The Library of Essays on Law and Privacy

Security and Privacy

Volume III

Joseph Savirimuthu

Security and Privacy

The Library of Essays on Law and Privacy
Series Editor: Philip Leith

Titles in the Series:

The Individual and Privacy
Volume I
Joseph A. Cannataci

Privacy in the Information Society
Volume II
Philip Leith

Security and Privacy
Volume III
Joseph Savirimuthu

Security and Privacy
Volume III

Edited by

Joseph Savirimuthu

University of Liverpool, UK

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First published 2015 by Ashgate Publishing

Published 2016 by Routledge
2 Park Square, Milton Park, Abingdon, Oxon OX14 4RN
711 Third Avenue, New York, NY 10017, USA

Routledge is an imprint of the Taylor & Francis Group, an informa business

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library.

Library of Congress Control Number: 2014946855

ISBN 9781409444879 (hbk)

Contents

PART III PRIVACY, DATA PROTECTION AND SECURITY

PART IV SMART TECHNOLOGIES, SOCIAL CONTROL AND HUMAN RIGHTS

Acknowledgements

Ashgate would like to thank our researchers and the contributing authors who provided copies, along with the following for their permission to reprint copyright material.

Association for Computing Machinery, Inc. for the essays: Steve Mann (2004), '"Sousveillance": Inverse Surveillance in Multimedia Imaging', *Proceedings of the ACM Multimedia*, pp. 620–27. Copyright © 2004 ACM. Reprinted by permission; Roger A. Clarke (1988), 'Information Technology and Dataveillance', *Communications of the ACM*, **31**, pp. 498–512. Copyright © 1988 ACM. Reprinted by permission; Donald A. Norman (1999), 'Affordance, Conventions, and Design', *Interactions*, **6**, pp. 38–42.

The Catholic University of America, Columbus School of Law for the essay: John T. Billings (2012), 'European Protectionism in Cloud Computing: Addressing Concerns over the PATRIOT Act', *CommLaw Conspectus: Journal of Communications Law and Policy*, **21**, pp. 211–31. Copyright © 2012 The Catholic University of America.

Data Protection Law & Policy for the essays: Deborah C. Peel (2013), 'eHealth: Roadmap to Finding a Successful Cure for Privacy Issues', *Data Protection Law and Policy*, **10**, pp. 14–16; Christopher Wolf (2013), 'The Privacy Bill of Rights: What Are the Expectations for 2013?', *Data Protection Law and Policy*, **10**, pp. 4–5.

Emerald Group Publishing Ltd for the essay: Benoît Dupont (2008), 'Hacking the Panopticon: Distributed Online Surveillance and Resistance', *Surveillance and Governance, Sociology of Crime, Law and Deviance*, **10**, pp. 257–78. Copyright © 2008 by Emerald Group Publishing Limited. All rights of reproduction in any form reserved.

Fordham Law Review for the essay: Jeffrey Rosen (2012), 'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google', *Fordham Law Review*, **80**, pp. 1525–38.

Gibson, Dunn & Crutcher LLP for the essay: Lisa Madelon Campbell (2011), 'Internet Intermediaries, Cloud Computing the Geospatial Data: How Competition and Privacy Converge in the Mobile Environment', *Competition Law International*, 7, pp. 60–66 (www.ibanet.org/Publications/competition_law_international.aspx).

Hart Publishing Ltd for the essay: Lee A. Bygrave (2010), 'The Body as Data? Biobank Regulation via the "Back Door" of Data Protection Law', *Law, Innovation and Technology*, **2**, pp. 1–25.

IEEE for the essay: Joseph A. Cannataci (2010), 'Squaring the Circle of Smart Surveillance and Privacy', *Fourth International Conference on Digital Society*, pp. 323–28. Copyright © 2010 IEEE.

Journal of Law, Technology & Policy, University of Illinois College of Law, for the essay: Daniel L. Pieringer (2012), 'There's No App for That: Protecting Users from Mobile Service Providers and Developers of Location-Based Applications', *University of Illinois Journal of Law, Technology & Policy*, **2012**, pp. 559–77.

Paul Maharg, editor of *European Journal of Law and Technology*, for the essay: Shara Monteleone (2012), 'Privacy and Data Protection at the Time of Facial Recognition: Towards a New Right to Digital Identity?', *European Journal of Law and Technology*, **3**(3).

Helen Nissenbaum for the essay: Helen Nissenbaum (2011), 'A Contextual Approach to Privacy Online', *Dædalus, the Journal of the American Academy of Arts & Sciences*, **140**, pp. 32–48. Copyright © 2011 by Helen Nissenbaum.

Notre Dame Journal of Law, Ethics and Public Policy and Oscar H. Gandy, Jr for the essay: Oscar H. Gandy, Jr (2000), 'Exploring Identity and Identification in Cyberspace', *Notre Dame Journal of Law, Ethics and Public Policy*, **14**, pp. 1085–111.

Oxford University Press for the essay: Lee A. Bygrave (1998), 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties', *International Journal of Law and Information Technology*, **6**, pp. 247–84. By permission of Oxford University Press.

SAGE for the essays: Ian Loader (1999), 'Consumer Culture and the Commodification of Policing and Security', *Sociology*, **33**, pp. 373–92. Reprinted by permission of SAGE; Vincenzo Pavone and Sara Degli Esposti (2012), 'Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security', *Public Understanding of Science*, **21**, pp. 556–72. Copyright © 2010 Vincenzo Pavone and Sara Degli Esposti. Reprinted by permission of SAGE.

Springer for the essay: L. Jean Camp (2002), 'Designing for Trust', in R. Falcone, S. Barber, L. Korba and M. Singh (eds), *Trust, Reputation, and Security: Theories and Practice*, Berlin–Heidelberg–New York: Springer-Verlag, pp. 15–29. Copyright © 2003 Springer-Verlag Berlin Heidelberg. With kind permission of Springer Science+Business Media.

Surveillance Studies Network for the essays: Oliver Leistert (2012), 'Resistance against Cyber-Surveillance within Social Movements and How Surveillance Adapts', *Surveillance & Society*, **9**, pp. 441–56. Copyright © 2012 Oliver Leistert; William Webster (2009), 'CCTV Policy in the UK: Reconsidering the Evidence Base', *Surveillance & Society*, **6**, pp. 10–22. Copyright © 2009 William Webster.

Taylor & Francis Group for the essays: Roger Clarke (1994), 'The Digital Persona and Its Application to Data Surveillance', *The Information Society*, **10**, pp. 77–92. Copyright © 1994 Taylor & Francis. Reproduced by permission of Taylor & Francis Group LLC (http://www.tandfonline.com); Torin Monahan (2006), 'Counter-Surveillance as Political Intervention?', *Social Semiotics*, **16**, pp. 515–34. Copyright © 2006 Taylor & Francis Ltd. Reproduced by permission of Taylor & Francis Group LLC (http://www.tandfonline.com); Jennifer Whitson and Kevin D. Haggerty (2007), 'Stolen Identities', *Criminal Justice Matters*, **68**, pp. 39–40. Copyright © 2007 Centre for Crime and Justice Studies and Taylor & Francis. Reproduced by

Publisher's Note

The material in this volume has been reproduced using the facsimile method. This means we can retain the original pagination to facilitate easy and correct citation of the original essays. It also explains the variety of typefaces, page layouts and numbering.

Series Preface

It was a pleasure to be asked to produce this series of essays, following in the footsteps of Eric Barendt's *Privacy* collection (Ashgate, 2001). Barendt had focused on the philosophical aspects of privacy at a time when academic interest in privacy was beginning to develop more seriously, and his chosen essays had been useful to both me and my students as we studied what 'right to privacy' the individual might have in the networked world. That collection enabled me to see quickly the main themes delineating privacy and also push students towards quickly grasping these themes. Over the past decade or so, the research field has exploded and a much more cross-disciplinarian approach is needed to understand better current trends and responses by the academic community. This series of volumes thus moves into – perhaps – a less philosophical approach about the individual and a more 'ethical' one as society attempts to determine what role privacy should have and how regulation might be enabled whether through law, technology or social norm. The new context is that there is now no technical limitation as to how privacy might be undermined: both the state and commerce have tools and techniques to know more about any individual than they know about themselves, whether through the daily collection of everyday data or through targeting of individuals or populations.

