available at www.sciencedirect.com

ScienceDirect

ELSEVIER

Information Security Technical Report

Privacy and consent in the digital era

Shirin Elahi

Scenario Architect, UK

Keywords:
Digital
Future
Collective
Trust
Scale
Rights
Privacy
Consent

ABSTRACT

In today's digital era no one has knowledge, access or control of all their available personal information. This makes the very concepts of privacy and consent increasingly illusory and raises questions that are likely to shape not only the future form of cyberspace, but also the political, social and economic interactions within it. The institutions tasked with regulation of the physical world are ill equipped to respond and undertake a similar role in the virtual world; the timescales, dimensions and scope are all materially different. This article sets out five dilemmas that will need to be addressed in the search for solutions.

1. Introduction

Every day, as we go about our daily lives, we are being observed. TV surveillance cameras silently record our actions as we walk around, travel to and fro, interact with others and conduct our affairs. Our purchases, bank records and personal details are recorded, manipulated, scrutinised and analysed and any anomalous patterns flagged. Privacy, the 'state in which one is not observed or disturbed by others' means different things to different people, cultures and nations, but in a digital era, it is clearly being redefined.

As technological advances increase the ability to gather, store and share information, so it becomes easier to find new ways to breach privacy and circumvent personal consent. Today there are staggering amounts of information shared digitally and stored in the worldwide databases of government departments, law enforcers, financial institutions, multinational organisations, health providers, phone operators, airline service providers, to name but a few. The result is that no one has knowledge of all the personal information that others might have access to – let alone control over this. Therefore, in today's digital era the concepts of privacy and consent are becoming increasingly illusory.

The virtual world is not only forcing redefinition of many concepts we have taken for granted but also shaping our world in countless unimaginable ways. There are fundamental differences in the concepts of privacy and consent in the physical world of atoms and in the digital world of bits. In contrast to physical security issues, potential breaches of information security are in a different order in terms of scale of intrusion and speed of execution. Data can be copied, at negligible cost, as many times as required, and disseminated on a scale previously unimaginable.

Data are ephemeral. Not only is there the potential for inaccuracies, errors, outdated information, missing values or distortions, but data can be changed, manipulated, lost or deleted – with vast potential personal impact. Data, its capture, storage and use, are transforming our lives and the amount collected seems, like Moore's Law, to be increasing exponentially. This raises certain questions that need to be addressed.

- What data is being stored? For what purpose?
- How is it being used?
- Who has access to it? For what period of time?

Finding acceptable answers to these questions will not be simple. In this article, I set out five key dilemmas that will need to be confronted in the search for solutions. Each of these dilemmas raises difficult decisions with long-term ramifications and the likelihood of unintended consequences.

E-mail address: shirin@shirinelahi.com

1363-4127/$ – see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2009.10.004

(Tenner, 1996). Addressing and resolving them will not be simple. Ideally, these issues should be debated by society, yet this would require increased public awareness, as well as a suitable forum for such a far reaching debate. The dilemmas I have identified are:

1. Kaleidoscope Society: shifting cultures, values and identities
2. Individual rights v society's wellbeing
3. Who owns what? Conflicting attitudes to ownership
4. Tensions of scale: different temporal, geographic and political environments
5. Trust and control

The rapid pace of technological change has a corollary – the obsolescence of well established practices and norms. The institutions tasked with regulation of the physical world are not equipped with the necessary speed and flexibility to undertake a similar role in the virtual world; the scale and scope of the task are materially different. The challenge for the future of privacy and consent in the cyberspace domain is one of adaptation. This would mean an examination and reconfiguration of attitudes, behaviour, business practices and regulations rather than the transposition of old practices into a radically different environment.

The issues of privacy and consent are of profound importance for society. They impact human relationships, human rights and societal governance on many different levels. A major risk for the future will be that the dilemmas and questions they raise in the digital era remain unaddressed. Inertia is also a decision, and it might result in unwelcome knee-jerk reactions when public emotions run high. The decisions taken today will create the world of tomorrow, and they can be taken with foresight or hindsight – in proactive or reactive mode. The results are likely to shape not only the future form of the virtual world, but also political, social and economic interactions between human beings in an interconnected cyberworld.

