courts to victims of corporate human rights abuses. *Columbia Journal of Law and Social Problems, 44*, 145.

Sommer, C., Stadtfeld, M., Murphy, G. J., Hochedlinger, K., Kotton, D. N,, Mostoslavsky, G. (2009). Induced pluripotent stem cell generation using a single lentiviral stem cell cassette. *Stem Cells, 27*(3), 543–549.

Stop Smart Meter. (2014). Some PG&E customs getting fees reversed as CPUC endlessly delays smart meter "Opt Out" decision. Retrieved August 15, 2014, from http://stopsmartmeters.org (home page).

Sudan, M., Kheifets,L., Arah, O., Olsen, J., Zeltzer, L. (2012). Prenatal and postnatal cell phone exposures and headaches in children. *The Open Pediatric Medicine Journal, 6*, 46–52.

Sunstein, C. (2005). *Laws of fear: Beyond the precautionary principle*. Cambridge: Cambridge University Press.

Thaler, R., & Sunstein, C. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. New Haven, CT: Yale University Press.

Tribunal des Conflits (14/05/2012) C3848, Publié au recueil Lebon, Legifrance.

Tversky, A., & Kahneman, D. (1981). The framing of decisions and the psychology of choice. *Science: New Series, 211*(4481), 453–458.

U.S. Food and Drug Administration. (2014). Children and cell phones. Retrieved February 20, 2016, from http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/HomeBusinessandEntertainment/CellPhones/ucm116331.htm

United Nations Commission on Human Rights. (2004). Norms on the responsibilities of transnational corporations and other business enterprises with respect to human rights, Panel Discussion, 60th Session.

United Nations Convention on the Rights of the Child. (1989). G.A. res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49, *entered into force* 2 September 1990.

Valentini, E., Curcio, G., Moroni, F., Ferrara, M., De Gennaro, L., Bertini, M. (2010). Systematic review and meta-analysis of psychomotor effects of mobile phone electromagnetic fields. *Occupational and Environmental Medicine, 67*(10), 708–716.

Vienna Convention on Road Traffic. (1968). United Nations Economic Commission for Europe. Retrieved March 6, 2016, from http://www.unece.org

Vienna Convention on the Law of Treaties. (1969). 1155 U.N.T.S. 331, U.S. No. 58 (1980), *reprinted in* I.L.M. 679 (1969), *entered into force*, 27 January 1980.

Ville de Paris. (2003). *Charte relative aux antennes relais de téléphonie mobile, Au sens de l'article 1 du décret n° 2002-775 du 3 mai 2002.*

Ville de Paris. (2012). *Charte relative à la téléphonie mobile, Au sens de l'article 1 du décret n° 2002-775 du 3 mai 2002.*

Wiart, J., Hadjem, A., Wong, M. F., Bloch, I. (2008). Analysis of RF exposure in the head tissues of children and adults. *Physics in Medicine and Biology, 53*(13), 3681–3695.

World Health Organization. (2012). Electromagnetic fields: Current standards. Retrieved March 12, 2016, from http://www.who.int (home page).

CHAPTER 3

User Privacy in a World of Digital Surveillance

The previous chapter explored the ways in which human rights law may be extended to the architecture and use of digital hardware, requiring states to protect vulnerable populations from the potentially harmful effects of electromagnetic radiation, as they would for any other type of pollution. The digital systems that comprise the Internet are a rapidly evolving combination of hardware and software that enables instantaneous communication, forming the cornerstone of the 'new economy'. These systems—the entities that capture, process or further disseminate information—generate reams of personal data that may be tracked by policing systems or sold to a third party without the user's knowledge. Moreover, governments and the private sector often cooperate to monitor or proscribe online content and user behaviour in the name of public interest or safety. Nonetheless, any action—public or private—explicitly directed at the unauthorized collection or distribution of personal data may violate an individual's right to privacy. Digital surveillance, like pollution, is carefully circumscribed in law and is subject to the recognition of privacy as a human right. In an age of Big Data, privacy enhancing technologies and privacy-by-design are a critical component in the delivery of technology that enhances democratic dialogue and facilitates human lifestyles, while reinforcing the premise of human rights. This chapter will (1) explain the technology necessary to track citizens for policing and commercial purposes, (2) examine the legal framework that protects user privacy, while still enabling the circulation of information that underpins modern social and economic structures and permits state surveillance in an emergency, and

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_3

(3) explore new ways of thinking about digital privacy that empower the user to have greater control over his or her personal data, thereby contributing to the reinforcement of democracy itself.

The Internet serves as a marketplace, library, entertainment venue and virtual platform for socio-political organization that defies description or regulation for the 3.2 billion annual users who connect via fixed or mobile broadband access (or both) worldwide.[1] At its inception, the Internet was intended to function as the ultimate public space, a computer-generated environment for communication and the sharing of information that was free and accessible to anyone with a telephone line and a modem.[2] Over time, however, public, corporate and even criminal actors have learned to control this virtual public arena. Two distinct systems have emerged: an open Internet space which is nominally free, but currently dominated by four US-owned technology companies that manage approximately 55 per cent of global user access and activity online;[3] and a closed Internet space theoretically sealed off from external content by filtering software, but often quite porous, as exemplified by the Great Firewall of China. As of this writing, neither system is entirely controlled, nor completely free.

The vast majority of personal activity on the Internet—from choosing a shade of lipstick to consulting the stock market—is unfettered by state regulation and ignored by government monitoring systems. Nonetheless, governments and the private sector often cooperate to monitor or proscribe online content and user behaviour in the name of public safety, at times overstepping fundamental human rights protections that guarantee individual freedom of thought, speech, and association. With the advent of terrorist attacks worldwide, many governments have pushed through legislation permitting online surveillance policies that may violate international treaty commitments and domestic law, particularly with respect to due process and legal consent. Electronic surveillance is a controversial form of data compilation because it is by nature virtual, leaving no physical trace to the untrained eye. Moreover, in certain cases judicial procedure for this type of surveillance is secretive (such as the warrants issued by the US Foreign Intelligence Surveillance Court[4]) or the procedure bypasses normal channels that ensure balance of power between the executive and judicial branches of government (such as actions by the French Ministry of the Interior during a declared state of emergency, as discussed in Chapter 4). Furthermore, electronic surveillance as currently practised by most states encroaches upon an individual's sacrosanct right to privacy, a fundamental right enshrined in article 17 of the International Covenant

on Civil and Political Rights. In many instances, electronic surveillance is a prelude to censorship. State censorship, which involves the suppression of proscribed content and eventual sanctions against the user, is the next step in the digital surveillance chain. Censorship may breach the individual's right to freedom of thought, expression and association—rights guaranteed under the same covenant, but which, like privacy, may be suspended 'to protect public safety, order, health, or morals or the fundamental rights and freedoms of others'.[5]

Because surveillance and censorship are usually sequential, but legally distinct, we have chosen to treat these issues in two separate chapters, thereby allowing for a more in-depth discussion of the ethical, political, and social ramifications of these practices. Consequently, this chapter will explore the indiscriminate collection of online personal data without individual or judicial consent, with the intention of using that information at a future point in time as possible evidence of illegal conduct or in aggregate form to predict future (criminal) behaviour or consumption patterns. Our next chapter will examine the challenges of online censorship for the state and the mistrust of citizens responding to a range of state censorship practices.

In this chapter, we analyse the complex task of large-scale data collection for a purpose—a process which involves the analysis of enormous combinations of data sets commonly referred to as 'Big Data'. Such 'predictive' profiling, whether by the state or the private sector, may constitute discrimination based on race, religion, social class, or other factors. This chapter makes an important distinction between data collected for security versus commercial purposes. Commercial tracking, the aggregation of huge sets of personal data with the aim of targeting individual consumers or exploring larger patterns of buyer behaviour, is insufficiently regulated in most national jurisdictions, exposing the citizen to interference that ranges from the annoying advertisement that pops up on the corner of a screen to the unwanted divulgation of personal information that could adversely affect employment or access to health services. Because personal data increases in value once aggregated, the user's privacy is doubly exposed: first, the user cannot engage in any online activity or social networking platform without divulging personal information (we assume that many social networking services are now available exclusively online and that social networking provides clear economic benefits that can influence corporate hiring and salary decisions); and second, the more personal exposure the user provides through a regular online presence, the more

valuable his or her personal data becomes. Such heightened exposure allows users to benefit from algorithmic price reductions or digitized price comparisons, but also locks the user into a business model based on the sale of the customer's personal information.

This chapter will examine privacy as a core legal and social value in democratic societies, solidly embedded in international treaty law, national constitutions and the legislation of post-industrialised states. State or corporate surveillance of users online, like any form of surveillance, is subject to the law in place, meaning that neither the information technology (IT) sector, nor the government are above the law. Both are obliged to protect user privacy in a digital environment. In the previous chapter, we explored the ways in which human rights law may be extended to the architecture and use of digital hardware, requiring states to protect vulnerable populations from the potentially harmful effects of electromagnetic radiation, as they would for any other type of pollution. Surveillance, like pollution, is carefully circumscribed by law and is subject to the recognition of online privacy as a human right. Several new legal opinions, discussed below, shed light on the subordinate place of digital tracking and surveillance systems within the human rights treaty framework; these cases confirm that binding human rights treaty law privileges the use of technology to empower individuals, rather than subject these same citizens to surveillance, manipulation or commercialisation of their personal data. Nevertheless, any privacy framework viewed exclusively through a legal lens will fall short of the desired goal to prevent widespread misuse of personal data. This chapter will (1) explain the technology necessary to track citizens for policing and commercial purposes, (2) examine the legal framework that protects user privacy, while permitting state surveillance in an emergency, and (3) explore new ways of thinking about digital privacy, such as privacy-by-design, that empower the user to have greater control over his or her personal data. We conclude our chapter with thoughts on the reinforcement of democracy through a more general concern for the value of our collective digital privacy.

3.1 Privacy Threats in Digital Systems

National and regional legal frameworks for the protection of privacy have struggled to keep pace with the breakneck rhythm of development in the technology sector. The use of digital systems may engender a number of privacy threats due to a variety of causes. Rachel Finn and her colleagues identify seven 'types' of privacy that we find useful for understand-

ing the range of privacy threats in a digital environment.[6] First, *privacy of the person* addresses the right to keep the body, its functions and its characteristics private, a right that is increasingly compromised by technologies such as whole body imaging scans (in airports, for example), whole gene sequencing and biometric measurements. Forthcoming nanotechnologies are likely to pose an even greater risk for this type of privacy.[7] Foreseeable developments of nanotechnology include, for example, microchip implants into humans which, if capable of transmitting or storing information, could lead to a brand new level of privacy infringements. Second, *privacy of behaviour and action* includes habits, political activities and religious practices, conduct that could be compromised by technologies that enable location and social network tracking, or by closed-circuit television and travel documents that are RFID-enabled (radio frequency identification). Third, *privacy of communication* is a right recognized by many national jurisdictions, but one that is endangered by telephone or wireless communication interception, discussed below, and by directional microphones. Fourth, *privacy of data and image,* may be jeopardized by gigapixel images, infrared cameras, closed-circuit television, and a range of similar devices. Fifth, *privacy of thoughts and feelings*, a loss of privacy that had only been possible in science fiction, is increasingly compromised by recent developments in EEG (electrophysiological monitoring to record electrical activity of the brain) and eye tracking technologies, together with a host of other physiological measurement tools and techniques.[8] Sixth, *privacy of location and space* refers to the right of an individual to access public or semi-public areas without being identified or monitored; this type of monitoring has become especially common in an effort to track criminality or terrorism in urban areas. Finally, *privacy of association* (including group privacy) is compromised by technologies such as crowd analysis, which uses algorithmic monitoring to conduct real-time assessment of crowd dynamics to inform urban policing.

Several recognized engineering bodies have addressed the issue of privacy, including the information security management section of the International Standard Organization,[9] the Internet Engineering Task Force (IETF),[10] the OASIS consortium,[11] and the Internet Privacy Engineering Network,[12] among others. Privacy threats primarily derive from poor data management (such as data stored in a way that does not protect it from unauthorized access); human or system errors (when someone's data is attributed to somebody else); or actions explicitly directed at the unauthorized collection or distribution of personal data. This chapter

focuses on the latter threat. According to the terminology proposed by the IETF,[13] privacy threats of the latter type include surveillance, correlation, identification and secondary use, each of which is briefly described below.

Surveillance systems, even when they are *not* designed to collect identifiable information (as in the case of Web traffic analysis), may eventually result in future collection and analysis that enable user identification. One important issue surrounding surveillance is the collection of meta-data (specific information about our communications, such as the quantity of phone calls made by the user and the numbers called, or the totality of connections to a certain server at a specific time of day). Experts generally agree that collection of this information does not infringe on user privacy, because this information does not provide the *content* of communications and, in principle, does not allow the unique identification of a single user. The aggregation of meta-data, however, may be used to generate a user profile that includes details about where the user is (through localization of a mobile phone or access to the Internet); who the user talks to (phone numbers called or recipients of instant messages); the user's interests, shopping habits, and political or religious viewpoints (recorded by Web searches, items purchased through credit cards, or online locations visited); and user medical conditions (such as the number of a doctor called or support forums accessed online). The Electronic Frontier Foundation provides a set of spoofed examples to demonstrate just how revealing meta-data can be:

> They know you rang a phone sex line at 2:24 am and spoke for 18 minutes. But they don't know what you talked about…They know you called the suicide prevention hotline from the Golden Gate Bridge. But the topic of the call remains a secret…They know you received an email from a digital rights activist group with the subject line "52 hours left to stop SOPA" and then called your elected representative immediately after. But the content of those communications remains safe from government intrusion.[14]

The collection and analysis of meta-data is relatively simple, leading governments and private companies to collect it broadly. Surprisingly, while much media attention has been devoted to meta-data collection by governments (in particular following the revelations of whistle-blower Edward Snowden), much less outcry has occurred over data collection by large Internet or telecom companies. These businesses not only gain considerable economic advantage by selling personal data to advertisers,

but also appear to benefit from significant political and decision-making power thanks to their ability to influence and, in certain situations, control user behaviour.

Correlation uses the multiple pieces of information about an individual garnered through surveillance to generate further information. For example, an observer may infer that the user is interested in SOPA (the Stop Online Piracy Act[15]) by relating two pieces of information, one about an email received and another concerning a phone call made to an elected representative. While collecting a large spectrum of meta-data from any one citizen's email and telephone communications would, in general, be very difficult for a private company or state, Big Data analytics make this task relatively easy. Big Data techniques are designed to identify correlations and analyse large volumes of data that may be structurally heterogeneous (such as text, voice, sound, or images) and may change quickly over time.[16] Big Data can also narrow down uncertainty; for example, after analysing the email exchanges and phone calls described above, Big Data analytics may derive that the user is likely to be 90 per cent interested in SOPA, and then use this probabilistic information to make further inferences about the same user.

Identification, strictly related to correlation, is the association of information with a particular user to infer his or her identity. In certain situations, this is both explicit and justified; for instance, identification is requested when a user wants to access the private pages on his or her company's intranet or when purchasing items online. In other cases, identification may be explicitly required by a server, but its justification may be dubious. Certain online services, for example, require personal, identifiable information when the transaction could be provided by requesting a pseudonym. Finally, and more problematically, identification may be neither explicit, nor justified. Some Web services do not overtly require identification, but ask their users to 'connect' to their social networks; because the latter identifies the user, the user's identity is then made available to the website operator. Further, many institutions choose to use cloud-based hosting services, which means that personal data leaves a local machine and becomes available for scrutiny by third parties.

The term 'secondary use' describes those situations in which information collected about an individual is used without his or her consent, for purposes other than those for which it was collected. Although most users click on the 'agree' button of 'Terms and Conditions' policies, few actually read the associated privacy statements. According to an Internet Society survey,

more than 80 per cent of users typically do not peruse a site's privacy policy before clicking on the 'agree' button.[17] Typically, online services make some secondary use of the information they collect. Such handling may include the recommendation of other services or advertising, and may also entail the release of user information to third parties. 'Disclosure' refers to those situations in which the information released about an individual may affect how others judge that individual; 'exclusion' describes those circumstances in which customers are unaware of the collection or distribution of their personal data, a situation which clearly violates user privacy.

Different mechanisms are used to collect meta-data and content data. When a user wants to access a Web page, for example, the Web browser sends requests and receives responses that are organized into two parts, generally called the 'header' and 'body'. Headers contain meta-data, such as who sent the request or response and when, and who should receive the message. They use standard formats, which means they may be easily inspected by any third party that wants to collect information about the communication. Information collected in this way may provide the domain name of the information being requested (such as 'http://www.aup.edu'), as well as the specific page being requested (such as 'Faculty'). A second mechanism, deep packet inspection (DPI), is used to access the body (content) section of the communication. DPI may be used for reasons that have nothing to do with collecting users' information. Examples include routine checks to assure that communication is virus free or the prioritization of certain traffic.[18] When used to collect information about a user, this second mechanism allows retrieval of the complete content of a message, such as the text of an email, the content of a YouTube video, or the details of a Skype conversation. On most occasions, however, inspection is limited to searching for certain keywords or patterns. The analysis of data in DPI is computationally heavy; therefore, in order to maintain quality of service (or to remain undetected), DPI normally relies on creating copies of the packets that are to be inspected, while the original packets are routed normally. Both the inspection of headers and body can be made much more difficult through encryption mechanisms; the https protocol, for example, relies on header encryption.

While the techniques described thus far (as well as those that gather information at different layers of the communication, such as Internet Protocol identification) collect information by eavesdropping on communications, other data may be gathered through applications, such as social networks and search engines. These applications may collect information

that is directly provided by the user: the name of a friend or connection in a social network, the keywords for a search, or the meta-data associated with pictures uploaded online. Finally, new technologies engender an increase in the user's loss of perception of the data being collected. Smart meters collect private information about our household habits, high resolution (gigapixel) cameras render individuals perfectly identifiable in pictures of large crowds, and mobile phones provide a stream of continuous data concerning our location. In sum, online data collection, whether it proceeds with or without the user's permission or knowledge, is ubiquitous.

3.2 The Legal Framework for Privacy

Privacy is a relative latecomer to the pantheon of civil and political rights enshrined in the International Covenant on Civil and Political Rights (ICCPR). Warren and Brandeis' seminal article of 1890 treated privacy as a critical right, related to the full protection of person and property.[19] As the age of photography weakened control over the individual's personal image, the protection of intangible property and the right to prevent publication required legal protection that extended beyond intellectual property protection and protection from libel or slander.[20] The 'right to be left alone' was thus linked from its inception with the right to prevent publication, an important factor when we consider the development of privacy-by-design as it relates to digital technology. The Universal Declaration of Human Rights, promulgated by the United Nations (UN) General Assembly in 1948, includes specific privacy protections in article 12, taking up the ideas first expressed by Warren and Brandeis on the special protection of an individual's 'honour and reputation'.[21] Article 17 of the ICCPR renders privacy protection legally binding in international law. General Comment 16, drafted by the UN Committee on Human Rights, focuses on the obligation of states to use legislative tools to protect their citizens' privacy: 'this right is required to be guaranteed against all…interferences and attacks whether they emanate from State authorities or from natural or legal persons'.[22] Although the General Comment was promulgated in 1988, before the advent of the digital revolution, clearly the term 'legal persons' is intended to mean business and consequently obliges states to guarantee the protection of user data by technology companies under their jurisdiction. More recently, the UN High Commissioner for Human Rights issued a report that concludes:

> International human rights law provides a clear and universal framework for the promotion and protection of the right to privacy, including in the context of domestic and extraterritorial surveillance, the interception of digital communications and the collection of personal data.[23]

On a national and regional level, the Fourth Amendment of the US Constitution and articles 7 and 8 of the Charter of Fundamental Rights of the European Union (EU) rigorously uphold the value of privacy. As of this writing, five important judgements or opinions have recognized state or business obligations to protect user privacy. In May 2015, a three-judge panel of the 2nd Circuit US Court of Appeals determined that the dragnet collection of US telephone call data did not constitute information relevant to terrorism investigations under section 215 of the Patriot Act, stating that the programme 'exceeds the scope of what Congress has authorized'.[24] The Second Circuit judges did not, however, move beyond statutory law in their decision, leaving a further discussion of the constitutional merits of the Fourth Amendment and protection from 'unreasonable searches' to future case law.

The European Court of Justice (ECJ) issued an advisory opinion in April 2014 declaring that the European Data Retention Directive of 2006 'interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data'.[25] In May of the same year, the court determined in *Google v. Costeja González*:

> As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the (online) information in question no longer be made available to the general public…those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name.[26]

In October 2015, the ECJ also rendered null and void the 'safe harbour' agreement between US servers and the European Commission, an agreement governing the treatment of European citizens' data by US social media companies. The so-called safe harbour framework, which applies to some 4000 US companies, offered these businesses immunity from the enforcement of stricter European privacy laws as long as they made a voluntary commitment to protect personal data to European standards. In July 2016, the US Department of Commerce announced a new agreement with the European Union called the EU-US Privacy Shield Framework.

Once a US company voluntary requests certification under the framework, the stricter EU privacy clauses will become enforceable under US law.

A complaint brought by Maximillian Schrems, in response to Edward Snowden's revelations that Facebook had cooperated with the US government's PRISM surveillance programme, argued that the social media giant was not adequately protecting the data of its European customers. In *Maximillian Schrems v. Data Protection Commissioner*, the ECJ found that:

> Legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life.[27]

Moreover, the court observed that:

> Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, compromises the essence of the fundamental right to effective judicial protection…[28]

Although our sample is limited to a handful of cases, we note that jurisprudence in the USA and, more specifically, in Europe is evolving towards a reinforcement of online user rights that places the burden of privacy compliance on search engine operators and governments.

As the burden shifts, technology companies are also moving to protect their clients from what they consider to be unwarranted government interference. Following the stand-off between Apple and the US Department of Justice over encrypted mobile phone data,[29] US technology companies became more forthright in their determination to protect user privacy from extensive government intrusion. The Snowden revelations alerted consumers to the fact that large technology companies initially cooperated with mass government surveillance and, in the case of China, censorship policies—cooperation which created a marked sense of unease amongst customers. A 2013 Pew survey indicated rising levels of mistrust concerning data protection; according to the survey, '86% of internet users have taken steps online to remove or mask their digital footprints—ranging from clearing cookies to encrypting their email'.[30] A 2015 Eurobarometer survey of 28,000 users across Europe revealed equally significant levels of mistrust concerning data protection; according to the survey, 81 per cent of

Internet users believed that they have little or no control over their online information, while 63 per cent said they do not trust online businesses.[31] In a likely effort to increase consumer confidence, Microsoft Corporation filed a suit against the US Department of Justice in April 2016, challenging the government's authority to bar the company from telling their customers when their data was being examined by federal agents.[32] Microsoft pointed to the fact that an individual knows when a judge issues a warrant to search his or her home or hard drive, but is banned from knowing when personal data stored in the cloud is searched. The company noted that nearly half of the 5624 demands for customer information from the federal government over the 18 month period preceding the filing were delivered with a gagging order, preventing Microsoft from telling clients that their data was being searched.[33]

When privacy is linked to private property, the issue of digital surveillance assumes even greater significance. The right to private property is far older than the right to privacy, and raises a key legal question relevant to our understanding of digital surveillance, namely who is the owner of our online personal data. Before exploring competing interpretations of data ownership, a very brief overview of the notion of private property may be helpful. According to Magna Carta, the cornerstone of English civil and political rights that a group of truculent barons forced King John to sign in 1215, the king's agents were required to respect the inviolability of the barons' private property. The first Declaration of the Rights of Man, drafted in 1789 at the outset of the French Revolution, declared private property sacred, inviolable, and subject to seizure only if public necessity warranted it and only with full indemnities according to its just value.[34] The Fifth Amendment to the US Constitution also includes a 'just compensation' clause for private property. By 1948, the UDHR proclaimed that '[e]veryone has the right to own property alone as well as in association with others' and that 'no one shall be arbitrarily deprived of his property'.[35] While the right to property is absent from binding international treaty law, primarily due to insurmountable ideological differences between the Eastern and Western blocks during the drafting process of the two international covenants,[36] it is referred to indirectly in the non-discrimination clauses and in several of the subsequent treaties. Finally, the right to private property is assured indirectly in various other clauses of the US Constitution and directly in article 1 of the First Protocol to the European Convention on Human Rights which guarantees that:

> Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by the law and by the general principles of international law.[37]

Thus, personal data would benefit from a long history of legal protection if online information belonged to the individual who produced it, rather than the server that processed or stored it.

The jury is still out, so to speak, on who owns our personal data.[38] We argue that, although law and jurisprudence reinforce the right to privacy in a robust fashion, the reluctance to determine who owns online personal data is an omission that weakens privacy protections. While the USA has promulgated particularly rigorous intellectual privacy law and certain EU states, such as France, have very strict privacy regulations,[39] it is German jurisprudence which has come closest to determining that property rights accrue to the individual who produces the data, the person at the origin of the information.[40] Nevertheless, the EU appears to be less certain. Under the auspices of the 2017 General Data Protection Regulation, the focus is on 'effective control' over online data, rather than individual ownership—privacy, rather than private property. Key reforms to the 1995 EU Data Protection Directive include (1) the right for the individual user to be forgotten or 'delisted' from a search engine, (2) explicit, informed user consent for all data processing, (3) the right to carry and transfer personal data to another server, (4) the right to be informed by the server of a data breach within 24 hours, and (5) the strengthening of national data protection authorities and one set of data protection rules across the EU. What is most interesting is the different approach taken by the USA in terms of data ownership, one that focuses on the concept of legal consent, rather than privacy.

The extension of legal consent to the use of personal data (Tweets or Instagram photos, for example) by a third party is problematic. The question of legal consent has its roots in seventeenth century England, when John Locke formulated the novel idea of a state built upon the model of free and equal citizens who actually had to consent to be governed. Informed consent has developed over time to constitute a cornerstone of common and civil law systems, and is pertinent to a host of disciplines ranging from informed consent for medical trials to consent for use of online personal data. Legal consent means that the individual should agree to do something or agree to allow something to happen only after all the

relevant facts are known. Theoretically, this notion poses a challenge for the digital environment in that 'all the relevant facts' are rarely known, either by the server or by the user. Consequently, an understanding of what constitutes legal consent for the use of online personal data in the USA has yet to be conclusively defined by the courts.[41] We argue that digital security for citizens is best served by a tripartite strategy: rigourous privacy protection for all users, reinforced by a clear framework for legal consent, with ownership of all digitally produced personal information claimed by the individual who generated the data.

3.3 Privacy-by-Design

In our work with IT researchers and engineers for project PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research, sponsored by the European Commission), we have noted that the engineer who creates a new digital product in an IT laboratory (or garage, according to the start-up myth engendered by Apple) feels far removed from the court decisions and legal implications of the product's use. Moreover, the notion of privacy is initially of little concern to an enthusiastic public ready to purchase the latest product on the market. Instead, the value of privacy appears to have diminished with the current pursuit of visibility on social networks and the emergence of digital tools that facilitate self-exposure of the user's private life; in this world, all that matters is grabbing the attention of other users, creating a buzz, remaining visible.[42] The value of privacy is temporarily lost in the thrill of a self-generated digital presence; the ease and rapidity of information transfer, the unremitting focus on the number of viewers reached, as well as the ability to narrate one's own existence at any time, create a heady cocktail of virtual control.

Privacy is inherently problematic to define as people often differ in their evaluation of how private certain information is in a given context. It is clear, however, that more data is being collected, stored, and processed thanks to the decreasing cost of these operations and the increasing value of the information gathered—a value that is social, cultural, and political, as well as financial. Furthermore, less privacy means more surveillance. And information that is collected for alleged security reasons may be misused, either willingly (by criminals, for example) or in error. In our research, we have found that technology users often tell us: 'I do not need to protect my privacy, because I have

nothing to hide'. This statement obviously does not take into account that seemingly innocuous information (i.e., information that normally should not be hidden) may be manipulated, stolen or used in a discriminatory manner in the case of digital profiling based on gender, age, or nationality, for example. A second type of justification—'I don't need extra protection, because I know how to protect my privacy'—often leads to privacy breaches caused by user ignorance about the data that devices and applications reveal, or behavioural biases leading to unwanted disclosure.[43] A third type of response—'I need to use this tool, so I am willing to give up my privacy'—is surrender to the status quo and often reflects a lack of awareness concerning user rights. The impact of the Snowden revelations, however, along with a rich trove of user anecdotes concerning online privacy violations, have led users to demand greater control over their online data in their headlong pursuit of digital exposure.

Privacy-by-design offers a technical response to the contradiction inherent in the hurried pursuit of online exposure versus rising levels of public mistrust regarding the eventual use of online data. As participants in project PRIPARE, we worked with an eleven partner consortium to facilitate the application of privacy- and security-by-design methodologies to protect against Internet disruptions, censorship, and surveillance and to foster a risk management culture through educational material targeted to a diversity of stakeholders.[44] Privacy-by-design, or the integration of user data protection mechanisms from the very outset of any digital design initiative, remains one of the surest means to protect the user's digital footprint and prevent access to personal data without the user's express, and informed permission.

Claudia Diaz and Seda Gurses identify three frameworks for privacy protection that are of interest for this chapter: privacy-as-control, privacy-as-confidentiality, and privacy-as-practice.[45] Privacy-as-control describes the ability of individuals to control which personal information is disclosed and processed, for example through privacy settings. Within this framework, organizations must have the means to enforce the privacy policies selected by users, thereby preventing the abuse of personal information. This framework, which most users are familiar with, requires that individuals trust the organization that holds the data to be both willing and capable of implementing a system for appropriate data usage. Furthermore, privacy 'control' in this instance may be limited to an expression of customer wishes with respect to the use made of their information because, once the

data is with the organization, it is almost impossible for the user to verify how the data is actually employed. Privacy-as-confidentiality, inspired by the definition of privacy as Warren and Brandeis' 'right to be let alone' mentioned above, aims to prevent intrusions into an individual's private sphere. Privacy enhancing technologies (PETs) that preserve the user's anonymity—such as anonymous authentication protocols,[46] anonymous communication networks,[47] or private information retrieval[48]—are all examples of privacy-as-confidentiality. Each of these techniques achieves privacy without having to trust a data holding organization to appropriately preserve users' data; privacy is thus assured by preventing disclosure. The privacy-as-practice framework aims at implementing awareness techniques to inform users continuously as to how information is collected, processed, analysed, and communicated.[49]

Tools such as a privacy impact assessment, a rigorous, rights-based evaluation of the impact of any software or IT system during the planning phase,[50] as well as private information retrieval, selective disclosure credentials, or secure multi-party computation,[51] form an integral part of any privacy-by-design methodology. The key to all data minimization strategies is that data should not be collected in the first place if it is not necessary for the functioning of the system. By ensuring that no unnecessary data is collected, the possible privacy impact is limited.[52] In straightforward cases, for example, a user may provide 'flagged' information, such as 'over-18' without necessarily providing a date of birth. Capability certificates, with electronic signatures issued from legitimate authorities or trusted third parties, might be one way of guaranteeing the veracity of flagged information. Certain scholars have suggested identity management architecture as a compromise measure. This primarily consists of identity-masking technology that enables users to provide information without compromising privacy. If a true name, birthdate and financial information are required for the digital transaction, Michael Froomkin has suggested a 'full-scale identity escrow schema' with encrypted data that would anonymize personal data, while allowing law enforcement officials, for instance, to access the true identity of the user.[53] Certain scholars have even suggested that executive compensation in technology or social networking firms should be linked to user surveys indicating satisfaction, or lack thereof, with the company's data management practices.[54] While a policy compelling social networking firms to internalize privacy risks is certainly necessary, we do not think that this will be enough.

Experts also warn that data minimization processes are misleading. Carmela Troncoso and colleagues suggest that privacy-by-design methodologies have become 'the holy grail' for organizations that collect and process personal data, enabling them to reduce privacy engineering to 'check-lists and pre-defined processes'.[55] In a privacy enhanced system 'sensitive data only resides in components of the system under the control of the user', meaning that the data is either kept on a device under user control, is encrypted by the user, or is distributed across several entities where the user is the only one who can recompile the data. As an example, we might consider the system that allows a driver to automatically pay a highway toll. This process is normally based on two communicating devices: one in-car device physically owned by the user, and a second device at the toll station. The toll payment system can be designed in at least two ways. In the first case, the in-car device transmits information about the car and its entry point on the highway to the toll station device, the toll station device calculates the amount due and the user is charged the appropriate amount. In the second case, the toll station device transmits its location to the in-car device (and possibly some information about current fees) that calculates the amount due and charges the user. It is clear that the latter type of design is better suited for protecting the user because sensitive information, such as the user's location, does not leave the data system of the in-car device. Troncoso and colleagues note, however, the following caveat:

> In a system with a privacy-preserving design, the flow of sensitive data to a centralized entity (the service provider) is indeed "minimal", yet all the privacy-sensitive user data is captured and still stored on devices within the boundaries of the system.[56]

Because the sensitive data still resides somewhere in the system, a technical approach alone is insufficient to protect individual privacy online. As discussed below, we must link 'the future of privacy with the future of democracy in a way that refuses to reduce privacy either to markets or to laws'.[57] Technology, law and ethics must work in consort to provide adequate user protection.

3.4 Digital Privacy as a Collective Value

French philosopher Michel Foucault insisted that 'power should be visible' in a democracy.[58] Systematic and subtle digital surveillance undermines this essential principle, disrupting the balance of power between citizen and state, consumer and corporation. We join proponents of privacy in maintaining that power should be visible in order to permit the practice of informed citizenship.

Richard Posner has argued that privacy is merely an overrated construct in a digital society,[59] while sociologist Richard Harper has suggested that our trust in technology will be an evolving paradigm.[60] Others claim that enhanced digital privacy protection leads to a decrease in competitiveness in the global marketplace and a decline in consumer welfare, because privacy limits the free flow of information.[61] In *Code and Other Laws of Cyberspace*, first published in 1999, Lawrence Lessig suggested the use of an 'electronic butler' that could negotiate user privacy with websites:

> The user sets her preferences once—specifies how she would negotiate privacy and what she is willing to give up—and from that moment on, when she enters a site, the site and her machine negotiate. Only if the machines can agree will the site be able to obtain her personal data.[62]

While we find this idea intriguing, it is a concept that could quickly go awry; as discussed in the following chapters, it is not clear who controls the machines in question.