It is clear that if there is now no technical constraint to intrusion, the current debate must be over the ethics of privacy: what should society consider to be 'right behaviour' (in the moral sense) in a world where no-one appears to agree what that behaviour should be or where the moral lines should be drawn. There is, of course, no real help given by Conventions such as the *European Convention on Human Rights* (ECHR) – Art. 8 and Art. 10 tell us only that we have a right to privacy and also a right to know about others, two abstract rights which clearly conflict. The much vaunted 'right to be left alone' hardly helps us understand privacy in the modern world either. The debate is now over how to construct more detailed rights and the ethical rationale for these constructions. Before this can be done, we must also understand the complexity of the concept of 'privacy'.

My colleagues in this project, Joseph Cannataci and Joseph Savirimuthu have aided me enormously by broadening the series' vision of what privacy is. Our goal has not been to present a collection which follows our own views on the ethical choices around the regulation of privacy (each of us, it seems to me, has a different perspective anyway). What they have done is to help to disentangle the strands which are lumped together under the rubric of privacy, and provide the reader with a means to approach these strands. We have done so by taking a decidedly multi-disciplinary approach.

Cannataci's volume, *The Individual and Privacy*, looks at privacy from a principally anthropological stance. What has been meant by privacy in the past? What has privacy meant in the various parts of the globe, each with their own culture? What is the nature of an individual's right as against the community? The reader could hardly leave Cannataci's volume without agreeing with his assertion that privacy is a complex multi-faceted matter. Understanding of that fact means that our proposed ethical solutions must match the complexity of the problem.

Savirimuthu, in *Security and Privacy*, deals with that strand of privacy related to the state – that of surveillance. A state has obligations to protect the individual from others but also obligations to respect the rights of the individual, all within a framework where the state is the most powerful actor. It was, after all, state intrusion which had brought Art. 8 ECHR into being. Yet any state now has more powerful techniques for overseeing the citizen than the Nazi or Soviet states ever had. Can we implement, through law, an ethical framework in which we can trust the state to behave responsibly? Savirimuthu's chosen essays focus on whether and how regulation might be possible.

My own collection, *Privacy in the Information Society*, looks at the conflict where the attempt to build an 'information economy' meets the attempt to protect privacy. The very notion of 'information economy' leads us to understand that there is value in information of all kinds – celebrity private lives, customer databases, user provided information to social media, email contents, health data, etc. etc. Presuming that an information economy is a 'good thing' (certainly most countries wish to develop this) does this mean that privacy is no longer possible? If it is, how might we set up the positive rights and responsibilities to match our expectations?

We had much debate when we first got together on this project as to how we might structure the collections. Hopefully the reader will find that our chosen approach is useful. We also had debate about which essays might appear and where, a problem since although the titles of each collection differ, we are really interested in the same complex issue. We also certainly each felt that we could have chosen two or three times as many essays, but hopefully – again – the reader will not be disappointed with those upon which we did eventually rest.

PHILIP LEITH
Series Editor
Queen's University of Belfast, UK

Introduction

Google Glass, WikiLeaks, PRISM, facial recognition technologies, health and bio databanks and smart meters – these are some of the technologies that define convergence in a highly connected and networked environment. They also represent the context for ongoing security and privacy concerns. At one level, the essays in this volume attest to the particular attributes of the Internet infrastructure and technologies where the meme, 'information wants to be free' is prized as a crucial value. However, at another level, as we transition into an increasingly converged environment of ubiquitous computing, augmented reality and Internet of Things, there is a real need to understand how society and its institutions cope with growing demands that erosions to privacy and threats to personal data be addressed. The EU Barometer Study indicated that many individuals in society did not have confidence in industry or governments to respect their privacy. This is a sentiment not unique to citizens living in the EU. It is not that this is the effect of living in a risk society or that we are particularly sceptical about claims made by governments and industry that our individual privacy rights will be respected. It may be that we have very little confidence in the institutions that are meant to regulate the way personal data is collected, processed and used. One does not need to be a privacy scholar to notice that resolving the privacy paradox is far from straightforward – governments need access to personal data to fulfil some of their public roles, there is a gradual blurring of the on-line/off-line space, convergence is redefining the way we express our choices, identities and values. There are so many questions that remain unanswered and these can be approached at various levels.

During the last decade in particular, the levels of critical engagement with the challenges new technologies pose for privacy have been on the rise. Many have continued to explore the big themes in a manner that typifies the complex interplay between privacy, identity, security and surveillance. This level of engagement is both welcome and timely particularly in a climate of growing public mistrust of state surveillance activities and business predisposition to monetize information relating to the on-line activities of users. This volume is very much informed by the range of discussions being conducted at scholarly and policy levels. The essays illustrate the value of viewing privacy concerns not only in terms of the means by which information is communicated but the political processes that are inevitably engaged and the institutional, regulatory and cultural contexts within which meanings regarding identity and security are constituted. Privacy scholarship has dealt with topics posed by emerging technologies and addressed a number of questions and issues raised as a consequence.

In the next four parts a snapshot will be provided of topics and issues that can provide a springboard for further research and studies. A caution should be noted at the outset – privacy, identity and security are multidimensional. The categories chosen are not exhaustive or determinative since privacy concerns often overlap and multiple perspectives can be presented to offer different insights. The diversity in the narratives chosen for this volume serves as a reminder that various policy frames could be used to address core privacy concerns such as identity and security.

Identity, Security and Privacy in Context

Rather than rehearse the foundations of concepts such as identity and security, the approach adopted here is to allow the authors in the selected essays to introduce their perspectives and emerging issues.

The dilemma for L. Jean Camp in 'Designing for Trust' (Chapter 1) is not so much to do with ascertaining the nature of privacy but the steps that must be taken to bridge the trust deficit. Camp draws on her considerable experience in computer science and social sciences to set the context for the way we ought to think about concepts such as identity and security. She moves away from orthodox treatments of the privacy dilemma and directs attention towards addressing the trust deficit that undermines users' confidence in networks and information systems. What does trust have to do with the way individuals manage the security and integrity of personal information and on-line activities? Camp adopts a techno-anthropology approach and shows that trust norms lie at the intersection of privacy, security and reliability. In the context of the privacy debate, Camp urges policy-makers and designers to operationalize trust by taking account of user perceptions of privacy and opportunities for designing confidence enhancing tools at user and network level. There are two policy implications to be noted. First, the governance strategy in formulating, implementing and embedding trust enhancing designs in networks and communication platforms. Second, the emphasis placed on the value of design solutions that accommodate human-centric needs, values and perceptions. Both raise valid governance challenges given consumers' concerns about identity theft and security lapses regarding the storage of personal data by data controllers. Let us pull back briefly. It is useful to recall some of the ways digital technologies enable information about individuals to be collected, processed and analysed. Designing for trust also ensures, among other things, that individuals can continue to define their identities and values. Privacy enables individuals to exhibit their freedoms and develop the 'self'. This should, rightly, extend to the right to create our digital identities. IT disrupts this norm.

Roger Clarke, a renowned specialist in the strategic and policy aspects of IT, surveillance and privacy introduces the concept of a digital persona in 'The Digital Persona and Its Application to Data Surveillance' (Chapter 2). This foreshadows the European Commission's proposal for a right to forget. The digital persona concept helps us frame the concerns and issues posed by the dynamics of the networked environment, particularly in acting as a catalyst for the formation of personas. Clarke stresses the need for policy-makers to undertake a critical assessment of the way IT processes can make inroads into fundamental freedoms often without transparency or accountability. It is this lack of democratic oversight that concerns Clarke, which he describes as capable of undermining the essence of human flourishing. The surveillance of individuals through their digital footprints is one manifestation of the normalization of surveillance – a common feature perhaps, of the concerns surrounding the pervasive nature of data surveillance via on-line profiling, behavioural targeting and information sharing.

