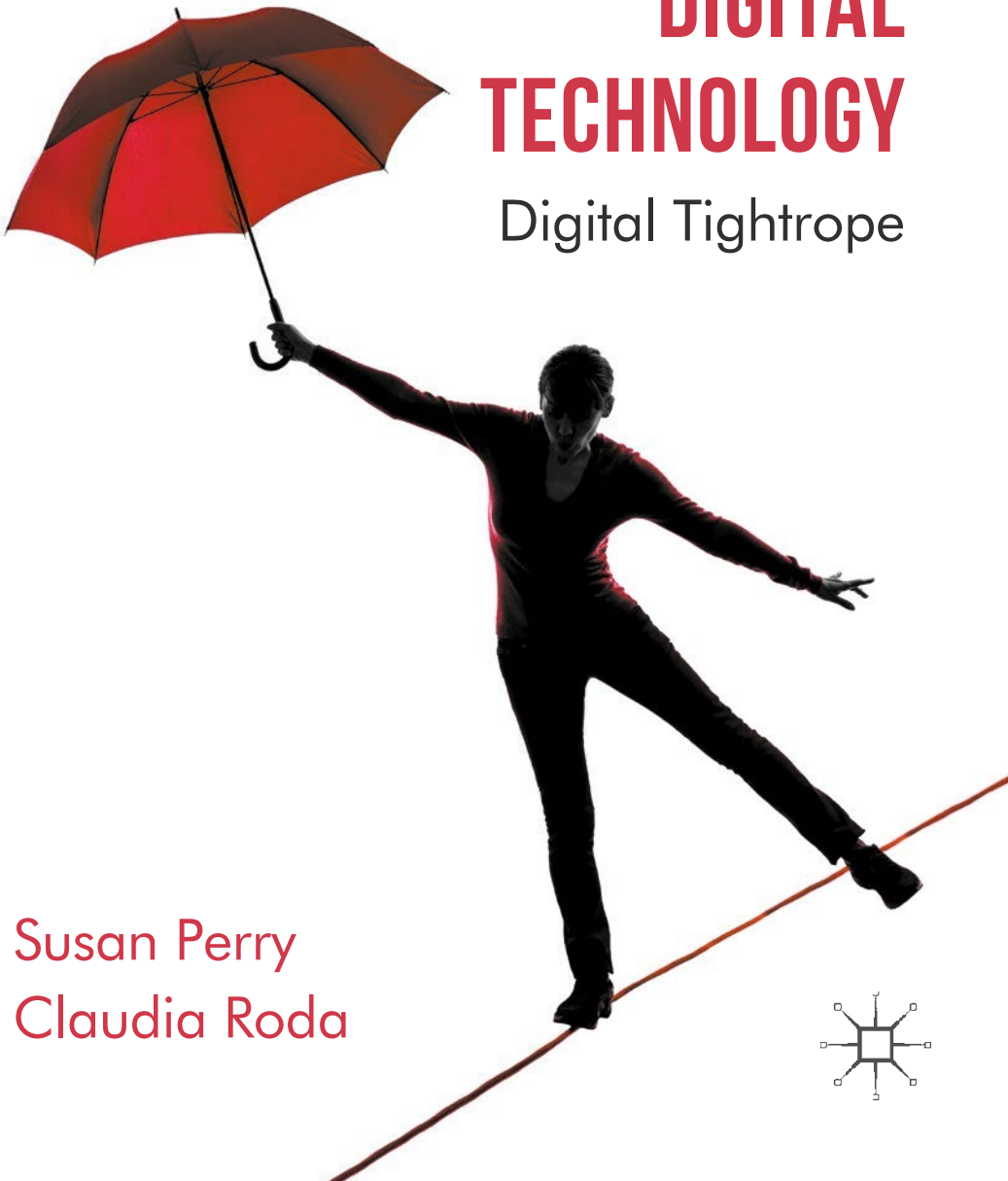
HUMAN RIGHTS AND DIGITAL TECHNOLOGY

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