Our survey results with student populations, discussed in Chapter 4, indicate that most individuals have a very clear, unchanging notion of what constitutes personal privacy. Helen Nissenbaum's theory of privacy proposes that contextual integrity is at the core of what we consider privacy violations.[63] Nissenbaum's focus on the context indicates that our notions of trust are unlikely to adapt to digital technology; it is technology that must adapt to human perceptions of trust. David Wright recommends a process of impact assessment that integrates privacy and other human rights concerns into the very design of the hardware and software systems that constitute digital technology.[64]

In the coming years, users may demand that digital systems provide privacy-by-design insurance, built in systems of protection that place digital technology within contextual parameters that value privacy. User trust requires guarantees against privacy violations, such as the wholescale spying

and data commercialization policies that have become an integral part of the IT sector—policies that resemble a gigantic bank heist. A bank client knows that his or her money may be stolen or lost in a run on the bank; nonetheless, obligatory federal or national banking insurance minimizes this type of risk for the customer. Technology users are certainly aware that their privacy may be violated, but they should demand a certain level of protection against data theft and retain the right to remove their data, render it anonymous, or go off-grid altogether. By assessing the security of systems before they are built and by providing a selection of privacy-enhancing tools to the user before he or she enters a data collection system, privacy-by-design functions much like insurance in the banking sector. Simple, straightforward, obligatory protections embedded at the design stage of all digital products and systems may function as a form of insurance, returning a certain level of control—and possibly trust—to the user.

Unmitigated enthusiasm for digital technology is the current norm, an orthodoxy shaped in part by the IT industry through a strategy of sleek, easy-to-use products and seductive marketing campaigns, and in part by a beleaguered public sector eager for quick, cost-saving solutions to pressing social problems. Yet, as French philosopher Edgar Morin reminds us, enthusiasm is not 'normal' for any society.[65] It is a significant social marker that indicates a strong desire for the illusion of control, demonstrating the public's willingness in this case to view technology as a substitute for other values and concepts that appear outdated in our world in transition. Such enthusiasm is at best temporary, since the sense of control engendered by digital technology is illusory.

Privacy scholars also note the trade-offs between privacy as a right and privacy as a technical endeavour: the accuracy, certainty, and correctness of data may vary according to the level of privacy protection offered by a digital system.[66] If users hope to dispense with unnecessary surveillance, correlation, identification, and secondary use of their data in order to protect their right to privacy, to what extent will they be willing to forgo data precision? While privacy engineers oversee the integration of data minimization strategies into the design of digital systems, users should also be made aware that they are responsible for enhancing their own privacy protection. In the graphic below, we build upon the work by Troncoso and her colleagues to create a virtuous circle, encouraging users to think about the functioning of their data throughout a design system. All users should be urged to (1) limit the capture and storage of their personal data,

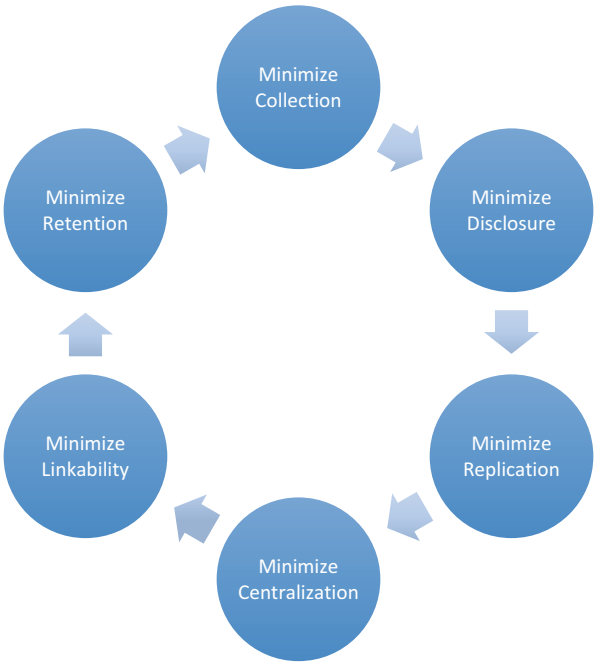

Fig. 3.1 Data minimization strategies for the user

(2) constrain the flow of information to no more than one or two parties within the system, (3) limit the number of entities which store and process their data, (4) avoid centralization of personal data (Google is unrepentant in this respect), (5) limit the possibility for inferences that could occur when linking data, and finally, (6) minimize the retention of personal data within any system (Fig. 3.1).

The aggregation of large sets of personal data is made possible by the 'just collect everything' strategy, which in turn feeds the burgeoning Big Data economy. Rather than view privacy engineering as an impediment to the Big Data economy, it would behove us to return to our comparison with the automobile introduced in Chapter 2. User safety is sold at a premium in the automobile sector and is an essential component in the marketing strategy of any automobile company. But, this was not always the case. Auto manufacturers resisted seatbelts for years, convinced that the consumer did not want the inconvenience of buckling up. Decades

of needless road deaths spurred consumer activism, public information campaigns and strict legislation to pave the way for improved automobile safety. Privacy-by-design should function like a seatbelt within the digital system; the consumer should know about it, demand it and use it within a proactive legislative framework that protects the citizen's security and long-term safety within the system.

In order for privacy engineering to be successful, all parties must be able to check that others have acted responsibly within the system. This is perhaps the greatest challenge, since current digital systems focus on the speed, precision or security of data transmission and storage, rather than on collective human rights. In the long term, individual privacy is of less importance than concern for general privacy in digital systems. French philosopher Marcel Gauchet has suggested that democracies risk falling victim to their own success. Because modern democracies have instituted 'a legal regime of rights that allow citizens to pursue their own private interests without any reference to what's good for the public, they stand to exhaust the very resources that have allowed them to flourish'.[67] Privacy is one such resource.

A user privacy matrix that combines knowledge of law, technology, and ethics is one way to approach the preservation of privacy as a resource necessary to the functioning of democracy. As Evgeny Mozorov has pointed out, neither too little privacy, nor too much privacy is good for democratic societies. Too little, and democratic debate is stifled; too much and society would be deprived of information needed to evaluate policies and form opinions.[68] If we view privacy as a collective, rather than an individual value, then our online behaviour may indeed shift towards a more balanced continuum. Building the new economy on data sharing schemes, while certainly beneficial for certain economic actors, is likely to reinforce existing inequalities. Mozorov proposes that by refusing to track our own caloric intake or heart rate, we may not only prevent a server from making money on the sale of our personal data to an insurance company, we may also prevent insurance rates from going up for those who do not track or who have health problems that are revealed through data surveillance, correlation, identification, and secondary use. By politicizing privacy, citizens can engage in information boycotts to protect vulnerable populations from Big Data:

> Privacy can then re-emerge as a political instrument for keeping the spirit of democracy alive: we want private spaces because we still believe in our ability

> to reflect on what ails the world and find a way to fix it, and we'd rather not surrender this capacity to algorithms and feedback loops.[69]

The value of individual privacy is reinforced if we view the protection of online personal data as a collective endeavour, a means of enhancing democratic dialogue and facilitating human lifestyles, while reinforcing the premise of human rights for all.

In conclusion, the value of privacy and even democracy is enhanced if individual privacy is protected in the digital arena. We suggest that individual control of personal data is a seminal right that outweighs government or business security concerns in the vast majority of circumstances and we advocate for the incorporation of human rights protection into the design of the actual software itself through methods such as privacy-by-design.

Protecting privacy through the legal system has been and continues to be recognized as the main component of a privacy protection infrastructure in Europe. This approach has led to the EU General Data Protection Regulation, a ground-breaking piece of legislation focused on control (rather than ownership) of personal data that is unique to Europe, but has international ramifications. Reinforced data control is not yet the case in countries with a more liberal tradition, where the 'market self-regulation' argument is applied to privacy protection. This means that privacy can be used as a marketing tool and users will select the products that respect their desired level of privacy. The obvious weakness of this arrangement is not only the disproportionately powerful legal and technical means that data controllers have at their disposal when compared to users, but also the unrealistic expectation that users, no matter how technically and legally savvy, will have sufficient cognitive resources available to evaluate the privacy risks associated with the use of a given technology, in a given context. Even if we disregard the complexity and opacity of privacy statements currently available, it is highly unlikely that users will always be able to make effective choices about their own privacy risk and privacy protection. In short, in these circumstances the user stands alone. Legal systems will not be able to protect users' privacy in cases where users provide information voluntarily and give explicit consent to its processing or distribution.

We advocate a combination of law, technology, and ethics to politicize privacy and return it to the centre of debate on the choices we make, or would like to make, in a digital environment. By encouraging users to take responsibility for their digital behaviour and prevent surveillance without consent, we then render all forms of surveillance

the exception, rather than the rule. As indicated in the introduction to this chapter, state censorship is the next step in the digital surveillance chain, involving the suppression of proscribed content and eventual sanctions against the user, actions which may breach the individual's right to freedom of thought, expression and association. These rights are guaranteed in human rights law but, like privacy, may be suspended 'to protect public safety, order, health, or morals or the fundamental rights and freedoms of others'. In the next chapter, we examine the effectiveness of state censorship and the response of civil society organizations engaged in the protection of our civil and political rights.

Notes

1. International Telecommunication Union (2016) The World in 2015: ICT Facts and Figures, http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdfhttp://www.itu.int (home page), date accessed 5 March 2016.
2. Internet Society (2016) *Internet Society Mission Statement*, http://www.internetsociety.org/who-we-are/mission, date accessed 30 April 2016.
3. FaberNovel (2014) 'GAFAnomics: New Economy, New Rules', *LinkedIn Corporation*, http://fr.slideshare.net/faberNovel/gafanomics, date accessed 15 October 2015.
4. See Cohen, D., Wells, J.W. (2004) *American National Security and Civil Liberties in an Era of Terrorism* (New York City: Palgrave Macmillan).
5. United Nations General Assembly (1966) *International Covenant on Civil and Political Rights*, G.A. res. 2200A(XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316, 999 U.N.T.S. 171, arts. 18, 19, 21, 22.
6. Finn, R., Wright, D., Friedewald, M. (2013) 'Seven Types of Privacy' in Gutwirth, S., Poullet, Y. *et al.* (eds.) *European Data Protection: coming of age?* (Dordrecht: Springer).
7. Gutierrez, E. (2004) 'Privacy Implications of Nanotechnology', *Electronic Privacy Information Center*, https://epic.org (home page), date accessed 28 April 2016.
8. The Frunhofer Institute, for example, released the beta-version of an application that recognises four different facial expressions on the basis eye and faces tracking. Frunhofer Institute (2016) 'SHORE™—Object and Face Recognition', http://www.iis.fraunhofer.de (home page), date accessed 28 April 2016.
9. International Organisation for Standardisation (2016) 'ISO/IEC 27001—Information security management', *ISO*.

10. Internet Engineering Task Force (2016) *IETF*, https://www.ietf.org (home page), date accessed 10 April 2016.
11. Organisation for Advancing Open Standards for the Information Society (2016) 'Oasis Consortium', https://www.oasis-open.org (home page), date accessed 10 April, 2016.
12. Internet Privacy Engineering Network (2016) *IPEN Objectives*, https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/IPEN, date accessed 10 April 2016.
13. Internet Architecture Board (2013) 'Privacy Considerations for Internet Protocols', *Internet Engineering Task Force*, RFC 6973, July.
14. The Electronic Frontier Foundation (2016) 'Why Metadata Matters', *EFF*, https://ssd.eff.org/en/module/why-metadata-matters, date accessed 10 April 2016.
15. The Stop Online Piracy Act, a bill proposed by the US Congress in 2012 to crack down on copyright infringement by restricting access to sites that host or facilitate the trading of pirated content, was met with well organised resistance by online communities. Opponents in the IT industry believed that the bill's language permitted censorship and was rife with the potential for unintended consequences. Its passage was 'postponed'. House of Representatives (2011–2012) Stop Online Piracy Act, 112th Congress, 2nd Session, H.R. 3261.
16. Gandomi and Haider provide a brief description of big data concepts: Gandomi, A., Haider, M. (2015) 'Beyond the hype: Big data concepts, methods, and analytics', *International Journal of Information Management*, Vol. 35, No. 2, pp. 137–144.
17. Internet Society (2012) 'Global Internet User Survey 2012', *ISOC*.
18. The prioritisation of some traffic has been proposed (and implemented) by certain internet service providers with the objective of optimising bandwidth usage. Traffic prioritisation may also be associated, for example, with differential user charges. See the debate on net neutrality for more details on the economic and legal issues related to this type of uses of deep packet inspection: https://www.eff.org/issues/net-neutrality.
19. Warren, S. and Brandeis, L. (1890) 'The Right to Privacy', *Harvard Law Review*. Vol. IV, No. 5, p. 1.
20. Warren and Brandeis, (1890) 'The Right to Privacy', p. 2.
21. United Nations General Assembly (1948) *Universal Declaration of Human Rights*, G.A. res. 217 A (III), adopted by the U.N. Doc. A/810, art. 12.
22. Office of the High Commissioner for Human Rights (1988) 'CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation', adopted at the Thirty-second Session of the United Nations Human Rights Committee, 8 April, p. 1.

23. Report of the Office of the United Nations High Commissioner for Human Rights (2014) 'The Right to Privacy in the Digital Age', United Nations Human Rights Council Twenty-seventh session, A/HRC/27/37, 30 June, para 47.
24. *ACLU v. Clapper* 2014. This decision narrowed the 'reasonable expectation' doctrine under the 1979 US Supreme Court decision in *Smith v. Maryland*, which established that people do not have a 'reasonable expectation' of privacy for electronic meta-data held by third parties like a mobile phone provider. Obviously, the justices in the latter case could not have predicted either the digital revolution or the massive surveillance procedures put in place after 9/11.
25. Court of Justice of the European Union (2014) Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April.
26. Court of Justice of the European Union (2014) Judgment in Case C-131/12, *Google v. Costeja González*, 13 May, para. 97.
27. Court of Justice of the European Union (2015) Judgment in Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October, para. 94.
28. *Maximillian Schrems v. Data Protection Commissioner*, para. 95.
29. Gershman, J. (2016) 'Apple v. Justice Department: Politicians and Activists Take Sides on Encryption Order', Law Blog, *The Wall Street Journal*, 17 February.
30. Pew Research Internet Project (2013) 'Anonymity, Privacy and Security Online'. http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online-2, date accessed 10 April 2016.
31. European Commission (2015) *Data protection Eurobarometer Factsheet*, http://ec.europa.eu (home page), date accessed 15 October 2015.
32. US District Court, Western District of Washington at Seattle (2016) Complaint for Declaratory Judgment, *Microsoft v. U.S. Department of Justice*, DWT 29162898v13 0025936-002444, 14 April.
33. Greene, J., Barrett, D. (2016) 'Microsoft Sues US on Secret Searches', *The Wall Street Journal*, 15–17 April, pp. A1 and A6.
34. It should be noted that the French revolutionaries had great difficulty applying notions of just compensation to the Church and the royalists, for example. *Déclaration des droits de l'homme et du citoyen de 1789*, art. 17.
35. Universal Declaration of Human Rights, A.G. res. 217A (III), UN Doc A/810 à 71 (1948), art. 17.
36. These differences are evident in the *travaux préparatoires*. See UN Secretary-General Hammarskjold (1955) *Annotations on the text of the draft International Covenants on Human Rights*, UN Doc. A/2929, 1 July, para. 197, 202, 206.
37. Article 1, First Protocol to the European Convention on Human Rights.

38. See Boyle, J. (2008) *The Public Domain. Enclosing the Commons of the Mind* (New Haven: Yale University Press); Lessig, L. (2004) *Free Culture. How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity* (New York: Penguin); Vaidhyanathan, S. (2011) *Copyrights and Copywrongs: The Rise of Intellectual Property and How It Threatens Creativity* (New York: NYU Press).
39. See Loi no. 78-17 (1978) 'Relative à l'informatique, aux fichiers et aux libertés, JORF du 7 Janvier 1978', p. 227.
40. T. Hoeren (2014) 'Big Data and the Ownership in Data. Recent Developments in Europe', *European Intellectual Property Review*, Issue 12, pp. 751–754.
41. See Fitzgerald, B., et al. (2011) Country of Origin and Internet Publication: Applying the Berne Convention in the Digital Age. *Journal of Intellectual Property (NJIP) Maiden Edition*, pp. 38–73.
42. Commission nationale de l'informatique et des libertés (2012) 'Vie privée à l'horizon 2020: paroles d'experts', *Cahiers IP: innovation et prospective*, No. 1.
43. Acquisti, A. Grossklags, J. (2007) 'What Can Behavioral Economics Teach Us About Privacy?', in Acquisti, A., et al. (eds.) *Digital Privacy: Theory, Technologies, and Practices* (CRC Press: Auerbach Publications).
44. See http://www.pripareproject.eu (home page), date accessed 30 March 2016.
45. Diaz, C., Gürses, S. (2012) 'Understanding the landscape of privacy technologies', extended abstract of invited talk for the *Proceedings of the Information Security Summit*, pp. 58–63.
46. Although anonymous authentication may seem a contradiction in terms, it is actually a powerful method to preserve privacy while also ensuring that a given resource is only manipulated by authorised users. Anonymous authentication refers to the ability of a server to verify that an authorised user is logging in, but without knowing exactly which user it is. See Lindell, Y. (2010) 'Anonymous Authentication', *Journal of Privacy and Confidentiality*, No. 2, pp. 35–63 for a very good introduction to the subject.
47. Anonymous communication networks enable users to communicate with each other without revealing their identities. See Peng, K. (2014) *Anonymous Communication Networks: Protecting Privacy on the Web* (Boca Raton, FL: CRC Press: Auerbach Publications).
48. Private information retrieval allows users to retrieve an item from a database without revealing which item is retrieved.
49. A classic technique for the implementation of privacy as practice is the Platform for Privacy Preferences, rarely used now, which requires that users trust the organisation. The Platform for Privacy Preferences Project (P3P) was defined as a protocol in which websites would declare how they

intended to use the information they collect on users. See World Wide Web Consortium (2016) 'Platform for Privacy Preferences (P3P) Project', *W3C,* https://www.w3.org/P3P, date accessed 29 April 2016. P3P has been criticised for its lack of real privacy protection. See, for example, Agrawal, R. (2002) 'Why is P3P Not a PET?' *Electronic Privacy Information Center*, https://www.w3.org/2002/p3p-ws/pp/epic.pdf, date accessed 28 April 2016.
50. Wright, D., Friedewald, M. (2013) 'Integrating Privacy and Ethical Impact Assessments', *Science and Public Policy,* Vol. 40, pp. 755–766.
51. Troncoso, C. (2015) 'Privacy-preserving tools to support privacy-by-design', *Security Engineering Forum*, http://www.securityengineeringforum.org/blog, date accessed 30 January.
52. Hoepman, J.H. (2014) 'Privacy Design Strategies', in Cuppens-Boulahia, N. et al. (eds.) 'ICT Systems Security and Privacy Protection', in *IFIP Advances in Information and Communication Technology*, Vol. 428, pp. 446–459.
53. Froomkin, M. (2015) 'Legal (and Political) Aspects of Designing Privacy-Enhanced Digital Personae', presented at the Amsterdam Privacy Conference 2015, 23–26 October.
54. Hannes, S., Helman, L., 'Corporate Solutions for Privacy Problems: the case of social networking platforms', presented at the Amsterdam Privacy Conference 2015, 23–26 October.
55. Gurses, S., Troncoso, C. and Diaz, C. (2015) 'Engineering Privacy by Design Reloaded', presented at the Amsterdam Privacy Conference 2015, 23–26 October.
56. Gurses, Troncoso, and Diaz (2015) 'Engineering Privacy by Design Reloaded', pp. 1–2.
57. Morozov, E. (2013) 'The Real Privacy Problem', *MIT Technology Review*, 22 October, p. 28.
58. Foucault, M. (1977) *Discipline and Punish: The Birth of the Prison* (New York, NY: Vintage Books).
59. Posner, R. (2013) 'Privacy is Overrated', *New York Daily News.* 28 April.
60. Harper, R. (ed.) (2014) *Trust, Computing and Society* (London: Cambridge University Press).
61. See Popsecu, M., Baruh, L. (2015) 'Consumer surveillance and risk of harm in the age of big data: an ethical analysis', presented at the Amsterdam Privacy Conference 2015, 23–26 October.
62. See Evgeny Morozov's remarkably lucid article on 'The Real Privacy Problem' for this quotation. Morozov, E. (2013) 'The Real Privacy Problem', *MIT Technology Review*, p. 23.
63. Nissenbaum, H. (2011) 'A Contextual Approach to Privacy Online', *Daedalus,* Vol. 140 No. 4, pp. 32–48.

64. Wright and Friedewald (2013) 'Integrating privacy and ethical impact assessments', pp. 755–766.
65. CNIL (2012) 'Vie privée à l'horizon 2020', No. 1, p. 47.
66. Gurses, Troncoso, and Diaz (2015) 'Engineering Privacy by Design Reloaded', presented at the Amsterdam Privacy Conference 2015, October.
67. For the Marcel Gauchet quotation see Morozov (2013) 'The Real Privacy Problem', p. 17.
68. Morozov (2013) 'The Real Privacy Problem', p. 16.
69. Ibid.

Bibliography

Acquisti, A., Grossklags, J. (2007). What can behavioral economics teach us about privacy? In Acquisti, A., et al. (Eds.), *Digital privacy: Theory, technologies, and practices*. Boca Raton, FL: CRC Press, Auerbach Publications.

Agrawal, R. (2002). Why is P3P Not a PET? Electronic privacy information center. Retrived April 28, 2016, from https://www.w3.org/2002/p3p-ws/pp/epic.pdf

Assemblée Nationale. (1789). Déclaration des droits de l'homme et du citoyen de 1789. Retrived April 10, 2016, from https://www.legifrance.gouv.fr/Droit-francais/Constitution/Declaration-des-Droits-de-l-Homme-et-du-Citoyen-de-1789

Boyle, J. (2008). *The public domain. Enclosing the commons of the mind*. New Haven, CT: Yale University Press.

Cohen, D., & Wells, J. W. (2004). *American national security and civil liberties in an era of terrorism*. New York City: Palgrave Macmillan.

Commission nationale de l'informatique et des libertés. (2012). Vie privée à l'horizon 2020: paroles d'experts, *Cahiers IP: innovation et prospective*, No. 1.

Council of Europe. (1952). *Protocol No. 1 to the European Convention for the Protection of Human Rights and Fundamental Freedoms*, E.T.S. 9, 213 U.N.T.S. 262, *entered into force* 18 May 1954.

Diaz, C., Gürses, S. (2012). *Understanding the landscape of privacy technologies. Extended abstract*. Information Security Summit 2012.

Electronic Frontier Foundation. (2016a). Net neutrality. *EFF*. Retrived April 10, 2016, from https://www.eff.org/issues/net neutrality

Electronic Frontier Foundation. (2016b) Why Metadata Matters. *EFF*. Retrived April 10, 2016, from https://ssd.eff.org/en/module/why-metadata-matters

European Commission. (2015) Data protection Eurobarometer Factsheet. Retrived October 15, 2015, from http://ec.europa.eu (home page).

FaberNovel. (2014). GAFAnomics: New economy, New Rules, LinkedIn Corporation. Retrived October 15, 2015, from http://fr.slideshare.net/faberNovel/gafanomics

Finn, R., Wright, D., & Friedewald, M. (2013). Seven types of privacy. In S. Gutwirth, Y. Poullet, et al. (Eds.), *European data protection: Coming of age?* Dordrecht: Springer.

Fitzgerald, B., Shi, S., Foong, C., & Pappalardo, K. (2011). Country of origin and internet publication: Applying the Berne Convention in the digital age. *Journal of Intellectual Property (NJIP) Maiden Edition*, 38–73.

Foucault, M. (1977). *Discipline and punish: The birth of the prison*. New York: Vintage Books.

Froomkin, M. (2015, October 23–26) *Legal (and political) aspects of designing privacy-enhanced digital personae*. Presented at the Amsterdam Privacy Conference 2015.

Fraunhofer Institute (2016). SHORE™—Object and face recognition. Fraunhofer Institute for Integrated Circuits IIS. Retrived April 28, 2016, from http://www.iis.fraunhofer.de (home page).

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management, 35*(2), 137–144.

Gershman, J. (2016, February 17). Apple v. Justice Department: Politicians and activists take sides on encryption order. Law Blog. *The Wall Street Journal*. Retrived April 30, 2016, from http://blogs.wsj.com/law (home page).

Greene, J., Barrett, D. (2016, April 15–7). Microsoft sues US on secret searches. *The Wall Street Journal*.

Gurses, S., Troncoso, C., & Diaz, C. (2015, October). *Engineering privacy by design reloaded*. Presented at the Amsterdam Privacy Conference 2015.

Gutierrez, E. (2004). Privacy implications of nanotechnology. Electronic privacy information center. Retrived April 28, 2016, from https://epic.org (home page).

Harper, R. (Ed.). (2014). *Trust, computing and society*. London: Cambridge University Press.

Hoepman, J. H. (2014). Privacy design strategies. In Cuppens-Boulahia, N., et al. (Eds.), *ICT Systems security and privacy protection*. IFIP Advances in Information and Communication Technology (p. 428, pp. 446–459).

Hoeren, T. (2014). Big data and the ownership in data. Recent developments in Europe. *European Intellectual Property Review, 12*, 751–754.

House of Representatives. (2011–2012). Stop Online Piracy Act, 112th Congress, 2nd Session, H.R. 3261, The Library of Congress. Retrived March 13, 2016, from https://www.loc.gov (home page).

Internet Engineering Task Force. (2016). *IETF*. Retrived April 10, 2016, from https://www.ietf.org (home page).

Internet Privacy Engineering Network. (2016). IPEN objectives. Retrived April 10, 2016, from https://secure.edps.europa.eu/EDPSWEB/edps/lang/en/EDPS/IPEN

Internet Society. (2012). Global internet user survey 2012, *ISOC*. Retrived March 30, 2016, from http://www.internetsociety.org (home page).

International Organisation for Standardisation. (2016). ISO/IEC 27001—Information security management, ISO. Retrived March 30, 2016, from http://www.iso.org/iso/home/standards/management-standards/iso27001.htm.

International Telecommunication Union. (2016). The world in 2015: ICT facts and figures. Retrived March 5, 2016, from http://www.itu.int (home page).

Internet Architecture Board. (2013). Privacy considerations for internet protocols. *Internet Engineering Task Force*, RFC 6973, July. Retrived April 10, 2016, from https://tools.ietf.org/html/rfc6973

Internet Society (2016). Internet society mission statement. Retrived April 30, 2016, from http://www.internetsociety.org/who-we-are/mission

Lessig, L. (2004). *Free culture. How big media uses technology and the law to lock down culture and control creativity*. New York: Penguin.

Lindell, Y. (2010). Anonymous authentication. *Journal of Privacy and Confidentiality, 2*, 35–63.

Loi no. 78-17. (1978). Relative à l'informatique, aux fichiers et aux libertés, JORF du 7 Janvier 1978, p. 227.

Morozov, E. (2013, October 22). The real privacy problem. *MIT Technology Review*, p. 23.

Office of the High Commissioner for Human Rights. (1988, April 8). *CCPR general comment no. 16: Article 17 (Right to Privacy) The right to respect of privacy, family, home and correspondence, and protection of honour and reputation*. Adopted at the Thirty second Session of the United Nations Human Rights Committee.

Office of the High Commissioner for Human Rights. (2014, June 30). *The right to privacy in the digital age*. Report presented at the Twenty-seventh Session of the United Nations Human Rights Council, A/HRC/27/37.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*(4), 32–48.

Organisation for Advancing Open Standards for the Information Society. (2016). Oasis consortium. Retrived April 10, 2016, from https://www.oasis-open.org (home page).

Peng, K. (2014). *Anonymous communication networks: Protecting privacy on the web*. Boca Raton, FL: CRC Press, Auerbach Publications.

Pew Research Internet Project. (2013). Anonymity, privacy and security online. Pew Research Center. Retrived April 10, 2016, from http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online-2

Popsecu, M., Baruh, L. (2015, October 23–26). *Consumer surveillance and risk of harm in the age of big data: An ethical analysis*. Presented at the Amsterdam Privacy Conference 2015.

Posner, R. (2013, April 28). Privacy is overrated. *New York Daily News*.
Troncoso, C. (2015). Privacy-preserving tools to support privacy-by-design. *Security Engineering Forum*. Retrived January 30, 2015, from http://www.securityengineeringforum.org/blog
United Nations General Assembly. (1948). *Universal Declaration of Human Rights*, G.A. res. 217 A (III), adopted by the U.N. Doc. A/810, 10 December.
United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*, G.A. res. 2200A(XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316, 999 U.N.T.S. 171, *entered into force* 23 March 1976.
United Nations Secretary-General Hammarskjold. (1955, July 1). *Annotations on the text of the draft International Covenants on Human Rights*, UN Doc. A/2929.
Vaidhyanathan, S. (2001). *Copyrights and copywrongs: The rise of intellectual property and how it threatens creativity*. New York: New York University Press.
Warren, S., & Brandeis, L. (1890). The right to privacy. *Harvard Law Review, 4*(5), 193–220.
World Wide Web Consortium. (2016). Platform for privacy preferences (P3P) Project, W3C. Retrived April 29, 2016, from https://www.w3.org/P3P
Wright, D., & Friedewald, M. (2013). Integrating privacy and ethical impact assessments. *Science and Public Policy, 40*, 755–766.

Cases

Court of Justice of the European Union. (2014). Judgment in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland*, 8 April.
Court of Justice of the European Union. (2014) Judgment in Case C-131/12, *Google v. Costeja González*, 13 May.
Court of Justice of the European Union. (2015) Judgment in Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 October.
United States Court of Appeals, Second Circuit. (2015) *American Civil Liberties Union v. James Clapper*, Docket No. 14-42-CV, decided 7 May.
United States District Court, Western District of Washington at Seattle. (2016) Complaint for declatory judgment. *Microsoft v. U.S. Department of Justice*, DWT 29162898v13 0025936-002444, 14 April.

CHAPTER 4

Online Censorship

The Internet provides a virtual locale for the highly diverse carnival of human experience, offering a display of the best, and the worst of human nature.[1] *As far as the latter is concerned, citizens expect their state to protect vulnerable populations, particularly minors, from online content that is hateful, violent or pornographic in nature by eliminating proscribed material from the Web. This chapter will examine the practice of online censorship in two very different settings: the closed Internet system in China and the open Internet system in Europe. In each case, the state acts as a guarantor of content, censoring proscribed material according to the law in place. However, not all material that is censored is hateful, violent, or pornographic; some, in fact, is highly political. The Chinese authorities have shown little tolerance for online activity that may threaten the monopoly of one-party rule in China, whereas European states have pursued a broad policy of hate speech censorship that has been extended to religious radicalism in recent years due to efforts to counteract online recruitment for jihadism. This chapter will compare and contrast (1) the interaction between Internet technology systems and censorship methods, (2) the legal constructs that frame government censorship policies, (3) the contested nature of information on the Internet, and (4) the impact of censorship on Internet users in both Europe and China. This chapter argues that, regardless of the governance system, digital censorship may violate or promote human rights according to the context. In the case of both China and Europe, Internet censorship has been relatively ineffective in countering real or perceived threats to the state and poses a problem for many in society who*

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_4

question the legitimacy of government officials more concerned with public opinion than the safeguarding of constitutional values.

Internet censorship primarily targets criminal activity, such as child trafficking, or content with a socio-political agenda that poses a real or perceived threat to the state. Censorship of any kind presents a challenge to the international human rights framework, since freedom of expression is considered a core value except in a state of emergency, when public order or safety may be at risk. This begs the question of what constitutes an emergency and how far governments may go in their efforts to protect citizens from themselves and from one another online. This chapter will examine two very different censorship paradigms, one occurring within the closed Internet system in China and the other within the open Internet system in Europe. In either case, the state acts as a guarantor of content, censoring proscribed material according to the law in place. The Chinese authorities have shown little tolerance for online activity that may threaten the monopoly of one-Party rule in China, whereas European states have pursued a broad policy of hate speech proscription that has intensified in recent years due to efforts to counteract online recruitment for jihadism. Our chapter will begin by examining censorship theory—new and old—and the dichotomy between repressive versus structural forms of censorship. The technological and legal underpinnings of censorship in China and in Europe embody both forms of social control, as is evident in our analysis of the contested nature of information on the Internet and the impact of government censorship on Internet users in both Europe and China. Recent regulations, such as the European 'right to be forgotten', also highlight situations in which one citizen's right to privacy may conflict with another citizen's right to free speech; this draws attention to the growing power of corporations in determining which data to retain or censor.

In terms of politicized content, ever since the Internet has been accessible in China, the Party-state has controlled access to anything crossing its digital borders through a set of filtering technologies that are commonly known as the Great Firewall. Nonetheless, the Party-State pays careful attention to online contestation as a means to monitor public opinion; scholarly evidence for government responsiveness to online campaigns around socio-economic issues, particularly the environment and corruption, is robust.[2] As will be discussed below, online censorship in China functions in a post facto manner: only when a critical mass of users have intensively discussed a 'sensitive' issue does the site regulator crack

down and begin to inhibit further diffusion of information. The Chinese government's concern with online jihadism has been restricted to the Uighur independence movement in Xinjiang province. In Europe, strict application of hate speech laws initially narrowed state efforts at online censorship to extremist political groups, such as neo-Nazi movements in France or Germany.[3] With the rise of online recruitment of European citizens for jihadism and a series of terrorist attacks in France and elsewhere in Europe, however, the focus has shifted to censorship of radical Islamic movements in an effort to stymie online enlistment of European nationals for armed struggle in the Middle East or terrorist attacks on European soil. Consequently, in both China and Europe, governments do more than protect public safety; they walk an extremely fine line between freedom of speech and censorship.