The next three essays pick up the recurring themes of transparency, visibility and accountability. Privacy lawyers have long explored these themes in privacy debates; scholars increasingly turn to other disciplines to generate critical policy perspectives. In 'Privacy, Visibility, Transparency, and Exposure' (Chapter 3) Julie E. Cohen draws inspiration from philosophers such as Langdon Winner, and urges us not to overlook the political character

of networked technologies and the values and interests these perpetuate. In real space, privacy norms aim to create a space, which enables individuals to control who, what and how information about them is accessed or made visible. According to Cohen, we need to reconceptualize risks and harms to privacy since erosions can be incremental, passive and often go unnoticed. Furthermore, calling for privacy policies that promote informational transparency, she concludes, does not bring to an end the risks to an individual's 'right to be left alone'. Cohen argues any move towards framing privacy rules and governance mechanisms must bring into the equation both spatial and informational dimensions. Cohen is right to point to the spatial dimension in privacy since convergence and mobile technologies now blur contexts. We can infer here that the experienced space is an integral aspect of privacy and may not necessarily fit into ordinary conceptions of 'public' and 'private' spaces. What Cohen, carefully brings to the foreground, is the possibility that in the experienced space, individuals should continue to determine the circumstances when their identities become visible to others. Data mining is not simply about the collection of personal data with the aim of formalizing consumers' identities and refining their choices, preferences and values. A different set of questions are generated if we consider the significance of the exponential growth in the data mining industry for the junctures between the social dynamics of power and the new wealth of the digital economy – personal data.

Oscar Gandy, 'Exploring Identity and Identification in Cyberspace' (Chapter 4), views the emergence of new technologies as normalizing discrimination, and designed to avoid regulatory scrutiny and accountability. This essay is a careful study of the ethics of surveillance and highlights approaches that enable privacy harms to be anticipated. Gandy suggests that we scrutinize the values and preferences hidden in data aggregation and profiling practices. He urges regulators to problematize data mining and surveillance activities so that a proper privacy impact assessment can be made between the risks and the benefits of surveillance and monitoring. Gandy's essay also reignites ongoing concerns that policy-makers often fall short of grappling with the central problem resulting from the use of panoptic surveillance tools by industry, namely, the creation of a hierarchical structure of relations, and automating and normalizing surveillance. His reference to the ethics of surveillance is apt – given the scale of data mining activity now taking place, it is imperative that policy-makers and industry take the lead in contending with the privacy concerns associated with digital curation (Marx, 1998, p. 174). One suggestion Gandy offers, and which is now emerging as a legitimate policy response is that data controllers be required to make clear how they balance their legitimate economic and security interests with the expectation of individuals that their civil liberties are not compromised.

The final essay in this part serves to remind us that privacy is about managing trust and expectations in social relations. Helen Nissenbaum, 'A Contextual Approach to Privacy Online' (Chapter 5), brings her philosophical and computer science expertise to illustrate the benefits of focusing on the context in which privacy concerns emerge. Do we need specific privacy rules for the on-line environment? One shortcoming in drafting a set of privacy rules particularly for the on-line environment is that we may end up losing sight of the *raison d'être* of privacy principles and norms – which is to provide individuals with adequate safeguards to their personal information and privacy. Nissenbaum stresses that emphasizing the distinctiveness of on-line and off-line privacy is the wrong way of addressing the privacy challenges in contemporary society. She suggests that we should concentrate on the subjects

of privacy protections – individuals. She has a point. New communication tools and social media disrupt the way we have traditionally managed our identities and security. Nissenbaum envisages that all stakeholders have an important role in brokering spaces for meaningful social and economic activity while being alert to the value and significance of informed consent. Since many individuals have social media accounts, we could, like Nissenbaum, consider how these technologies disrupt social norms such as preserving user privacy in on-line social interactions and obtain informed consent before accessing and processing personal information.

Surveillance, Security and Anonymity

On 17 July 2013 the Chairman of the Intelligence and Security Committee of Parliament, the Rt Hon Sir Malcolm Rifkind MP, issued a statement regarding GCHQ's alleged interception of communications under the US PRISM Programme (see Intelligence and Security Committee of Parliament, 2013a, 2013b). The statement was intended to reassure the general public that GCHQ had not circumvented or attempted to circumvent UK law, by using the United States' National Security Agency's PRISM programme to access the content of its citizens' private communications. Should we provide governments with some latitude in the way personal information or communications data are accessed to ensure our safety? Under what circumstances should an individual's right to privacy or anonymity be subordinated to the safety interests of the broader community? On the face of it, there are arguments for and against placing trust in security and intelligence agencies. As the recent *cause celebré* involving US National Security Agency's intelligence gathering activities highlight, some scepticism is no doubt healthy in a democracy. A starting point to help frame the essays in this part would be to note the default position as stated in Article 8 of the European Convention on Human Rights (ECHR). It provides that 'Everyone has the right to respect for his private and family life, his home and his correspondence', and that:

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

What is the intersection between surveillance, secrecy and anonymity? Unregulated access to communications data can provide information about the individual's private life, which includes identity, location, interactions and interests. Secrecy and anonymity have undoubted social value – anonymity allows us to vote freely or express our thoughts without fear of reprisal. Secrecy allows intimate relations and communications to be conducted away from the public gaze. With regard to surveillance, Article 8 ECHR is directly relevant to the subject of privacy since all forms of covert monitoring and data gathering activities potentially create an imbalance in the relationship between the individual and the body undertaking the monitoring (Haggerty and Samatas, 2010). In the *Case of Liberty and Others* v. *The United Kingdom* Application no. 58243/00 (2008), the European Court of Human Rights indicated that a state's ability to enact legislation, which enabled it to undertake secret monitoring of citizens'

communications had to be circumscribed by clear safeguards to fundamental freedoms.[1] The democratization of innovation and technology has now made available another layer of privacy safeguards. Individuals can avail themselves of technological tools to preserve secrecy and anonymity. Instant messaging, cryptography and anonymous browsers are some of the tools that enable individuals to engage in social communications without fear of monitoring. The human rights provision also acknowledges that surveillance and other forms of monitoring can augment democratic values by creating an environment where citizens can freely engage in their daily activities without fear to their safety and well-being (Lyon, 2001).

The essays chosen in this part are only a sample of the burgeoning literature on surveillance. Before examining the ideas underpinning countersurveillance, we can briefly turn to a working definition of surveillance, which focuses on the collection and processing of personal data for making decisions. The fundamental objection to surveillance is the creation of asymmetrical power relations. The power relations can exist as between the state and its citizens or between organizations and individuals. The mischief, anti-surveillance and civil libertarian scholars highlight is that indiscriminate collection of personal information can lead to political misuse (for example, censorship and propaganda) or corporate manipulation of end users' choices and preferences (for example, on-line profiling and behavioural targeting). New technologies have been used by commerce and industry to profile individuals for behavioural advertising or sale of goods and services. There is a body of literature that explores surveillance from a different vantage point. A number of scholars regard technologies such as CCTV cameras, facial recognition technologies and the Internet as ushering in a new aesthetic to surveillance. The focus on the role and potential of resistance to destabilize the power relations surveillance aims to establish should not be overstated.

Two essays advocate a cautious stance. Benoît Dupont's essay, 'Hacking the Panopticon: Distributed Online Surveillance and Resistance' (Chapter 6), questions the uncritical transposition of the panopticon metaphor to the Internet and digital technologies. He suggests that two trends in the evolution of new technologies and distributed architecture of the Internet have significant consequences for institutionalizing power relations. First, surveillance technologies are now readily available. Their ready availability Dupont (Chapter 6) suggests has resulted in the '"democratization of surveillance"' (p. 106). Second, these technologies can be used to counter surveillance activities. Kevin D. Haggerty and Richard V. Ericson advocate a different approach in 'The Surveillant Assemblage' (Chapter 7). They offer the concept of the '*surveillant assemblage*' as a rhetorical frame to visualize the role of IT in deconstructing individuals and aggregating the information into depersonalized data and profiles. Haggerty and Ericson adapt the heuristic employed by Deleuze and Guattari (1987) in *A Thousand Plateaus*. It may be recalled that Deleuze and Guattari viewed the human face, ontologically, as an abstract machine. They suggested that the constitution of the face into identities and categories is in essence an assemblage of power. Haggerty and Ericson (Chapter 7) regard a similar assemblage as taking place when surveillance technologies collate and aggregate data to profile, create new knowledge and define particular identities. They conclude that 'we are witnessing a rhizomatic leveling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored' (p. 128).