2. Kaleidoscope society: shifting cultures, values and identities

> The fragmented Kaleidoscope Society is a challenge for societal governance, particularly with ephemeral global issues such as privacy and consent. When there is little cohesion within society and different cultural groups espouse different, often conflicting values and identities, it becomes difficult to make decisions. Who has the right to decide on critical issues such as levels of privacy and control on behalf of the collective?

Several generations ago, culture within Western societies was relatively static, underpinning the collective identities and values shared across societies. Social identities were generally forged by family and location – issues such as class, religion or creed were generally unquestioned. Even where waves of immigration created heterogeneity, there was generally a dominant culture that defined the rules of society (Hofstede, 2001).

Today this has changed. Across the developed world, societies have become increasingly diverse, and many traditional galvanisers of identity, such as religion, socio-economic grouping, marriage and lifestyle have become more fluid. The Kaleidoscope Society is interconnected yet fragmented in terms of culture, values and identities (European Patent Office, 2007). If *"culture can be described as the shared schemata that define categories, relationships and contexts, making it possible to process meanings and order information,"*[1] then in a Kaleidoscope Society encompassing multiple different cultures, finding shared schemata and meanings becomes problematical.

This kaleidoscopic process has been intensified by modern technology, which has provided the tools that enable individuals to interconnect across traditional geographic and social boundaries to form new groupings with more focused identities and aligned interests. People today are more likely to have multiple identities, depending on context, often espousing distinctive values that reflect the prevailing attitude of the specific group they are interacting with at the time.

The diversity described here is likely to be even more apparent in the virtual world. As one author muses,[2] when humans have the capacity to physically intervene and enhance their human bodies, it raises profound questions about the very concept of identity. A recent survey of the Internet by the Pew Centre (Pew Internet and American Life Project, 2006) indicated that the boundaries between the physical and virtual worlds might become so fluid that boundaries become blurred. As more people make continual and seamless transitions between the harsh realities of the physical world, and the compelling addictive alternate world, what happens to the cultural values and attitudes required to underpin society?

In today's Kaleidoscope Society, interconnected both physically and virtually in unprecedented fashion, establishing the common ground is becoming increasingly problematical. The same tools that enable new groupings within society to emerge can also mobilise around particular issues and challenge traditional forms of authority. Establishment of the common ground requires a shared understanding of the issues at stake (Elahi, 2008). However, when there is great diversity of cultures, with their allied interests, it is clearly more difficult to reach a consensus about the many complex technological, social, economic and environmental challenges that abound.

As policymakers grapple with the complexity of multicultural societal governance, how do they to define society and so establish and meet its needs? As the major challenges of the future become more global and ephemeral, the result is a clash of cultures and worldviews – and more moral dilemmas. With respect to issues of privacy and consent, who has the right to decide on critical issues such as privacy and consent on behalf of the collective, and how to do so? Within this context, the key question might be:

How to find common ground across a Kaleidoscope Society?

[1] Prof. A. Boholm, Centre for Public Sector Studies, Gothenburg University. RiskWorld 2020 Interview.

[2] Dr. B. Gordijn, Department of Ethics, Philosophy and Medicine, University of Nijmegen. EPO Interview.

3. Individual rights v society's wellbeing

> For authorities or businesses everywhere, that operate under growing performance demands or competition coupled with increasing pressure on resources, more detailed information regarding the personal habits of the public offers both convenience and efficiency. Data collection of confidential personal information enables authorities or businesses to monitor the habits and movements of individuals in the quest for anomalies, performance or profit. However, whilst the invasion of the privacy of the individual often provides collective advantage, it potentially discriminates against the human rights of individuals who have cannot gain full access or control of their personal information.

Thomas Friedman asserted several years ago that the world had become flat (Friedman, 2005). By this he meant that the global competitive playing field was being levelled and that technological innovation had enabled individuals to collaborate and compete globally. A flat world has undermined the traditional forms of authority, changing rules, roles and relationships. There are many notable examples to substantiate this: the ability of a subversive network to change the political landscape of the world and shape the policies of a global superpower, e.g. al-Quaeda; the ability of a university dropout student to become one of the richest and most powerful men in the world, e.g. Bill Gates; the rise of a celebrity with no particular skill other than self-promotion, e.g. Paris Hilton.