User response to government censorship is highly varied. While Chinese citizens generally support government restriction of websites promoting jihadism,[4] many netizens delight in leaping over the Great Firewall, invading the Chinese Communist Party's space of controlled dialogue and raising havoc with the orderly expectations of China's *nomenklatura*. European citizens, like their Chinese counterparts, have come to expect government censorship of online jihadism, but citizens' groups across the continent question the extent to which governments may censor digital content in an emergency. This chapter will examine spheres of contestation where citizens challenge government censorship and probe the motivations behind sustained drives to shut down controversial online political content.

4.1 New (and Old) Censorship Theory

The traditional liberal concept of censorship pits legitimate rule against arbitrary domination,[5] with censorship as an explicitly coercive process—an act of arbitrary power infringing upon the natural communicative rights of the individual; all else is 'merely editing'.[6] Nonetheless, citizens of even the most democratic states accept that certain speech acts that cause undue harm 'might justifiably be censored, provided the harm caused by the speech outweighs the harm caused by violating the general proscription against censorship'.[7] Thus, the debate on censorship in democratic societies usually focuses on the degree of harm permissible—a determination left to an independent judiciary.[8] Because freedom of expression is limited in this way, philosopher John Stuart Mill complained that censorship is

'as noxious, or more noxious, when exercised in accordance with public opinion, than when in opposition to it.'[9] It should be noted that both the Chinese and European examples selected for this chapter occur within a context of majority public support, despite clear constitutional overstep on the part of government authorities.

New Censorship Theory extends repression beyond the state to a host of actors and structural processes, 'foreclosing openness in order to render thought communicable' in the words of Judith Butler.[10] New Censorship Theory includes the effects of the market, ingrained cultural grammars and self-censorship as potent forms of repression that may act in consort with the state. As Matthew Bunn points out, both Pierre Bourdieu and Michel Foucault stressed how power takes on 'ostensibly consensual, often invisible forms through the cultural and social authority of nonstate actors'.[11] New Censorship Theory critics note, however, that the theory suffers from 'semantic inflation': if we apply it to everything that is structural, then the term is analytically useless.[12] Consequently, this chapter will build on Bunn's work, which analyses both the state and contextual confines of censorship, by applying his hybrid censorship theory to the Internet. In the case of China, the state is assisted by a '50 cent army' of Internet commentators, paid for each microblog post in support of government policy or each disparaging comment against online political dissent that sways public opinion.[13] In France, families of potential jihadists recruited online are encouraged by the French government to denounce their relative before that individual can travel to the Middle East or engage in harmful activity in Europe. In both instances, state censorship efforts are mirrored by non-state actors, a factor which reinforces the impact of a repressive campaign.[14]

4.2 Censorship Technology in China and in Europe

The Chinese Party-State, the European Union (EU) and European national governments have all been proactive proponents of Internet development. In China, according to the China Internet Network Information Centre (CNNIC), the number of citizens on the Web has soared from a few thousand users in 1994 to over 668 million by 2016, with an Internet penetration rate of just over 50 per cent.[15] The 2010 Network Readiness Index of the World Economic Forum reported that, 'China consolidates its position in the rankings at 36th, after years of vibrant progression. It is by far the

country that leverages ICT the most among the four BRICs'.[16] Five years later, the same index ranked China at a far lower 62nd position, due to slower business innovation and challenges related to government control of infrastructure and content.[17] Comparatively, in the same index, Finland, Sweden, the Netherlands, Norway, and Switzerland ranked ahead of the USA, and only Greece was ranked lower than China. Nonetheless, China continues to have one of the world's largest telecom markets.[18] CNNIC reported in 2012 that for the first time, 'the mobile phone has become the Internet access terminal with the greatest number of Internet users in the country', surpassing desktop access, and that a steady growth was registered in the number of online video users, microblog users, mobile microbloggers, online shoppers, and e-bank and online payment users.[19] In the same year, 36 per cent of individuals aged 16 to 74 within the EU used a mobile device to connect to the Internet; by 2015, this share had risen to 75 per cent.[20]

In Europe, the Internet was celebrated as the ultimate tool for free expression and sharing of information. A 1997 incident that involved Austrian police seizure of equipment belonging to a well-known Internet service provider—following a tip from the German police about a pornographic post by a former user—resulted in all major Austrian Internet service providers (ISPs) taking themselves offline to protest.[21] Following this incident, Internet censorship in Austria has been rare. This is the case in all European countries, where historically online censorship has been directed at child pornography and neo-Nazi propaganda, as mentioned above.[22] In Europe and the USA, however, access to certain sites may be denied to protect copyright; there is ongoing debate as to who is responsible for copyright protection of online material, the extent to which copyright protection may infringe upon other rights, and the best technical measures to enforce protection.[23]

The Chinese government has always controlled access to any content crossing its digital borders through a set of filtering technologies that have evolved over time and are commonly known as the Great Firewall. Initially, Internet users were required to register with the police and violations of Internet access restrictions could be fined with the equivalent of the annual salary for an average worker.[24] State control was facilitated by a set of regulations that centralized all connections to the Internet's international circuits, sending them through one of four interconnecting networks.[25] This centralized configuration, which persists today, has allowed the liberalization of the ISP market, since the Chinese government maintains

control by requiring that all ISPs subscribe via the interconnecting network operators and are licensed through the Ministry of Industry and Information Technology.

As Internet usage grew, impacting every aspect of Chinese society and the economy, it became increasingly difficult for the government to strike a balance between maintaining control over Internet access and satisfying the needs of its industry and citizens. Growth in Internet use was driven by a set of correlated factors, including the liberalization of the telecom industry through a series of competition reforms that took place in three stages between 1994 and 2007,[26] a general improvement in the Chinese economy, along with the entry of China into the World Trade Organization in December 2001, and the accelerated opening of industry to Western capital. Although the gateway filtering mechanisms of the Great Firewall became a major pillar of China's censorship programme, other mechanisms were needed to provide sufficient Party-state control in an environment of rapid technological development.

Government initiatives ranged from support of commercial Internet services (the Golden Bridge project) to information sharing between government bodies (the Golden Macro project). Certain project objectives, such as the promotion of national technology and terminology norms, the enhancing of network safety and data integrity, or the provision of a network management mechanism, were necessary to standardize China's Internet. Other measures, such as the creation of an enhanced database for the Chinese police, the interconnection of public security forces, and implementation of a 'public network information surveillance system that monitors real time traffic and keeps undesirable content out of China cyberspace', suggest that the real objective was to police cyberspace.[27] At a cost of over one billion dollars, China relied heavily on technological expertise and investment from Western countries whose surveillance practices already made widespread use of data collected from networked devices,[28] raising public concern and many ethical questions.[29] In November 2002, Amnesty International listed a number of well-known American technology companies that supported China in its surveillance efforts.[30] China's Golden Shield project was further facilitated by standardization efforts such as those prompted by the Communications Assistance for Law Enforcement Act,[31] a US law passed in 1994 requiring all telecommunications equipment and services to have built-in surveillance capabilities to monitor telephone, broadband Internet, and VoIP (Voice over Internet Protocol) traffic in real-time. The project relies on an

expanding fibre-optic infrastructure which incorporates multimedia data from sources such as video cameras and monitoring of mobile devices.

China's integrated IT infrastructure was based on two main components: a monitoring and surveillance system comparable to that of the most technologically advanced countries, and a China-specific access control system relying on the centralized network configuration described above. The infrastructure, when combined with an evolving set of laws and regulations and a Party-guided labour force, facilitated state monitoring, tracking, and control of Internet traffic, and international traffic in particular. The Chinese Communist Party's content control strategy still consists of three primary techniques that include automated technical filtering, forced self-censorship by service providers, and proactive manipulation.[32] Scholar Gary King and his colleagues have demonstrated that in order to implement such control, hundreds of thousands of people are employed to monitor, censor, and manipulate online content, with up to one thousand censors employed by each private site and approximately 20,000–50,000 Internet police, and the estimated 250,000–300,000 '50 cent Party members' at all levels of government.[33] European police, by comparison, are able to budget for a few hundred agents dedicated to monitoring and censorship, compared to the tens of thousands employed by the Chinese Party-State.

From a technical point of view, two main strategies are used for filtering in Europe and in China: the monitoring of requests for access to specific pages, a technique that blocks access to entire websites for a prolonged span of time (the means by which access to Facebook, YouTube and Twitter is blocked in China); and the use of Deep Packet Inspection (DPI) to thwart access to specific pages of otherwise allowed websites on the basis of keywords, a technique discussed in Chapter 3. Keyword filtering may also be applied to mobile phone text-messaging and instant messaging services.[34] In Europe these techniques are most often employed to collect users' data in order to sell it to third parties, such as advertisers, rather than filter access to website. In order to implement these blocking strategies, several network catches may be employed to impose a failure in the communication protocol.[35]

When trying to connect to a website, we instruct a computer (the 'client') to contact a domain name server (DNS), which in turn accesses the IP address (Internet Protocol address) of the machine hosting the desired website (the web server). The computer then uses this address to request a web server connection and delivery of the website. DNS injection blocks

page requests by interfering with the translation of page names into IP addresses. If the user issues a request that, for example, contains a blacklisted term, a fake DNS reply is injected with an invalid Internet address. As a consequence, the client tries to access a wrong IP and either will be unable to connect or will be taken to an erroneous website. This technique is one of the many that has been used in the USA and Europe to implement phishing attacks (with the purpose of fooling users into believing that a message or a website comes from a reliable source, so as to extract information from the user). Technology savvy users can circumvent DNS injection by using different virtual private networks (VPN) or sending requests for the IP addresses directly, so as to avoid the need to go through a domain name server. Sometimes users outside the censorship area are directed through a controlled DNS, which results in censorship being applied more widely than desired. Finally, poor implementation of DNS injection may cause serious network disruptions; *Agence France Press* reported that one of the largest Internet outages ever in China was due to an improperly configured DNS poisoning implemented by the Party-State itself.[36]

The second type of interference consists of IP address blocking, which relies on a blacklist of IP addresses and injects null routing information when a user tries to access one of the proscribed ones. This catch is easy to implement, but it can be circumvented by setting up a proxy outside of China or changing the IP address for the site. An inquiry by the European Commission found that IP blocking, and geo-blocking in particular,[37] is widely used by European companies:

> As regards online digital content, the majority (68 %) of providers replied that they geo-block users located in other EU Member States. This is mainly done on the basis of the user's internet protocol (IP) address that identifies and gives the location of a computer/smartphone. 59 % of the responding content providers indicated that they are contractually required by suppliers to geo-block.[38]

Finally, as discussed in Chapter 3, DPI is probably the most powerful identification method, and can be used to monitor traffic to determine if the content is acceptable. Unlike other techniques, DPI examines the application 'data' rather than the header of the packet. This makes it possible to identify keywords or use additional packet and flow characteristics to identify and then censor content. If content should be blocked, the

connection is terminated by injecting a series of reset packets. DPI is expensive to implement, may have a negative impact on the quality of service and, when used as a keyword filter, can block non-targeted users. The technique most frequently employed to circumvent DPI is the VPN mentioned above.[39]

China is of particular interest because of its extensive external and internal Internet censorship. The censorship techniques apply to international communication entering China and achieve complete control thanks to the centralized configuration of the international connection. Within China, there are just a few central nodes that route all traffic; for this reason, censorship is achieved by employing the large number of censors mentioned above who, either automatically or manually, remove undesirable content. Several analysts report that the monitoring of Internet traffic in China does not aim at exhaustive coverage, because of technical difficulties, limited manpower and unwillingness on the side of the Communist Party to take steps that could endanger economic development or generate excessive social resentment.[40] Scholars concede a range of opinion on what exactly the Party chooses to censor. The majority agrees that online censorship functions after the fact: only when a critical mass of users have intensively discussed one sensitive issue does the site regulator crack down and begin to inhibit further diffusion of information. Some large-scale studies have explored the precise terms which provoke censorship measures. A study of 56 million messages from Sina Weibo and 11 million Chinese language messages from Twitter reveals that censorship is driven by topical, politically sensitive terms, so that users may be prohibited from searching for specific terms at a given time (such as 'Egypt' during the Arab Spring). Politically sensitive messages are occasionally deleted retroactively with a policy that appears not to be uniform across the country (for example, messages from Tibet and Qinghai are deleted more frequently).[41] In another large-scale analysis of censored communication, King and his team conclude 'the purpose of the censorship program is to reduce the probability of collective action by clipping social ties whenever any collective movements are in evidence or expected'.[42] They found that posts that are critical of the Party are not necessarily targeted by censors, while posts connected to possible collective action in the street are censored regardless of whether they are critical of the state or not.

This effort is directed by the Central Leading Small Group for Cyberspace Affairs. According to President Xi Jinping, the group, created at end of 2013, 'is designed to lead and coordinate Internet security

and informatisation work among different sectors, as well as draft national strategies, development plans and major policies in this field'.[43] The group's executive office is known as the Cyberspace Administration of China (CAC). Several observers note that since the creation of the CAC the Party's control over Internet activity has significantly strengthened.[44] Restrictions include a campaign launched in 2014 'to clean up content, such as pornography, violence, terror and rumours in online videos',[45] the disruption of access to several foreign websites (Google, Yahoo, and Outlook, for example) from the China Educational and Research Network,[46] the blocking of virtual private network services in January 2015,[47] and the creation of official online accounts for provincial or city-level police to aid anti-cybercrime work.[48] *China Daily* reported in late 2015 that even 'Chinese web giant Sina will face suspension of its Internet news services if it fails to improve censorship of illegal content'[49] (Box 4.1).

Box 4.1 Virtual access in the PRC

Faced with the government filtering strategy, Internet users soon realized that only a rapid, bottom-up, many-to-many format would allow Chinese citizens to engage one another and the State in their exploration of multi-faceted dialogue under Party-State control. In what scholar Jin Liwen refers to as a 'dynamic and dense sphere',[50] netizens first embraced the ingenious use of quick-fire bulletin board postings[51] in response to news before moving on to Weibo and then WeChat. We note that the bulletin board system (BBS) played a seminal role in the construction of Chinese Internet life. The topic-centric character of online fora made BBS a popular choice with Chinese users.[52] In 2008, China counted over 3 billion registered BBS users (users could register at multiple BBS sites), 80 per cent of Chinese sites ran their own BBS and the total number of daily page views across bulletin board systems reached over 1.6 billion, with 10 million posts published every day.[53]

BBS began ceding ground to Weibo, a Chinese Twitter hybrid, in 2009. By 2012, 54 per cent of China's half a billion Internet users

(continued)

Box 1.1 (*continued*)

were on Weibo, and of that number two-thirds were accessing Weibo on their mobile phones.[54] The reasons for the success of Weibo in China were initially the same as those that prompted Twitter's success in the West. Nonetheless, several unique characteristics enhanced its popularity: much more can be expressed in 140 Chinese characters than in 140 English letters; Weibo has an augmented platform allowing post comments in classic BBS style and its users can post images, video, and sound directly into their Weibo feeds; users who re-tweet messages can add more characters; and Weibo has more metrics to encourage participation than Twitter.[55]

Weibo's popularity started declining in favour of instant messaging tools such as WeChat in part due to the 'real name' policy enforcement on Weibo. Chinese President Xi Jinping ramped up online policing and chose to clamp down on Internet dissent. As of September 2013, all Weibo users had to supply their real name to their service provider. According to China's state Internet regulator, 56 million people in China stopped using their Weibo accounts in 2014.[56] This policy has now been applied to public accounts on instant messaging tools,[57] and is starting to be enforced widely as part of the larger effort to increase cybersecurity.[58]

4.3 Freedom of Expression in China and in Europe

The Universal Declaration of Human Rights, ratified by China and by all of the EU member states, guarantees freedom of opinion and expression—rights reinforced by the binding International Covenant on Civil and Political Rights, ratified by all EU countries and signed, but not ratified by China. Because freedom of expression is a derogable right, treaty signatories may suspend the exercise of this right in order to (a) respect the rights or reputations of others, or (b) protect national security, public order, or public health or morals.[59] While EU member states traditionally have practised fairly liberal policies with respect to freedom of expression, primarily censoring material that offends the rights or reputation of others, China has a long history of censorship[60] and any Chinese government's commitment to freedom of expression has been coloured by an overriding concern with national security and public order.

The 1982 Chinese Constitution guarantees freedom of speech, publication, assembly, association, procession, and demonstration under article 35.[61] Citizens also have the right to criticize and make suggestions to any state organ or functionary under article 41, as long as they do not fabricate or distort facts.[62] With the latter caveat in mind, the government extended existing media restrictions to the Internet as early as 1997, using language already widely employed to censor newspaper, radio, and television material that was critical of the Chinese Party-state. While much of what the government chose to describe as 'harmful' clearly poses a threat to public order (such as violating the Constitution, inciting hatred or discrimination among nationalities, or terrorism), other somewhat vague activities (such as spreading rumours, promoting feudal superstitions, or injuring the reputation of state organizations) do not appear to fall within the confines of legitimate national security.[63] State Council Order No. 292, promulgated in 2000, created the first restrictions for Internet providers, making them 'responsible for ensuring the legality of any information disseminated through their services'.[64] Article 23 of the Regulations on the Administration of Internet Access Service Business Establishments (2002) required that Internet cafés 'examine, register, and keep a record of the identification card or other effective document of those customers who go online'.[65] The 2002 Interim Provisions on the Administration of Internet Publication repeat the historically vague restrictions on content: Internet publications may not harm 'the honour or the interests of the nation', nor may users engage in 'spreading rumours, disturbing social order, or disrupting social stability'.[66] It is precisely because these interdictions are so difficult to define from a legal point of view that Chinese courts have been able to sentence Internet dissidents to prison terms, an effective means to encourage self-censorship for China's millions of netizens who might otherwise be tempted to criticize the government. This practice, known in Chinese as 'killing the chicken to scare the monkey',[67] allows the judicial system to curb freedom of expression online through the limited use of cases selected to send a broader message.[68]

Under the guise of centralizing China's Internet policy, the Party-state further restricted online freedom of expression with the arrival of Xi Jinping in 2012. Within a year, Xi announced China's current policy of 'cyber sovereignty', a strategy of control articulated in an internal speech at a National Propaganda and Ideology Work Conference, and reminiscent of Maoist discourse from an earlier era: 'The internet has become the main battlefield for public opinion struggle.'[69] Rather than 'guidance'

or 'channelling' of public opinion online, terms used under the previous president Hu Jintao, the Party-state committed to online struggle in an effort to gain full control of an unruly space that threatened one-party governance. In late 2015, the Standing Committee of the 12th National People's Congress submitted a draft Cybersecurity Law to the public on the Chinese National People's Congress website for collection of public comments, to be provided online or by letter.[70] Despite this remarkable effort to test domestic and international public opinion (the draft was available both in Chinese and in English), the final version of the law which came into force on January 1, 2016 challenged China's Constitution in several ways. Chinese netizens immediately noted that the law legalizes China's use of the Great Firewall to deny domestic citizens' access to information the authorities deem forbidden by laws and regulations.[71] The law obliges network operators to provide the authorities with real user identity information when signing service agreements to ensure the traceability of Internet content. Interestingly, the law imposes obligations for privacy protection on the service provider, but does not guarantee that the public authorities operate under the same privacy constraints with respect to their use of personal data. The law also requires relevant organizations to adopt technological and other necessary measures to block the transmission of information that is prohibited by Chinese laws and regulations. Finally, the text allows for the total shut down of the Internet in certain regions to protect national security and social public order and respond to major social security incidents, through the offices of the State Council in coordination with provincial and municipal governments. The goal in promulgating such vague, but far-reaching legislation was clear: making the views of the country's ruling Communist Party the 'strongest voice in cyberspace' its top priority, foregrounding the Party's theories and achievements to garner public support for the 13th Five-Year Plan (2016–2020).[72]

In response to the crisis in Ukraine, domestic terrorist attacks, and an unprecedented influx of refugees, several EU member states have promulgated wide-ranging security legislation that mirrors the spirit of China's Cybersecurity Law, despite the far-reaching protections and freedoms guaranteed by the European Convention on Human Rights. The 47 member states of the Council of Europe are required under article 10 of the Convention to extend freedom of expression, opinion, and the right 'to receive and impart information and ideas without interference by public authority and regardless of frontiers', except in a public emergency or in order to protect the rights or reputation of others, when this right may

be temporarily abrogated.[73] In 2003, the Council of Europe promulgated an *Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems,* an extension of Europe's hate speech laws to online content. The protocol's definition of cyber hate speech provides a fairly broad 'margin of appreciation':

> *Racist and xenophobic material* means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.[74]

While a more precise interpretation of hate speech has been left to national courts and the European Court of Human Rights (ECHR), the latter court has not, as of this writing, specifically defined hate speech.[75] Nonetheless, ECHR judgments have determined that legislation relating to defamation, hate speech, and blasphemy, as well as laws aimed at protecting public order, morals, or national security, should take into account the requirements of article 10 of the ECHR and the case law of the court. In particular, 'all laws limiting freedom of expression must (1) respond to a pressing social need, (2) be clearly and narrowly defined, and (3) be proportionate in scope and sanctions'.[76]

Council of Europe member states are very much aware of the fine line between freedom of expression and censorship, and have used the term 'democratic security' to describe their efforts to counteract terrorism and other extremist movements. Like the Chinese government's 'cyber sovereignty', democratic security extends the scope for censorship in Europe,[77] with the Internet as a key battleground for testing the limits of freedom of expression. When Polish voters, responding in part to Russian sabre-rattling under Putin,[78] elected a conservative government to office in 2015, the parliament quickly promulgated new legislation that delegated control of public media to the Ministry of the Treasury; despite alarmed protest from the European Commission and the Council of Europe, Poland's Law and Justice Party indicated that such legislation was necessary so that the media may 'fulfil their role of uniting and educating the nation'.[79] While the new law did not extend to the Internet, certain journalists worried that this was the beginning of a push to restrict freedom of expression throughout Polish society for 'patriotic' purposes.[80] Furthermore, the parliament

also promulgated an amendment that interfered with the separation of judicial and executive powers, increasing the number of judges needed to pass judgments on the Constitutional Court and changing the order in which cases are heard, thereby making it difficult to rule on controversial issues. The potential combined impact of these two legislative initiatives was striking. Given that 70 per cent of young Poles had encountered hate speech on the Internet through popular portals such as Onet or Gazeta,[81] Poland faced a real risk of selective censorship in combination with hamstrung judicial review: in a scenario not that different from China, websites in support of the government might be allowed to continue, regardless of content, while dissident portals would be shut down.

Democratic security was also on socialist president François Hollande's agenda when his government presented a new anti-terrorist law to the French parliament in 2014 in response to the steadily increasing numbers of French recruits to jihadism. The law was noteworthy in that it allows investigators to search the 'cloud' or to shut down Internet sites without a judge's warrant.[82] Although initial criticism of the law, discussed below, was extremely sharp, support for freedom of expression was muted following the devastating terrorist attacks of 2015 and 2016. In the wake of the first attack against the satirical review *Charlie Hebdo* in January 2015, the French parliament promulgated a surveillance law that permitted interception of all online personal data and communications generated by French citizens in hope of detecting suspicious behaviour.[83] A new volley of constitutional initiatives followed the Paris attacks of November 2015, extending the timespan of the state of emergency, transferring certain judicial powers to the executive, and introducing the forfeiture of French citizenship for dual nationals inculpated for terrorism, the latter a controversial amendment that the French Senate voted to remove from the proposed text.[84] It should be noted that, under an extended state of emergency, the French government used executive warrants and house arrests not only for those suspected of terrorism, but also for environmentalists opposed to the installation of a new airport and common criminals, such as drug smugglers.[85] We suggest that what began in France as an attempt to censor recruitment for online jihadism in 2014 quickly evolved into an empowered executive which took advantage of the state of emergency at the expense of individual liberties.

Consequently, China's *cyber sovereignty* and Europe's *democratic security* may well be two sides of the same coin: euphemisms that disguise a swing towards more conservative policies that include a broader use of

censorship to track and control public opinion. While the Chinese Party-state purported to garner public support for its 13th Five-Year Plan, the Polish government aimed to bolster patriotism, and the French government ostensibly intended to protect their domestic population from terrorism. Each of these objectives was a laudable policy goal, but the extended means used to achieve them violated time-honoured notions of freedom of expression. Moreover, the ECHR has indicated that censorship must respond to a pressing social need, be clearly and narrowly defined, and be proportionate in scope and sanctions. While French terrorist legislation clearly responded to a 'pressing social need', Polish 'patriotic' legislation did not; censorship by the French executive can never be as 'clear or narrow' as a written warrant provided by an independent judiciary; and while initial sanctions for proscribed content may be 'proportionate' in scope, the long-term impact of expanded censorship on a democracy may be anything but balanced. The next section will examine those citizens who are the objects of government censorship, and how they and other social groups have responded to online curtailment of their opinions.

4.4 Contested Content and the Impact of Censorship

European citizens rarely think of the Internet as a censored locale, whereas their Chinese counterparts are far more aware of repressive government practices. This section will examine two proscribed groups: political dissidents in China and jihadists in France. While these two virtual populations could hardly be more different, the practice of online censorship has raised similar concerns with netizens across civil society in both countries. This section will also explore reactions to the muzzling of freedom of expression in both societies and suggest that censorship by the executive has not been an effective means to control online political content.

In China, the current profile of regular mobile Internet users has remained consistent since the introduction of bulletin board system (BBS) online forums over ten years ago: well-educated, urban students and professionals between the ages of 20 and 30, who are online three to six hours per day. In a small survey of Chinese Internet users that we carried out in 2013,[86] our respondents indicated that the contested arena of Internet debate was an integral part of their everyday lives, and most were hostile towards the government's refusal to respect due process on the Internet. One of the more interesting features of netizen response to government

censorship in China has been the creation of a 'grass-mud horse lexicon', the use of online codes to evade censorship.[87] When scholar Xiao Qiang launched this initiative online in 2010, his staff trawled the net and solicited entries from Chinese netizens, leading to a rich and playful example of language use that is not immediately comprehensible to the average Chinese speaker. Although King's study, discussed above, goes a long way towards establishing that censorship targets the dismantlement of collective action that could spill over into the street, the respondents in our survey assumed that the purpose of government censorship is to shut down all criticism of the Party-state online. Consequently, when discussing political matters, those posting commentary have been prompt to use the grass-mud horse lexicon for skirting perceived or real censorship, a method that bonds users and creates what scholar Xiao Qiang calls a 'resistance lexicon'.[88] Our respondents indicated that they followed online campaigns closely. The array of campaigns has been addressed in full by a series of scholarly publications that demonstrate the often virulent online response to government corruption, lying or incompetence, particularly in the face of man-made or natural disasters.[89] The most significant online campaigns that prompted a change in government response took place immediately after the 2008 Szechuan earthquake (a BBS event), the 2011 Wenzhou train crash (a Weibo event), and Chai Jing's anti-pollution video (a WeChat event). The latter was pulled offline, despite having been vetted by the Ministry of the Environment, after it was viewed by 155 million netizens in a single day.[90]

We have noted in our own online searches that the terms rights (*quanli*) and human rights (*renquan*) are not only ubiquitous and uncensored on the Chinese Internet, but they are frequently used in a purely political context. While our respondents indicated that they were willing to make informed use of terms such as 'human rights' in their online posts, they considered any attempt to organize a political protest in the street as a form of professional suicide. Their reasoning on the latter was divided: while half of our respondents consider the maintenance of social stability by the government as a right in and of itself, the other half deemed government repression of political assembly a violation of their rights, but acknowledged that any attempt to organize a street protest would land them in trouble. Some of those who considered social stability a right had also engaged in 'cyber nationalism', while several of those who favoured the right to assembly pointed out the government's manipulation of Internet forums to cultivate nationalism.

In short, this highly educated urban cohort of nearly 700 million active users appeared willing to read about human rights on their smartphones, but shied away from any sort of political engagement that might cause difficulties. Nonetheless, spaces unhindered by censorship do exist in China. Cyber game platforms, such as World of Warcraft, are active with political commentary as users share opinions on current events, such as Hong Kong's umbrella revolution; even if computer console games have lost ground in China to games easier to play on a mobile phone,[91] the World of Warcraft discussion groups experienced no overt censorship whatsoever even though this event was subject to a total online blackout in China.[92] This may be due to the fact that each individual plays in isolation in front of a computer and is unlikely to organize a street protest, or that the Party-State's manual censors do not have access to the closed gaming platforms, making them an ideal locale for the practice of freedom of speech.

In Europe, the profile of the cyber jihadist appears to be diametrically opposed to that of the online human rights defender in China. Nonetheless, in both cases, their respective governments are searching for a call to action that threatens public order. At the time of this writing, Daech was using online recruitment for primarily European audiences, targeting men and women who are psychologically vulnerable and in some, but not all cases, living on the margins of society. According to Gilles Kepel, Daech launched its successful recruitment drive in France's notoriously overcrowded and understaffed prisons.[93] The country's recent terrorists were all French citizens; some were raised through foster care, had spent time in prison for petty crime, attended services led by a radical imam, trained in Syria or Yemen, and returned to France as sleepers, waiting for the call to die as a martyr. Our colleague Ziad Majed explains that this recruitment drive was extended to individuals attracted to the spectacular violence of online jihadist videos who sought a confirmation of their virility.[94] Majed describes these individuals as 'angry and humiliated young men, victims of discrimination, with no future in France'. An estimated 2000 French men and women were fighting in Iraq and Syria at the time of the November 2015 attacks.[95] Another survey indicated that French recruits under the age of eighteen, both male and female, were psychologically fragile, but otherwise came from middle class families of which 56 per cent were not Muslim.[96] The vast majority were initially recruited online. Daech contacted European recruits individually through Facebook, YouTube and Twitter accounts, patiently searching for the use of jihadist terms, inviting the potential recruit to join a discussion forum

or to play a video game, engaging in a cat and mouse game of increasing psychological dependence, either encouraging the recruit to move to the Middle East (citing the example of the Prophet who moved from Mecca to Medina in 632AD) or to remain at home, waiting for the call to martyrdom. According to Majed, the French government was shutting down up to 500 French language jihadist Twitter accounts per week in 2015 (out of an approximate 76,000 jihadist Twitter accounts worldwide), only to find new ones opened up just as quickly as old ones were censored.

The genius of Daech, according to Oliver Roy, is the call to action. Unlike the Salafist movement, which is opposed to a secular state but not necessarily in a violent manner, Daech uses violence to breed violence, bypassing traditional religious codes of acceptable human conduct. Internet censorship has been relatively unsuccessful against Daech for the simple reason that the authorities are focused on the wrong target. Ninety-five per cent of newcomers to jihadism have been recruited in person after an online contact.[97] Thus, rather than attempting to infiltrate Daech sleeper cells, for example, the French government has 'wasted time' on what Majed terms 'ignorant imams and radical mosques', even though religious radicals do not necessarily become jihadists. Moreover, Daech's online monthly newsletter *Dabeq*, which provided a review of caliphate policy in several languages, arrived to its Listserv subscribers as a pdf file, impervious to online keyword searches; *Aamak*, the caliphate's professional news agency, contacted all media outlets with propaganda content, regardless of their affiliation, and ran a website that proved difficult to pull down. It should be noted that the French authorities were fairly active in creating anti-jihadist websites, YouTube and Twitter accounts to expose the myriad inaccuracies of Daech propaganda to young viewers,[98] and humorous videos ridiculing extremists appeared to have the greatest impact of all. Nonetheless, by outsourcing its cyber war to talented computer scientists, Daech was one step ahead of European censors, who did not allocate the budgets, the manpower, nor the political will to organize a cohort of thousands of manual censors who can read Arabic.

No one in Europe questions state attempts to censor online recruitment efforts that target children. However, the issue is a larger one and concerns which moral and legal strategies to use in order to control a small group of European citizens who no longer recognize European values. The Islamicization of radicalism in Europe, to use Olivier Roy's term,[99] means that Europe's time-honoured notions of freedom of expression are made to serve a form of religious fundamentalism that threatens

liberty itself. François Burgat, who disagrees with Roy's term, suggests that France's jihadists are responding to racism and islamophobia in their country of origin, identifying with the Palestinian cause while rejecting Western intervention in the Middle East.[100] Consequently, in reacting to what Kepel describes as the imposition of a separate space for Muslim identity across European society according to terms that do not resonate with European human rights,[101] online censorship appears to be a viable response. Or is it?

China and France censor online content in an attempt to eliminate a call to action that poses a serious threat to the government in power. Neither polity has been particularly successful in its attempts to counter popular discontent, in the case of China, or terrorism, in the case of France, even though Beijing is simply attempting to warn by example, whereas Paris cannot afford to make a mistake that might result in another terrorist attack. Perhaps what is most striking in this comparison is the exceptionally dissimilar profile of those subject to government censorship. Yet, in both cases, censorship has led citizens to question government policy on political plurality, discrimination, or which measures are necessary to protect citizens in a national emergency. The Internet has become an arena *par excellence* for an exploration of the contested notion of freedom of expression, one where citizens and their governments debate on where to draw the line.

As of this writing, online protest of Party-State censorship continues to be most active outside of China, led by the *China Digital Times*, with its e-book *Decoding the Chinese Internet*, a wiki of subversive Chinese Internet language, and a steady stream of examples of user sarcasm against the Party-State cherry-picked from the closed Chinese Internet space. Websites such as Tea Leaf Nation or Chinese Human Rights Defenders also use their extensive contact networks within China to expose human rights abuses and growing censorship of online expression. Inside China, coded criticism is the rule and only a few timorous lawyers dare to take on Internet censorship cases. Clearly, censorship of politicized online content would not be as extensive as it is if rule of law were implemented in China.