---

[1] See also Articles 17–19 of the International Covenant on Civil and Political Rights. Regulatory oversight mechanisms in the United Kingdom include the Regulatory Investigatory Power Act 2000.

The ubiquity of surveillance technologies and their ready accessibility mean that all of us, and not simply those in power or authority, have the tools to monitor people and events. Voyeurism, exhibitionism and spying seem unexceptional in the networked environment. We appear to be living in an era of liquid surveillance where the previous boundaries between the watchers and the watched on the one hand and surveillance and resistance on the other, are ill-defined. Many hardly register any concerns when tagging material on social networking sites, searching through user profiles and updating timelines. Steve Mann, '"Sousveillance": Inverse Surveillance in Multimedia Imaging' (Chapter 8), focuses on the aesthetic of *sousveillance* to provide a counterpoint to orthodox perceptions of surveillance. *Sousveillance* it should be remembered is not countersurveillance. He suggests that individuals by wearing small wearable or portable personal recording technologies in their daily lives can gain new perspectives about society and its institutions. *Sousveillance* renders the external environment and institutions as objects of veillance. His well-documented lifelogging of personal experiences creates vivid images of surveillance practices and public reactions to *sousveillance*. Mann's recounting of his personal experiences instils the well-known claim that technologies are culturally situated and that may at times bring with it their own problems.

Surveillance systems cannot be disassociated cultural practices and symbols. In short, surveillance does not exist in a vacuum. This is the focus of Torin Monahan in 'Surveillance as Cultural Practice' (Chapter 9) as he considers how media, art and film narratives provide researchers with new avenues for studying surveillance. Surveillance when understood within a socio-technological constructivist frame, he argues, opens up new avenues for exploring this sphere of culture and increases our consciousness about its politics. Monahan illustrates some of the situations where meanings, knowledge and experiences of individuals' engagement with surveillance can even emerge at the localized level. Surveillance tools such as loyalty cards and social networking affordances could be regarded as instances of individuals appropriating such tokens regardless of the purposes for which they were originally made publicly available. How do we reconcile *sousveillance* or even surveillance as forms of cultural practice within the risk society?

One hallmark of a risk society is society's desire that threats to its safety are minimized, if not eliminated. Our politicians may have tapped into the public's deep-seated psyche when justifying the installation of CCTV cameras in public spaces and use body scanners in airports. The risk society is also a security conscious society with maturing surveillance tools. What are the trade-offs? Are security tools nothing more than surveillance creep? Walter Peissl, 'Surveillance and Security: A Dodgy Relationship' (Chapter 10), challenges the received political rhetoric that more surveillance will enhance the security of citizens. Mainstreaming security, he suggests, does not invariably lead to greater public safety but will lead to the emergence of a panoptic society where surveillance becomes normalized. There is a subtle point being made by Peissl. Security has become a major part of political and social discourse and there is a perception that the resulting 'moral panic' has generated increased public surveillance of citizens without corresponding reduction of fears of safety.[2] Many will agree that an uncritical acceptance of these technologies will only embed asymmetric hierarchical power relations. These power relations are not typically between the state and its citizens.

[2] See, for example, Schedule 7 Terrorism Act 2000.

Increasingly, the state and its law enforcement agencies have turned to intermediaries to act as proxies for targeted surveillance activities.

Is there an appropriate response to the emerging 'intelligence-industrial' complex? In 'Counter-Surveillance as Political Intervention?' (Chapter 11) Torin Monahan undertakes a review of countersurveillance strategies such as activist demonstrations and artistic displays of resistance but fears that despite the short-term symbolic gains in disrupting institutional mechanisms of power and control, such interventions may be counterproductive. Often institutions and agencies use these temporary displays of resistance to remove the inefficiencies in the mechanisms of control. Oliver Leistert, 'Resistance against Cyber-Surveillance within Social Movements and How Surveillance Adapts' (Chapter 12), offers a nuanced analysis. He focuses on the intelligence gathering practices of both the watchers and the watched. He suggests that both parties in the age of the Internet and mobile communications paradoxically utilize telecommunications infrastructures to engage in monitoring activities while preserving their anonymity.

Not all lawyers take the view that privacy values are subordinated to surveillance. Richard A. Posner, 'Privacy, Surveillance, and Law' (Chapter 13), argues that in the light of increased threats to society posed by terrorists and other criminals a firm stance needs to be taken by the state and its law enforcement agencies. He asks whether those who claim that surveillance harms society are able to quantify the costs and benefits of these measures. He suggests that privacy concerns may either be exaggerated or taken out of context. As efforts are made to develop a model that better calibrates the competing public policy interests, Joseph A. Cannataci, 'Squaring the Circle of Smart Surveillance and Privacy' (Chapter 14), regards the trend towards investing in smart surveillance as worrying. There is sound basis for his concern. One report forecasts that the market for surveillance tags is likely to see an increase (see ReportsnReports, 2013). It is not simply the drivers and scale of the market for smart surveillance that concern privacy advocates. Smart surveillance not only occupies a broad landscape comprising both the technologies and types of data used to gather, assemble and analyse personal data – it is also automated. The trend towards assuaging a risk averse culture with distributed intelligent surveillance systems needs to be balanced with concrete privacy safeguards.

Privacy, Data Protection and Security

Data protection laws provide an important framework regulating the processing of an individual's personal data. Privacy is an important concern when personal data are processed. New communication technologies create opportunities to safeguard communities and citizens but they also threaten to undermine privacy protections. In the EU, national courts and data protection authorities are not the only entities ensuring that data controllers comply with data protection laws. The Court of Justice of the European Union (CJEU) and the European Court of Human Rights have played an important role in providing invaluable case law from their interpretation of human rights provisions such as the EU Charter of Fundamental Rights and the European Convention on Human Rights (ECHR) respectively. Human rights and privacy lawyers have increasingly been interested in examining whether data protection and human rights provisions provide an adequate response to privacy concerns. Article 8 of the EU's

Charter of Fundamental Rights states that data protection is a fundamental right. The respect for private and family life is regarded as a separate right in Article 7.

Lee A. Bygrave, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' (Chapter 15), looks at the emerging jurisprudence on Article 17 of the International Covenant on Civil and Political Rights and Articles 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. He explains how these treaties interact with each other and stresses that these provisions have sufficient flexibility to integrate data protection principles into human rights treaties. It may be mentioned here that under the European Commission's proposed reform to Directive 95/46/EC, the protection of personal data is to be regarded as a fundamental right.[3] Some circumspection is warranted. Observers have noted that the proposed regulation does not make specific reference to the importance of member states in protecting individuals' right to privacy with respect to the processing of personal data (Article 1(1) of Directive 95/46/EC). The protection of personal data under Directive 95/46/EC and privacy are not interchangeable concepts. How national courts and the European Court of Human Rights handle this aspect concerns privacy lawyers.

One policy area where the courts may have an important role to play in clarifying whether these new proposals should be read as incorporating individuals' right to privacy relates to the privatization of the security market. Increasingly, with the expansion of the security market in the private sector questions have been raised regarding the privacy safeguards for individuals when private firms discharge public security functions. Ian Loader's contribution, 'Consumer Culture and the Commodification of Policing and Security' (Chapter 16), examines the implications of the overlap in functions. He argues that security is a public not a private good. The crossover of security from public to private domains, he cautions, has transformed security into a commodity. The blurring of the distinction between state and non-state security actors he observes could lead to policy responses being shaped by market rules and norms and undermines the role of the state as a provider of security for the public good. Opinions vary on how the knowledge base of personal information is to be managed.

There is another approach or conceptual frame that may be of assistance in the way we unbundle the risks of personal data straddling private and public sector domains. Roger Clarke, 'Information Technology and Dataveillance' (Chapter 17), provides us with a timely introduction to the concept of 'dataveillance'. He describes this form of processing activity as involving the systematic monitoring of individuals' actions or communications through information technology. Roger's concerns that the centralization of monitoring activity and the reactive nature of privacy and consumer protection laws are well founded. Increased access to the Internet, on-line social media and mobile communications, he notes, only leads to an exponential increase in communications data but it provides a fertile landscape for dataveillance. While these technologies can provide consumers and individuals with considerable benefits, the seamless nature of the networks and communication platforms create new opportunities for industry and the state's intelligence agencies to assert their control by collating data from multiple sources.