The flattening of the world has other profound implications. It has both been caused by and causes growing disintermediation, i.e. the removal of the intermediaries or buffers between producer and end user. Disintermediation has also removed the protective buffers within the system, making it more efficient and open – and thereby impacting issues of privacy and consent. The result is many new instant anonymous forms of communication that are unfettered by the traditional checks and balances that were once provided by third parties.

While digital technology has increased the power of the individual, it has also challenged the human rights of the individual with regard to privacy and consent. The same technologies that have forced governments and institutions to become more transparent and driven down costs for the consumer have also enabled governments and businesses to collect personal information on the public to an unprecedented degree. As a result, citizens everywhere are subject to growing surveillance and intrusion (O'Hara and Shadbolt, 2008). Information about physical and communication movements, purchase patterns, financial records, confidential legal, educational, health and other personal details are collected and stored on countless databases accessed by numerous government departments or businesses (Anderson et al, 2009). Information persists, so it remains available to be profiled and shared on a semi-permanent basis. Its uses can optimise public good: detecting cases of credit card fraud, bringing criminals on the street to justice, punishing transgressors who ignore regulations, providing more efficient services to the public. However, there is great potential for misuse – over zealous application of regulations, unauthorised sharing of confidential information, breaches of security, incorrect profiling, to name but a few. The impacts of these blunders can have potentially devastating consequences for the individuals involved.

The growing quantities of personal data collection expose the fault lines between individual human rights and those of society. There are innate tensions between the conflicting requirements of individuals going about their business and utilising digital technologies, and governments and businesses capturing and monitoring the digital footprints left behind. Any balance that is struck will have a profound impact upon the very structure of economic and political societal governance. Social responses to this dilemma will not be uniform either. The Google generation, the digital natives of the world, have a very different concept of privacy to those of their digital immigrant predecessors (Palfrey and Gasser, 2008). A generation that is content to record and distribute its most intimate personal details with the world at large is unlikely to have the same reservations about sharing, modifying and interacting with information, ideas – or perhaps even identities as their predecessors.

Here, the key question here might be:

> How to balance protection of data with individual freedom of information?

4. Who owns what? Conflicting attitudes to ownership

> Data is valuable. Unlike a physical asset, a database containing information can be copied at negligible cost and the contents can be sold many times over without impacting the quality of the original. This intrinsic value is one of the great incentives for businesses (and possibly governments) to invest scarce resources in the collection of data and is likely to shape their policies on privacy and consent. For the subjects whose information is held within the database there is an equity issue – the data has not been purchased or knowingly donated, so why should it be sold?

"Globalisation is not simply about the sharing of economics and markets, but also about the sharing of knowledge."[3] Knowledge is power, and the key to wealth. Knowledge goods are scalable, replicable and once obtained, can be sold but still maintained – unlike physical goods. In a global knowledge-based economy, the owner of valuable knowledge is king. Understanding what knowledge has value in a rapidly changing environment and owning it, is something many aspire to.

Ownership of knowledge is underpinned by the intellectual property rights system. The IPR system includes copyright, patents and geographical indicators, and it is enforced internationally by the World Trade Organisation via TRIPS, the Trade Related Intellectual Property Rights System, a side agreement of the WTO framework established in 1994. The

[3] Prof. Ruth Chadwick, Director, ESRC Centre for Economic and Social Aspects of Genomics (CESAGen). EPO Interview.

intellectual property system has been spectacularly successful and the number of stakeholders involved in the system and asserting their rights has increased – new countries, university technological transfer offices, venture capital companies, to name but a few (European Patent Office, 2007). The input of all these new stakeholders previously unaquainted with the functions and role of intellectual property has led to growing questioning of the system and its role.