It is because rule of law is robust in Europe that growing protest of the extensive use of executive power began appearing from numerous quarters. The French National Council on Digital Technology considered the 2014 online censorship law utterly ineffective in preventing terrorism and a real threat to online freedom of expression.[102] Legal scholars and technology specialists pointed out that the executive, rather than the judiciary, has

become the judge in matters pertaining to online terrorist content; that the technology used by the government to shut down sites was simplistic (censorship based on domain names only, without consideration of VPNs or the use of TOR, for example); that the Internet functioned as a window for investigators, allowing them to track careless content posted on these sites; and that the blacklist of censored sites would undoubtedly leak to the press, enhancing the prestige of their jihadist authors.[103] Reporters without Borders criticized the law as disproportionate, and France's anti-terrorism judge Marc Trévidic insisted that censorship of jihadist websites must remain within the boundaries of classic judicial procedures: the filtering of social media, an extremely vast and complex task, will undoubtedly prove to be inefficient, as the July 2016 attacks in Nice demonstrated, and very risky for freedom of expression with respect to other members of society.[104] Consequently, in order to protect all members of society, censorship functions best within a balance of powers framework that mitigates executive overreach, while protecting society's most vulnerable populations.

To conclude, we fully accept, as scholars and citizens, the necessity of online censorship to protect populations in an emergency. Moreover, states are obliged to protect vulnerable populations, particularly minors, from toxic online content that is hateful, violent or pornographic in nature. Given the crossover between physical and virtual worlds for many users, the Internet remains a powerful recruitment tool, one that is especially adept at influencing marginalized members of society whose online lives become richer in activity or excitement than their daily routines. Consequently, government censorship policies matter, providing an effective bulwark against extremism of all kinds.

While the apposite and contrasting profiles of the *contestataires* discussed in this chapter—educated, urban elites in China versus a marginalized or disaffected population in Europe—are particularly striking, these communities unquestionably posed a legitimate threat to their governments, aiming to replace the Party-State in China with a political plurality and the secular, democratically elected government in France with a religious caliphate. Nonetheless, online censorship in China and in Europe appeared to be unsuccessful in terms of proscribing content—the content remained available online for certain communities who knew how to avoid state censorship.

More importantly, political censorship poses a problem for larger groups in society that question the government's legitimacy in upholding constitutional values. Although in each case presented in this chapter censorship

targeted a particular group that represented a threat to the state, the fine line between protection of civilian populations and a proactive, paranoid state was not lost on users. While citizens may uphold the state's role as a guarantor of stability, many questioned the efficacy of the censorship methods used and the self-serving interests of the government in power.

We ask whether online censorship may pose more of a threat to state legitimacy than the content of the proscribed material that is removed from the Web. Challengers engage in a cat and mouse game, launching subversive material into cyberspace faster than the state can pull it down, underscoring the state's inability to counter what constitutes a virtual guerrilla war. Censorship of politicized cyber content appears to function only if the state is able to master its own proscription policies (an adequate number of censors, the proven ability to technically remove sites) and remains within very strict boundaries in terms of who is targeted (terrorists and not environmentalists, for example). In the case of Europe, these threats became real through a series of murderous terrorist attacks, despite ongoing state censorship. But, these threats materialized due to social and cultural exclusion, not in cyberspace, and online recruitment became most effective only once an individual met a jihadist in person or travelled to Syria or Yemen, where he or she became radicalized before returning to Europe. Consequently, the question remains one of balance: control of the digital space will not make a state more legitimate in the eyes of its citizens, and may even defeat the purpose of censorship in certain cases. In our next chapter, we extend the question of balance to the more general digital environment, to that of the Internet of Things, a virtual world where more machines are connected than people.

Notes

1. See Yang G. (2009) *The Power of the Internet in China: Citizen Activism Online*.
2. Florini A, Lai H. and Tan Y. (2012) *China Experiments: from Local Innovations to National Reform*; Xiao, Q. (2011) 'The Rise of Online Public Opinion and Its Impact', *in* Shirk, S. (ed.), *Changing Media, Changing China*; Yang (2009) *The Power of the Internet in China*.
3. Manners, I. (2008) 'The Normative Ethics of the European Union', *International Affairs*. Vol. 84, No. 1, pp. 45–60; Weber, A. (2014) *Manual on Hate Speech*, Council of Europe.

4. Following the execution of Chinese hostage Fan Jinghui in Mali on 19 November 2015, the authors noted a good deal of WeChat discussion focused on the need to protect Chinese citizens abroad through heightened security measures and those at home through censorship of online jihadist content.
5. See Ian Shapiro (2012) 'On Non-Domination', *University of Toronto Law Journal*. Vol 62, No. 3.
6. Matthew Bunn (2015) 'Reimagining Repression: New Censorship Theory and After', *History and Theory*, Vol. 54, February, pp. 25–44, p. 30.
7. Bunn, 'Reimagining Repression', p. 31.
8. Bunn, 'Reimagining Repression', p. 32.
9. John Stuart Mill (2008) *On Liberty* (Boston: Bedford St Martin's) p. 35.
10. Judith Butler (1997) *Excitable Speech: A Politics of the Performative* (New York: Routledge).
11. Bunn, 'Reimagining Repression', p. 27.
12. Beate Müller, ed. (2004) *Censorship and Cultural Regulation in the Modern Age* (Amsterdam: Rodopi).
13. China Digital Times (2016) 'Fifty Cent Party'.
14. Cornevin, C. (2016) 'Islamisme: 8250 individus radicalisés en France', *Le Figaro*, 3 February, p. 2.
15. China Internet Network Information Centre (2016) 'The 37th Statistical Report on Internet Development in China'.
16. World Economic Forum (2011) 'Global Information Technology Report: China'.
17. World Economic Forum (2015) 'Global Information Technology Report: China'.
18. Qiang, C. Z. (2007) 'China's Information Revolution: Managing the Economic and Social Transformation', The World Bank.
19. CNNIC (2012) 'The 30th Statistical Report on Internet Development in China'.
20. Eurobarometer (2016) E-communications and the Digital Single Market. Special Eurobarometer 438, p. 21. Retrieved June 22, 2016 from http://ec.europa.eu/information_society/newsroom/image/document/2016–22/sp438_eb84_2_ecomm_summary_en_15829.pdf
21. In the US, where freedom of speech is inscribed in the constitution, the first digital censorship case dates from 1994 and involved the distribution of obscene material over a bulletin board system. In 1996, the US Congress passed the Communications Decency Act (CDA), which punished the dissemination of 'indecent' material over the Internet. The Supreme Court struck down the law, however, ruling soon afterwards that the CDA abridged freedom of speech and therefore was unconstitutional.

22. Wang Fangfei (2014) 'Site-blocking Orders in the EU: Justifications and Feasibility', 14th Annual Intellectual Property Scholars Conference, Boalt Hall School of Law, University of California, Berkeley, 7–8 August.
23. Ang, P.H. (1997) 'How Countries Are Regulating Internet Content', 7th Annual Conference of the Internet Society, Kuala Lumpur', *Internet Society.*
24. Tan, Z., Mueller M., and Foster W. (1997) 'China's New Internet Regulations: two steps forward, one step back', *Communications of the ACM,* Vol. 40, No. 12, pp. 11–16.
25. Zheng, S., Ward, M.R. (2011) 'The Effects of Market Liberalization and Privatization on Chinese Telecommunications', *China Economic Review*, Vol. 22, No. 2, pp. 210–220.
26. Tai, Z. (2010) 'Internet Surveillance in China from Golden Shield to Green Dam', in Duarte, F., Firmino, R.J., and Ultramari, C. eds, *ICTs for Mobile and Ubiquitous Urban Infrastructures: Surveillance, Locative Media and Global Networks.* (Hershey, Pennsylvania: IGI Global), p. 239.
27. See, for example, the survey of the Global Internet Liberty Campaign. Global Internet Liberty Campaign (1998) 'Privacy and Human Rights: An International Survey of Privacy Laws and Practice', http://gilc.org/privacy/survey, date accessed 3 April 2016.
28. Lyon, D. (2001) 'Facing the future: Seeking ethics for everyday surveillance', Vol. 3, No. 3, pp. 171–181.
29. Amnesty International (2002) 'People's Republic of China: State Control of the Internet in China', Index number: ASA 17/007/2002, https://www.amnesty.org/en/documents/ASA17/007/2002/en, date accessed 3 April 2016.
30. House of Representatives (1994) Communications Assistance for Law Enforcement Act, 103rd Congress, 2nd Session, H.R. 4922.
31. Kelly, S., Cook, S. and Truong, M. eds. (2012) 'Freedom of the Net 2012: A Global Assessment of Internet and Digital Media', *Freedom House,* p. 131.
32. King, G., Pan, J., and Roberts, M.E. (2013) 'How Censorship in China Allows Government Criticism but Silences Collective Expression', *American Political Science Review,* Vol. 102, No. 2, pp. 1–18.
33. Kelly et al. (eds.) (2012) 'Freedom of the Net'.
34. It should be noted that, because most protocols are based on an acknowledgment system, it does not matter if the interference occurs with respect to the incoming or outgoing communication.
35. Agence France Presse (2014) China Has Massive Internet Breakdown Reportedly Caused By Their Own Censoring Tools', 23 January, http://www.businessinsider.com/chinas-internet-breakdown-reportedly-caused-by-censoring-tools-2014-1?IR=T, date accessed 3 April 2016.

36. Geo-blocking refers to the blocking of IP-addresses allocated to a specific geographical region.
37. European Commission (2016), 'Antitrust: e-commerce sector inquiry finds geo-blocking is widespread throughout EU', http://europa.eu/rapid/press-release_IP-16-922_en.htm, date accessed 4 April 2016.
38. For a more detailed discussion, see Clayton, R., Murdoch, S.J., and Watson R.N.M. (2006) 'Ignoring the Great Firewall of China', 6th Workshop on Privacy Enhancing Technologies Conference Paper, Cambridge; or Fallows, J. (2008) 'The Connection Has Been Reset', *The Atlantic*, March Issue.
39. See Fallows (2008) 'The Connection Has Been Reset', or Tan et al. (1997) 'China's New Internet Regulations'.
40. Bamman, D., O'Connor, B., and Smith, N (2012) 'Censorship and deletion practices in Chinese social media', *First Monday*, Vol. 17, No. 3, p. 2.
41. King et al. (2013) 'How Censorship in China Allows Government Criticism but Silences Collective Expression'.
42. China Daily Online (2015) 'Snapshot of Xi on making Internet an interconnected world'.
43. Yuen, S. (2015) 'Becoming a Cyber Power', *China Perspectives*, Vol. 2015, No. 2, pp. 53–58.
44. Shaohui, T. ed (2014) 'China inspects online videos in porn, rumour crackdown', *Xinhua*.
45. GreatFire.org, (2014) 'Authorities launch man-in-the-middle attack on Google', *GreatFire.org Blog*.
46. Yuan, G. (2015) 'Blocking VPN is for Internet safety: Official', *China Daily*.
47. Shaohui, T. ed (2015) 'China beefs up cyber police force', *Xinhua*.
48. Xinhua (2015) 'Sina faces suspension over lack of censorship', *China Daily*.
49. Jin, L. (2008) 'Chinese outline BBS sphere: What BBS has brought to China?' Thesis (S.M.) Massachusetts Institute of Technology, Dept. of Comparative Media Studies.
50. The online bulletin board is literally referred to as 'unnamed space' in Chinese. Weibo (Chinese Twitter) is the Chinese expression for 'microblog', whereas WeChat (the equivalent of WhatsApp) means 'micro message' in Chinese.
51. Lu, G. (2008) 'Old School BBS: The Chinese Social Networking Phenomenon', *ReadWrite*.
52. Lu, 'Old School BBS'.
53. CNNIC (2013) 'The 31st Statistical Report on Internet Development'.

54. Pihl, N. (2011) Why Sina Weibo is Winning. *Tech Rice*.
55. Hatton, C. (2016) 'Is Weibo on the way out?' *BBC China Blog*.
56. Yin, C. (2015) 'Push for real IDs to expand', *China Daily*.
57. Reuters (2015) 'China to ban online impersonation accounts, enforce real-name registration'.
58. UN General Assembly (1966) International Covenant of Civil and Political Rights, article 19.
59. For an interesting historical perspective, see Jonathan Spence (2001) *Treason by the Book* (London: Allen Lane History, Penguin Books).
60. National People's Congress (1982) Constitution of the People's Republic of China, Fifth National People's Congress, art. 35, § 1.
61. Constitution of the PRC, art. 41, § 1.
62. State Council of the People's Republic of China (1997) 'Computer Information Network and Internet Security, Protection, and Management Regulations', *State Council PRC,* Section 5.
63. Congressional Executive Commission on China (2002) 'International Agreements and Domestic Legislation Affecting Freedom of Expression', Order No. 292.
64. CECC (2002) 'PRC Legal Provisions: Regulations on the Administration of Internet Access Service Business Establishments'.
65. Congressional Executive Commission on China (2002) 'Interim Provisions on the Administration of Internet Publication', Article 17.
66. *sha ji jing hou*.
67. For a detailed account of arrested netizens from June 2014 to May 2015, see: https://freedomhouse.org/sites/default/files/resources/FOTN%202015_China%20%28new%29.pdf
68. *China Digital Times* (2013) 网传习近平8•19讲话全文:言论方面要敢抓敢管敢于亮剑.
69. Standing Committee (2015) 'China's Draft Cybersecurity Law', Nation's People's Congress of the People's Republic of China.
70. Cheung, J. (2015) 'China's great firewall just got taller', *Open Democracy*.
71. Xinhua (2016) 'China vows to make Party's voice strongest in cyberspace', *Xinhuanet*.
72. Council of Europe (1953) 'European Convention for the Protection of Human Rights and Fundamental Freedoms', 231 U.N.T.S. 222, art. 10.
73. Council of Europe (2003) 'Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems', *European Treaty Series*, No. 189, Strasbourg, entered into force entered into force 1 March 2006, art. 2(1).
74. McGonagle, T. (2015) 'Freedom of Expression: still a precondition for democracy?' Conference Report (Strasbourg: Council of Europe).

75. Secretary General of the Council of Europe (2015) 'State of Democracy, Human Rights and the Rule of Law in Europe: a shared responsibility for democratic security in Europe' (Strasbourg: Council of Europe), p. 10.
76. Secretary General of the Council of Europe, 'State of Democracy'.
77. Chapman, A. (2015) 'Don't Bring a Dove to a Polish Hawk Fight: as Poland readies for its presidential election, one thing is certain: Russia is a threat', *Foreign Policy.*
78. Associated Press (2015) 'Poland's Lawmakers Approve New Law on State Media Control', *Associated Press.*
79. Kandziora, K. (2016) 'Le théâtre menacé de censure en Pologne', *Arte.*
80. Bilewicz, M. et al. (2014) 'Hate speech in Poland 2014: summary of the national opinion poll', Stefan Batory Foundation, Warsaw.
81. *Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*, JORF n°0263 du 14 novembre 2014, p. 19162, texte n° 5, article 9.
82. *Loi no 2015-912 du 24 juillet 2015 relative au renseignement.* JORF no 0171 du 26 juillet 2015 page 12735, texte no 2.
83. Bekmezian, Hélène (2016) 'Le Sénat enterre la déchéance de nationalité', *Le Monde*, 17 March.
84. Laurent, Samuel (2015) 'Etat d'urgence: la carte des perquisitions administratives', *Le Monde*, 21 December.
85. Perry, S., and Roda, C. (2013) 'Conceptualizing and Contextualizing the Changing Nature of Internet Usage in China', China and the New Internet World: The Eleventh Chinese Internet Research Conference (CIRC11).
86. The online *China Digital Times,* edited by scholar Xiao Qiang, provides a detailed list of political codes devised by online dissidents and used by many netizens, Xiao Q. (2013) 'The Grass-Mud Horse Lexicon: Translating the Resistance Discourse of Chinese Netizens', *China Digital Times.*
87. Xiao, 'The Grass-Mud Horse Lexicon'.
88. Tai, Z. (2006) *The Internet in China: Cyberspace and Civil Society;* Zhou, Y. (2006) *Historicizing Online Politics: Telegraphy, the Internet and Political Participation in China*; Lu, J. and Weber, I. (2007) 'Internet and self-regulation in China: The cultural logic of controlled commodification', *Media Culture & Society,* Vol. 29, No. 5, pp. 772–789;
Zheng, Y. (2008) *Technological Empowerment: The Internet, State, and Society in China*; Zhang, X. and Zheng, Y. eds. (2009) *China's Information and Communications Technology Revolution: Social Changes and State Responses*; Yang (2009) *The Power of the Internet in China*; Jiang, M. (2010) 'Spaces of authoritarian deliberation: Online public deliberation in China', in He, B. and Leib, E.J. eds. *The Search for*

Deliberative Democracy in China (New York: Palgrave MacMillan), pp 261–287; Lei, Y. (2011) 'The political consequences of the rise of the Internet: Political beliefs and practices of Chinese netizens', *Political Communication*, Vol. 28, No. 3, pp. 291–322; Shirk, S. ed. (2011) *Changing Media, Changing China*; Esarey A., and Xiao, Q (2011) 'Digital Communication and Political Change in China', *International Journal of Communication*, Vol. 5, pp. 289–319.

89. Ng, T. (2015) 'Chinese celebrity's air pollution video stirs online dust-up', *South China Morning Post*.
90. Einhorn, B. (2013) 'World of Warcraft No Longer Rules in China', *Bloomberg*, 11 July.
91. Our graduate student, Francisco Vassallo, ran a World of Warcraft online forum survey in 2015 of 152 respondants which revealed very little government censorship, although users indicated that they were cautious online.
92. See Kepel, G. (2015) *Passion française: les voix des cités* (Paris: Gallimard).
93. Authors' interview with Ziad Majed, 11 December 2015, Paris. See Majed, Z. (2014) *Syrie, La Révolution Orpheline*, Paris: Actes Sud et l'Orient des Livres.
94. Cazeneuve, B., *et al.* (2016) 'La Lutte Contre le Terrorisme', Statement, 8 March.
95. Bouzar, D., Caupenne, C., Valsan, S. (2014) *La Metamorphose operée chez le jeune par les nouveaux discours terroristes*. Paris: CPDSI.
96. Cornevin, C. (2016) 'Islamisme: 8250 individus radicalisés en France', *Le Figaro*, http://www.lefigaro.fr/ (home page), date accessed 3 February 2016.
97. See the Stop Djihadisme Index at http://www.stop-djihadisme.gouv.fr/index.html.
98. French scholar Alain Bertho claims that he was, in fact, the first to use this expression. Bertho, A. (2016) 'De la rage sans espoir au martyre: penser la complexité du jihadisme, *Libération*, 25 March, pp. 22–23.
99. Burgat, F. (2015) 'Réponse à Olivier Roy; les non-dits de « l'islamisation de la radicalité »', *L'Obs avec Rue 89*.
100. Kepel, G. (2015) *Passion française: les voix des cités*.
101. Conseil National Numérique (2014) 'Avis n°2014-3 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme', *Conseil National Numérique*, 15 July.
102. Poncet, G. (2014) 'La France, en route vers la censure d'Internet', *Le Point*.
103. Sénat de la République Française (2016) 'Le contrôle et l'évaluation des dispositifs législatifs relatifs à la sécurité intérieure et à la lutte contre le terrorisme: Annexes', *Sénat de la République Français*, http://www.senat.fr/ (home page), date accessed 17 January 2016.

Bibliography

Agence France Presse. (2014). China has massive internet breakdown reportedly caused by their own censoring tools. January 23. Retrieved April 3, 2016, from http://www.businessinsider.com/chinas-internet-breakdown-reportedly-caused-by-censoring-tools-2014-1?IR=T

Amnesty International. (2002). People's Republic of China: State control of the internet in China. Index number: ASA 17/007/2002. Retrieved April 3, 2016, from https://www.amnesty.org/en/documents/ASA17/007/2002/en

Ang, P.H. (1997). *How countries are regulating internet content*. 7th Annual Conference of the Internet Society, Kuala Lumpur. Internet Society. Retrieved March 17, 2016, from http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM

Associated Press. (2015) Poland's lawmakers approve new law on state media control. *Associated Press*. Retrieved December 30, 2015, from http://www.ap.org (home page).

Bamman, D., O'Connor, B., & Smith, N. (2012). Censorship and deletion practices in Chinese social media. *First Monday*, *17*(3), 2.

Bekmezian, H. (2016, March 17). Le Sénat enterre la déchéance de nationalité. *Le Monde*.

Bertho, A. (2016, March 25). De la rage sans espoir au martyre: penser la complexité du jihadisme. *Libération*.

Bilewicz, M., Marchlewska, M., Soral, W., Winiewski, M. (2014). Hate speech in Poland 2014: Summary of the national opinion poll. Stefan Batory Foundation, Warsaw. Retrieved March 17, 2016, from http://www.ngofund.org.pl (home page).

Bouzar, D., Caupenne, C., & Valsan, S. (2014). *La Metamorphose operée chez le jeune par les nouveaux discours terroristes*. Paris: CPDSI.

Bunn, M. (2015, February). Reimagining repression: New censorship theory and after. *History and Theory, 54*, 25–44.

Burgat, F. (2015, December 1). Réponse à Olivier Roy: les non-dits de l'islamisation de la radicalité. *L'Obs avec Rue 89*.

Butler, J. (1997). *Excitable speech: A politics of the performative*. New York: Routledge.

Cazeneuve, B., et al. (2016, March 8). La Lutte Contre le Terrorisme, Statement. *Gouvernement.fr*. Retrieved March 17, 2016, from http://www.gouvernement.fr/action/la-lutte-contre-le-terrorisme

Chapman, A. (2015). Don't bring a dove to a Polish hawk fight: As Poland readies for its presidential election, one thing is certain: Russia is a threat. *Foreign Policy*. Retrieved May 9, 2015, fromhttp://foreignpolicy.com/2015/05/09/dont-bring-a-dove-to-a-polish-hawk-fight-presidential-election-russia-ukraine http://foreignpolicy.com (home page).

Cheung, J. (2015). China's great firewall just got taller. Open democracy. Retrieved July 14, 2015, from https://www.opendemocracy.net (home page).
China Daily Online (2015). Snapshot of Xi on making internet an interconnected world. Retrieved January 6, 2016, from http://www.chinadaily.com.cn/china/2015-12/11/content_22692734_7.htm
China Digital Times. (2016). Fifty cent party. Retrieved March 19, 2016, from http://chinadigitaltimes.net/space/Fifty_Cent_Party
China Internet Network Information Center. (2012). The 30th Statistical report on internet development in China. Retrieved January 31, 2013, from http://www1.cnnic.cn (home page).
China Internet Network Information Center. (2013) The 31st Statistical report on internet development in China. Retrieved January 31, 2013, from http://www1.cnnic.cn (home page).
China Internet Network Information Center. (2016) The 37th Statistical report on internet development in China. Retrieved March 17, 2016, from http://www1.cnnic.cn (home page).
Clayton, R., Murdoch, S. J., & Watson R. N. M. (2006). *Ignoring the great firewall of China*. 6th Workshop on Privacy Enhancing Technologies Conference Paper, Cambridge.
Congressional Executive Commission on China. (2002a) Interim provisions on the administration of internet publication, Article 17, CECC. Retrieved March 17, 2016, from http://www.cecc.gov (home page).
Congressional Executive Commission on China. (2002b) International agreements and domestic legislation affecting freedom of expression. Order No. 292, CECC. Retrieved March 17, 2016, from http://www.cecc.gov (home page).
Congressional Executive Commission on China. (2002c). PRC legal provisions: Regulations on the administration of internet access service business establishments. CECC. Retrieved March 17, 2016, from http://www.cecc.gov (home page).
Conseil National Numérique. (2014, July 15). Avis n°2014-3 sur l'article 9 du projet de loi renforçant les dispositions relatives à la lutte contre le terrorisme. *Conseil National Numérique*.
Cornevin, C. (2016, February 3). Islamisme: 8250 individus radicalisés en France. *Le Figaro*.
Council of Europe. (1953). European convention for the protection of human rights and fundamental freedoms. 231 U.N.T.S. 222, Article 10, *Council of Europe*, Rome.
Council of Europe. (2003). Additional protocol to the convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. *European Treaty Series*, 189.

Einhorn, B. (2013). World of warcraft no longer rules in China. *Bloomberg*. Retrieved July 11, 2016, from http://www.bloomberg.com/bw/articles/2013-07-11/world-of-warcraft-no-longer-rules-in-china

Esarey, A., & Xiao, Q. (2011). Digital communication and political change in China. *International Journal of Communication, 5*, 289–319.

European Commission. (2016). Antitrust: E-commerce sector inquiry finds geo-blocking is widespread throughout EU. Retrieved April 4, 2016, from http://europa.eu/rapid/press-release_IP-16-922_en.htm

Eurostat. (2015). Information society statistics—households and individuals. Retrieved April 3, 2016, from http://ec.europa.eu/eurostat/statistics (homepage).

Fallows, J. (2008, March). The connection has been reset. *The Atlantic*.

Florini, A., Lai, H., & Tan, Y. (2012). *China experiments: From local innovations to national reform*. Washington, DC: Brookings Institute.

Freedom House. (2015). Freedom on the net: China. *Freedom House*. Retrieved March 18, 2016, from https://freedomhouse.org/report/freedom-net/2015/china

Global Internet Liberty Campaign. (1998). Privacy and human rights: An international survey of privacy laws and practice. Retrieved April 3, 2016, from http://gilc.org/privacy/survey

GreatFire.org. (2014). Authorities launch man-in-the-middle attack on Google. *GreatFire.org Blog*. Retrieved January 6, 2016, from https://en.greatfire.org/blog/2014/sep/authorities-launch-man-middle-attack-google

Hatton, C. (2016). Is Weibo on the way out? *BBC China Blog*. Retrieved January 6, 2016, from http://www.bbc.com/news/blogs-china-blog-31598865

House of Representatives. (1994). Communications Assistance for Law Enforcement Act, 103rd Congress, 2nd Session, H.R. 4922, The Library of Congress. Retrieved March 13, 2016, fromhttp://thomas.loc.gov/cgi-bin/query/z?c103:H.R.1494.IH: https://www.loc.gov (home page).

Jiang, M. (2010). Spaces of authoritarian deliberation: Online public deliberation in China. In B. He & E. J. Leib (Eds.), *The search for deliberative democracy in China* (pp. 261–287). New York: Palgrave Macmillan.

Jin, L. (2008). *Chinese outline BBS sphere: What BBS has brought to China?* Thesis (S.M.), Massachusetts Institute of Technology, Dept. of Comparative Media Studies.

Kandziora, K. (2016). Le théâtre menacé de censure en Pologne, *Arte*. Retrieved March 17, 2016, from http://info.arte.tv/fr/tentative-de-censure-wroclaw

Kelly, S., Cook, S., & Truong, M. Eds. (2012). Freedom of the Net 2012: A global assessment of internet and digital media. *Freedom House*, p. 131.

Kepel, G. (2015). *Passion française: les voix des cités*. Paris: Gallimard.

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review, 102*(2), 1–18.

Kunzru, H. (1997, January 6). Austria turns off. *Wired Magazine*. Retrieved April 3, 2016, from http://www.wired.com/1997/06/austria-turns-off

Laurent, S. (2015, December 21). Etat d'urgence: la carte des perquisitions administratives. *Le Monde*.

Lei, Y. (2011). The political consequences of the rise of the internet: Political beliefs and practices of Chinese netizens. *Political Communication, 28*(3), 291–322.

Loi no. 2014-1353. (2014). *Renforçant les dispositions relatives à la lutte contre le terrorisme*, JORF n°0263 du 14 novembre 2014', Article 9, p. 19162, Texte n° 5.

Loi no. 2015-912. (2015). *Relative au renseignement*, JORF n°0171 du 26 juillet 2015', p. 12735, Texte n° 2.

Lu, G. (2008). Old school BBS: The Chinese social networking phenomenon. *ReadWrite*. Retrieved March 17, 2016, from http://readwrite.com/2008/01/16/bbs_china_social_networking

Lu, J., & Weber, I. (2007). Internet and self-regulation in China: The cultural logic of controlled commodification. *Media Culture & Society, 29*(5), 772–789.

Lyon, D. (2001). Facing the future. *Seeking ethics for everyday surveillance, 3*(3), 171–181.

Majed, Z. (2014). *Syrie, La Révolution Orpheline*. Paris: Actes Sud et l'Orient des Livres.

Manners, I. (2008). The normative ethics of the European Union. *International Affairs, 84*(1), 45–60.

McGonagle, T. (2015). Freedom of expression: Still a precondition for democracy? Conference Report, Strasbourg, Council of Europe. Retrieved March 16, 2016, from http://www.ivir.nl/publicaties/download/1707

Mill, J. S. (2008). *On liberty*. Boston, MA: Bedford St Martin's.

Müller, B. (Ed.). (2004). *Censorship and cultural regulation in the modern age*. Amsterdam: Rodopi.

National People's Congress. (1982). Constitution of the People's Republic of China, Fifth National People's Congress. Retrieved January 10, 2015, from http://en.people.cn/constitution/constitution.html

Ng, T. (2015). Chinese celebrity's air pollution video stirs online dust-up. *South China Morning Post*. Retrieved February 25, 2016, from http://www.scmp.com (home page).

Perry, S., & Roda, C. (2013). *Conceptualizing and contextualizing the changing nature of internet usage in China. China and the new internet world*. The Eleventh Chinese Internet Research Conference (CIRC11), Oxford Internet Institute, Oxford.

Pihl, N. (2011). Why Sina Weibo is winning. *Tech Rice*.

Poncet, G. (2014). La France, en route vers la censure d'Internet. *Le Point*. Retrieved March 17, 2016, from http://www.lepoint.fr (home page).

Qiang, C. Z. (2007). China's information revolution: Managing the economic and social transformation. The World Bank. Retrieved March 17, 2016, from http://www.worldbank.org (home page).

Reuters. (2015). China to ban online impersonation accounts, enforce real-name registration. Thomson Reuters. Retrieved January 6, 2016, from http://uk.reuters.com (home page).

Secretary General of the Council of Europe. (2015). State of democracy, human rights and the rule of law in Europe: A shared responsibility for democratic security in Europe. *Council of Europe*, p. 10.

Sénat de la République Française. (2016). Le contrôle et l'évaluation des dispositifs législatifs relatifs à la sécurité intérieure et à la lutte contre le terrorisme: Annexes, *Sénat de la République Français*. Retrieved January 17, 2016, from http://www.senat.fr/ (home page).

Shaohui, T. (2014). China inspects online videos in porn, rumour crackdown. *Xinhua*. Retrieved January 6, 2016, from http://news.xinhuanet.com/english/china/2014-11/06/c_133771062.htm

Shaohui, T. (2015). China beefs up cyber police force. *Xinhua*. Retrieved January 6, 2016, from http://news.xinhuanet.com/english/2015-08/12/c_134509062.htm

Shapiro, I. (2012). On non-domination. *University of Toronto Law Journal, 62*(3), 293–336.

Shirk, S. (Ed.). (2011). *Changing media, changing China*. New York: Oxford University Press.

Spence, J. (2001). *Treason by the book*. London: Allen Lane History, Penguin Books.

Standing Committee. (2015). China's draft cybersecurity Law. National People's Congress of the People's Republic of China. Retrieved March 17, 2016, from http://chinalawtranslate.com/cybersecuritydraft

State Council of the People's Republic of China. (1997). Computer information network and internet security, protection, and management regulations. *State Council PRC*, Section 5.

Stop-Dijihadism. (2015). Stop djihadisme index. Gouvernement.fr. Retrieved December 30, 2015, from http://www.stop-djihadisme.gouv.fr/index.html

Tai, Z. (2006). *The internet in China: Cyberspace and civil society*. New York: Routledge.

Tai, Z. (2010). Internet surveillance in China from golden shield to green dam. In F. Duarte, R. J. Firmino, & C. Ultramari (Eds.), *ICTs for mobile and ubiquitous urban infrastructures: Surveillance, locative media and global networks*. Hershey, PA: IGI Global.

Tan, Z., Mueller, M., & Foster, W. (1997). China's new internet regulations: Two steps forward, one step back. *Communications of the ACM, 40*(12), 11–16.

United Nations General Assembly. (1966). International Covenant of Civil and Political Rights, G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171, *entered into force* 23 March 1976, article 19.

Wang F. (2014, August 7–8). *Site-blocking orders in the EU: Justifications and feasibility*. 14th Annual Intellectual Property Scholars Conference (IPSC), Boalt Hall School of Law, University of California, Berkeley.

Weber, A. (2014). *Manual on hate speech*. Strasbourg: Council of Europe.

World Economic Forum. (2015). Global information technology report: China. *World Economic Forum*. Retrieved March 17, 2016, from http://www.weforum.org (home page).

Xi, J. (2013). Outline of Xi Jinping's speech at the National Propaganda and Ideology Work Conference (网传习近平8•19讲话全文:言论方面要敢抓敢管敢于亮剑). *China Digital Times. Retrieved October 23, 2016 from http://chinadigitaltimes.net/chinese/2013/11*

Xiao, Q. (2011). The rise of online public opinion and its impact. In S. Shirk (Ed.), *Changing media, changing China*. New York: Oxford University Press.

Xiao Q. (2013). The grass-mud horse lexicon: Translating the resistance discourse of Chinese netizens. *China Digital Times*. Retrieved March 17, 2016, from http://chinadigitaltimes.net (home page).

Xinhua. (2015). Sina faces suspension over lack of censorship. *China Daily*. Retrieved January 6, 2016, from http://www.chinadaily.com.cn/business/tech/2015-04/11/content_20410487.htm

Xinhua. (2016). China vows to make Party's voice strongest in cyberspace. *Xinhuanet*. Retrieved January 17, 2016, from http://news.xinhuanet.com/english/2016-01/07/c_134986363.htm

Yang, G. (2009). *The power of the internet in China: Citizen activism online*. New York: Columbia University Press.

Yin, C. (2015). Push for real IDs to expand. *China Daily*. Retrieved January 14, 2015, from http://usa.chinadaily.com.cn/china/2015-01/14/content_19312751.htm

Yuan, G. (2015). Blocking VPN is for internet safety: Official. *China Daily*. Retrieved January 6, 2016, from http://usa.chinadaily.com.cn (home page).