In 'Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security' (Chapter 18) Vincenzo Pavone and Sara Degli Esposti deal with the question of how individuals respond to security enhancing technologies

[3] COM(2012) 11 final.

that also bring them inherent risks to privacy. Privacy management is a pragmatic enterprise influenced by tools, information, choices and preferences at the disposal of individuals. Their empirical study underlines some of the observations raised by Camp and Nissenbaum. The essay also sheds additional light on the mosaic of reactions of individuals to surveillance-oriented security technologies. Contexts matter and the caricature of such technologies as invariably involving a trade-off are held to be simplistic. For example, during times of intense security tensions and risks, citizens may regard the political response in developing monitoring processes as necessary and do not view privacy as an exchangeable good. However, in other contexts their attitudes to the deployment of surveillance technologies may depend on variables such as personal, economic and social factors, which cannot be exchanged.

The next two essays look at cloud computing. Should we avoid US-based cloud services providers given that EU data protection laws provide far greater safeguards for individuals' privacy? John T. Billings' essay, 'European Protectionism in Cloud Computing: Addressing Concerns over the PATRIOT Act' (Chapter 19), provides a critical examination of United States and European Union Law. He concludes that one must not attach too much significance to the distinction between US- and non-US-based cloud services providers since US jurisdictional rules and mutual legal assistance treaties permit access to EU consumer data.[4] The distinction nevertheless is still important. The European Data Protection Supervisor Peter Hustinx has published an Opinion on the European Commission's Communication on cloud computing, which highlights the importance of clarifying the responsibilities and obligations of all parties involved in cloud computing in the context of Directive 95/46/EC and the proposed General Data Protection Regulation.[5] New technologies allow data to be used to promote innovation or realize outcomes which benefit society. For example, geospatial data could be harnessed for critical policy responses to situations such as disaster management, monitoring of environment conditions and tracking of infectious diseases. Geospatial data could also be used for purposes that subordinate the privacy interests of individuals to business or political goals. Complex issues arise when geospatial data include personal data. The collection of personal data can provide opportunities for innovation but can result in curbing competition (see also Almunia, 2012). Lisa Madelon Campbell's essay, 'Internet Intermediaries, Cloud Computing the Geospatial Data: How Competition and Privacy Converge in the Mobile Environment' (Chapter 20), explores the legal effects of the convergence between competition and privacy law issues on innovation and competition.

Finally, in 'Stolen Identities' (Chapter 21), Jennifer Whitson and Kevin D. Haggerty argue that companies' zest for customer data and the huge growth in e-commerce are exacerbating the problem of identity theft. In the process, informational security measures are poised

---

[4] Article 29 Working Party Opinion 05/2012 on Cloud Computing clarifying the rules in the cloud computing context. Reference should now be made to the document, 'Clarifications Regarding the U.S.–EU Safe Harbor Framework and Cloud Computing', issued by the Department of Commerce's International Trade Administration regarding the transfer of personal data from the European Union to the United States, at: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf. Information from the European Commission strategy on cloud computing, entitled 'Unleashing the Potential of Cloud Computing in Europe' can be found at: http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy.

[5] At:http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-11-16_Cloud_Computing_EN.pdf.

to become more elaborate and intrusive as they simultaneously reproduce the institutional reliance on personal information that has ultimately made identity theft possible.

Smart Technologies, Social Control and Human Rights

An aspect of managing risks to individual security concerns the way IT and new technologies are employed to maintain social control. Smart technologies can by definition normalize surveillance. An important privacy impact assessment issue is whether living under the overarching umbrella of surveillance technologies will lead to more proactive social control activities emerging as a consequence. Privacy scholars are already beginning to come to grips with smart technologies – radio-frequency identification (RFID), ambient intelligence, smart meters, sensor technologies, augmented reality and so on. Social control potentially becomes pervasive and invisible since the interests and power relations are embedded in software algorithms. Software algorithms automate control. How will we wrestle with the uncertainties smart technologies create for our privacy? We may find some clues in the following essays.

In 'The Body as Data? Biobank Regulation via the "Back Door" of Data Protection Law' (Chapter 22) Lee A. Bygrave warns of the dangers of conceptual seepage between data and information and suggests that we must resist our continued reliance on data protection law. William Webster, 'CCTV Policy in the UK: Reconsidering the Evidence Base' (Chapter 23), notes that insights can be derived from adopting a policy perspective to the adoption of particular technologies. The essay posits that a 'policy perspective' approach to understanding the CCTV revolution is illuminating as it highlights the complex intertwined interactions between government, policy-makers, the media and other stakeholders, and that CCTV does not necessarily have to 'work' if it meets other purposes. Barrie Sheldon, 'Camera Surveillance within the UK: Enhancing Public Safety or a Social Threat?' (Chapter 24), suggests that we should locate policies and government interventions in relation to CCTV cameras on empirical evidence. He questions if there is evidence justifying their proliferation in public spaces on the assumption that use of surveillance cameras significantly contributes to public safety and prevents crime and terrorist activity.

A not dissimilar set of questions is raised in the remainder of the essays. Personalized health care policies, for example, hold out the prospects of placing patients at the centre of decision making and delivery of health care services. Health care accounting may create new power elites. The Health and Social Care legislation may provide a blueprint for new social relations and which may perpetuate asymmetrical power relations. At the moment the dilemma for the law is to create a robust technological infrastructure maintaining security of health information. There is a role for policy-makers and regulators. Governments must be sensitive to concerns about privacy, security and the logistics of implementation. Compare and contrast however these concerns with those raised with regard to social networks. In the age of modernity, information is collected seamlessly. The networked terrain of social networking communication platforms surpasses the windowless cells in George Orwell's Ministry of Love and Bentham's involuntary penal servitude. Digital convergence creates a host of problems for individuals to manage not only some control over the processing of personal data but also the way these same data are subsequently used to create profiles and inform decision-making.

Shara Monteleone argues in 'Privacy and Data Protection at the Time of Facial Recognition: Towards a New Right to Digital Identity?' (Chapter 25) that the current data protection frameworks are wanting in their ability to safeguard users' privacy. She uses the social networking platform, Facebook, to highlight the shortcomings in current privacy protection and calls for a policy that empowers users, and in particular acknowledges the individual's right to digital identity. She suggests that without empowering individuals, industry will continue to utilize individuals' personal data with impunity.

Jeffrey Rosen, 'The Deciders: The Future of Privacy and Free Speech in the Age of Facebook and Google' (Chapter 26), identifies the constitutional dilemmas placed on law. He argues that in the age of Google and Facebook, corporations should take the lead and adopt a version of enlightened stakeholder value that will neutralize the information pathologies of the digital age.

Is there a third way? While law strives to respond to progress through appeals to the Enlightenment's ideals such as human reason and quest for progress, affordances may help release us from the self-imposed immaturity. Donald A. Norman suggests in 'Affordance, Conventions, and Design' (Chapter 27) that if designers make affordances visible this may lead to empowering users and help them better constitute their social relations, and manage the freedoms and opportunities technology make possible. There is a deeper point pursued by Norman, which is the absence of a coherent and understandable conceptual model that informs design solutions. We can infer from the tenor of his observations that designers need to make transparent the necessity for security and make clear the choices open to users in managing their personal data. How does this relate to the health IT infrastructure? The design of centralized databases is motivated by the need, not least to leverage the exponential storage space to hold patient data and the opportunities these create for promoting innovation and efficiency in the delivery of health care. This is a well-discussed area of public policy.

In 'eHealth: Roadmap to Finding a Successful Cure for Privacy Issues' (Chapter 28) Deborah Peel provides an accessible account into the likely impact of digitalizing the health sector for patients. She draws on her considerable experience working with patients' rights organizations to find ways of harnessing the potential of health-related information for the benefit of individuals, communities and the health care industry. For Deborah, access to aggregated health information can assist planning and pre-emptive targeting of resources to meet the needs of communities and vulnerable individuals. However, the electronic health information infrastructure needs to become more mainstream to enable the economies of scale to be realized. More importantly there is some scepticism whether the security protocols are sufficiently robust and ongoing concerns that health information may be used for purposes other than providing medical care or treatment. Deborah's essay provides us with an opportunity to reflect on how best we can design and deploy trusted electronic systems in a way that coheres with Article 8 ECHR and at the same time remain cost effective. Those who remember the 'National Programme for IT' in the NHS in 2002 will recall the massive expenses incurred by the British taxpayer for the public sector disaster. Furthermore, questions continue to be raised about the effectiveness of security protocols to preserve the confidentiality of patient data.