In a world where information is modified and shared, where do the boundaries lie with the world of private property rights? What happens when information is voluntarily put into the commons domain and then transformed into private property (Benkler, 2006)? Issues within the intellectual property arena are likely to cause pressure as obsolete business models are replaced with a new "free" culture of sharing – one that is often based on nonmonetary markets such as exchange of labour and the gift economy (Andersen, 2009).

The gift economy raises moral issues as the very concept is at odds with financial enrichment. *"In law, the gift is the simplest, least complicated form of transfer of property rights. In a contract, the transfer of property is central and the relationship between the contracting parties is secondary and instrumental; in the gift, the transfer of property is secondary and instrumental to the purpose of gifts – creating and sustaining relationships. The gift signifies the importance of the relationship; it is not about the price tag."*[4] This particular quote refers to databases established by families with genetic conditions in the quest for a cure, where the information was manipulated and then patented by the researcher involved, but the principle applies in many different contexts. Perhaps it is time for new conceptualisations, that redefine ownership or alternatively, modify the relationship between parties. One solution might be for the transmutation of ownership into trusteeship of a valued resource.

Here, the key question here might be:

> What are the limits between the commons domain and private property rights?

5. Tensions of scale: different temporal, geographic and political environments

> Cyberspace is global in scale, and its interactions take place almost instantly. By contrast, the institutions tasked with its regulation are usually national in scale and their deliberations take place over months or even years. Clearly, there is a mismatch between these scales that can be exploited. When privacy and consent transgressions take place, they can be in a different magnitude in terms of speed of execution and geographical reach with little scope for redress for the individuals concerned.

The digital world enables global interconnections – yet the territorial structures that regulate it are usually national in scale. Each of these territorial jurisdictions has its own unique political, social, economic and regulatory environment – together with the necessary institutions supporting it. These environments vary and their characteristics, structures and practices will depend on their socio-political and historical backgrounds (Fischhoff, 1995). Geographical differences make the supra-national regulatory agreements required to respond to a globally interconnected system difficult to achieve. *"The lessons of the past have raised some hard, complex questions and highlighted that there are no simple ways to achieve international agreements on issues. There is no characterisation of a successful model, and we need to find new modes to solve new issues of global public goods."*[5]

The interlocking sets of national, regional and global territorial environments have obvious loopholes. They create structural weaknesses that can be exploited by individuals and organisations, by accident or design. In addition, they create systemic risks with no risk mitigation measures in place.

In addition to geographical differences, there is also a temporal mismatch of timescales between the digital and physical worlds. Cyberspace enables virtually instant switching from one set of values to another, from markets to markets, currencies to currencies, creating unprecedented complexity, size and volatility. This means that potential breaches of rights to privacy and consent information can be in a different magnitude in terms of speed of execution and geographical reach. This makes it almost impossible for regulators, located in bureaucratic institutions with long time horizons to deal with the risks of such a different order.

In addition to the geographic and temporal tensions, there are internal tensions to consider. The digital world is a complex system, the combination of multiple interactions of myriads of dynamic and adaptive nested structures operating simultaneously. However, like any system there can be certain species or technologies that become pervasive, so creating monocultures that discourage the diversity and self organisation inherent in a healthy system (Gunderson and Holling, 2002). So, although the sheer scale of the system might lead some to assume its healthy functioning, this is not necessarily the case.

"Complex systems work in rhythms, with a front-loop phase of slow, incremental growth and accumulation, and a back-loop stage of rapid reorganisation leading to renewal. Growing connectedness leads to increasing rigidity in its ability to retain control, and the system becomes ever more tightly bound together. This reduces resilience and the capacity of the system to absorb change, thus increasing the threat of abrupt change. Should abrupt change occur, there is a move to the back-loop stage. This phase is inherently unpredictable and uncertain."[6]

A way to counter the systemic risks described above would be by societal governance at the meta-level to examine the system as a whole. This would involve cross-disciplinary agencies, linking all the physical, financial and political issues implicating upon and implicated by the system. However,

[4] Dr. Tom Murray, President, Hastings Center. EPO Interview.

[5] Prof. Tom Heller, Lewis Talbot and Nadien Hearn Shelton Professor of International Studies, Stanford University. RiskWorld 2020 Interview.