Yuen, S. (2015). Becoming a cyber power. *China Perspectives, 2015*(2), 53–58.

Zhang, X., & Zheng, Y. (Eds.). (2009). *China's information and communications technology revolution: Social changes and state responses*. London: Routledge.

Zheng, S., & Ward, M. R. (2011). The effects of market liberalization and privatization on Chinese telecommunications. *China Economic Review, 22*(2), 210–220.

Zheng, Y. (2008). *Technological empowerment: The internet, state, and society in China*. Stanford, CA: Stanford University Press.

Zhou, Y. (2006). *Historicizing online politics: Telegraphy, the internet and political participation in China*. Stanford, CA: Stanford University Press.

CHAPTER 5

The Internet of Things

Contrary to the popular perception, the Internet of Things is a physical reality. Often imagined as an amorphous interconnection of machines and people, it generates, stores, transmits and analyses data through physical infrastructure that influences decision-making processes. Decision-making was once the sole purview of humans; today machines organize the bulk of our choices, in an array of activities ranging from an automatic bank withdrawal to putting on the seatbelt in a computerized automobile. This new reality of the physical interconnectivity of machines and data is one that, at first glance, appears to have no precedent in law. This chapter will argue that the legal framework necessary for maintaining our human autonomy and living in harmony with an automated world is already in place. The international human rights body of treaty and customary law provides a principled reference for determining the subordinate place of machines in a digitized environment, but the existing law must be applied to new circumstances. This chapter will present three scenarios of life in a digital world of the not-so-distant future, a future where technology provides relief and autonomy for certain individuals, while subjugating others to subtle forms of discrimination or dependence. It will then discuss the technology embedded in our scenarios and examine some of the major legal principles invoked by the Internet of Things. These scenarios demonstrate the need to engage in a rigorous, comprehensive assessment of ubiquitous technology use in order to preserve our global public goods and individual rights in a digitized world.

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_5

The Internet of Things (IoT) is not virtual, but physical—a complex infrastructure of material hardware, electronic signals, and electromagnetic emissions that generates, stores, transmits and analyses data. The interconnectivity of humans and objects reached a milestone in 2008, the first year when more machines were connected than people.[1] This unprecedented paradigm has led many public officials to ask whether brand new legislation is needed to address the IoT or if legislative plans already under consideration or in place could be adjusted to include this amorphic phenomenon.[2] Chapter 5 will examine the physicality of the IoT, arguing that the international human rights body of treaty and customary law provides a principled reference for determining the subordinate place of machines in a digitized environment, but that existing law must be reinterpreted to apply to new circumstances.

In our previous chapters, we examined the potential health consequences of wireless infrastructure, the privacy impacts of government security systems, and the effectiveness of digital censorship. This chapter will explore these same issues within the realm of interconnected objects. The IoT encompasses human-computer interaction, device-to-device interaction, and human-data interaction,[3] but also raises broader questions of how we construct the public space, how we perceive the social contract between governments and citizens, and why human autonomy is vital in a digital environment. Throughout this chapter, we use the term 'machine' to describe the hardware and software technology that surrounds us and is embedded within the connected objects that form the IoT. Although 'machine' is a loaded term in contemporary philosophy,[4] it is one that enables us to situate our relationship with digital technology within the broader historical arc of human-machine interaction. We define data as an output of this interconnectivity that belongs to the individual who generates the information, rather than the entity that controls its use. Data is physical in two respects: first, this chapter posits that personal data functions much like intellectual property in that it is owned by the human who produces it; second, data generation, transmission, analysis and storage require complex hardware systems that have a physical address, one that enables us to assign a geographic jurisdiction to a good deal of human-data interaction. To better understand the challenges posed by the IoT, this chapter presents three scenarios of life in a digital world of the not-so-distant future, a future where technology provides relief and autonomy for certain individuals, while subjugating others to oblique forms of discrimination or—what is worse—a loss of human autonomy. This chapter then examines

the framing of certain foundational principles in ethics and international law, such as our interpretation of what constitutes a global public good and how Rousseau's social contract may be extended to machines in the context of a digital environment. We suggest the need to engage in a rigorous, comprehensive assessment of ubiquitous technology use in order to preserve our democratic institutions and individual, human rights.

5.1 Internet of Things Scenario One: Enabling the Disabled

It is 7.00 am and Adil is woken up by the usual sound of his alarm. Getting up is not a problem this morning. He smiles to himself; who would have ever imagined that having to stop by City Hall before work would put him in such a good mood? He gets out of bed and heads to the shower room. With an automatic everyday reflex, he touches the soap holder before getting under the shower to make sure the soap is there and then turns on the water. He knows that he will have to hurry if he does not want to be late to work. He will skip breakfast. As he heads out the door, Adil wonders where he put his house keys: not in his coat pocket as they should be! He reaches for his phone and asks 'where are the house keys?' A beeping sound comes from the kitchen and, as he approaches, the telephone says 'to your left'. Adil picks up the keys from the kitchen table and leaves in a hurry. Warsaw's sidewalks are already quite crowded. Adil's phone warns him of red lights and some roadwork on the way to the bus stop. He tells the phone that he intends to go to City Hall and once he reaches the stop, the phone informs him that his bus is seven minutes away. After about seven minutes a bus arrives, but the phone announces that this is not the 74 bus going to the City Hall, but another one. As the 74 finally approaches, Adil's phone informs him that this is the correct bus. He boards the bus and, seeing his white cane, a lady invites him to sit in her place. As he nears City Hall, the phone activates a stop request for the bus and tells Adil to get ready to disembark. Once on the street, the phone gives him the right directions to reach his destination. Inside the municipal building, Adil indicates to the phone that he needs to go to the Registry Office, where his phone then guides him to a machine that allows him to book his turn in line. He will be able to pick up his birth certificate in order to complete the paperwork for his upcoming wedding ceremony. Wedding licences are not yet digitized.

5.2 Wireless Technology

The above scenario, one in which visually impaired people receive personalized assistance allowing them to independently navigate a city both indoors and out, is not science fiction. With its Virtual Warsaw project, aiming 'to give the visually impaired greater freedom of movement across the city, particularly in the use of public transport and public facilities',[5] the city of Warsaw (Poland) was one of the winners of the Bloomberg Philanthropies 2014 Mayors Challenge. A successful indoor pilot has been run with disabled users demonstrating the feasibility of the project. Technology similar to that used in Warsaw is also being applied by other cities to supply services to their citizens. For example, Bucharest is implementing a service to enable use of the public transport system by the visually impaired.[6]

These systems are based on providing location-context information to the user. In order to do this, they are generally designed with two components: (1) a set of transmitters emitting signals that can be used to identify the position of the user; and (2) a device—normally a smart phone or other enabled mobile device—that runs applications capable of detecting the signals and communicating the appropriate information to the user. In outdoor contexts, systems of this type have been available for quite some time and they use the signal received from the Global Positioning System (GPS) to help users navigate to their destinations, share their location with other users,[7] or find nearby interesting places to visit.[8] GPS works thanks to a set of satellite signals that, once transmitted and interpreted by the appropriate application, can be used to determine the device position on earth, as well as its orientation and direction. GPS-based applications, however, have been problematic to use indoors because the signal is often significantly attenuated or even completely unavailable inside buildings (normally the receiver needs a signal from at least four satellites to be able to compute its location). Under these conditions, because the accuracy of position detection is degraded by signal attenuation, location information, even if available, is no longer accurate enough to be used by a location-based application. For these reasons, several wireless technologies have been developed to support indoor location detection: amongst the most common are RFID (radio frequency identification), NFC (near field communication) and Bluetooth. Each one of these technologies has characteristics that are best adapted to specific applications. These technologies may also be used in combination, or with GPS.

An RFID tag produces a radio signal that can be read by a special reader located no more than a few metres away. While RFID has been broadly applied (for example, in travel cards, tracking of animals and goods, or anti-theft tags) and was initially considered the right technology to accelerate the widespread use of the IoT, imperfect reliability has slowed down its application.[9] Just like RFID, NFC allows interaction with special labels or tags, but is much more widely integrated into consumer devices and supports two way communication (NFC-enabled devices may both receive signals and emit them); nonetheless, NFC has a very short communication distance of just a few centimetres.

Bluetooth is more widely applicable than RFID and NFC, because it supports two way communication and can regularly reach distances of five to ten metres (or even 20–30 metres, depending on the quality of the device).[10] Bluetooth is already widely used and available on most mobile phones and consumer electronic devices; for example, consumers can play music from a mobile phone through the audio system of a car or use a wireless mouse or keyboard with the computer via Bluetooth technology. One of the major problems with Bluetooth has been the high power consumption of devices using this type of communication. However, Bluetooth low energy (BLE) technology addresses the energy problem by providing considerably reduced power consumption and cost while maintaining a similar communication range.[11]

The city of Warsaw has implemented the services mentioned above using beacon technology based on BLE, which is both low cost and low power: a beacon transmits signals revealing its identity (and possibly other information, such as a URL). The signals are received by devices that recognize their proximity to the beacon and may deliver a specific service. In the scenario above, a beacon may signal to Adil's phone that he has entered City Hall; the phone contains an application which has a map of the municipal building, and uses signalled location information to guide him to the appropriate office. As Adil walks towards the right office, other beacons along the way indicate his new position so that directions can be provided on a continual basis.

An important difference between beacon technology and GPS is that beacons do not send location coordinates, but self-identifying information. It is up to the application on the mobile device to decide what to do once it knows it is near a beacon with a specific identity. For example, in the museum scenario below, a designated beacon may identify the nineteenth century European paintings area and, when recognized by the museum

application, trigger the display of video and audio descriptions relevant to that area. If the app is running on a smart phone and has access to the default language for the phone, then the information can be adapted to the language of the user. If the app has access to further information, such as the art history expertise of the phone owner, or the fact that the owner has visited several recent exhibitions on European painters, then it can further customize the presentation.

5.3 Internet of Things Scenario Two: Tracking User Profiles

Lydia and Sarah live in Paris in the same neighbourhood and are both 21 years old. They have not met and probably never will. Lydia, the daughter of a wealthy banker, is finishing her undergraduate degree in art history at a private university where she also met Larry, her boyfriend. Sarah works as a waiteress in a café, and in her spare time volunteers with Free Access, an association that provides help to illegal migrants. On Sunday, Lydia and Larry decide to go to a municipal fine arts museum at the same time as Sarah and her friend Sally. In order to enter the museum, they all need to download the app which allows them to pay the entrance fee and open an automatic entry gate with a barcode; the app is designed to then guide them through the exhibition. Lydia and Larry are charged a discounted fee because the app recognizes them as students, while Sarah and Sally pay the normal entrance fee. Once inside, Sarah and Sally are guided through a short tour of the museum's main works of art, while Lydia and Larry are led through many more rooms that are reserved for visitors with a strong background in the humanities; the app recognizes their education level and academic specialization through the university's digital badge that provided them with their student entry discount.[12] The curators, in fact, have decided that access to certain rooms should be limited to art historians in order to ensure that experts are able to view the art in uncrowded rooms, an their experience is enhanced by the detailed information available on their phones.

Over the past six months, Sarah's smartphone has repeatedly sent geo-localization signals from the offices of Free Access and even during a march for migrant rights, thus the app recognizes her commitment to the cause of illegal migrants. Once inside the museum, Sarah and Sally regularly approach museum beacons at the same time, so the app on their phones (which also exchanges information with the apps of other

visitors) recognizes that they are visiting the exhibition together. As Sarah and Sally approach the end of the exhibition, they are both guided into a room with a government-sponsored documentary on illegal migration that focuses on the dangers involved in helping illegal immigrants and the threat migration poses to the nation's identity and economic development. When Lydia and Larry reach the end of their museum tour, their apps display an invitation to an upcoming conference on 'Arts in Society' and a discounted entrance to several other exhibitions in town.

5.4 Location Privacy Issues

Mobile phones continuously try to establish contact with nearby towers by emitting a signal or beacon; the towers, in turn, coordinate the targeting of their signals so that the one positioned to provide the strongest signal takes charge of the telephone service. Telecom companies usually collect this data and locate the phone. A GPS-enabled phone or the GPS in cars will provide the company with more precise information about the user's location. Until recently, however, it was difficult to track people inside buildings with a sufficient level of accuracy; but the indoor localization services described above now make this possible. Furthermore, unlike mobile phone operators, location-based service providers often have a business model based on reusing or selling information collected thanks to the users' agreement to provide their location. Even when users do not explicitly share their location, probe requests to networks other than mobile phone networks constitute an increasing challenge to privacy because the Wi-Fi and Bluetooth chips in these devices are assigned a unique identifier, called a MAC (media access control) address. This address identifies each device communicating on the network; when Wi-Fi or Bluetooth is activated, the chips regularly send out a probe request to discover nearby Wi-Fi access points or Bluetooth devices. Probe requests are unique identifiers as they contain the MAC address of the mobile device in use, and may also include a list of preferred Wi-Fi networks accessed by the device in the past. A tracking system for Wi-Fi or Bluetooth can reliably infer the position of an individual carrying the device, even if not connected to a network, by listening for these discovery requests and collecting the MAC address.

The privacy issues associated with the identification of MAC addresses are well-known to information technology companies and have been studied by researchers.[13] Julien Freudiger, for example, concludes a

detailed study aimed at quantifying possible privacy breaches caused by Wi-Fi probe requests by noting that 'as of 2015, billions of smartphones in the world are publicly broadcasting their unique identifiers at a high frequency. Although wireless network discovery is an important problem, privacy consequences seem at odds with technical gains associated with active network discovery'.[14] He found that the frequency of the probe signal (how often the device will try to find a network) varies depending on the device and operating system and he highlights that the more frequent the signal, the more likely users will be located and identified. Freudiger also points out that the broadcasting of previously used networks, which is common in probe signals, constitutes a further privacy threat. When introducing its operating system iOS 8, Apple widely publicized a feature that automatically randomizes MAC addresses when their devices search for a Wi-Fi network. This feature was explicitly designed to make it much more difficult to track a device through data collection of access points to Wi-Fi networks.[15] While as of this writing Apple is the only company providing MAC address randomization for its devices, this feature still does not afford real protection for the user. On the one hand, the current implementation of Apple's MAC randomization service has little impact on tracking services.[16] On the other hand, several observers report that the conditions under which MAC address randomization actually occur are so strict that only a few users will benefit from privacy protection. For example, randomization only takes place when the device is locked (every time the device wakes up and goes back to sleep, a new MAC address is generated), location services are disabled, and mobile phone data connections are disabled.[17] These conditions make it very unlikely that randomization would actually happen in most situations. Finally, researchers have reported that it is possible to re-identify iOS randomized MAC addresses by using sequence numbers in probe requests.[18]

While mobile communication is essential for the implementation of the IoT, the privacy issues connected with its current implementation are so vast that the Electronic Frontier Foundation, a leading non-profit-making organization defending civil liberties in the digital world, equates one of the most important corporate actions towards the protection of user privacy, Apple's move to limit mobile device location tracking, to 'something like opening an umbrella in the middle of a hurricane'.[19] The issue of privacy, as depicted in scenario two, is a much larger societal issue which relates not only to free access to information, but also to freedom of association and expression and possible discrimination. Sarah and Sally are

discouraged from accessing certain rooms in the museum and the chance to see the art hung in these rooms is negated by the very design of the application that guides their visit; moreover, they might never know they have only seen a small part of the exhibition. In other words, the application reinforces 'by design' the knowledge separation between those who have access to higher education and those who do not. Furthermore, Sally and Sarah were both guided towards a government-sponsored film aimed at limiting their individual freedom of association through a negative portrayal of their charitable work. The design of the application reinforces certain values and social patterns by targeting those who are perceived as a threat to the social order.

5.5 Legal Ownership of Global Public Goods

In addition to potential health and privacy issues, our first two scenarios share several common themes that are of pivotal importance for humans living in a digital environment. The protagonists rely on digital technology to enhance their everyday living experience, and this experience is more positive for some than for others. All of our characters traverse public areas (City Hall or a museum) that have privatized air space. Governments rent out air, a global public good according to international law, to technology companies in order to accommodate the bandwidth needed for the wireless transmission of information. In much the same way that a state might rent out a concession stand in a public park, governments and businesses work in partnership to provide wireless access to users. The difference between a concession stand and the rental of air space is a question of degree: although the concession stand might sell snacks that are high in saturated fats, the consumer can refuse to purchase unhealthy food. Choice is not an option, however, with respect to electromagnetic wave frequencies, which connect citizens and machines everywhere night and day. In addition to the rental of airspace for the transmission of bandwidth, states and technology companies also manipulate personal data in order to provide much-needed or desired services to someone like Adil, or to monitor individual activity and personal communication to promote public 'security', as in the case of Sarah. For those users who are either permanently or temporarily disabled, manipulation of their location data enables them to partially overcome their disability and to engage with society to a greater extent than would be possible in a non-digitized environment. For those users (able or disabled) who are fully engaged in political activism,

the invisible service provider in a digitized environment may manipulate or censor their actions far more than they realize. In short, the merging of two kinds of power—that of the State and the burgeoning communications revolution[20]—has raised new questions of how we interpret public space, private property, the citizen's social contract with the state, and democracy itself. At the present time, no state has developed sufficient oversight of the communications revolution, instead delegating control of hardware and software development and implementation to private companies that are subject to very little government intervention in comparison to the automobile, chemical or pharmaceutical industries.

Over the course of centuries, humans have slowly but surely transformed their surrounding environment, utilizing the notion of ownership to claim space that is to be held collectively by the group or privately by the individual, thereby creating new legal principles in order to consolidate actual possession of the designated space. As discussed in Chapter 3, we think of this notion as property, a concept protected in customary law under article 17 of the Universal Declaration of Human Rights. We consider that certain elements of our surrounding environment, however, remain within the public domain, and belong to the nation, society or the planet as a whole. Termed global public goods (GPG), these are resources that can be consumed by one individual (or country) without diminishing availability of the good to another, and are non-exclusionary in that no individual (or country) can be barred from GPG benefits.[21] The air that surrounds us is one such public good. Air pollution threatens the non-exclusionary nature of this GPG in that pollution prevents certain individuals or countries from accessing the benefits of clean air. Article 1(a) of the 1979 United Nations (UN) Convention on Long-range Transboundary Air Pollution provides a baseline definition of two types of pollution:

> '"air pollution" means the introduction by man, directly or indirectly, of *substances* or *energy* into the air resulting in deleterious effects of such a nature as to endanger human health…' (author's emphasis).

As noted in Chapter 2, electromagnetic waves are an invisible, yet material form of energy that travels through the air and has an impact on all living things. Scientists cannot yet establish with certainty what the long-term health consequences of low-level radiation on humans will be, particularly on today's generation of children who have been exposed in the womb. In response to these 'epistemic cultures of non-knowledge' discussed in the

second chapter, we advocate application of the precautionary principle, as European and American governments have done to protect their populations from sulphur dioxide emitted by large, coal-fired power plants or nitrate particles from motor vehicle exhaust.[22] The above treaty addresses both energy and particle pollution, but the formal legal thresholds for 'energy' pollution worldwide recognize only thermal reactions to low-level radiation, rather than the far more common non-thermal reactions that are part and parcel of our everyday experience as humans in a wireless universe.

According to the OECD's *Environmental Outlook to 2050*, urban particle air pollution is set to become the top environmental cause of mortality worldwide by 2050, ahead of dirty water and lack of sanitation.[23] In arguing that burgeoning levels of electromagnetic wave frequencies constitute an additional form of air pollution, we recognize several important obstacles: (1) any broadening of the air pollution framework may be resisted by activists who have devoted considerable time and resources to push for regulation of the 12 forms of particle air pollution currently monitored by the European Union under the 1996 Framework Directive on ambient air quality assessment and management, and its daughter directives; (2) national governments earn significant revenues through rental of bandwidth space to telecom companies; (3) standards of measurement and biological proof regarding electromagnetic emissions are still contested by telecom companies, which earn nearly 300 billion euros in taxable revenue and employ more than a million people in Europe;[24] and (4) consumers have come to depend on the wireless transmission of information. These obstacles make it difficult to render electromagnetic pollution visible to the citizen.

Because particle air pollution is visible, while electromagnetic waves emissions are not, our sense of the air as a global public good is very much influenced by what we can see. And particle pollution activists had a head start; they first campaigning against smog began in the late nineteenth century, when the digital revolution was still 100 years into the future.[25] Nonetheless, there are past examples of eloquent campaigning to recognize invisible pollutants, including against those polluters that had substantive economic clout with respect to government revenues and employment. At the start of her ground-breaking book on pesticide pollution, author Rachel Carson notes: 'There once was a town in the heart of America where all life seemed to live in harmony with its surroundings.' *Silent Spring* portrays a spring without voices, an environment where the birds 'trembled violently and could not fly'. American chemical manufacturers

claimed that pesticides were perfectly safe and that Carson was a hysterical scientist, but the scientific community came to fully accept the impact of invisible chemicals on living organisms.[26] A well-informed reading of environmental history suggests that electromagnetic wave pollution will eventually be taken seriously. These emissions fall squarely within the ambit of international, regional and national air pollution legislation; it is up to scholars and activists to expand our understanding of air as a GPG and make electromagnetic field emissions 'visible' to concerned citizens.

The Internet constitutes our second example of a GPG that appears invisible or 'virtual' but is, in fact, solidly anchored in a sophisticated infrastructure of physical hardware, the electricity necessary to make that hardware function, and the patented algorithms that run technology systems. At its beginnings, ARPANET (Advanced Research Projects Agency Network) was a packet-switching *intranet* project for the military funded by the US government. As the *intranet* moved into the public space as an *internet*, it initially functioned as a free and open zone managed close to the source of data generation—i.e., by users themselves. This virtual Garden of Eden was an accessible venue for all technologically inclined users, free from corporate or government interference. John Perry Barlow began his 1996 Declaration of Independence of Cyberspace with the provocative preamble:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.[27]

Despite Barlow's flowery rhetoric, cyberspace was inexorably taken over by a public-private partnership. Barlow's 'new home of (the) Mind' was quickly recognized as the motor for a new economy, one that generated employment and consequential profits that could be taxed by governments.[28] As the Internet was transformed from 'a government sponsored backbone network to multiple commercially owned backbone networks', public supervision of Internet governance, competition, and performance accelerated.[29] The desire on the part of telecom companies to sell connectivity or infrastructure required government regulation to level the playing field and protect the consumer from price-fixing, as is the case with any other industry. As indicated above, however, government intervention was slow and inadequate when compared to the breakneck pace of digital

development, providing technology companies with an opportunity to 'colonize' the Internet.[30] According to French pundits, the means by which we access the Internet and our behaviour online were taken over at the turn of the century by the so-called GAFA, an acronym used to describe ownership by four American multinationals of what was once a fully public space.[31] These technology companies cooperated as governments stepped in to impose geographic border control of this virtual space, often in the name of heightened public security. This is hardly different from any other legal paradigm in place: Volkswagen, for example, is obliged to respect national environmental protection laws governing air pollution for all vehicles it sells within the continental USA. Legal experts were hardly surprised by the scandal that erupted when the corporation was discovered to have cheated on obligatory American emissions caps by installing software in diesel engines that could detect when they were being tested, changing the performance accordingly to improve results.[32] As governments stepped in to force technology companies to respect national or regional law across their international operations, the original vision of the Internet as a free and open space vanished.

In her work on the governance of public goods, Nobel prize-winning economist Elinor Ostrom noted a net reduction in public space over the past two hundred years due to the encroachment of private ownership, a pattern that accelerated at the end of the twentieth century.[33] Despite the trend towards privatization of the public space, Ostrom's theory of polycentric governance developed the idea that individuals, when faced with a shortage of a public good such as water, were able to share resources far more effectively and equitably at the local level than at the national level. When applied to the Internet, Ostrom's theory helps to explain why certain national governments have done such a poor job protecting the rights of individual users from privacy or health violations, or in providing an equitable platform for all to access the benefits of digital technology, since they are too far removed from the grassroots networks that constitute the Internet. If we extend this line of reasoning to the Internet of Things, that very material combination of invisible air, data and connectivity, the IoT is likewise a public good that—in theory—would be most equitably managed by the users themselves, rather than by national governments or multinational corporations. Virtual connectivity, however, is not water. Given the transboundary nature of the Internet and the IoT, government regulation effectively implemented at the local level is the citizens' best protection against commercial colonization of these GPGs. The law in

place obliges governments to take on that responsibility, to improve the lives of all citizens—disabled, marginalized and active—through a public-private partnership that physically monitors the air around us and protects the private transmission of our personal data within the newly designated national boundaries of cyberspace.

5.6 Extending Rousseau's Social Contract

In the above scenarios, our characters were treated differently by the machines around them according to their digital profiles, a series of signals that triggered subtle forms of either positive or negative discrimination. But, can machines discriminate? Can machines become citizens? Do we include them within our ethical framework on the rights and duties of citizens, or do we exclude them and hold human programmers or corporate entities responsible for machine behaviour? We have many questions about human responsibility for machine behaviour. David Gunkel notes in a remarkable book that 'the machine is not just one kind of excluded other; it is the very mechanism of the exclusion of the other.'[34] The machine is both the 'other' and the instrument of 'othering' in contemporary society. We assign machines a lesser status, while using them to enhance methods of commercially exploitable discrimination, both positive and negative.

International human rights law derives from the social reconstruction of reality that took place in the seventeenth and eighteenth centuries, the Enlightenment thinking that was embodied in Jean Jacques Rousseau's work on the social contract between citizens and their State.[35] Rousseau's work on what constitutes legitimate political authority continues to have a seminal influence on our understanding of ethics and democratic governance in a digitized world. The social contract initially promoted the civil and political rights of property-owning men with respect to their government, but its ambit expanded overtime to include the rights of slaves, non-property-owning men, women, ethnic minorities and the disabled. We also aim to uphold the rights of children and animals, extending protection, but very little agency, for beings whom we believe incapable of reasoned judgement. Nevertheless, some machines now engage in reasoned judgement. Does this mean that we should expand our understanding of the social contract to include the rights and duties of machines? The Universal Declaration of Human Rights makes it clear that machines are not to be included in the human family:

> Article 1. All *human beings* are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood. (Authors' emphasis)[36]

If we extend our analysis to another instrument, the International Covenant on Economic, Social and Cultural Rights, we must also take into account the one imperative of the treaty, namely the right of *human beings* to be free of discrimination of any kind in enjoying the benefits of scientific progress.[37] Consequently, despite current trends in science fiction,[38] Rousseau's social contract is between *human* citizens and their State, regardless of whether machines are 'endowed with reason and conscience' as noted in the Universal Declaration, or not.

Scholars have examined issues such as responsibility, culpability, causality and intentionality in law and determined that humans are in fact accountable for the behaviour of the machines they design or own.[39] Thus, if the New York City Police Department uses technology to engage in racial profiling, this is patently discriminatory, but it is the human police officers who are responsible for these practices, not the machines. Data collection technology can also be used to determine whether police are in fact taking part in racially biased 'stops'. This information can be used as a training mechanism that, if handled correctly, can actually reduce racism amongst law enforcement officers.[40] In a world of interconnected objects, however, it is not clear who is responsible for the information (or algorithm-driven assumptions) generated by location tracking software, especially when those connections lead to the display of information based on immutable characteristics, such as race, social class or religion, information that the user has not requested, but that guides user behaviour. We note the developments in Internet intermediary law, which holds the companies that host search engines, microblogs, social media, and user generated content platforms responsible for user content.[41] But, these developments do not cover the communication between geo-localizing devices and the subtle ways in which these devices influence human behaviour through information generation and machine 'decision-making', issues that are currently termed predictive profiling and treated as a privacy violation. Nevertheless, the roll-out of such technology could lead to discriminatory treatment of large sectors of society, treatment which is proscribed under international human rights law.

5.7 Scenario Three: What a Day!

Adil and Sarah are married and live in a comfortable house with their two children. Adil has implanted digital eyes[42] that allow him to see enough to move independently, type in the pin number of a credit card, recognize people and street signals, and even drive. Adil has recently bought a self-driving car, which allows him to get to and from his office, almost an hour away from home. The family home is fully equipped with digital appliances which minimize energy consumption by adjusting automatically to the presence or absence of people in the house, according to their specific location and habits—no need to warm up the house in a hurry when returning from work or holidays, or to remind the little ones to turn off the light in the bathroom.

The smart portable devices that Adil and Sarah use to control and communicate with their home appliances have an even more important function. These machines facilitate contact with their loved ones. Adil and Sarah know, for example, that they will be alerted if Adil's mother, who lives alone in her own apartment despite a mild heart condition and some memory problems, needs help. A personalized health tracking device regularly collects her physiological measurements (heartbeat, blood pressure and temperature) and reports to Adil and the family doctor if the statistics indicate a possibly dangerous condition. Adil's mother has an emergency button installed on her watch and any unusual behaviour, such as not moving around the house for several hours during the day or not using water around meal times, are signalled to Adil who can call her to verify if everything is fine. Sarah and Adil are amongst the early adopters of these technologies, but they are not unusual in this respect.

It is still bright and sunny when Sarah leaves work; she quickly picks up a few groceries from the shop on her way home because she knows that Jack, their eldest son, is waiting for her to help him revise for a test the next day. Although only nine years old, Jack is very ambitious when it comes to school results! Sarah is surprised when the house gate does not recognize her and she has to manually open it, but that happens every once in a while and certainly does not prepare her for what is coming next. The house door does not recognize her either. As she starts to worry and looks for the special emergency opener, she wonders how Jack got into the house…In fact, while frantically interrogating her phone and pulling objects out of her bag to locate the emergency opener, she realizes that if Jack is not locked out and waiting for her, he must be locked inside the

house. As she shouts one more time to her phone 'Where is the emergency opener' she finally hears the beeping signal locating the opener in a side pocket. As Sarah opens the door, a wave of unbearable heat hits her and she instinctively closes her eyes. Quickly forcing them open, she drops her bag and calls for her son.

Although it is still light outside, the house is very dim—the house lights must be running on the emergency battery. Sarah glances at the home control panel as she runs towards Jack's room and sees flashing alarm signals. Breathing is difficult. She finds Jack lying on the floor unconscious next to his computer, with the image of his own avatar in one of his favourite video games frozen on the screen. With great effort, Sarah disconnects the automated windows, opens them wide and splashes water on Jack to cool him down. Shouting at her phone again, she sends for an ambulance. She also leaves a panicked voice message for her husband explaining what has happened and asking him to pick up their younger son from school.

Adil immediately gets into his car and indicates that he needs to get to his son's school in a hurry. He knows that, unfortunately, his car is not able to get anywhere quickly in self-driving mode. Sarah calls to tell him that Jack has woken up and looks okay; she gives him the name of the hospital where he is being taken and asks that Adil meet her there after he has picked up their younger son. As soon as the car stops at the next traffic light, Adil asks his phone to locate the hospital on a map. When Adil raises his eyes, he notices that the street light has turned green and, as usual, his car is taking time to restart. He takes control of the car and drives forward, just in time to hit another vehicle crossing the junction. A few months later, the enquiry requested by Adil's insurance company establishes that his eye implant malfunctioned, resulting in a temporary Daltonism which caused the accident.

5.8 The Internet of Things—Technology

It is widely recognized that it is very difficult, or even impossible, to predict exactly how technology will be used and will respond within the many conceivable operational configurations of the Internet of Things. This is because the IoT is an extremely large network of interconnected objects, applications and humans. Companies such as Gartner expect 21 billion connected 'things' by 2020,[43] while Cisco forecasts 24 billion networked devices by 2019,[44] Morgan Stanley over three times this amount by 2020,[45] and Huawei Technologies Co., a Chinese multinational and

the largest telecommunications equipment manufacturer in the world, forecasts 100 billion IoT connections by 2025.[46]

IoT security represents a seminal challenge. A group of researchers from the University of Central Florida demonstrated to their colleagues at a conference on information security how a well-known brand of smart thermostats could be hacked into and then used to spy on the owner, steal wireless network credentials, or attack other devices on the network.[47] Although this specific attack required having physical access to the thermostat, the fact that entry into the system could be completed in just a few seconds (in front of a stupefied audience) demonstrates how, in a very fast-growing and lucrative market, time to market may trump security considerations. While Adil's temporary Daltonism mentioned in our third scenario is pure fiction, his implanted eyes could be reality. For example, a patient with a retinal implant was capable in 2015 of converting video images from a miniature video camera worn on his glasses into electrical pulses that were transmitted wirelessly to an array of electrodes attached to the retina; this information was then sent to the brain.[48]

While the societal impacts of the IoT are extremely broad, the technological challenges remaining in order to ensure that the IoT realizes its full potential, guaranteeing both effective service and protection of users' rights, are just as far-reaching. First, in addition to the already mentioned privacy concerns, security problems, such as those that have afflicted the information and communication technology industry for decades, are growing. As the IoT progressively reduces the gap between the virtual and the physical, security-related challenges take on a whole new dimension and require more robust, scalable, and sustainable solutions. Second, interoperability will no longer be a desirable attribute of digital systems, but a fundamental requirement for the very existence of the IoT. Third, sensor systems that until recently had only been used for specific application domains will become more widespread (accelerometers, GPS receivers, and cameras, for example, are already integrated in many of our smart phones); more stringent requirements will be necessary to ensure their levels of accuracy, resistance, reliability and security. Finally, the transition from embedded computing and communication capabilities to a greater number of physical systems (transport systems, industry or the home) makes each arrangement more vulnerable to intentional or unintentional malfunction.