The coherent conceptual model theme is pursued by Daniel L. Pieringer in 'There's No App for That: Protecting Users from Mobile Service Providers and Developers of Location-Based Applications' (Chapter 29). He argues that proliferation of communication service providers, application developers and location-based services has found the law wanting. He

fears that legislators, the IT industry and Apps developers tend to have different approaches to the intersection between usability, security and privacy. He suggests that these parties need to understand the end user better and adopt a comprehensive model that standardizes the philosophies, policies and design solutions.

Will a Privacy Bill of Rights help steer us towards a coherent, effective and sustainable framework balancing the interests of all parties? Christopher Wolf, 'The Privacy Bill of Rights: What Are the Expectations for 2013?' (Chapter 30), is clearly optimistic and suggests that we will move towards this solution. He compares the current status quo in privacy laws to the position in relation to environmental laws. The Consumer Privacy Bill of Rights, proposed by the United States administration, he suggests is a move towards developing a conceptual model that makes explicit the values, norms and goals regarding the collection and use of personal data.

Conclusion

The essays in this volume illustrate the challenges posed by new technologies and the issues that require attention. Two goals are intended to be served. First, to identify the role and value of trust in addressing concerns many feel that the data protection framework is failing them. Second, to provide a snapshot of how we can begin to shape the 'privacy agenda' that can be reconciled with an environment that is diverse, rich and complex, so that it works for individuals, society, industry and governments. More broadly, the essays chosen are intended to provide a commencing point for thinking about how issues relating to identity, surveillance and dependence on smart technologies challenge orthodox conceptions of autonomy, identity and privacy. Why is a multidisciplinary coverage adopted in this volume? Even though privacy laws and regulations have a critical role, smart technologies and the distributed mobile computing environment create an additional layer of complexity. Insights from criminology, sociology and anthropology can assist lawyers, scholars, activists, industry and policy-makers to embrace these perspectives when thinking creatively about developing democratic technological, regulatory and institutional responses. It should be clear from the selected essays in this volume that as new technologies become pervasive we need to think creatively about how we integrate orthodox conceptions of the public and private sphere – it cannot be right to state that we have 'zero privacy'. Neither, it should be added, that we insist on total anonymity. These are some of the issues currently occupying our policy-makers. For example, the European Parliament has recently called on its member states to produce an acceptable outcome to the data protection package. The spread of information sharing between the public and private sector and the exponential rise in the use of surveillance technologies to collect personal information have resulted in the Home Office issuing a code of practice following concerns expressed by the public and the media about the violation of citizens' privacy (Home Office, 2013). The City of London Corporation has asked a company, Renew London, to stop using recycling bins to track the smartphones of passers-by (Datoo, 2013). These examples illustrate the continued tensions between control and access encountered in privacy debates. Although there is very little agreement, for example, on how the concept of privacy is to be understood, the essays illustrate that individuals in society have become a little more sensitive to the contexts in which frequent battles over the ideological and policy arguments about what data processing and surveillance activities cohere with democratic ideals. A timely reminder

perhaps for the need to be cautious and circumspect about any uncritical acceptance of claims for policy fixes.

References

Almunia, J. (2012), 'Competition and Personal Data Protection', SPEECH/12/860, 26 November, at: http://europa.eu/rapid/press-release_SPEECH-12-860_en.htm.

Datoo, S. (2013), 'This Recycling Bin Is Following You', 8 August, at: http://qz.com/112873/this-recycling-bin-is-following-you/.

Deleuze, G. and Guattari, F. (1987), *A Thousand Plateaus*, Minneapolis, MN: University of Minnesota Press.

Haggerty, K.D. and Samatas, M. (eds) (2010), *Surveillance and Democracy*, London: Routledge.

Home Office (2013), *Surveillance Camera Code of Practice*, London: Stationery Office.

Intelligence and Security Committee of Parliament (2013a), 'Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme', at: http://isc.independent.gov.uk/files/20130717_ISC_statement_GCHQ.pdf.

Intelligence and Security Committee of Parliament (2013b), *Report: Access to Communications Data by the Intelligence and Security Agencies*, Cm. 8514, London: HMSO.

Lyon, D. (2001), *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University.

Marx, Gary T. (1998), 'Ethics for the New Surveillance', *The Information Society*, **14**, pp. 171–85.

ReportsnReports (2013), 'Global Electronic Article Surveillance Tags Market 2012–2016', November, at: http://www.reportsnreports.com/reports/270724-global-electronic-article-surveillance-tags-market-2012-2016.html.

Part I
Identity, Security and Privacy in Context

[1]

Designing for Trust

L. Jean Camp

Associate Professor of Public Policy
Kennedy School of Government, Harvard University
Jean_camp@harvard.edu

Abstract. Designing for trust requires identification of the sometimes subtle trust assumptions embedded into systems. Defining trust as the intersection of privacy, security and reliability can simplify the identification of trust as embedded in a technical design. Yet while this definition simplifies, it also illuminates a sometimes overlooked problem. Because privacy is an element of trust, purely operational definitions of trust are inadequate for developing systems to enable humans to extend trust across the network. Privacy is both operational (in the sharing of data) and internal (based on user perception of privacy). Designing trust metrics for the next generation Internet, and indeed implementing designs that embed trust for any digital environment. requires an understanding of not only the technical nuances of security but also the human subtleties of trust perception. What is needed is a greater understanding of how individuals interact with computers with respect to the extension of trust, and how those extensions can be addressed by design.

1 Introduction

Trust is built into all systems, even those without security. Trust assumptions are included when data are collected, or coordination is enabled. Trust is embedded when resources are reserved (as shown by denial of service attacks). If trust is an element of all systems, what does it mean to design for trust?

Trust is a complex word with multiple dimensions. There has been much work and progress on trust since the first crystallization of this concept. Combining the three-dimensional trust perspective with studies of humans, I conclude that a new approach to understanding and designing mechanisms for peer to peer trust is critically needed.

The first section of this work gives a quick overview of the alternative perspectives on trust: rational trust exhibited through behavior and internal trust which cannot be directly observed. The second section revisits the definition of trust offered in Camp 2001, by considering privacy, security, and reliability. At the end of that second section is an examination of how trust has evolved in whois.

Thus at the beginning of the third section there is a clearly defined concept of trust. Using that definition, the third section argues for a trust system that allows users to aggregate trust, make transitive trust decisions, and manage their own electronic domains. This leads to the conclusion - that current trust management systems are hampered by designing for computers rather than humans. Trust systems for the next generation Internet must be built on solid conceptions of human trust drawn from the social sciences.

2 Alternative Perspective on Trust

Multiple authors have offered distinct perspectives on trust. In this section the three dimensional concept of trust is contrasted with other selected concepts of trust. Trust is a concept that crosses disciplines as well as domains, so the focus of the definition differs. There are two dominant definitions of trust: operational and internal.

Operational definitions of trust require a party to make a rational decision based on knowledge of possible rewards for trusting and not trusting. Trust enables higher gains while distrust avoids potential loss. Risk aversion a critical parameter in defining trust in operational terms. In game theory-based analyses of operation trust (e.g., Axelrod, 1994) competence is not at issue. A person is perfectly capable of implementing decisions made in a prisoner's dilemma without hiring a graduate of Carnegie Mellon or MIT.

In the case of trust on the Internet, operational trust must include both evaluation of intent and competence. Particularly in the case of intent, the information available in an equivalent physical interaction is absent. Cultural as well as individual clues are difficult to discern on the Internet as the face of most web pages is impersonal almost by definition.

In the three dimensional definition of trust privacy, reliability, and security are based neither entirely on intention or competence. Both good intent and technical competence are required to ensure security. The result for the user (fraudulent use of data, usually to charge services) from a failure in either intention or competence are the same. Thus an operational approach arguably supports a focus on the types of harms resulting from trust betrayed[1].