[6] Prof. C. S. Holling, Arthur R. Marshall Jr Chair in Ecological Sciences, University of Florida, RiskWorld 2020 Interview.

institutional fragmentation and disciplinary thinking make such a societal governance structure unlikely.[7]

I have discussed how the mismatch between the geographic and temporal timescales of the physical world and those of the digital world might impact societal governance of privacy and consent issues. In particular, there are institutional and psychological barriers to overcome. Regulations in the physical world are usually based on historical and cultural precedents, but these are unlikely be suitable to meet the rapidly changing requirements and challenges of the digital world. In addition, there are internal threats to the long-term stability of the system that come from over reliance on monocultures (Wilkinson et al., 2003). Privacy and consent issues do not respect geographic and institutional boundaries and there are real questions as to where the boundaries of cyberspace should be set.

Here, the key question here might be:

How do humans and their institutions reconcile these tensions of scale?

6. Trust and control

As societal homogeneity dissolves, issues of trust and identity become more important, but also more fluid. This fragmentation is likely to prompt a cycle of increasing surveillance by governments – and increasing distrust by society. The cycle will be exacerbated by cases of data breaches, accidental losses and deliberate thefts, which reduce societal trust even further.

"*A good working position, as far as data quality goes, is one of suspicion…If the data cleaning has been informal and subjective, it is possible that all sorts of biases might have been introduced. One has no way of knowing.*"(Hand, 2007: 206) In the light of the vast quantities of personal information available, one has to take the quality of the data on trust. However, that trust can be misplaced, and the only way anyone will become aware of this is when they come across the consequences of that mistake. In addition, this data is often collected without consent and shared well beyond the purposes for which they were gathered.

How to deal with this? No individual has the ability or power to check or control all the information held about him or herself, yet this information has the power to remove financial credit, curtail the movements of an individual – indeed, to ruin lives. The levels of intrusion into personal privacy are likely to grow – as are the risks of data breaches, accidental losses and deliberate thefts which have become simpler due to technological innovations in information storage. Information and communications technology is ubiquitous, and privacy and consent issues impact everyone. As public perception of the subject and its inherent risks grows, it is likely to reconfigure social, political and economic relationships between the public and institutions or businesses that store this information.

Privacy and consent issues lie at the frontier of information and communications technology in uncharted territory. There are no simple historic precedents that can be called upon to adapt to the dilemmas that they raise. As societies become increasingly aware of 'Big Brother', there will be a price to pay in terms of trust. Trust is the lubricant of a functioning society (Nye et al., 1997; Cvetkovich and Löfstedt, 1999; Löfstedt, 2005), and its loss will create transaction costs politically, economically as well as socially – which would then redefine societal governance.

Here, the key question here might be:

In the face of the information avalanche, how to ensure societal governance?

7. Conclusion

The growing reach and scale of the connected world has had enormous implications for the evolution of different types of online services. Politicians, civil society groups, businesses and individuals are gradually realising the importance and impact of this virtual world. Just as the railways transformed the very nature of work, living conditions and social relations in the 19th century, cyberspace promises to reconfigure the form of society and its functions in this 21st century version. It is likely to impact upon and possibly transform every aspect of our lives - economics, politics, environment, society and technology – as well as drive new innovations in each of these fields.

As technological innovations gather pace, privacy and consent issues will continue to be at the forefront of the individual quest for cyber freedom as well as institutional and business desire for control. There are no simple historic precedents that can be called upon to set the balance between the innate tensions between them. In this article, I have attempted to set out the key dilemmas that society will have to examine in relation to privacy and consent.

- o **Kaleidoscope Society: shifting cultures, values and identities**
  How to find common ground across a Kaleidoscope Society?
- o **Individual rights v society's wellbeing**
  How to balance protection of data with individual freedom of information?
- o **Who owns what? Conflicting attitudes to ownership**
  What are the limits between the commons domain and private property rights?
- o **Tensions of scale: different temporal, geographic and political environments**
  How do humans and their institutions reconcile these tensions of scale?
- o **Trust and control**
  In the face of the information avalanche, how to ensure societal control?