5.9 Human-Machine Protocols

Our third scenario highlights the need for human-machine protocols that articulate the circumstances under which humans are responsible for machine behaviour in an interconnected society. Human-machine collaborative systems are generally referred to as cognitive systems, in which machines carry out the tasks machines are good at, such as computations and data analysis, and people carry out the tasks people are good at, such as interpreting data patterns and decision-making.[49] Sarah and Adil depend on digitized technology for convenience, to alleviate the constraints of Adil's disability and to call an ambulance in an emergency. But machines, like humans, make mistakes. In cognitive systems, we cannot assume that machines will be adequately programmed to interpret data patterns or to make decisions that would allow them to cope with an evolving catastrophe. Nonetheless, research demonstrates that we 'humanize' our interaction with certain machines, expecting them to respond like people, whether they have been programmed to do so, or not.[50] Rapid technological progress in the domain of artificial intelligence and machine learning, for example, has created autonomous robots that arouse human feelings of empathy, making them possible companions for the elderly.[51] In addition to free-standing robots, intelligent prostheses that roboticize human capacity and allow the disabled to recover normal body functions that have been lost to illness or handicap redefine our notions of what it means to be human. As we expand our interpretation of the social contract to include human interaction with machines, how may we draw on existing law to guide us in our assumptions? And to what extent should we distinguish between humanized robots, integrated body parts, and invisibly interconnected objects?

5.10 Killer Robots, Prostheses, and Avatars

The case of killer robots starkly reveals the ambiguous nature of these questions. The need for civilian governments and their national militaries to avoid the haunting imagery of body bags returned home for burial in flag-draped coffins is understandable. The loss of solders in conflict is both tragic and economically wasteful, as the training of even one human military pilot is a substantive investment for the armed forces. However, if robots are to replace human solders, who will be answerable for their

conduct in a war zone? When Human Rights Watch first called for an absolute ban on the use of robots in warfare in 2012, the organization argued that the ban was necessary since robots could not be held responsible for their behaviour.[52] We agree, but given the frenzied race towards roboticized combat announced by the US military, the outright ban (supported by both the UN Special Rapporteur on extrajudicial, summary, or arbitrary executions and the Special Rapporteur on the rights to peaceful assembly and association) will be difficult to implement effectively.[53] Since there has not been an international ban on killer robots as of this writing, legal responsibility for machine behaviour in war may be understood within one of two existing frameworks: command responsibility under international humanitarian law, or manufacturers' criminal or civil liability under domestic law. Both are problematic.

In the first case, article 28 of the Rome Statute of the International Criminal Court is clear on the responsibility of military or civilian hierarchies in wartime. The commanding officer—a human—is responsible for the behaviour of troops under his or her orders, under the following circumstances: if he or she knew or should have known that such troops were about to commit or had committed crimes and 'failed to take all necessary and reasonable measures within his or her power to prevent or repress their commission or to submit the matter to the competent authorities for investigation and prosecution'.[54]The treaty does not refer to *human* solders, but to '*forces* under his or her effective command and control',[55] a term that leaves judges with considerable margin in their interpretation of what constitutes a solder in wartime. Nonetheless, Human Rights Watch argues that the bar for command responsibility is too high and that criminal liability in war has been designed for humans, not machines.[56] We may consider the case of a robot to be similar to that of a minor in the sense that, much like a child soldier, a robot is likely to be malleable and programmed to kill without recourse to moral or ethical reflexes that might inhibit violent behaviour. Child soldiers and robots alike are capable of carrying out criminal attacks on civilian populations without remorse and may be unstoppable once the violence has begun.[57] Under article 26 of the Rome Statute, a child soldier is not responsible for his or her acts, but the child's commanding officer is. As in the case of a child soldier who, once instructed, acts in a partially autonomous manner, the commanding officer of a semi-autonomous robot would also be responsible for heinous acts committed on his or her watch.

Nonetheless, if we consider that child soldiers have the right to due process, but do not possess the necessary *mens rea* under the international legal regime to be responsible for the commission of core crimes, then we may be prompted to extend the same logic to machines with human characteristics. In this case, robots endowed with artificial intelligence might also claim rights.

Manufacturers' civil or criminal responsibility presents another avenue of exploration, one that would be of interest to our characters Sarah and Adil. There is considerable debate on the responsibility of corporate actors for grave breaches of humanitarian law. Legal scholar Bonnie Dougherty considers that it would be 'unreasonable to impose criminal punishment on the programmer or manufacturer, who might not specifically intend, or even foresee, the robot's commission of wrongful acts'.[58] She notes that in the USA, manufacturers contracted by the military are 'immune from suit when they design a weapon in accordance with government specifications and without deliberately misleading the military'.[59] Moreover, product liability defects due to manufacturing error are intended to address tangible hardware defects, rather than software-related defects, such as the household heating and door lock systems run amok in our third scenario. Since an autonomous robot in war is most likely programmed to kill, it would be difficult for the families of civilian murder victims to sue a manufacturer for product liability in the event that a robot hits its human target. Murder of a civilian in war is a crime, not a software defect subject to manufacturer's liability under a civil suit. The only viable recourse would be to prosecute corporate leadership for aiding and abetting a war crime, a legal possibility that is still in its infancy at the International Criminal Court.[60]

While we interpret the legal texts as making it clear that robots do *not* have rights and remain outside of the international human rights treaty framework, what about roboticized adult humans, those cyborgs or technologically enhanced individuals amongst us whose bodies incorporate mechanized functions that were once human? If humans are responsible for the machines they design or own, who is to be held accountable for our character's digital eye implants that develop Daltonism and cause a traffic accident: the human who invented the technology that allows the digital eye to function, the company that produced the digital eye, or the human who now uses a prosthesis in place of an eye? In law, if a free-standing robot is considered a movable, tangible item or product, then liability for its actions would fall under extensive jurisprudence, except in wartime. As far as the bodily integration of a machine is concerned,

a faulty hip or knee replacement is subject to medical or manufacturer liability. Once the human brain signals behaviour to a prosthesis through bio-sensoring technology, however, we have very few guidelines on how to determine responsibility. Obligatory human-machine protocols that assign to humans the responsibility for digitally enhanced human performance may be a start in the right direction. The integrated body part would most likely engage the legal responsibility of the human in charge of it (unless the digitized body part is defective or hacked into, in which case responsibility would shift to the manufacturer or the hacker). While certain scholars argue that machines could be considered independent agents in law (third-party actors authorized to act on behalf of someone else[61]), we anticipate difficulties with this approach in the years to come: for example, could a mechanical arm that is able to 'learn' claim rights that conflict with those of the human who is said to control the same arm?

Finally, our third scenario makes reference to the troubling issue of human avatars. Legal scholarship has established that avatars are protected as intellectual property, particularly in France, and may be considered as legal persons, much like corporations.[62] This is an important step in determining who may benefit from royalties generated by massive multiplayer online games (MMOG) and who owns the avatars created by the thousands of players involved in online gaming platforms. Nonetheless, the avatar is unlikely to be confined to the MMOG. In 2009, Microsoft patented an avatar that produces a 'physiological characteristic of the user' based on data gleaned from 'a third party health data collection repository, a healthcare smart card, or a real-time physiological sensor (e.g., blood pressure, heart rate, blood glucose, peak flow, pedometer, etc.)'.[63] While the patent's stated objective appeared to encourage avatars and their human likenesses to exercise more, the long-term potential is disturbing, particularly since the physical characteristics will be obtained 'non-volitionally' from the user, thereby 'avoiding the inconvenience or unaccountability of voluntarily supplied information'.[64]

Privacy violations aside (these engineers were apparently unschooled in privacy-by-design methodology), the larger human rights concerns include freedom from discrimination and individual autonomy. Should avatars be considered legal minors, like robots, legal persons, like corporations, or have full-fledged responsibiity for their actions like their human sponsors? Once avatars begin to replace their human counterparts at work stations, conferences or in the execution of simple household tasks, could an avatar be responsible for a crime? Could it go to prison in lieu of a human

sponsor? Or take over substantive decision-making, thereby limiting the autonomy of the human who created the avatar? Despite the virtual nature of the avatar, we consider it to be machine-generated and therefore subject to a thoughtfully broad human-machine protocol that would begin to answer some of these questions. While we have argued throughout that the social contract should be extended to protect the rights of humans in human-computer or human-data interactions, machines are not human and do not (yet) qualify for rights protection.

To conclude, the argument that the digital environment, particularly the IoT, is virtual will stymy the application of viable, existing law to regulate its use. The seemingly virtual nature of the IoT should not blind us to its physical reality. The physical hardware—beacons, RFIDs, smartphones, base transceiver stations, electric cables, computers, data storage units, power stations and patented algorithms—is tangible proof of its material nature. This chapter has argued that certain seminal principles of international human rights law provide us with a necessary framework for understanding human-computer and human-data interaction in a digital environment. Rousseau's social contract, which has been extended to all human beings in international law, does not yet include machines; as the legal texts cited in this chapter indicate, machines are not citizens. Our first two scenarios provided us with a window on human-machine interaction in the IoT, a view in which the public air space is occupied by invisibly conversant bandwidth that guides human behaviour and may discriminate in favour of certain users and against the interests of others. The third scenario described machines gone amok, the takeover of a cognitive system by a combination of malfunctioning hardware and software that misinterpreted data patterns and made the wrong 'decisions', thereby endangering human lives.

David Mindell writes that 'The challenges of robotics in the twenty-first century are those of situating machines within human and social systems. They are challenges of relationship.'[65] If humans and machines are to work together, then the 'challenges of relationship' should be carefully thought through, not only on the level of hardware or software design, but also ethically, legally and practically, so that human knowledge and presence remain crucial to the relationship.[66] We discussed the importance of privacy impact assessments in Chapter 3, noting that the humans involved in software design were able to build human rights protections into the planning stages of their work. We also support the use of human-machine protocols to guide the design and construction of cognitive systems,

protocols that identify human knowledge input and responsibility, even when the designer, manufacturer or user are not present. The IoT will promote deeper intimacy with our machines, thereby making the distinction between human and machine responsibility all the more necessary.

While we think it highly unlikely that machines will take over from humans anytime soon, we are concerned by the potential of interconnected machines to generate discriminatory paradigms that impact human behaviour. Despite the right of all humans to be free from discrimination in their enjoyment of scientific progress, immutable characteristics mix with geolocalizing software and consumer behaviour to form digital profiles that elicit differentiated signals from the machines that surround us. This is perhaps the most arresting challenge posed by the IoT—the silent, steady data-generated prompting that changes the way we experience the world and may alter the way we view ourselves. Despite the general interdiction against discrimination in human rights law, digital prompting may trigger forms of self-oppression that are difficult to detect and even more difficult to assign responsibility for. Education undoubtedly provides the most effective means of remedying this by alerting students, the 'digital natives' whom we teach,[67] of their rights and the ways in which technology providers may promote or violate these rights. In the next chapter, we examine the impact of digital technology on higher education and present a blended learning curriculum that addresses rights training in the context of the digital revolution.

Notes

1. Evans, D. (2011) 'The Internet of Things How the Next Evolution of the Internet Is Changing Everything', *Cisco Internet Business Solutions Group White Paper*, p. 3.
2. Kleiner, T. (2016) 'Time to unleash the potential of the Internet of Things in Europe', *Digital Single Market*, European Commission.
3. See discussion on human-data interaction in Mortier, R., et al. (2014) 'Human-Data Interaction: The Human Face of the Data-Driven Society', paper presented at IT-as-a-Utility Network and Human-Data Interaction Workshop, Oxford University.
4. See Gunkel, D. J. (2012) *The Machine Question: Critical Perspectives on AI, Robots, and Ethics*; Coeckelbergh, M. (2012) *Growing Moral Relations: Critique of Moral Status Ascription*, Chapter 9.3.
5. London School of Economics Cities (2014) 'Innovation in Europe's Cities: A report by LSE Cities on Bloomberg Philanthropes' 2014 Mayors Challenge', *LSE Cities,* p. 42.

6. Boden, R. (2015) 'Bucharest Buses to Use Bluetooth Beacons to Guide the Blind', *Near Field Communications World*.
7. See for example https://foursquare.com/about/.
8. See for example https://www.fieldtripper.com/.
9. Want, R., Schilit, B.N., and Jenson, S. (2015) 'Enabling the Internet of Things', *IEEE, Computer Society,* Vol. 48, No. 1, pp 28–35.
10. These measures refer to real application conditions; officially the two classes are respectively defined as ranging ten meters and 100 meters.
11. Released in 2010 as Bluetooth Core Specification Version 4.0.
12. Gibson, D., et al. (2013) 'Digital Badges in Education', *Education and Information Technologies*, Vol. 20, No. 2, pp 1–8.; Raths, D. (2013) 'How Badges Really Work in Higher Education', *Campus Technology*.
13. Cunche, M., Kaafar, M.A., and Boreli, R. (2013)'Linking wireless devices using information contained in Wi-Fi probe requests', *Pervasive and Mobile Computing*, Elsevier; Musa, A., and Eriksson, J. (2012) 'Tracking unmodified smartphones using Wi-Fi monitors', *SenSys*, 10th Association for Computing Machinery Conference on Embedded Network Sensor Systems, pp. 281–294; Cunche, M., et al. (2012)'I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests', *World of Wireless, Mobile and Multimedia Networks,* 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks; Eckersley, P. and Gillula, J.(2014)'Is Your Android Device Telling the World Where You've Been?', *Electronic Frontier Foundation*.
14. Freudiger, J. (2015) 'How talkative is your mobile device?: an experimental study of Wi-Fi probe requests', ACM Conference on Security and Privacy in Wireless and Mobile Networks, *ACM WiSec*, Article No. 8, pp. 1–6.
15. See http://www.apple.com/ph/privacy/privacy-built-in/.
16. Zebra Technology (2014) 'Analysis of iOS 8 MAC randomization on locationing', White Paper, http://mpact.zebra.com/documents/iOS8-White-Paper.pdf, date accessed 28 February 2016.
17. Misra, B. (2014) 'iOS8 MAC Randomization – Analyzed!' *Mojo Networks Blog*; Misra (2014) 'iOS8 MAC Randomization Update', *Mojo Networks Blog*.
18. Freudiger (2015) 'How talkative is your mobile device?'
19. Gillula, J. and Schoen, S. (2014) 'An Umbrella in the Hurricane: Apple Limits Mobile Device Location Tracking', *Electronic Frontier Foundation*.
20. Darnton, R. (2014) *Censors at Work: How States Shaped Literature*, p. 20.
21. International Task Force on Global Public Goods (2006) 'Meeting the Global Challenges: International Cooperation in the National Interest'.
22. Environmental Protection Agency (2009) 'Final Report: Integrated Science Assessment for Particulate Matter'.

23. Organization for Economic Co-operation and Development (2012) 'Environmental Outlook to 2050: The Consequences of Inaction: Highlights' (Paris: OECD) p. 5.
24. European Telecommunications Network Operators' Association (2012) Third Annual Economic Report', *EurActiv Press Release*.
25. The UK's Public Health Act 1875 contained a smoke abatement section in an attempt to reduce industrial emissions in urban areas, but it was the Great London Smog of 1952, resulting in nearly 4000 extra deaths, which led to the Clean Air Acts of 1956 and 1968. See UK-AIR: Air Information Resource http://uk-air.defra.gov.uk/index.php.
26. See Buell, F. (2004) *From Apocalypse to Way of Life: Environmental Crisis in the American Century*.
27. Barlow, J.P. (1996) 'A Declaration of the Independence of Cyberspace', Davos, Switzerland, 8 February.
28. This was the case even at the Davos Forum where Barlow launched his Declaration.
29. Shah, R.C., and Kesan, J.P. (2007) 'The Privatization of the Internet's Backbone Network', *Journal of Broadcasting and Electronic Media*, Vol. 51, No. 1, pp. 93–109.
30. Casati, R. (2013) *Contre le colonialisme numérique: manifeste pour continuer à lire*.
31. Octo Technology (2012) *Les Géants du Web: Culture - Pratiques – Architecture*; FaberNovel (2014) *GAFAnomics: New Economy, New Rules*. The four companies selected are Google, Apple, Facebook and Amazon. It should be noted that this study does not include Baidu, the Chinese search engine that accommodates five billion searches per day behind China's Great Firewall as discussed in Chapter 4, an operating space where the GAFA companies are no longer entirely welcome.
32. Hotten, R. (2015) 'Volkswagen: The Scandal Explained', BBC News.
33. Ostrom, E. (1990) *Governing the Commons: The Evolution of Institutions for Collective Action*.
34. Gunkel (2012) *The Machine Question,* p. 128.
35. Rousseau, J.J. (1762) *Du contrat social ou Principes du droit politique*.
36. 1948 Universal Declaration of Human Rights, article 1.
37. See articles 2 and 17 of the 1966 International Covenant on Economic, Social and Cultural Rights.
38. The Swedish television series 'Real Humans' or the British series 'Black Mirror' come to mind.
39. Noorman, M. and Johnson, D.G. (2014) 'Negotiating autonomy and responsibility in military robots', in *Ethics and Information Technology,* Vol. 16, No. 1, pp. 51–62; Van den Hoven, M.J. (1998) 'Moral responsibility, public office and information technology', in *Public Administration*

in an Information Age: a Handbook, pp. 97–112; Lucas, G.R. (2014) 'Legal and Ethical Precepts Governing Emerging Military Technologies: Research and Use', *Amsterdam Law Forum*, Vol. 6, No. 1, pp. 23–34.
40. Ramirez, D., McDevitt, J. and Farrell, A. (2000) *A Resource Guide on Racial Profiling Data Collection Systems: Promising Practices and Lessons Learned*.
41. Two studies are particularly noteworthy: (1) Riordan, J. (2016) *The Liability of Internet Intermediaries* and (2) Gasser, U. and Schulz, W. (2015) 'Governance of Online Intermediaries: Observations from a Series of National Case Studies: NoC Online Intermediaries Research Project'.
42. Walsh, F. (2015) 'Bionic Eye Implant World First', *BBC News Online*.
43. Gartner (2015) 'Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent From 2015' (Stamford, Connecticut: Gartner Press Release) 10 November, http://www.gartner.com/newsroom/id/3165317, date accessed 27 February 2016.
44. Cisco (2015) 'Cloud and Mobile Network Traffic Forecast - Visual Networking Index (VNI)', http://cisco.com/c/en/us/solutions/serviceprovider/visual-networking-index-vni/index.html, date accessed 27 February 2016.
45. Danova, T. (2013) 'Morgan Stanley: 75 Billion Devices Will Be Connected To The Internet Of Things By 2020', *Business Insider*, 2 October, http://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020, date accessed 27 February 2016.
46. Huawei (2015) 'Global Connectivity Index 2015; Benchmarking Digital Economy Transformation', Huawei Technologies Co., Ltd., http://www.huawei.com/minisite/gci/en/huawei-global-connectivity-index-2015-whitepaper-en-0507.pdf.
47. Hernandez, G., Arias, O., Buentello, D., and Jin, Y. (2016) 'Smart Nest Thermostat: A Smart Spy in Your Home', Black Hat USA, https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home.pdf.
48. Walsh, F. (2015) 'Bionic eye implant world first', BBC News Online, http://www.bbc.com/news/health-33571412, date accessed 26 February 2016.
49. Peeters, M., Baar, T.J. and Harbers, M. (2014) 'Responsible Innovation, Development, and Deployment of Automated Technology', Responsible Innovation Conference Paper, p. 1.
50. Coeckelbergh (2012) *Growing Moral Relations*, Chapter 9.3.
51. Coeckelbergh (2012) *Growing Moral Relations*, Chapter 9.3.
52. Docherty, B. (2015) 'Mind the Gap: the Lack of Accountability for Killer Robots. *Human Rights Watch Reports.*
53. Campaign to Stop Killer Robots (2016) 'UN Rapporteurs Call for Ban'.

54. Rome Statute of the International Criminal Court, UN Doc 2187, U.N.T.S. 90, entry into force 1 July 2002.
55. Rome Statute of the International Criminal Court.
56. Docherty (2015) 'Mind the Gap'.
57. Perry, S. (2012) 'Child Soldiers: the Pursuit of Peace or Justice for Child Combatants?'
58. Docherty (2015) 'Mind the Gap'.
59. Docherty (2015) 'Mind the Gap'.
60. Ambach, P. (2011) 'International Criminal Responsibility of Transnational Corporate Actors Doing Business in Zones of Armed Conflict', paper presented at *The Interaction of International Investment Law with Other Fields of Public International Law*; Stewart, J. (2011) *Corporate War Crimes: Prosecuting the Pillage of Natural Resources.*
61. Santosuosso, A. (2013) 'Legal Problems of Modern Robotics', paper presented at *Legislation for Technical Systems: Robotics, Autonomous Systems and Industry 4.0 are challenging law*.
62. Van den Bulck, P. and De Bellefroid, M. (2009) 'Legal Regime of Avatars Created in the Framework of Video Games: Some Reflections in Light of French and Other Legal Systems', *Convergence*, Vol. 5, No. 2, pp. 257–268.
63. Karkanias, C. D. et al. (2009) Avatar Individualized by Physical Characteristic, US Patent Application 20090309891, *US Trademark and Patent Office*, 17 December.
64. Karkanias, et al. (2009) Avatar Individualized by Physical Characteristic, *US Trademark and Patent Office*.
65. Mindell, D. (2015) *Our Robots, Ourselves.*
66. Mindell (2015) *Our Robots, Ourselves*, p. 6.
67. See Marc Prensky's article on 'Digital Natives, Digital Immigrants' which links the decline in American education to the distinction between generations and their use(s) of technology. Prensky, M. (2001) 'Digital Natives, Digital Immigrants', *On the Horizon,* Vol. 9, No. 5, pp. 1–6.

Bibliography

Ambach, P. (2011). *International criminal responsibility of transnational corporate actors doing business in zones of armed conflict.* Paper presented at The Interaction of International Investment Law with Other Fields of Public International Law, Leiden Law School.

Apple. (2016). Apple privacy policy, Apple Inc. Retrieved March 19, 2016, from http://www.apple.com/ph/privacy/privacy-built-in/

Barlow, J. P. (1996). A declaration of the independence of cyberspace, davos, electronic frontier foundation. Retrieved March 20, 2016, from https://www.eff.org/cyberspace-independence

Boden, R. (2015). Bucharest buses to use bluetooth beacons to guide the blind. *Near Field Communications World*. Retrieved March 1, 2016, from http://www.nfcworld.com (home page).

Buell, F. (2004). *From apocalypse to way of Life: Environmental crisis in the American century*. New York: Routledge.

Campaign to Stop Killer Robots. (2016). UN rapporteurs call for ban. Campaign to stop killer robots. Retrieved March 20, 2016, from http://www.stopkillerrobots.org/2016/03/unreport

Casati, R. (2013). *Contre le colonialisme numérique: manifeste pour continuer à lire*. Paris: Albin Michel.

Cisco. (2015). Cloud and mobile network traffic forecast—Visual Networking Index (VNI). Retrieved February 27, 2016, from http://cisco.com/c/en/us/solutions/serviceprovider/visual-networking-index-vni/index.html

Coeckelbergh, M. (2012). *Growing moral relations: Critique of moral status ascription*. New York: Palgrave Macmillan.

Cunche, M., Kaafar, M. A., & Boreli, R. (2012). *I know who you will meet this evening! Linking wireless devices using Wi-Fi probe requests*. World of Wireless, Mobile and Multimedia Networks. 13th IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, San Francisco.

Cunche, M., Kaafar, M. A., & Boreli, R. (2013). Linking wireless devices using information contained in Wi-Fi probe requests. *Pervasive and Mobile Computing*, *11*, 56–69. Elsevier.

Danova, T. (2013, October 2). Morgan Stanley: 75 billion devices will be connected to the Internet of Things by 2020. *Business Insider*. Retrieved February 27,2016,fromhttp://www.businessinsider.com/75-billion-devices-will-be-connected-to-the-internet-by-2020

Darnton, R. (2014). *Censors at work: How states shaped literature*. New York: WW Norton.

Docherty, B. (2015). Mind the gap: The lack of accountability for killer robots. *Human Rights Watch Reports*. Retrieved March 20, 2016, from https://www.hrw.org/ (home page).

Eckersley, P., & Gillula, J. (2014). Is your android device telling the world where you've been? *Electronic Frontier Foundation*, l. Retrieved March 19, 2016, from http://goo.gl/3XezqR

Environmental Protection Agency. (2009). Final report: Integrated science assessment for particulate matter. *U.S. Environmental Protection Agency*. Retrieved March 19, 2016, from http://www.epa.gov (home page).

European Telecommunications Network Operators' Association. (2012) Third Annual Economic Report. *EurActiv Press Release*. Retrieved March 19, 2016, from http://pr.euractiv.com (home page).

Evans, D. (2011). *The Internet of Things how the next evolution of the internet is changing everything*. Cisco Internet Business Solutions Group White Paper, p. 3.

FaberNovel. (2014) *GAFAnomics: New economy, new rules.* Fabernovel study. Retrieved March 20, 2016, from http://www.fabernovel.com/(home page).

Field Trip. (2016). Retrieved March 19, 2016, from https://www.fieldtripper.com (home page).

Foursquare Labs, Inc. (2016). Retrieved March 19, 2016, from https://foursquare.com (home page).

Freudiger, J. (2015). How talkative is your mobile device? An experimental study of Wi-Fi probe requests. ACM Conference on Security and Privacy in Wireless and Mobile Networks. *ACM WiSec, 8*, 1–6.

Gartner. (2015, November 10). Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. Stamford, CT: Gartner Press Release. Retrieved February 27, 2016, from http://www.gartner.com/newsroom/id/3165317

Gasser, U., & Schulz, W. (2015). Governance of online intermediaries: Observations from a series of national case studies: NoC online intermediaries research project. *Global Network of Internet & Society Research Centers.* Retrieved March 20, 2016, from https://publixphere.net (home page).

Gibson, D., Ostashewski, N., Flintoff, K., Grant, S., Knight, E. (2013). Digital badges in education. *Education and Information Technologies*, *20*(2), 1–8. Springer Science and Business Media, New York.

Gillula, J., & Schoen, S. (2014). An Umbrella in the hurricane: Apple limits mobile device location tracking. *Electronic Frontier Foundation*. Retrieved February 28, 2016, from https://www.eff.org (home page).

Gunkel, D. J. (2012). *The machine question: Critical perspectives on AI, robots, and ethics.* Cambridge: MIT Press.

Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2016). Smart nest thermostat: A smart spy in your home. Black Hat USA. https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your--Home.pdf

Hotten, R. (2015). Volkswagen: The scandal explained. *BBC News.* Retrieved March 20, 2016, from http://www.bbc.com (home page).

Huawei. (2015). Global Connectivity Index 2015; Benchmarking digital economy transformation. Huawei Technologies Co., Ltd. http://www.huawei.com/minisite/gci/en/huawei-global-connectivity-index-2015-whitepaper-en-0507.pdf

International Task Force on Global Public Goods. (2006). Meeting the global challenges: International cooperation in the national interest. *Global Public Goods,* Global Policy Forum. Retrieved March 19, 2016, from https://www.globalpolicy.org (home page).

Karkanias, C. D., et al. (2009). Avatar individualized by physical characteristic, US Patent Application 20090309891, *US Trademark and Patent Office*, 17 December.

Kleiner, T. (2016). Time to unleash the potential of the Internet of Things in Europe. *Digital Single Market*. European Commission. Retrieved February 15, 2016, from https://ec.europa.eu (home page).

London School of Economics Cities. (2014). Innovation in Europe's cities: A report by LSE cities on Bloomberg Philanthropes 2014 Mayors Challenge. *LSE Cities*. Retrieved Febraury 28, 2016, from https://lsecities.net (home page).

Lucas, G. R. (2014). Legal and ethical precepts governing emerging military technologies: Research and use. *Amsterdam Law Forum, 6*(1), 23–34.

Mindell, D. (2015). *Our robots, ourselves*. New York: Viking.

Misra. (2014a). iOS8 MAC randomization update. *Mojo Networks Blog*. Retrieved February 28, 2016, from http://blog.mojonetworks.com/ios8-mac-randomgate/

Misra, B. (2014b). iOS8 MAC randomization–analyzed! Mojo networks blog. Retrieved February 28, 2016, from http://blog.mojonetworks.com/ios8-mac-randomization-analyzed/

Mortier, R., et al. (2014). *Human-data interaction: The human face of the data-driven society*. Paper presented at IT-as-a-Utility Network and Human-Data Interaction Workshop, Oxford University.

Musa, A., & Eriksson, J. (2012). *Tracking unmodified smartphones using Wi-Fi monitors*. SenSys, 10th Association for Computing Machinery Conference on Embedded Network Sensor Systems (pp. 281–294).

Noorman, M., & Johnson, D. G. (2014). Negotiating autonomy and responsibility in military robots. *Ethics and Information Technology, 16*(1), 51–62.

OctoTechnology. (2012). *Les Géants du Web: Culture—Pratiques—Architecture*. Paris: Octo.

Organization for Economic Co-operation and Development. (2012). Environmental outlook to 2050: The consequences of inaction: Highlights. *OECD*. Retrieved March 20, 2016, from https://www.oecd.org (home page).

Ostrom, E. (1990). *Governing the commons: The evolution of institutions for collective action*. Cambridge, UK: Cambridge UniversityPress.

Parliament of the United Kingdom. (1875). Public Health Act, Citation 38 & 39 Ch. 55. *The National Archives*. Retrieved March 20, 2016, from http://www.legislation.gov.uk (home page).

Parliament of the United Kingdom. (1956). Clean Air Act. *The National Archives*. Retrieved March 20, 2016, from http://www.legislation.gov.uk (home page).

Parliament of the United Kingdom. (1968). Clean Air Act. *The National Archives*. Retrieved March 20, 2016, from http://www.legislation.gov.uk (home page).

Peeters, M., Baar, T. J., & Harbers, M. (2014). Responsible innovation, development, and deployment of automated technology. Responsible Innovation Conference Paper. *Interactive Intelligence Group*. Retrieved March 20, 2016, from https://ii.tudelft.nl (home page).

Perry, S. (2012). Child soldiers: The pursuit of peace or justice for child combatants? In Gardner & Kobtzeff (Eds.), *The Ashgate research companion to war: Origins and prevention*. London: Ashgate Press.

Prensky, M. (2001). Digital natives, digital immigrants. *On the Horizon, 9*(5), 1–6.
Ramirez, D., McDevitt, J., & Farrell, A. (2000). *A resource guide on racial profiling data collection systems: Promising practices and lessons learned*. Monograph National Contest Journal. Washington, DC: U.S. Department of Justice.
Raths, D. (2013). How badges really work in higher education. *Campus Technology*. Public Sector Media Group. Retrieved February 28, 2016, from https://campustechnology.com (home page).
Riordan, J. (2016). *The liability of internet intermediaries*. Oxford: Oxford University Press.
Rome Statute of the International Criminal Court, U.N. Doc 2187 U.N.T.S. 90, *entered into force*. July 1, 2002.
Rousseau, J. J. (1762). *Du contrat social ou Principes du droit politique*. Paris: LibrioPhilosophie.
Santosuosso, A. (2013). *Legal problems of modern robotics*. Paper delivered at Legislation for Technical Systems: Robotics, Autonomous Systems and Industry 4.0 are challenging law, European Center for Law, Science and New Technologies, Università degli Studi di Pavia, Wuerzburg, Germany.
Shah, R. C., & Kesan, J. P. (2007). The privatization of the internet's backbone network. *Journal of Broadcasting and Electronic Media, 51*(1), 93–109.
Stewart, J. (2011). *Corporate war crimes: Prosecuting the pillage of natural resources*. New York: Open Societies Foundation.
United Nations General Assembly. (1948). *Universal Declaration of Human Rights*, G.A. res.217 A (III), adopted by the U.N. Doc. A/810, 10 December.
United Nations General Assembly. (1966). *International Covenant on Civil and Political Rights*, G.A. res. 2200A(XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316, 999 U.N.T.S. 171, *entered into force* 23 March 1976.
Van den Bulck, P., & De Bellefroid, M. (2009). Legal regime of avatars created in the framework of video games: Some reflections in light of french and other legal systems. *Convergence, 5*(2), 257–268.
Van den Hoven, M. J. (1998). Moral responsibility, public office and information technology. In Snellen & van de Donk (Eds.), *Public Administration in an Information Age: A Handbook. Amsterdam: IOS Press*. (pp. 97–112).
Walsh, F. (2015). Bionic eye implant world first. *BBC News Online*. Retrieved February 26, 2016, from http://www.bbc.com (home page).
Want, R., Schilit, B. N., & Jenson, S. (2015). Enabling the Internet of Things. *IEEE, Computer Society, 48*(1), 28–35.
Zebra Technology. (2014). Analysis of iOS 8 MAC randomization on locationing. White Paper. Retrieved February 28, 2016, from http://mpact.zebra.com/documents/iOS8-White-Paper.pdf

CHAPTER 6

Teaching Human Rights and Digital Technology

The preceding chapters have examined the intersection between human rights and digital technology for a variety of stakeholders. This chapter presents a comprehensive approach, one that integrates the lessons learned in the four preceding chapters and brings this knowledge into the university classroom. Educational curricula offer an ideal platform for exploring the relationship between our rights and our use of technology, encouraging a rigorous examination of their complex interstice as part of either a general education programme or a specialized degree. Of particular interest is the blended classroom: this hybrid of the physical and virtual space allows students and teachers to learn by doing, to utilize technology in creative and singular ways that privilege the tangible classroom space, while providing digitized access to materials, people and discussions that are physically out of reach. This chapter examines the potential for blended, interdisciplinary learning through (1) a discussion of the right to access education and to enjoy the benefits of scientific progress, rights that the digital divide calls into question, (2) an analysis of human attention in digital environments and the consequences for higher education, (3) the presentation of a curriculum that blends the traditional classroom and the Internet, and (4) a viewpoint on the future of blended learning in an increasingly digitized university environment.