One operation definition of trust is reliance. (Golberg, Hill and Shostack, 2001) In this case reliance is considered a result of belief in the integrity or authority of the party to be trusted. Reliance is based on the concept of mutual self-interest. In that way, reliance is built up the assumptions of human beings as *homo economicus* (Olson, 1965). Therefore the creation of trust requires structures to provide information about the trusted party to ensure that the self-interest of the trusted party is aligned with the interest of the trusting party. Reliance-based trust requires that the trusted party be motivated to insure the security of the site and protect the privacy of the user. Under this conception the final placement of trust is illustrated by a willingness to share personal information.

Another definition of trust, popular among social psychologists, assumes that trust is an internal state. (e.g., Tyler, 1990: Fukyama, 1999) From this perspective, trust is a state of belief in the motivations of others. The operational concept of trust is considered confidence. Based on this argument, social psychologists measure trust using structured interviews and surveys. The results of the interviews often illustrate that trust underlies exhibited behavior, finding high correlations between trust and a willingness to cooperate. Yet trust is not *defined as* but rather *correlated with* an exhibited willingness to cooperate.

The difference between these perspectives is a difference in conception of trust a foundation for behavior rather than the behavior itself. To some degree this can be

[1] Betrayal is used in operational definitions in part because to choose not to cooperate is always a function of intent. The same ill intent or moral implications are not appropriate in failures of technical competence; however, the word is still useful for the results of trust ill-placed.

modeled operationally as the difference between perceived (e.g., internal sense of) versus measurable risk (statistical or deterministic). (e.g., Morgan at. al, 2002)

Is willingness to share information based on the risk of secondary use of information rather than a psychological sensitivity to information exposure? Consider the case of medical information. Risks in the United States include loss of employment or medical insurance. Risks in the United Kingdom include loss of employment. In both nations medical issues are considered private. An internalized definition of trust would assume roughly equivalent sensitivity of information exposure in both nations assuming both had the same cultural sensitivity to medical privacy. An operational perspective would argue that medical privacy is more important in the US because the risks are greater[2]. Yet should there be differences it would be impossible to distinguish exactly the elements of risk and the elements of culture that are the foundation of that risk.

These definitions of trust will merge only when observed behavior can be explained by internal state. Yet without understanding trust behaviors, designs for enabling peer to peer trust over the digital network will be flawed.

3 The Three Dimensions of Trust: Privacy, Security, Reliability

The definition of trust offered in (Camp, 2000) is operational when privacy is ensured by anonymity. Absent that assurance, the definition of privacy inevitably included internal considerations. The earlier definition of trust as a function of privacy, security and reliability is operational. It is based on risks rather than user perception of risk. In the operational sense, anonymity offers a definition for privacy that focuses on the existence of risk rather quantifying the risk. In that way it is not stochastic but rather Boolean. Yet with the removal of anonymity, granular issues of privacy arise. There still remains the operational perspective, where privacy is a measure of willingness to share information.

Understanding elements of rationality and elements of internal state requires a finer delineation of privacy than available with a discussion of anonymity. In order to further the discussion of trust in operational and internal terms, this section offers three definitions of privacy. The first, the right to autonomy, is based on fear of state action. The second, a right to seclusion, is based on an internal right to define contact as unwanted. The third, data as property, is based on a strictly rational view of privacy as a market good.

A common approach to the examination of privacy is based on jurisdiction. As travelers cross jurisdictional boundaries their privacy rights, indeed basic human rights, are altered. Any consideration of privacy on the Internet based on jurisdiction must be sufficiently flexible in order to describe any legal regime of privacy. Yet an exhaustive examination of privacy in the jurisdictions of the member states of the United Nations would provide little guidance, as well as exceeding the patience of the reader.

A second concept of privacy is based on cultural concepts of space. Spatial privacy is of particular interest on the Internet because of the lack of cultural or social

[2] This question is an element of the dissertation currently being completed by Sara Wilford at the Kennedy School (contact: sara_wilford@harvard.edu).

clues in virtual spaces. Virtual spaces differ from physical spaces with respect to simultaneity, permeability and exclusivity. (Camp and Chien, 2000). Permeability is the ability to move seamlessly between spaces. (Shapiro, 1998) Simultaneity is ability to move into one space without moving out of another - even when there is no overlap. For example, one my have multiple threads in discrete email lists, or view multiple new sources from a single framed browser. Exclusivity refers to the ability to create spaces that are not only private, but also invisible from the outside. (Nissenbaum and Introna, 2000) Clearly different privacy rules and expectations are appropriate for the marketplace, the avant-guard theater, and the home. Yet there is no single analysis that offers a single coherent theory about spatial privacy across the globe, despite some progress on this track. The goal of this paper is not to move the frontier of the understanding of cultural and spatial concepts of privacy across the planet.

A third approach is to consider identifiable data as the issue, and govern data. The privacy regimes of Europe are designed to provide protection against violations of data protection. The data protection regimes can fit well within the taxonomy presented here if data are addressed under privacy as a human right and privacy as a property right. The data elements prohibited from collection (e.g., orientation) by the data collective would fall under privacy as autonomy.

Beginning with an operational approach, I necessarily fall back on process and structure to define privacy. The American federalist legal system provides an effective parsing of privacy into those issues that are criminal and civil, corresponding with Federal and state law.

Thus my operational framing and the carefully structured (if not particularly rational in outcome) American legal system offer a conception of personal data as a property right, a Federal right of autonomy and a civil right of seclusion. At the risk of self-plagiarism I review the concepts of privacy as embedded in United States law. Any design addressing privacy requires some definition of privacy that states clearly the perception of privacy built into the code. If all is included, then nothing is defined, and the definition is without worth. Definitions of privacy such as those provided by iPrivacy in which transactions are said to be as private "as in the off-line world" are meaningless. The off-line world of political action, idle gossip or commercial transactions? As private as cash transactions or credit card transactions? By including the world in the definition, no limit is placed on concept of privacy. There is no guidance provided for system design. (See iPrivacy.com for that organization's definitions.)

3.1 Privacy as Autonomy - The Human Right

Privacy is the right to act without being subject to external observation. People under constant surveillance are not free.

Arguments against privacy on the basis of autonomy often imply that the ability to act freely and without surveillance offers only the ability to commit those acts normally subject to social sanction. Privacy is sometimes presented as a moral good only to the sinner and the criminal. Yet privacy as an element of autonomy also enhances the public good. The right to privacy allowed the National Association for the Advancement of Colored People (NAACP) by the Supreme Court was the "right of members to pursue their lawful private interests privately and to associate freely with

others." In 1956 this was a right to pursue justice. At the time the members of the NAACP were seen by law enforcement as troublesome at best and subversive at worst. Those left bereaved by the murder of members of the NAACP did not seek justice from the state in the American South in 1956.

In addition to the historical arguments for privacy as autonomy for the greater good there are empirical arguments. Making this argument on the basis of empirical research requires three assumptions. The essence of these assumptions is contained in the second sentence of the first paragraph in the section. First, assume that the opposite of privacy is recorded surveillance. That is, not only is some act observed via real time surveillance but there is also a record of the act created. Second, assume that when privacy is violated the user is aware of that fact. (If this is true is the basis of some debate. Certainly some data compilations are obvious, while some technical mechanisms to obtain user information are devious.) Lastly assume that the existence of the record implies some ability to coerce either by rewarding good behavior or punishing bad behavior. (In this case good or bad can be defined by the party with surveillance capacities.)

Based on the three assumptions above, *homo economicus* would increase his or her good behavior. Yet the arguments that individuals respond in a strictly irrational way when faced with rewards (Kahan, 2001) or punishment (Lawler, 1988) are not reflected in empirical studies. When individuals are paid, required, or recorded in some "good" act the motivation to do that act decreases. A well-documented example of this is the drop in blood donations when individuals are paid (Titmuss, 1971).

Privacy as autonomy offers free people the right to act freely. It enhances not only the power to choose socially prohibited acts, but also the power and tendency to choose socially optimal acts. Surveillance alters action. The constraint on action created by observation is the basis of the autonomy right of privacy.