Each dilemma raises difficult decisions that the diverse range of stakeholders will perceive differently. Has society the

[7] Prof. Ortwin Renn, Chair, Environmental Sociology Department, University of Stuttgart, RiskWorld 2020 Interview.

capacity to regulate these changes in the broadest sense of the word, or will the accelerating pace of technological change outstrip institutional arrangements? Issues of privacy and consent impact the very nature of society and governance, so can society set in place dynamic policies that enable switching, change or adaptation? If so, how to do this, and who to make these decisions finding acceptable answers will not be simple.

A major risk will be that these dilemmas and the questions they raise remain unaddressed. Privacy is a fundamental human right, underpinning many other values. The virtual world is not only forcing its redefinition of many concepts we have taken for granted but also shaping the environment in countless ways. The modern world is complex, interconnected and turbulent. It requires dynamic adaption to deal with the inherent uncertainty – control can be at best a dangerous illusion. Today's policies will create tomorrow's world. These decisions can be taken with foresight or hindsight – in proactive or reactive mode. The results are likely to shape not only the future form of cyberworld, but also political, social and economic interactions between human beings at large.

REFERENCES

Andersen C. Free: the future of a radical price. London: Random House Business Books; 2009.

Anderson R, Brown I, Dowty T, Inglesant P, Heath W, Sasse A. Database state. York: Joseph Rowntree Reform Trust Ltd, Refer to: www.jrrt.org.uk; 2009.

Benkler Y. The wealth of networks: how social production transforms markets and freedom. Yale University Press; 2006.

Cvetkovich G, Löfstedt RL, editors. Social trust and the management of risk. London: Earthscan Publications; 1999.

Elahi S. Conceptions of fairness and forming the common ground. In: Ramirez R, Selsky JW, van der Heijden K, editors. Business planning for turbulent times: new methods for applying scenarios. London: Earthscan; 2008. p. 223–41.

European Patent Office (EPO). Scenarios for the future. Munich: Author, Refer to: http://www.epo.org/topics/patent-system/scenarios-for-the-future.html; 2007.

Fischhoff B. Risk perception and communication unplugged: twenty years of process. Risk Analysis 1995;15(2):137–45.

Friedman TL. The world is flat. London: Penguin Books; 2005.

Gunderson LH, Holling CS, editors. Panarchy: understanding transformations in human and natural systems. Washington: Island Press; 2002.

Hand DJ. Information generation: how data rule our world. Oxford: Oneworld Publications; 2007.

Hofstede G. Culture's consequences: comparing values, behaviours, institutions and organisations across nations. 2nd ed. Thousand Oaks, CA, USA: Sage; 2001.

Löfstedt RE. Risk management in post-trust societies. Hampshire: Palgrave Macmillan; 2005.

Nye JS, Zelikow PD, King DC. Why people don't trust government. Cambridge, MA: Harvard University Press; 1997.

O'Hara K, Shadbolt N. The spy in the coffee machine. Oxford: Oneworld Publications; 2008.

Palfrey J, Gasser U. Born digital: understanding the first generation of digital natives. MA: Basic Books; 2008.

Pew Internet and American Life Project. The future of the Internet II. Washington: Pew Internet and Elon University, Refer to: http://www.pewinternet.org; 2006.

Tenner E. Why things bite back: predicting the problems of progress. London: Fourth Estate; 1996.

Wilkinson A, Elahi S, Eidinow E. Special issue: riskworld. Journal of Risk Research 2003;6(4–6):289–579.

Shirin Elahi is a scenario architect, specialising in scenario projects on complex global risk issues. She has examined knowledge risks for the European Patent Office (EPO Scenarios for the Future), health risks for UNAIDS (AIDS in Africa: Three Scenarios to 2025), societal risks for Shell International, UK Health and Safety Executive, European Patent Office and Electricité de France (RiskWorld 2020: The Future of Risk and Society) and environmental risks for the insurance industry (TSUNAMI project: Uninsured Losses from Natural Hazards). Shirin's interests lie in using scenarios to examine the risk trade-offs societies make and how this takes place at global level within the context of trust, equity and scientific uncertainty. She has interviewed and lectured widely on scenarios, risk and strategic change.