As university professors, we are particularly interested in the impact of digital technology on higher education. If we travel back in time to the origins of the modern university, the basic elements of higher education as we know it today were already in place. Academic freedom, the

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_6

erasure of social difference in the pursuit of knowledge, the merit-based awarding of degrees, and rigorous scholarly research were all considered seminal components. The first of these elements was an influential factor in prompting masters and students to formalize their relationship as a *universitas* in 1150 with their preliminary act of incorporation in Paris, the second such initiative after Bologna. This act was designed to protect professors and pupils from local political and religious interference, assuring their intellectual independence through provision of a special judicial status within the city walls of Paris.[1] The University of Paris was well under way by the time the pious Robert de Sorbon sat his students down on hard wooden benches in 1250 to discuss theology in the open air. The son of a peasant and a successful ecclesiastic, Sorbon hoped to make learning available for all students (at least for all males) and organized a society of learned clergymen who taught for free. This was a novelty. According to French historian Jacques Le Goff, one of the main innovations of the medieval university was a mechanism for social advancement based on the acquisition of knowledge.[2] The university degree system served not only as a certification of acquired skills, but also as a means of social differentiation that conferred status.[3] By 1257, Robert de Sorbon welcomed his first student boarders to what we now call the Sorbonne, one of several independent college buildings on the city's left bank where students studied theology, canon law, medicine and the liberal arts in Latin.[4] The library, which catalogued over 1000 volumes in 1290 and still houses one of the oldest collections of medieval scholarship in Europe, was a reference base and repository for faculty research, its remarkable collections drawing the best scholars in Christendom to Paris.[5] The Sorbonne quickly became an authority on theological and canonical questions, extending its influence down through the centuries as an independent reference on religious and, eventually, secular matters.[6] For the purposes of this chapter, the university's first free and open-air classrooms still exercise a certain influence on what we mean by education and how we transmit knowledge to future generations.

This is particularly true in an age of e-learning, where the massive open online course (MOOC) provides free instruction for anyone with access to the Internet. As an open learning platform, the MOOC arguably promotes academic freedom (the liberty to learn and to make course content accessible online) and the erasure of social difference in the pursuit of knowledge, while the Internet serves as a vast repository for scholarship, including some of the original thirteenth century

Sorbonne manuscripts now digitized and available online. One university president has suggested that MOOCs may eventually replace the university in the years to come.[7] By reorganizing the vertical transmission of 'knowledge creation, teaching, testing, and credentialing' into a horizontal format available to anyone with Internet access, MOOCs 'decouple teaching and learning from the campus on a mass scale'.[8] While much ink has been spilled on what scholars call the democratization of university learning,[9] we are not fully convinced that e-learning platforms will replace the campus as we know it. In fact, we argue in this chapter that the physical classroom space still has value in twenty-first century society as a site for the transmission of intellectual rigour. Our definition of blended learning—a hybrid of the physical and virtual space which allows teachers and students to apply theory to practice, to utilize technology in creative and singular ways that privilege the tangible classroom discussion space, while providing digitized access to materials, people and discussions that are physically out of reach—is a distant echo of the earlier open-air classrooms of medieval Paris. The designated classroom space provides a geographic locale for animated, interactive discussion where human intelligence and emotion are not limited to the information sharing of Web platforms. Student attention is captured by vibrant exchange and learning is focused on collective input, particularly if individual screen use is kept to a minimum. The virtual component of the blended classroom brings university students into contact with learners and experts from across the globe to test and expand their knowledge. This component also prepares students to use technology with discernment, learning to hold online resources and exchanges to the same standards as those used when engaging with university faculty members and academic scholarship.

University curricula offer an ideal platform for exploring the relationship between our rights and our use of technology, encouraging a rigorous examination of this complex interstice as part of a general education programme or a specialized degree in ethics, law, engineering or policy-making. This chapter argues for a more comprehensive approach to this subject, one that integrates the lessons learned in the preceding chapters and brings this knowledge into the classroom. We begin by examining access to education and to scientific progress, rights enshrined in the International Covenant on Economic, Social and Cultural Rights. Access to these rights, termed 'progressive rights', should

in theory be facilitated by digital technology. Nonetheless, we argue that this may not always be the case. In addition to the digital divide, the potential for blended, interdisciplinary learning may be jeopardized by other issues, such as questions on human attention in digital environments. In previous publications, one of the authors of this book has explored the effects of information and communication technology on human attention[10] and how systems could be designed in order to eliminate extraneous cognitive load and help users navigate an increasing number and quality of different solicitations.[11] This includes specific situations, such as reading comprehension in electronic versus print formats[12] and attention-aware computer systems in learning environments, where frequent interruptions, multitasking and information overload are the norm.[13] In the second section, we analyse how attention is shaped and influenced by the same digital tools employed to support learning and how this may inflect learning in the blended classroom. We posit that in order to access our rights to an education and to scientific progress, we must first be able to pay attention. This attention may take a shape that is different from the focused attention normally associated with effective knowledge acquisition, leaving us with many questions on how best to employ digital tools in an educational context.

In the third section, we present a curriculum for teaching human rights and digital technology to university students in the social sciences. The chapters of this book and the issues raised therein constitute a series of curricular units that foster classroom discussion and online outreach, a mix of theory and practice that encourages students to question how they are going to live with digital technology in their personal and professional lives in the years to come. UNESCO (United Nations Educational, Scientific and Cultural Organization) has designated higher education as the forum for acquisition of 'critical thinking', a broad based learning objective that operates much like a holy grail in the academy. The World Conference on Higher Education Partners has pointed out the importance of critical thinking in claiming that at no time in human history has 'the welfare of nations' been 'so closely linked to the quality and outreach of their higher education systems and institutions'.[14] The fourth section of this chapter closes with a broader reflection on the university in a digitized world. What impact does the current discourse on technology and numeracy more generally have on the university learning experience? We hope that by asking the right questions we may preserve for future generations the age-old tradition of university scholarship.

6.1 Progressive Rights

We introduced the International Covenant on Economic, Social and Cultural Rights in our second chapter in discussion of human health and the protection of children from electromagnetic wave pollution generated by wireless technology infrastructure. According to article 2(1) of the Covenant, each state signatory agrees:

> 'to take steps … to the maximum of its *available* resources, with a view to achieving *progressively* the full realization of the rights recognized in the present Covenant by all appropriate means ….' (Authors' emphasis)

Consequently, the right to an education or the right to enjoy scientific progress in the form of digital technology, as acknowledged in articles 13, 14, and 15(b) of the Covenant, are to be *progressively* implemented according to the economic resources *available* to the state. General Comment 13, which articulates a normative interpretation of articles 13 and 14 of the Covenant, emphasizes that 'education shall be directed to the full development of the human personality' and that higher education 'is to respond to the needs of students in different social and cultural settings, and have flexible curricula and varied delivery systems, such as distance learning.'[15] Nevertheless, 'the right to an education must not only be understood as a social right … but also as a liberal right which provides protection against an omnipresent state authority'.[16] Despite the importance in promoting education as a bulwark against despotism, economic, cultural, and social rights are more often than not interpreted as human needs,[17] a legal demotion which hinders full application of what the treaty views as a progressive *obligation*.

The only imperative of the treaty is the non-derogable clause in article 2 on freedom from discrimination, discussed in Chapter 5:

> the rights enunciated in the present Covenant will be exercised without discrimination of any kind as to race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Thus, our understanding of the application of the Covenant to the use of digital technology in a learning environment must take into account the one imperative of this treaty, namely the right to be free of discrimination of any kind in accessing an education or enjoying the benefits of

scientific progress. The Committee on Economic, Social and Cultural Rights has dealt at length with the anti-discrimination clause, signifying its importance in each of its general comments, especially General Comments 3, 16, and 20. Many commentators, including the UN Commission on Science and Technology Development, believe that digital technology may offer a silver bullet for free and fair access to education and scientific progress for all. Nonetheless, although 97 per cent of the global population uses a mobile phone, only 43 per cent has access to the Internet on a phone or computer,[18] a factor that the UN Broadband Commission for Sustainable Development hopes to address by connecting another 1.5 billion people by 2020.[19] According to a report of the International Telecommunications Union (ITU), Internet connectivity is impeded by factors such as lack of infrastructure or affordability, and the absence of e-skills or appropriate digital content in an accessible language.[20] Thus, given the higher rates of mobile phone connectivity, the future of distance education, for example, may be tied to the small screens of our mobile devices—portable phones and tablets. But, what kind of education are we talking about? Three issues are of seminal importance when discussing the use of digital technology to provide equal access to education for all: the digital access divide, the digital capital divide, and the role of teachers in an evolving electronic landscape.

As noted in the ITU study above, the access divide is due to lack of hardware infrastructure and product affordability, which make it impossible for just over half of the world's citizens to access the Internet. The Pew Foundation has noted a persistent access gap in the USA that is closely tied to marginalizing characteristics, such as low household income, geographic remoteness, old age, disability or immigration status.[21] Still, Internet access for US adults increased from 52 per cent in 2000 to 84 per cent in 2015, and the gap in use has continued to narrow for marginalized populations.[22] It is likely that a global strategy of increased Internet connection for another 1.5 billion people and the ongoing adaptation of mobile devices for digital learning will contribute to narrowing the physical access gap worldwide in the coming decades. Even as this occurs, we currently have no democratic institutional framework to evaluate the way digital networks distribute benefits, or how they may discriminate or provide differential access.[23]

Certain populations that are already marginalized may find their vulnerabilities exacerbated by digital technology. We discussed the issue of vulnerability and digital hardware in our second chapter, arguing that wireless

technology has been rolled out by force, with scant attention paid to the potential long-term health impact of exposure to heightened electromagnetic wave pollution. But, for every school child or adult who requires protection from electromagnetic pollution, there is a marginalized individual who is clamouring for access to the digital universe. Cabled access to digital systems with built-in privacy enhancing technologies may be one way to offer both protection for the hyper-electro sensitive and access to digitized assistance for an array of marginalised populations with very different needs. The elderly and the disabled may benefit from regular monitoring, robotic assistance with household tasks, and reduced isolation through online visits with family, e-learning, e-voting and enriched discussion platforms. As the cost of technology continues to decline, populations of all ages may benefit from access to online learning platforms, significantly enriching their daily lives and contributing to 'the full development of the human personality'. Yet, rather than simply assuming that online learning is positive, it would behove scholars and policymakers to expand their understanding of the digital divide, question the quality of user experiences, and ask whether the core human rights of learners are enhanced or violated in a digital environment.

Secondly, as noted by the OECD (Organisation for Economic Co-operation and Development), access is not enough in ensuring education for all; there is also a digital divide between 'those who have the right competencies to benefit from computer use, and those who do not'.[24] The economic, cultural and social capital of the individual plays a determining role in how students use digital technology to learn. As Jeroen van den Hoven has pointed out, those 'who cannot keep pace with the pervasiveness (of digital technology) will progressively become de-skilled, disempowered and less knowledgeable'.[25] Data suggests that the majority of those who use online learning platforms have a university diploma and sign up for a MOOC to reinforce their professional skills or retool their capacities.[26] Martin Hilbert has done interesting comparative work on gendered digital access in Latin America and Africa, demonstrating that the digital divide is 'a direct reflection of existing gender-related inequalities'. Nonetheless, in those circumstances where men and women have the same employment, income and education levels, women are more likely to use digital technology than men.[27] Hilbert suggests that 'policy actions should make use of the natural communication skills and media capacities of women and their proven embrace of the new digital opportunities to overcome longstanding gender inequalities'.[28] While women's communication skills may or

may not be 'natural', this study reinforces the social capital theory that highlights the importance of previously acquired skills in making use of digital technology for the acquisition of additional knowledge.

Finally, a 2015 report on online education in the USA noted reluctance on the part of teachers to use digital technology in their courses.[29] This raises two important questions. Is this reticence due to technological foot-dragging? Or is the promise of a tailor-made course for every student with a mobile phone unnerving for the majority of teachers and professors? Most professionals note that it takes far more time to prepare and run an online course than a traditional classroom course.[30] Nonetheless, enthusiasm for digitized education remains high amongst researchers. In a recent paper, Darrell West suggests that mobile technology 'is a catalyst for creating impactful change in the current system and crucial to student development in the areas of critical-thinking and collaborative learning'.[31] While we certainly agree with West that critical thinking and collaborative learning are skills that young people need to acquire, we are surprised that mobile phones could be considered viable agents to foster critical thinking. Critical thinking is often learned in an effort to solve what Ken Bain calls intriguing, beautiful or important problems.[32] Collaborative work with fellow students is not always reinforced by individual mobile phone use. In short, teaching professionals may know something that researchers and technology pundits do not: namely that the digital revolution, like the print revolution before it, is not the end, but rather one of a multitude of means to access an education. The high levels of mobile phone use worldwide suggest that portable devices have interesting potential as a support mechanism for blended learning. But, by depending on technology alone to deliver critical thinking and collaborative skills, we risk creating new problems that affect non-discriminatory access to education and the enjoyment of scientific progress, including unforeseen challenges related to human learning and attention in digital environments.

6.2 Attention in the Blended Classroom

Attention is a determining factor in every human activity, whether mental or physical, personal or relational. Our ability to appropriately allocate attention determines the success of our interaction with the world, our creative activities, and our learning and collaboration. In general, the right choice in terms of attention focus is essential for efficient time management, sustained deliberation, learning and, ultimately, for the achievement of our goals and desires.

Structuring the way in which students are mentored and educated requires recognizing that their networked, fast paced, multitasked operational style inflects the manner in which educators reach and communicate with them. Some authors go as far as to state that 'we are in the midst of a generational shift in cognitive styles that poses challenges to education at all levels, including colleges and universities'.[33] Educators must assess their role in reinforcing reflection and deep analysis within a system that privileges the opposite—rapid negotiation in an environment of multiple attention foci. Policymakers should also consider, as many educators already do, ways to exploit technological infrastructure and students' mode of operation to capture their interest, imagination and creativity so as to enhance the nurturing of enriched learning environments.

The advent of information and communications technologies has radically changed the balance between the availability of information and the human capacity to process it. Most observers acknowledge that information was a scarce resource throughout history and that this situation began to evolve rapidly in the second half of the twentieth century. Already in the late 1960s Herbert Simon remarked:

> 'When we speak of an information-rich world, we may expect, analogically, that the wealth of information means a dearth of something else—a scarcity of whatever it is that information consumes. What information consumes is rather obvious: it consumes the attention of its recipients'.[34]

As we have seen in previous chapters, available information not only includes online material or messages from humans, but also the information increasingly generated by multiple sensing devices that track the surrounding environment and our actions; examples include information produced by push messages on smartphones and wearables like smart watches or fitness trackers.

Human experience, as well as studies in cognitive psychology and neuroscience, demonstrates that our brain has a limited capacity for processing stimuli that come from within (as we try to follow a train of thought) or from outside (as we take note of the images, sounds or smells of our surrounding environment). Similarly, our body can only perform a limited number of actions at once: we can turn our head to one side or the other, extend one leg at a time over the other. Everything we do, see, hear or think is the result of continuous choices between a very large number of

activities we could potentially engage in. We refer to the processes underlying these choices as 'attention'.

When interacting with the world, we receive a number of solicitations that are orders of magnitude larger than what we can actually handle; attentional processes allow us to allocate our limited cognitive resources to the processing of certain stimuli rather than others. At a party, for example, we generally can select the conversation of our friends and distinguish it from other conversations at close range. However, if something draws our attention to a conversation taking place nearby—if we hear someone pronounce our name, for example—we can 'tune in' to the other conversation, but at the price of not knowing what our friends are saying.[35] Similarly, we may not see a friend's name on the gate interphone, even if it is perfectly visible in front of us, until someone tells us it is located at the top of the left-hand column of names. By turning our attention to this focus, our brain becomes more responsive to visual stimuli from this zone.[36] When our visual attention is cued on a specific area, object or event, however, everything that is outside of this privileged area will leave only a minimal trace in our memory (and in our consciousness). Some authors argue that we only have a conscious perception of those parts of the perceptual world to which we pay attention.[37] Further, attention affects our actions by allowing us to adapt to situations that are not habitual. Some readers may have experienced walking out of their home at the usual time in the morning and taking the road to work even on occasions when, in fact, they had to go elsewhere. This is a form of automaticity that can only be overridden by 'paying attention', and thereby allocating appropriate cognitive resources to the new situation. In their seminal work, Donald Norman and Tim Shallice have proposed that 'two complementary processes operate in the selection and control of action. One is sufficient for relatively simple or well-learned acts. The other allows for conscious, attentional control to modulate the performance.'[38]

Given these few examples, it is clear that most forms of information overload and attention scarcity existed well before the advent of information and communication technologies. The question we ask is why current digital technologies have such a significant impact on the way we structure our activity, learn and perceive the world. One of the authors of this book has argued that information and communication technologies stress our attention in two related manners.[39] First, they disrupt well-established communication rules by providing a continuously growing amount of

information and communication streams in a manner that is ill-suited for human processing. A defining factor of successful human communication is the ability of a speaker (or communicator) to adapt to the attentional state of the listener (or receiver). As humans, we learn at an early age that successful communication requires that the receiver pays attention to the message; we then learn to recognize the conditions under which such attention is obtainable (and is polite to obtain) and we also learn how to best adapt our message (its content, modality and conspicuousness, for example) to the specific attentional state of the receiver. Further, we follow up on our messages to ensure that communication has effectively taken place (we may repeat a sentence to check whether it has been heard, for example). We also organize our dialogues around a set of rules that, until the advent of digital technology, allowed us to limit the cognitive load associated with communication. Paul Grice, for example, has described these rules under the umbrella of the 'cooperative principle.'[40] This ability to detect, reflect on and adapt to the attentional state of communication partners is continually lost in computer-mediated communication. While no one would ever dare, except in the case of a real emergency, to walk into a classroom with a lecture in session to say something to a student attending the lecture, that same person would feel perfectly comfortable sending a text or voice message. The digital tool, which is not designed to recognize the 'lecture in session' context, will deliver the message and may do so with a loud notification sound. Everyone's attention will be disrupted. This is a very simple example of how, through the use of technology, well-established communication rules are often bypassed.[41] The disruption would be limited if the receiver had simply ignored the message or, ideally, turned off his or her device. However, humans increasingly use in a synchronous manner technology that was originally conceived and designed to be used asynchronously; this is linked to the second stress factor described below.

Digital technologies act as a vehicle for a set of new social norms that demand the fast processing of the large amount of information they provide us with. This problem arises from the role that attention and digital technology play in the power relations of our society. Jonathan Crary notes that since the late nineteenth century the notion of attention has been reshaped:

> It is possible to see one crucial aspect of modernity as an on-going crisis of attentiveness, in which the changing configurations of capitalism con-

> tinually push attention and distraction to new limits and thresholds with an endless sequence of new products, sources of stimulation, and streams of information.[42]

The development of digital technologies (as with every form of technology) is ultimately guided by economic needs aimed at increasing both labour efficiency and consumption. The digital tools we use necessarily reflect the social and economic structures within which they have been created, so that attention has become a 'valuable currency', as Thomas Davenport and John Beck described it.[43] Firms compete for the attention of their customers, employers strive to control the attention of their employees, politicians contend for the attention of voters, the media have created a star system completely dedicated to attracting audience attention, and people expect the full attention of their friends. Consequently, not only has digital technology increased demands on our limited cognitive resources because of its power to disrupt human communication principles, but it also transmits a pressing encouragement (and, in certain situations, an obligation) to attend to the ever growing amount of information provided.

This is the context within which digital tools join education. These devices provide many sources of information, the possibility to communicate across continents, and the opportunity for creative management and distribution of knowledge; but, these same tools also generate constant pressure for greater productivity and 'social survival', both of which challenge our students to immediately respond to a variety of solicitations.[44] This new mode of being is characterized by very frequent interruptions and multitasking. Although interruptions may bring information to one's attention that is useful for a primary (current) task or, in the case of simple primary tasks, facilitate task performance,[45] it has been widely reported that interruptions increase the load on attention and memory.[46] This is turn may generate stress,[47] reduce satisfaction with one's own performance,[48] disrupt reading comprehension,[49] and compromise the performance of the primary task.[50] One study found that medium-level multitaskers perform significantly better (complete the task faster) than both high- and low-level multitaskers. The same study also found that increased levels of multitasking lead to a significant loss in accuracy and more mistakes.[51] Another study demonstrated that interruptions are more likely to reduce performance in cognitive tasks and to reduce accuracy in skilled tasks.[52] It also appears that multitasking has particularly negative effects on the performance of tasks that are considered to be difficult[53]

and that interruptions are more disruptive for people with low working memory capacity.[54] Still, recent studies in neuroscience have demonstrated that multitasking limitations could be due to the slow speed of information processing in the human prefrontal cortex, a limitation that may be improved to a certain extent with training.[55] Very few experiments analyse the effect of digital interruptions on learning; those that do report a relatively small effect on students—4.5 per cent of a test score—a result that remains significant for the test taker.[56] One experiment also found that interest, although generally correlated with an intrinsic motivation to learn and long-term retention, does not mitigate the negative effects caused by digital interruptions.[57]

In order to take full advantage of blended learning, we need a better understanding of the mechanisms that regulate attention allocation. If the use of digital tools requires multitasking, it is essential to comprehend under which circumstances and for what type of student multitasking may be effective and under which sort of guidance. While technology promises extreme personalization of learning with just-in-time, ubiquitous and tailored material for every student, this may come at a cost that we have not yet fully analysed. In the same way that not every book is adapted to support learning in every situation, not every digital tool can be equally useful in achieving every learning objective and, in certain situations, removing the devices altogether may be the more effective solution. At the same time, we need to recognize that focused attention, the type of attention we have historically associated with effective learning, may not be the sole form of attention that is best suited to all types of knowledge acquisition.

6.3 Teaching Human Rights and Digital Technology

This section presents an example of a blended learning curriculum, one that aims to explore the theoretical intersection of human rights and digital technology, while integrating a practical component that allows students to produce educational materials for stakeholder audiences.[58] The educational and reference material generated by the course targets the social, ethical, legal and technical issues that the use of digital tools raises for stakeholders across society. It is important to note that, given our interest in human attention in digital environments, we are equally sensitive to boredom in the classroom; getting just the right mix of theory and

practice, teaching and learning input, physical and virtual communication is challenging for even the most experienced students and their professors.

Our curriculum encourages students to identify the trade-offs that occur as new technologies are regulated, or not regulated, by their governments. We emphasize that no public or private actor is above the law or the general public interest. We take issue with the idea that human rights protection of digital technology users is a win-win equation for all concerned. Rights protection is often expensive for governments or businesses to implement, but such protection reinforces the social contract that underpins democratic governance and provides an ethical legitimacy for political and corporate actors. The example of online privacy runs as a multifaceted theme throughout our course, focusing student attention on a problem that creates a variety of different expectations amongst stakeholders and affords multiple technical solutions. We explore the diversity of privacy paradigms that populate the online experience (such as user control, confidentiality and practice); we compare the regulatory frameworks currently applied in various countries with a focus on European and US law; and introduce several privacy enhancing technologies, explaining how privacy may be embedded into digital systems.

Our syllabus incorporates the following discussion units:

1. Histories of human rights and digital technology;
2. Hardware systems and wireless technology;
3. National security paradigms and the integration of privacy as a default setting for all digital systems;
4. Contours of online censorship and the protection of vulnerable populations;
5. Human autonomy and the Internet of Things;
6. Ecological end-to-end product design and use of digital technology;
7. Student production of user-centric material to raise awareness of human rights-based digital technology use.

The first time that we offered this course, we encouraged our students to reflect on users and their needs by asking them to design educational materials on privacy for a variety of stakeholder communities. Few guidelines were issued in an effort to encourage intellectual autonomy. Thanks to the small class size typical of liberal arts institutions, we were able to establish groups of no more than five students, each with an assigned

target audience: the general public; the digitally reluctant; children; EU regulators not working on privacy; national regulators not working on privacy; and human rights advocates. None of these audiences can be considered specialists on privacy issues. Students were given the option to make their final product available on the Creative Commons portal, following a discussion of copyright protection and whether the Creative Commons offered an opportunity to influence political discourse on the issue of privacy protection. Students presented their projects to their classmates in order to receive peer feedback, and submitted regular drafts for our comments before handing in their final project in electronic form. In our determination to empower our students, we underestimated their initial sense of panic caused by the lack of detailed guidelines. Nonetheless, within three months, our students demonstrated, through their production of rich, yet streamlined educational material, a mature understanding of the theoretical convergence of human rights and digital technology as manifested in online privacy issues. Each of the final products embodied the incorporation of students' user experiences into the design of educational materials; a commitment to striking visual design; and a sophisticated awareness of the Internet as a public good, an online extension of their 'heterogeneous and thickly integrated' social lives.[59] Figure 6.1 is an example of the material produced by the students, in this case a recto-verso infographic for the general public (only the front page is shown). Additional student-produced material can be accessed on the PRIPARE project repository for educational material.[60]

By working closely with six student teams over the course of the semester, we were provided with a window on the thinking of the general user. Non-engineering students who spend an average of two to three hours a day online are ideally situated to design knowledge products that promote online security and privacy to the general public. The highly critical analyses embedded in the student knowledge products is a reflection of the curriculum's assigned readings, lectures and discussions that bring together law and science in an effort to explore technology as it impacts our lived experience. By transferring privacy principles to the larger domain of human rights and digital technology, our students were able to view security and privacy protection as part of a larger exploration of how we are going to live in a digitally connected society.

The blended learning component—that hybrid space that allows students and teachers to use technology in creative and singular ways that privilege classroom discussion and feedback, while providing access to

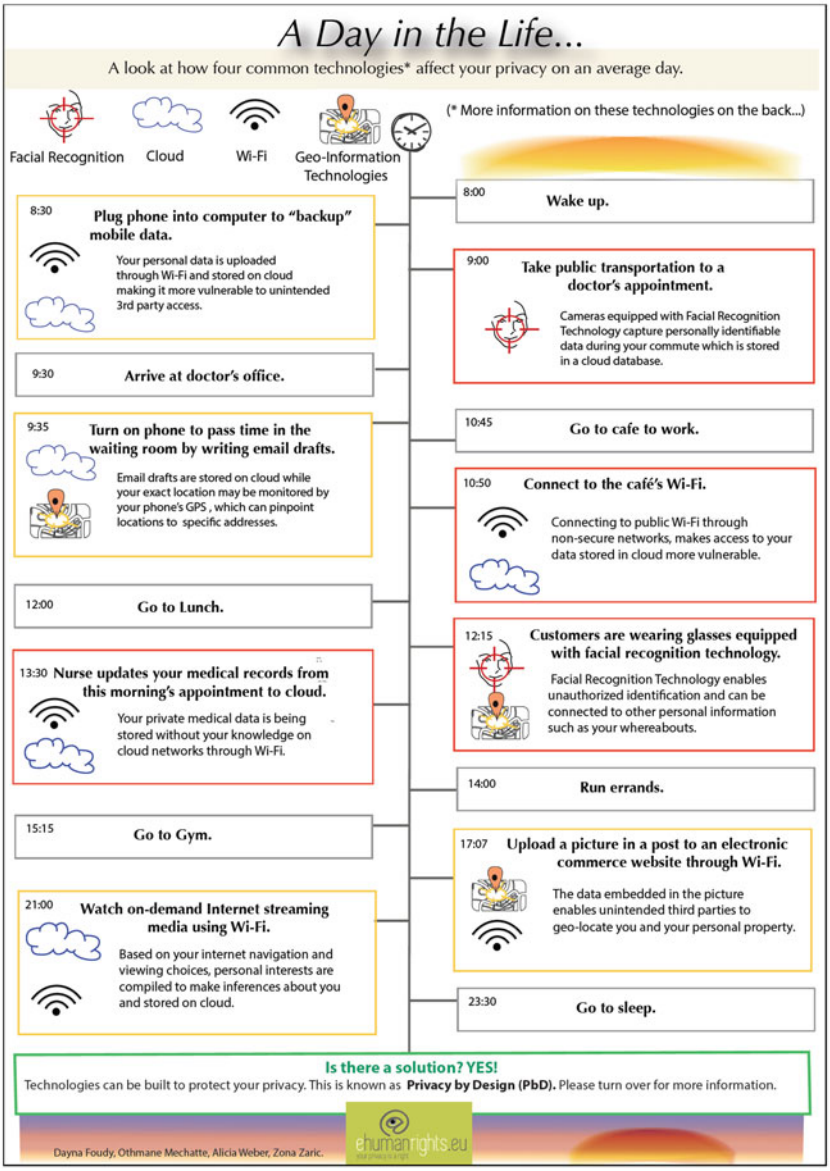

Fig. 6.1 A day in the life—A student-created infographic

materials and expertise that are physically out of reach—was certainly manifest in this course. Technology use was both the subject and the medium of this collective intellectual exercise. Nonetheless, at no point could technology alone have replaced the central role of in-class exchanges in developing a critical approach to human use of digital tools. Our experience indicates that digital technology is not a silver bullet that guarantees access to education for all. In order to harvest the full potential of student attention in a learning environment, we need teachers rather than machines to provide the sophisticated, idiosyncratic analysis that guides student understanding of the world around them.

6.4 Digital Learning and Higher Education

The digital revolution has demystified knowledge and is forcing us to rethink how we deliver a university education. Certain scholars have suggested that humans will eventually be reduced to 'communications portals' in a world of ubiquitous computing. We refute the notion that our students may serve as mere communication portals, but we note the creeping virtualization and disruption of our physical interaction with the surrounding environment, a phenomenon that is likely to impact the realisation of certain individual rights. We suggest that virtualization and disruption of our physical experience through digital technology may present an unprecedented opportunity for higher education. The university, for example, could focus on the transmission of intellectual autonomy and critical thinking in an effort to prepare students to fully engage in the extension of these hard-won human rights from the material to the virtual universe.

Blended learning as described in this chapter may provide just the right balance between the physical and virtual experience. In an age of information glut, education can no longer be concerned with the strict transmission of knowledge per se, but must privilege the teaching of intellectual discernment, selective powers of concentration and creative problem-solving in a fast changing global environment. Kristen Luker has suggested that we learn to salsa dance our way through the realms of data, teaching our students to invest in causal analysis rather than descriptive repetition, using interdisciplinary overlap as a means to frame canonical intersections and assign order to a virtual world of ubiquitous information.[61] Richard Lanham puts the importance of the digital revolution into perspective when he notes that the last time such a learning revolution occurred was

when medieval scribes started putting spaces between words and adding punctuation nearly 1000 years ago.[62] More importantly, he points to the rich mixture of oral and literary tradition that forms the cornerstone of Western culture and argues that we 'toggle back and forth between them' because we cannot hold both in our minds at the same time. A blended learning environment encourages university students to master yet a third element—the newly formed virtual tradition—and to toggle back and forth among all three without losing the 'power of propositional thought' (or their attention span).[63] By combining the physical teaching space with a virtual learning platform, students learn to toggle between the oral, literary and virtual traditions and to compare the resonance of propositional thought in a seminar classroom versus an online setting. Proponents of 'deep learning' expect that 'the intention to extract meaning produces active learning processes that involve relating ideas and looking for patterns and principles on the one hand, … and using evidence and examining the logic of the argument on the other.'[64] Given the challenges of human attention in digital environments discussed above, a blended curriculum both recognizes and legitimizes the digital space and trains students to work in it and with it, while continuing the millennial university tradition of propositional thought.

To conclude, the power of propositional thought is critical to our understanding of how to live in a digital environment. The secular human rights framework, a successor to Kant's 'moral law' that guides our understanding of human dignity and justice,[65] provides a framework for analysing the impact of the escalating shift from the physical to the virtual experience. Rather than provide free education for all, we are concerned that digital technology as an educational tool is far too dependent on non-technological factors, such as an individual's socio-economic and cultural capital or attention span, considerations which may render the promise of universal access to education and the enjoyment of scientific progress moot. Technology may exacerbate already widening inequalities across societies unless we use it in conjunction with human to human transmission of knowledge. Before investing in costly digital classroom systems, we suggest that educators everywhere evaluate how and why they use technology, and do so on a regular basis, as their students and society evolve around them. Our students are 'digital natives' who have shown us that they require experienced human input in order to master propositional thought. Their attention is compromised in a digital environment at the same time that their use of digital tools provides them with greater access to

a broader variety of knowledge than ever before. How well educators master this new set of contradictions will determine whether the university's humanistic components of academic freedom, erasure of social difference in the pursuit of knowledge, the merit-based awarding of degrees, and rigorous scholarly research will continue in the centuries to come.

Notes

1. See Roux, S. (1992) *La Rive gauche des escholiers (XVe siècle)* (Paris, Éditions Christian); Charle, C. and Verger, J. (2015) *Histoire des universités XIIe au XXIe siècle* (Paris: Presses universitaires de France).
2. Le Goff, J. (1964) 'Quelle conscience l'université médiévale a-t-elle eue d'elle-même ?', *Miscellanea Mediaevalia III*, pp. 15–29.
3. Destemberg, A. (2009) 'Un système rituel ? Rites d'intégration et passages de grades dans le système universitaire médiéval (XIIIe-XVe siècle)', *Cahiers de Recherches Médievales et Humanistes*, Vol. 18, pp. 113–132.
4. Donation de Saint Louis en faveur de Robert de Sorbon, février 1257. A digital reproduction of the document is available at Archives de France: http://www.archives-defrance.culture.gouv.fr/action-culturelle/celebrations-nationales/2007/vie-politique/la-fondation-du-college-de-sorbonne.
5. Jolly, C. (1989). *Histoire des bibliothèques françaises: Les bibliothèques médiévales, du VIe siècle à 1530* (Vol. 1), *A. Vernet Ed,* (Paris: Promodis-Éditions du Cercle de la librairie).
6. Charle and Verger (2015) *Histoire des universités XIIe au XXIe siècle.*
7. Aoun, J. (2012) 'A shake-up of higher education', *Boston Globe*, November 17.
8. Aoun, (2012) 'A shake-up of higher education'.
9. See: Schmid, L., et al. (2015) 'Fulfilling the Promise: Do MOOCs Reach the Educationally Underserved?', *Educational Media International*, Vol. 52, No. 2, pp. 116–128; Rhoads, R.A., et al. (2015) 'The Massive Open Online Course Movement, MOOCs, and Faculty Labor', *The Review of Higher Education,* Vol. 38, No. 3, pp. 397–424; Alcock, S.E., Dufton, J.A. and Durusu-Tanriöver, M. (2015) 'Archaeology and the MOOC: Massive, Open, Online, and Opportunistic', *Journal of Social Archaeology,* Vol. 16, No. 1, pp. 3–31; Carver, L. and Harrison, L.M. (2013) 'Moocs and Democratic Education', *Liberal Education* Vol. 99, No. 4 pp. 20–25.
10. Roda, C. (2014) 'Économiser l'attention dans l'interaction homme-machine', In Yves Citton (ed.), *L'économie de l'attention: révolutions à venir?* (Paris: La Découverte).
11. Roda, C. (2011) 'Human Attention and its Implications for Human-Computer Interaction', pp. 11–62 *in* Roda, C. (ed.) *Human Attention in Digital Environments* (Cambridge: Cambridge University Press).

12. Lee, H., Young, T., Roda, C. (2013) 'E-Books Usability: Reading Time and Comprehension', *The Tablet Symposium: Examining New Media Objects,* University of Sussex, 10th April.
13. Roda, C. (2010) 'Attention support in digital environments, nine questions to be addressed', *New Ideas in Psychology*, Vol. 28, No. 3, December 2010, pp. 354–364.
14. See United Nations Educational, Scientific and Cultural Organization (2015) 'Draft Preliminary Report Concerning the Preparation of a Global Convention on the Recognition of Higher Education Qualifications', *UNESCO,* http://www.unesco.org/new/en/education/themes/strengthening-education-systems/higher-education, date accessed 25 March 2016.
15. United Nations Committee on Economic, Social and Cultural Rights (1999) 'General Comment No.13: The Right to Education (Art. 13)', adopted at Twenty-first session, in document E/C.12/1999/10, *Office of the High Commissioner on Human Rights,* paragraphs 4 and 18.
16. Beiter, K.D. (2005) *The Protection of the Right to an Education by International Law* (Leiden: Martinus Nijhoff Publishers), p. 41.
17. Beiter (2005) *The Protection of the Right to an Education by International Law*, p. 2.
18. International Telecommunication Union (2016) The World in 2015: ICT Facts and Figures.
19. Philbeck, I. (2016) 'Working Together to Connect the World by 2020', *International Telecommunications Union.*
20. Philbeck (2016) 'Working Together to Connect the World by 2020', p. 4.
21. Perrin, A. and Duggan, M. (2015) 'Americans' Internet Access: 2000–2015', *Pew Research Center.*
22. Perrin and Duggan (2015) 'Americans' Internet Access: 2000–2015'.
23. van den Hoven, J. (2012) 'Fact Sheet-Ethics Subgroup IoT-Version 4.0', Chair Ethics Subgroup IoT Expert Group, *Deft University of Technology,* p. 6.
24. Pedro, F. (2010) 'Educational Research and Innovation: Are the New Millennium Learners Making the Grade? Technology Use and Educational Performance in PISA 2006', *Center for Educational Research and Innovation*, OECD.
25. van den Hoven (2012) 'Fact Sheet-Ethics Subgroup IoT-Version 4.0', p. 8.
26. Tucker, L. (2014) '7 Reasons to take a MOOC', *QS Top Universities*, 29 August, http://www.topuniversities.com/blog/7-reasons-take-mooc.
27. Hilbert, M. (2011) 'Digital gender divide or technologically empowered women in developing countries?' *Women's Studies International Forum*, Vol. 34, No. 6, pp. 479–489.
28. Hilbert (2011) 'Digital gender divide or technologically empowered women in developing countries?' pp. 21–22.

29. Allen, I.E. and Seaman, J. (2015) 'Grade Level: Tracking Online Education in the United States', *Babson Survey Research Group*, p. 30.
30. Allen (2015) 'Grade Level: Tracking Online Education in the United States', p. 30.
31. West, D.M. (2015) 'Connected learning: How mobile technology can improve education', *Center for Technology Innovation at Brookings*, p. 6.
32. Bain, K. (2004) *What the Best College Teachers Do* (Cambridge, MA: Harvard University Press).
33. Hayles, N.K. (2007) 'Hyper and deep attention: the generational divide in cognitive modes', *Profession*, Vol. 13, pp. 187–199, p. 187.
34. Simon, H.A. (1971) 'Designing Organizations for an Information-rich World', Greenberger, M. (ed), *Computers, Communications, and the Public Interest*, (Baltimore: John Hopkins Press), pp. 38–52.
35. In several experiments, Colin Cherry demonstrated in 1953 that we are able to privilege certain sounds, but at the price of having almost no trace of the sounds that we have not listened to.
36. In a series of experiments, Michael Posner demonstrated the existence of the mechanisms we use to orient our visual attention towards the areas where we expect to see what we are looking for.
37. Mack, A., Rock, I. (1998), *Inattentional blindness*, (Cambridge: MIT Press); Simons, D.J. and Chabris, C.F. (1999) 'Gorillas in our midst: Sustained inattentional blindness for dynamic events', *Perception*, Vol. 28, No. 9, pp. 1059–1074.
38. Norman, D., and Shallice, T (1986) 'Attention to action: Willed and automatic control of behavior', in Davidson, R.J., Schwartz, G.E. and Shapiro, D. (eds.), *Consciousness and Self-Regulation* (New York: Plenum), Vol. IV: pp. 1–18, citation on p. 3.
39. Roda, C. (2014) 'Économiser l'attention dans l'interaction homme-machine'.
40. To extract the meaning of sentences in a dialogue, for example, we assume that the speaker will deliver relevant sentences (Grice's 'relevance maxim'). Relevance is internal to the conversation. When the conversation is fragmented by the use of asynchronous communication devices, fragments of conversations, relevant within a dialogue, are presented to the listener in situations where they are no longer relevant. While engaged in face-to-face contact we naturally minimize dialogue fragmentation, whereas digital tools increase fragmentation.

Grice, H.P. (1975) 'Logic and Conversation', In P. Cole & J. Morgan (eds.), *Syntax and Semantics,* Vol. 3, (Cambridge: Academic Press).

41. Several researchers have explored how digital tools may be made more respectful of human attentional characteristics: see, Roda, C. ed. (2011) *Human Attention in Digital Environments* (Cambridge: Cambridge

University Press); and Bulling A. (2016) Pervasive attentive user interfaces, *Computer*, Vol. 49, No. 1, pp. 94–98.
42. Crary J. (1999) *Suspension of Perception: attention, spectacle, and modern culture*, (Cambridge, MIT Press) pp. 13–14.
43. Davenport, T.H. and J. Beck (2001) *The Attention Economy* (Boston: Harvard Business School).
44. Georg Franck draws a portrait of the social value of the attention stating that 'The attention of others is the most irresistible of drugs. Its acquisition eclipses any other sort of income.' Frank, G. (2014). 'Économie de l'attention', In Yves Citton (ed) *L'économie de l'attention: Nouvel horizon du capitalisme?* (Paris: La Découverte) p. 179.
45. Speier, C., Vessey, I., and Valacich, J.S. (2003) 'The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance,' *Decision Sciences*, Vol. 34, No. 4, pp. 771–797.
46. Gillie, T., and Broadbent, D.E. (1989) 'What makes interruptions disruptive? A study of length, similarity and complexity', *Psychological Research Policy*, Vol. 50, pp. 243–250.
47. Bailey, B. P., Konstan, J.A., and Carlis, J.V. (2001) 'The effects of interruptions on task performance, annoyance, and anxiety in the user interface', *Proceedings INTERACT '01*, pp. 593–601; Zijlstra, F., et al. (1999) 'Temporal factors in mental work: Effects of interrupted activities', *Journal of Occupational and Organizational Psychology*, Vol. 72, pp. 163–185.
48. Baethge A., Rigotti T. (2013) 'Interruptions to workflow: Their relationship with irritation and satisfaction with performance, and the mediating roles of time pressure and mental demands', *Work & Stress*, Vol. 27, No. 1, pp. 43–63; Kirchberg, D.M., Roe, R. A., van Eerde, W. (2015) 'Polychronicity and multitasking: A diary study at work', *Human Performance*, Vol. 28, No. 2, pp. 112–136.
49. Foroughi C. K., et al. (2015) 'Interruptions disrupt reading comprehension', *Journal of Experimental Psychology: General*, Vol. 144, No. 3, pp. 704–709.
50. See, Franke, J.L., Daniels, J.J., and McFarlane, D.C. (2002) 'Recovering context after interruption', Proceedings 24th Annual Meeting of the Cognitive Science Society, *CogSci 2002*, pp. 310–315; McFarlane, D.C., and Latorella, K.A. (2002) 'The scope and importance of human interruption in human-computer interaction design', *Human-Computer Interaction*, Vol. 17, No. 1, pp. 1–62; Nagata, S.F. (2003) Multitasking and interruptions during mobile web tasks', Proceedings 47th Annual Meeting of the Human Factors and Ergonomics Society, pp. 1341–1345; Speier, C., Vessey, I., and Valacich, J.S. (2003) 'The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance', *Decision Sciences*, Vo. 34, No. 4, pp. 771–797.
51. Adler, R. F., Benbunan-Fich, R. (2012) 'Juggling on a high wire: Multitasking effects on performance', *International Journal of Human-Computer Studies*, Vol. 70, No. 2, pp. 156–168.

52. Lee, B.C., Duffy, V.G. (2015) 'The effects of task interruption on human performance: A study of the systematic classification of human behavior and interruption frequency', *Human Factors and Ergonomics in Manufacturing & Service Industries*, Vol. 25, No. 2, pp. 137–152.
53. Adler, R.F., Benbunan-Fich, R. (2014) 'The effects of task difficulty and multitasking on performance', *Interacting with Computers*, 9 March.
54. Drews, F.A., Musters, A. (2015) 'Individual differences in interrupted task performance: One size does not fit all', *International Journal of Human-Computer Studies*, Vol. 79, pp. 97–105.
55. Dux, P.E., et al. (2009) 'Training improves multitasking performance by increasing the speed of information processing in human prefrontal cortex', *Neuron*, Vol. 63, pp. 127–138.
56. See, Conard, M.A., Marsh, R.F. (2014) 'Interest level improves learning but does not moderate the effects of interruptions: An experiment using simultaneous multitasking', *Learning and Individual Differences*, Vol. 30, pp. 112–117; Hembrooke, H. and Gay, G. (2003) 'The laptop and the lecture: The effects of multitasking in learning environments', *Journal of Computing in Higher Education*, Vol. 15, pp. 46–64; Rosen, L.D., et al. (2011) 'An examination of the educational impact of text message-induced task switching in the classroom: Educational implications and strategies to enhance learning', *Psicologia Educativa*, Vol. 17, pp. 163–177.
57. Conard and Marsh (2014) 'Interest level improves learning but does not moderate the effects of interruptions', *Learning and Individual Differences*, pp. 112–117.
58. This curriculum was selected by the European Union Agency for Network and Information Security (ENISA) for the 2014 *Roadmap for NIS Education Programmes in Europe*, pp 4–6. See: www.enisa.europa.eu
59. Nissenbaum, H. (2011) 'A Contextual Approach to Privacy Online', *Daedalus,* Vol. 140, No. 4, p. 12, pp. 32–48.
60. PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in Research) project educational material repository: https://pripare.aup.edu/.
61. Luker, K. (2008) *Salsa Dancing into the Social Sciences: research in the age of info-glut* (Cambridge: Harvard University Press).
62. Lanham, R. and Merkoski, D. (2008) 'The Economics of Attention', moderated by Kaplan, M., *The Norman Lear Center,* USC Annenberg School of Communication.
63. Lanham and Merkoski (2008) 'The Economics of Attention'.
64. Morin, D., Thomas, J.D.E. and Saade, R.G. (2012) 'Deep Learning and Virtual Environment', *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*. Vol. 6, No.11, p 3163.
65. Kant, I. (1781) *Critique of Practical Reason* (London: Cambridge University Press, 1997 ed., tr. Gregor, M.).

Bibliography

Adler, R. F., & Benbunan-Fich, R. (2012). Juggling on a high wire: Multitasking effects on performance. *International Journal of Human-Computer Studies, 70*(2), 156–168.

Adler, R. F., Benbunan-Fich, R. (2014, March 9). The effects of task difficulty and multitasking on performance. *Interacting with Computers*. First published online.

Alcock, S. E., Dufton, J. A., & Durusu-Tanriöver, M. (2015). Archaeology and the MOOC: Massive, open, online, and opportunistic. *Journal of Social Archaeology, 16*(1), 3–31.

Allen, I. E., & Seaman, J. (2015). *Grade level: Tracking online education in the United States*. Babson park, MA: Babson Survey Research Group.

Aoun, J. (2012). A shake-up of higher education. *Boston Globe*. Retrieved March 25, 2016, from https://www.bostonglobe.com (home page).

Baethge, A., & Rigotti, T. (2013). Interruptions to workflow: Their relationship with irritation and satisfaction with performance, and the mediating roles of time pressure and mental demands. *Work & Stress, 27*(1), 43–63.

Bailey B., Konstan J., Carlis J. (2001) The effects of interruptions on task performance, annoyance, and anxiety in the user interface, In M. Hirose (Ed.) Human-Computer Interaction - INTERACT 2001 Conference Proceedings. Amsterdam: IOS Press, 593–601.

Bain, K. (2004). *What the best college teachers do*. Cambridge, MA: Harvard University Press.

Beiter, K. D. (2005). *The protection of the right to an education by international law*. Leiden: Martinus Nijhoff Publishers.

Bulling, A. (2016). Pervasive attentive user interfaces. *Computer, 49*(1), 94–98.

Carver, L., & Harrison, L. M. (2013). Moocs and democratic education. *Liberal Education, 99*(4), 20–25.

Charle, C., & Verger, J. (2015). *Histoire des universités XIIe au XXIe siècle*. Paris: Presses universitaires de France.

Conard, M. A., & Marsh, R. F. (2014). Interest level improves learning but does not moderate the effects of interruptions: An experiment using simultaneous multitasking. *Learning and Individual Differences, 30*, 112–117.

Crary, J. (1999). *Suspension of perception: Attention, spectacle, and modern culture*. Cambridge: MIT Press.

Davenport, T., & Beck, J. (2001). *The attention economy*. Cambridge: Harvard Business School Press.

Destemberg, A. (2009). Un système rituel? Rites d'intégration et passages de grades dans le système universitaire médiéval (XIIIe-XVe siècle). *Cahiers de Recherches Médievales et Humanistes, 18*, 113–132.

Drews, F. A., & Musters, A. (2015). Individual differences in interrupted task performance: One size does not fit all. *International Journal of Human-Computer Studies, 79*, 97–105.

European Union Agency for Network and Information Security. (2014). Roadmap for NIS Education Programmes in Europe. *ENISA*. Retrieved March 25, 2016, from https://www.enisa.europa.eu (home page).

Dux, P. E., Tombu, M. N., Harrison, S., Rogers, B. P., Tong, F., & Marois, R. (2009). Training improves multitasking performance by increasing the speed of information processing in human prefrontal cortex. *Neuron, 63*, 127–138.

Foroughi, C. K., Werner, N. E., Barragán, D., & Boehm-Davis, D. A. (2015). Interruptions disrupt reading comprehension. *Journal of Experimental Psychology: General, 144*(3), 704–709.

Frank, G. (2014). Économie de l'attention. In Y. Citton (Ed.), *L'économie de l'attention: Nouvel horizon du capitalisme*? Paris: La Découverte.

Franke, J. L., Daniels, J. J., & McFarlane, D. C. (2002). Recovering context after interruption. Proceedings 24th Annual Meeting of the Cognitive Science Society. *Cognitive Science Society*, *2002*, 310–315.

Gillie, T., & Broadbent, D. (1989). What makes interruptions disruptive? A study of length, similarity and complexity. *Psychological Research Policy, 50*, 243–250.

Grice, H. P. (1975). Logic and conversation. In P. Cole & J. Morgan (Eds.), *Syntax and semantics: Vol. 3. Speech Acts*. New York: Academic Press, 41-58.

Hayles, N. (2007). Hyper and deep attention: The generational divide in cognitive modes. *Profession, 13*, 187–199.

Hembrooke, H., & Gay, G. (2003). The laptop and the lecture: The effects of multitasking in learning environments. *Journal of Computing in Higher Education, 15*, 46–64.

Hilbert, M. (2011). Digital gender divide or technologically empowered women in developing countries? *Women's Studies International Forum*, *34*(6), 21–22. 479–489.

van den Hoven, J. (2012). Fact Sheet-Ethics Subgroup IoT—Version 4.0. Chair Ethics Subgroup IoT Expert Group. Delft University of Technology. 6–8.

International Telecommunication Union. (2016). The World in 2015: ICT Facts and Figures. Retrieved March 5, 2016, fromhttp://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf http://www.itu.int (home page).

Jolly, C. (1989). *Histoire des bibliothèques françaises*. In A. Vernet (Ed.), *Les bibliothèques médiévales, du VIe siècle à 1530*. Paris: Promodis-Éditions du Cercle de la librairie.

Kant, I. (1781/1997). *Critique of practical reason* (M. Gregor, Ed. & Trans.). London: Cambridge University Press.

Kirchberg, D., Roe, R., & Van Eerde, W. (2015). Polychronicity and multitasking: A diary study at work. *Human Performance, 28*(2), 112–136.

Lanham, R., & Merkoski, D. (2008). The economics of attention. Moderated by Kaplan, M., *The Norman Lear Center,* USC Annenberg School of Communication. Retrieved March 25, 2016, from http://learcenter.org/pdf/EconofAttention.pdf

Lee, B. C., & Duffy, V. G. (2015). The effects of task interruption on human performance: A study of the systematic classification of human behavior and interruption frequency. *Human Factors and Ergonomics in Manufacturing & Service Industries, 25*(2), 137–152.

Lee, H., Young, T., Roda, C. (2013, April 10). *E-books usability: Reading time and comprehension*. Abstract for The Tablet Symposium: Examining new media objects. University of Sussex.

Le Goff, J. (1964). Quelle conscience l'université médiévale a-t-elle eue d'elle-même ? *Miscellanea Mediaevalia, 3*, 15–29.

Luker, K. (2008). *Salsa dancing into the social sciences: Research in the age of info-glut*. Cambridge: Harvard University Press.

Mack, A., & Rock, I. (1998). *Inattentional blindness*. Cambridge: MIT Press.

McFarlane, D. C., & Latorella, K. A. (2002). The scope and importance of human interruption in human-computer interaction design. *Human-Computer Interaction, 17*(1), 1–62.

Morin, D., Thomas, J. D. E., & Saade, R. G. (2012). Deep learning and virtual environment. *International Journal of Social, Behavioral, Educational, Economic, Business and Industrial Engineering*, *6*(11), 3163.

Nagata, S. F. (2003). *Multitasking and interruptions during mobile web tasks*. Proceedings 47th Annual Meeting of the Human Factors and Ergonomics Society (pp. 1341–1345).

Nissenbaum, H. (2011). A contextal approach to privacy online. *Daedalus, 140*(4), 32–48.

Norman, D., & Shallice, T. (1986). Attention to action: Willed and automatic control of behavior. In R. J. Davidson, G. E. Schwartz, & D. Shapiro (Eds.), *Consciousness and self-regulation*. New York: Plenum.

Pedro, F. (2010). *Educational research and innovation: Are the new millennium learners making the grade? Technology use and educational performance in PISA 2006*. Center for Educational Research and Innovation. Paris: OECD.

Perrin, A., & Duggan, M. (2015). 'Americans' internet access: 2000–2015. Pew Research Center. Retrieved March 25, 2016, from http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015

Philbeck, I. (2016). Working together to connect the world by 2020. *International Telecommunications Union*. Retrieved March 25, 2016, from http://www.itu.int (home page).

Rhoads, R., Camacho, M., Toven-Lindsey, B., Berdan Lozano, J. (2015). The massive open online course movement, MOOCs, and faculty labor. *The Review of Higher Education, 38*(3), 397–424.

Roda, C. (2010). Attention support in digital environments, nine questions to be addressed. *New Ideas in Psychology, 28*(3), 354–364.

Roda, C. (2014). Économiser l'attention dans l'interaction homme-machine. In Y. Citton (Ed.), *L'économie de l'attention: révolutions à venir?* Paris: La Découverte.

Roda, C. (2011). *Human attention in digital environments.* Cambridge University Press.

Rosen, L. D., Lim, A. F., Carrier, M., & Cheever, N. A. (2011). An examination of the educational impact of text message-induced task switching in the classroom: Educational implications and strategies to enhance learning. *Psicologia Educativa, 17*, 163–177.

Roux, S. (1992). *La Rive gauche des escholiers (XVe siècle)*. Paris: Éditions Christian.

Schmid, L., Manturuk, K., Simpkins, I., Goldwasser, M., Whitfield, K. (2015). Fulfilling the promise: Do MOOCs reach the educationally underserved? *Educational Media International, 52*(2), 116–128.

Simons, D. J., & Chabris, C. F. (1999). Gorillas in our midst: Sustained inattentional blindness for dynamic events. *Perception, 28*(9), 1059–1074.

Simon, H. A. (1971). Designing organizations for an information-rich world. In M. Greenberger (Ed.), *Computers, Communications, and the Public Interest* (pp. 38–52). Baltimore, MD: John Hopkins Press.

Speier, C., Vessey, I., & Valacich, J. (2003). The effects of interruptions, task complexity, and information presentation on computer-supported decision-making performance. *Decision Sciences, 34*(4), 771–797.

Tucker, L. (2014). 7 Reasons to take a MOOC. QS Top Universities, August 29. http://www.topuniversities.com/blog/7-reasons-take-mooc

United Nations Committee on Economic, Social and Cultural Rights. (1999). General Comment No.13: The Right to Education (Art. 13). Adopted at Twenty-first session, in document E/C.12/1999/10. Office of the High Commissioner on Human Rights.

United Nations Educational, Scientific and Cultural Organization. (2015). Draft Preliminary Report concerning the preparation of a global convention on the recognition of Higher Education Qualifications. UNESCO. Retrieved March 25, 2016, from http://www.unesco.org/new/en/education/themes/strengthening-education-systems/higher-education

West, D. M. (2015). *Connected learning: How mobile technology can improve education.* Center for Technology Innovation at Brookings. Retrieved March 25, 2016 from https://www.brookings.edu/wp-content/uploads/2016/07/west_connected-learning_v11.pdf

Zijlstra, F. R. H., Roe, R. A., Leonova, A. B., & Krediet, I. (1999). Temporal factors in mental work: Effects of interrupted activities. *Journal of Occupational and Organizational Psychology, 72*, 163–185.

CHAPTER 7

Conclusions: Collective Human Rights and Low-Tech

As we reflect on how we are going to live with new technology in the decades to come, balance is a key component in our evaluation of the costs and benefits of the digital revolution. The digital tightrope—a balancing act between breakneck technological development on the one side, countered by unforeseen consequences that may promote or violate time-honoured rights on the other—represents a conundrum for humans, both as individuals and as a collective. This book has explored a series of challenges that require thoughtful reflection, the evaluation of one set of interests with respect to another, all within the framework of binding state obligations to protect vulnerable populations. We have argued that the law necessary to regulate use of digital technology for the greater common good is already in place, situated within the architecture of international human rights law and articulated in the constitutions of most nation states.

We began this book with a discussion of wireless technology, an innovation that allows our mobile phones to function through the emission of invisible, low-level electromagnetic pollution in the air around us. The total absence of legislation to set binding, scientifically vetted emissions thresholds stems from a 'conflict of epistemic cultures of non-knowledge'; scientists do not yet have enough knowledge to agree on what to measure and how long to measure it in order to determine possible health effects. Nonetheless, all scientific literature agrees that children are more vulnerable than adults due to a more rapid and penetrating absorption of electromagnetic emissions. We have argued that children require special protection in law from all forms of pollution. Rather than wait twenty

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0_7

years to determine beyond a shadow of a doubt that radio frequency electromagnetic waves have negative consequences on human health, we suggest immediate application of the principle of precaution, particularly with respect to vulnerable populations. This would entail: (1) establishing age limits for the use of wireless communication devices, (2) barring installations from sensitive areas, such as schools and hospitals, and (3) requiring maximization of wired, rather than wireless networks. These are reasonable solutions that would have no more than a moderate impact on the roll-out of new technologies. More importantly, we advocate exploration of safer means for the transmission of electronic information and changes in how we use wireless technology on a daily basis. Digital hardware, while 'invisible', constitutes a heavy material investment, is energy intensive, and allows for little to no consumer input as to where and how it is used. All other industry that impacts the physical environment on such a scale is carefully regulated. Why not digital hardware?

In our third chapter we moved from hardware to software systems, and the equally invisible phenomenon of widespread surveillance. The Snowden disclosures revealed the massive character of the US government's surveillance programs—information collected on all citizens across all digital media in an attempt to use pattern recognition to uncover security threats. Large corporations routinely collect, store, manipulate and profit from private sensitive information gathered from customers who use their services. Citizens and customers are rarely in a position to evaluate clearly the extent of the information being collected and how it is then used. We pointed to philosopher Michel Foucault's insistence that power be visible in a democracy as an explanation for growing public objection to both state and corporate surveillance. The practice of informed citizenship requires the recognition of privacy as a human right, one that is guaranteed in international law and the national constitutions of most democracies. Nonetheless, it is not clear that privacy will survive the new impetus of Big Data unless we use law, technology and ethics to develop a protection framework for all citizens.

This chapter presented several court cases that demonstrate the reluctance of judicial systems in the USA and Europe to permit extensive corporate or government spying on citizens (except in an emergency). We explored 'privacy-by-design' as a technical response to the contradiction inherent in the pursuit of online exposure versus rising levels of public mistrust regarding the eventual use of online data. We explored new ways

of thinking about digital privacy that empower the user to have greater control over his or her personal data through privacy enhancing technologies that are built into the design of software before commercialization, and user privacy awareness to minimize the retention of personal data in any system. Privacy-by-design should function much like a seatbelt within the digital system, protecting the user and others as thoroughly as possible at the design stage of all digital devices and systems. Finally, we argued for privacy as a collective right. All users must act responsibly within a data system, and should not hesitate to organize information boycotts if a corporate or state actor has engaged in criminal behaviour or violated the public's sacrosanct right to privacy. We assume that our face-to-face and paper transactions will be treated with discretion by government or business actors: why not expect the same for digital privacy?

Our fourth chapter made the distinction between surveillance and censorship. The growth of executive power in China, Europe and the USA, often at the expense of the judiciary, has combined with new technologies to offer unparalleled opportunity for censoring digital content. Straightforward government proscription of online content, when combined with various forms of self-censorship, impacts the Internet in both democratic and authoritarian societies. Censorship constitutes a challenge to the international human rights framework, since freedom of expression constitutes a core value except in a state of emergency, when public order or safety may be at risk. Thus, Internet censorship that primarily targets criminal activity, such as child trafficking or jihadist recruitment of minors, is considered acceptable, but the proscription of content with a socio-political agenda that poses a real or perceived threat to the state may be questionable.

User response to censorship is highly varied. Chinese netizens have developed a specific online vocabulary that disguises messages with a political content, creating a 'resistance lexicon' for democratic dissidents, one that is appreciated by the Chinese student population whom we surveyed. European jihadists also skirt French government censorship, using encrypted phone messaging and setting up Twitter accounts or uploading online videos as quickly as the government pulls them down. While China's Party-State has developed a far more complex censorship system than individual European states (which have proven loath to cooperate on the proscription of content across borders), neither has been successful in addressing the underlying concerns that foster online dissent. We have argued that censorship functions best within a balance of powers

framework that mitigates executive overreach, while protecting society's most vulnerable populations from criminal activity.

Our fifth chapter explored a digital world in the making—the Internet of Things (IoT). This seemingly virtual phenomenon is in fact physical, a complex infrastructure of material hardware, electronic signals and electromagnetic emissions which generates, stores, transmits and analyses data that influences human activity. This chapter examined the extension of human rights law to the physical reality of the IoT, providing a principled reference for determining the subordinate place of machines in a digitized environment. We provided three scenarios to encourage the reader to reflect on the implications of this second stage of the digital revolution, demonstrating that technology usually serves, but may also endanger human beings. We analysed IoT technology and its eventual impact on individual and collective rights, demonstrating that societies may require new understandings of the public space and the social contract in order to live in harmony with a machine-driven environment.

The IoT is a double-edged sword, providing remarkable mobility and freedom for a large part of the population including vulnerable groups such as the elderly or the disabled, while enacting subtle, yet ubiquitous forms of discrimination against algorithmically targeted groups, despite the general interdiction against discrimination in human right law. This is perhaps the greatest challenge posed by the IoT. Silent, steady, data-generated prompting may change the way we experience the world and alter the way we view ourselves. As discussed in our chapter, digital prompting may also trigger forms of self-oppression that are difficult to detect and even more difficult to assign responsibility for. We argued that ethics remain crucial to the relationship between people and machines, and that it would behove us to draw clear, legal distinctions as to the responsibilities of both parties.

Our sixth chapter suggested that education offers an ideal platform for exploring the relationship between rights and technology use. Our curriculum for teaching human rights and digital technology to the 'digital natives' in our university classroom has shown us that students require experienced human input in order to master propositional thought. While digital tools provide them with greater access to a broader variety of knowledge than ever before, their attention is compromised by the very tools that expand their access to the world. We have suggested a form of blended learning to address the challenges inherent in mastering propositional thought in a technology-driven environment. As our

students learn to 'toggle' between oral, literary and virtual traditions that now inform university education and to compare the resonance of propositional thought in a seminar classroom versus an online setting, their professors learn to toggle with them, finding new ways to transmit the critical thinking necessary to solve 'intriguing, beautiful, or important problems'.

Since the Universal Declaration of Human Rights in 1948, the human rights paradigm has protected the individual citizen from state violations, civil and political, economic and social, and has provided quasi-judicial recourse for the individual through the United Nations (UN) treaty body monitoring system, a procedure that is more symbolic than effective. The emphasis on the individual reveals the influence of the European Enlightenment and does not always resonate with societies that privilege a more group oriented approach to human problem solving. The question of group rights emerged only gradually at the end of the twentieth century, with particular attention to trade union rights and issues such as peace or environmental protection. Because collective rights often create the necessary framework for the development of individual autonomy and identity, they are incorporated into our understanding of human rights law. The UN has extended binding treaty obligations to the explicit protection of indigenous peoples, the disabled and minorities, as well as larger groups such as women and children. This book has explored both individual and collective rights with respect to digital technology, recognizing that the individual right to enjoy scientific progress or receive an online education may violate the right of children everywhere to live in an environment free of electromagnetic pollution, or the right of a group of people to be protected from unwarranted digital surveillance. The balancing of individual and collective rights is challenging, nuanced and not always successful.

If we consider human rights through the lens of group rights to public health and to a clean environment, the sustainability of the digital revolution quickly comes into focus. Over the past half-century of computing, technological infrastructure has moved from a configuration where several people shared a computer, to one in which each user has several personal pieces of technology in play at any given time. A business strategy of personal objects for consumption, rather than collective, low energy systems made perfect sense from a marketing perspective; the cheap energy costs of the twentieth century and the shifting of the burden of health and pollution costs from the corporation to the consumer rendered this acceleration possible. Each of the digital systems discussed in the preceding chapters—wireless communication, massive online surveillance and censorship,

and individualized interconnected objects—all require the extraction of increasingly rare minerals and ever greater amounts of energy to function. And yet consumers may be less willing to pay for externalized health and pollution costs (in addition to those generated by the tobacco or nuclear industries) in an era of tight government budgets and growing economic inequity. Government policy has attempted in part to address this two-fold challenge by creating more energy-guzzling technology systems to create energy-saving solutions. The European Union, for example, requires the installation of 'smart meters' for tomorrow's 'smart cities'. These meters bring additional electromagnetic wave pollution into the home of every European family and cost more in energy to install, run and recycle than they save, a factor that was not lost on Germany, which abandoned obligatory installation of wireless meters for all but the most energy inefficient households and businesses. We question whether the current technology paradigm is the right one and suggest that a collective rights framework might help us find balance in the pursuit of innovation.

Digital technology may soon become too expensive for long-term human use, unless we begin to explore the installation of collective, low energy systems. Initially, these systems were equated with 'going off-grid', the domain of radical environmentalists living off the land on the margins of society. We argue that it is the collective interest to privilege low-tech machines and systems that use recycled materials in their construction and little energy to function, leaving a smaller environmental footprint with fewer human rights violations. We suggest thoughtful consideration of initiatives, such as 'ecology by design', an analysis of end-to-end impacts that would precede development of every digitized object, or UN oversight of extractable resources, as means to encourage a more sustainable use of new technologies.

Climate change and questions of environmental sustainability are likely to trigger an evolution in our understanding of human rights from the individual to the collective. As we apply hard-won individual rights to groups, vocal insistence on equally sustainable technologies may intensify. Digital systems that incorporate privacy, ecology and health concerns right into the preliminary design phase are ideally constructed to permit a global shift in public perception. Our primary objective in writing this book has been to promote an idea of technology that prevents, rather than facilitates subtle forms of discrimination; that provides free access to education and scientific progress, rather than reinforcing the social or economic capital paradigms in place; that helps us to learn to live with machines, rather

than surrendering our decision-making power to them. While celebrating the freedom and empowerment that modern technology brings to citizens around the globe, this book attempts to raise awareness about the complex connections between technological advancements and citizens' rights. Guided by visionary researchers and enlightened governance, technological progress may open the way to healthier, more inclusive and free societies. This same progress, however, is a source of enormous wealth for those who are more interested in selling their inventions, while purposefully concealing the problems they may generate. Decision-makers often lack the information and power necessary to protect citizens. And these same citizens are often divided between the advantages offered by new technologies and the risks involved. Ignoring, or delaying to address these problems is not only dangerous, but unnecessary.

The 'great transformation' that we are living will require a collective approach to the integration of technology into the human experience. Given the environmental, health, discrimination and privacy concerns, we believe that Gollier was right: present and future actions are not the same. Consequently, we must act now to protect vulnerable populations, while providing all citizens with the benefits of safe digital systems. Low-tech digital systems should be explored as a viable alternative to the current model in place. If we intend to apply the legal and moral framework of human rights to a host of new and exciting developments in the course of the great transformation that aptly describes the digital revolution, then we must do so in a coherent and systematic fashion, encouraging innovation and dignity for all.

Index

S. Perry, C. Roda, *Human Rights and Digital Technology*,
DOI 10.1057/978-1-137-58805-0