The American Constitutional right to privacy is grounded in the First, Third, Fourth, Fifth, Ninth and Fourteenth Amendments (Compaine, 1988; Trublow, 1991).

The First Amendment states:

"*Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.*"

The right to read is the right to read anonymously (Cohen, 1996). The argument above suggest that people are not only less likely to go to assemblies and support organizations subject to official sanction, but also that people are less likely to offer their efforts to those socially sanctioned public actions. If every appearance at a social function is marked and credited, then the internal motivation is diminished. People are less free, less autonomous, and less active.

The Third Amendment states:

"*No soldier shall, in time of peace be quartered in any house, without the consent of the owner, nor in time of war, but in a manner to be prescribed by law.*"

The Fourth Amendment states:

"*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*"

Certainly no person argues for law enforcement or military personnel to be placed in the homes of those they police or control. Yet this Amendment is not only a re-

minder of the progress of global concepts of property and human rights, but also a statement about the limits of government's reach. (The Third Amendment is also a personal favorite, and can be used as reminder against nostalgia.) Combined with the Fourth Amendment, this creates of space safe from direct government intervention or even casual surveillance.

The element of the Fifth Amendment that is relevant to privacy states:
"*No person shall ... be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.*"

In terms of privacy the limits on forced testimony are of greatest interest. One cannot be required to testify against oneself. The implications for wiretaps, key stroke tapping programs, and lie detectors remain in dispute. Yet it is certain that while some technology and all possible wiles can be used against a suspect, compelling testimony is simply not acceptable. Neither can an innocent person's movements nor his thoughts be constrained by governmental force.

The Ninth Amendment states that the set of Constitutional rights is neither exclusive nor exhaustive. The Ninth Amendment allows the right to privacy to exist in a Constitutional sense. The Fourteenth Amendment (which primarily implemented a punitive and destructive approach to nation-building for the American south) states the rights given by the Federal government cannot be abridged by the states.

The question with respect to rights of autonomy on the Internet are questions of economic and corporate power. The coercive power of the state was well-recognized by the eighteenth century. Yet the modern corporation did not yet exist. The ability to gather information and violate privacy was held by the state alone until the rise of the popular press in the nineteenth century. Because of the First Amendment, weak privacy rights were necessarily trumped by strong speech rights. Yet the debate on the Fourteenth Amendment asks if the state has a positive responsibility to guarantee those rights, or simply the responsibility not to violate them directly.

When building a system specific to digital government, an understanding of autonomy is required. Yet the legal understanding of autonomy in the commercial corporate world is yet inchoate. Because of the uncertainty of the policy outcome, and the reality of the risk faced by a median worker, technical designs that promise a level of trust appropriate for the person concerned with autonomy must meet a high standards than designs based on seclusion or property concepts. (Camp and Osorio, 2002).

3.2 Privacy as Seclusion – The Right to Be Let Alone

"The right to be let alone." Warren and Brandies' alliteration of privacy has come to be a definitive work. A century and half later the work was either refined (Prosser, 1941) or destroyed (Bloustein, 1968) by determining that right to be free from intrusions consists of four possible torts: intrusion upon seclusion, appropriation of name and likeness, false light, and public disclosure of private facts.

Each of these torts is framed by the technology of the printing press. Understanding their meaning in a networked digital world requires a reach across an economic and technological chasm. In fact, the work singled out the then-emerging popular press for reprobation: "Gossip is no longer the resource of the idle and of the vicious, but has become a trade which is pursued with industry as well as effrontery." (Warren

and Brandeis, 1890). Now gossip is not only the vocation of journalist but also the avocation of many with a modem.

Appropriation of name and likeness may include names in meta-data in order to associate with amore successful site. It may include the use of domain names to obtain the attention of those seeking a related site, as when Colonial Williamsburg was used by the service employee unions (Mueller, 2001). Or it may include the use of a person's name or publications to attract those interested in related materials. Yet such appropriations are treated very differently. Meta data is not generally actionable while domain names have been subject to action based on the expansion of the rights of trademark holders. Visibility of meta-data allows detection of mis-appropriation. Trust systems that implement ratings, meta-moderating and ordering of sites can address misleading and appropriate practices.

False light is so common on the web that making it actionable seems impossible. When everyone is a journalist, everyone has the right to frame content. Private persons need show only falsehood, yet how can on be an active participant in networked conversations and remain a private participant? False light is entirely content based. Again implementation of content-ratings systems can address false light, assuming that the majority do not choose falsity over truth.

Public disclosure of private facts implies individual control over information. Registration systems that send information about the user (also known as spyware) violate this concept of privacy. Spyware is used in browsers and peer-to-peer systems including Kazaa and Limewire. The sharing of this information and targeting of ads provides the financial incentive for the systems to continue to function. Arguably the networks would not exist without the spyware. Yet the design for trust perspective would allow such designs only if the systems were easy to delete, and adequate notice was part of the design. Adequate notice may be as simple as allowing a add-on to be disabled during use rather than asking for a one-time installation permission.

3.3 Privacy as Data Ownership – The Property Right

For those who believe that privacy is property, what is required is a fair trade for private data. Much of the legislative debate about privacy concerns the existence and intensity of concerns about privacy. Observations of the diffusion of the Internet commerce are in contrast with surveys identifying increasing privacy concerns.

The privacy as property argument is enhanced by considering private information as a form of intellectual property (Mell, 1996). In that case the transfer of data subject to data owner is fairly conceptually simple.

The concept of privacy as property can explain this conflict. Individuals are ready to provide information to Amazon. Amazon decided that legal risk prevented the personalization and affinity marketing provided by user data. Therefore Amazon issued a privacy policy removing all possible expectation of privacy from users. The Free Software Foundation and Computer Professionals for Social Responsibility issued a call for a boycott. Amazon was only marginally affected. Amazon used consumer information for consumer benefit.

In contrast, Geocities used consumer information only for the benefit of Geocities. Geocities, like Amazon, depends entirely on customer relationships. After the Federal Trade Commission announced that Geocities had substantially violated the pri-

vacy of it's the total value of Geocities fell nearly $1,000,000 for each minute that the stock market remained open. Geocities never recovered the value.

If privacy is property then programs that send personal information or trap personal information are theft. In that case the most basic market frameworks are all that is required in designing for privacy.

3.4 Privacy and Security

Security is not privacy. Confidentiality allows a person to communicate with another without eavesdroppers. As confidentiality is a function of security and an enabler of privacy, security and privacy are sometimes confused. Yet in the general case, the control of information enabled by security does not imply privacy. Security enables the control of digital information, while social and organizational forces determine who exercises the power of that control. Privacy requires that a person be able to control information about his or her self.

Security provides to privacy the ability to generate privacy in a specific case (as with confidentiality of communication). Security also provides the capacity for cryptography. Cryptography is the art of hiding information. When the information that is hidden is identifying information then security can be said to provide anonymity. Anonymity is a technical guarantee of privacy.

Thus, unlike many social values, the concept of privacy has an excellent mapping into implementation because of anonymity. Yet the simplicity of removing individual names is misleading. For example, inclusion of date of birth, current residence and place of birth will uniquely identify most Americans.

3.5 Trust as Reliability

Trust implies more than secure endpoints – it requires that such security not come at the expense of survivability. Two of the greatest strengths of the Internet Protocol are that it is distributed, and it exhibits graceful degradation. Graceful degradation means any person can connect to the a network without altering others' access, and the loss of one machine does not effect those not using its services. Even during the most effective assault to date on the Internet, the Morris worm incident, staying connected proved to be the best strategy for recovery. Obtaining defenses against the worm, and information regarding these defenses, required remaining connected. Those who disconnected were isolated, with only their own resources to develop defenses. The ability of any network – the Internet or an intranet – to degrade gracefully rather than suffering catastrophic failure is survivability.

Trust architectures have developed significantly in the past decade. Yet despite that innovation, security can come at the cost of reliability and survivability. Security systems (as well as a lack of security systems) both enable denial of service attacks. Security systems that are computationally intensive or intolerant of user input increase the likelihood of a user experiencing the system as unreliable.

An element of design for trust should be designing the survivability of distributed trust mechanisms. Proposals for trust include short-lived attribute-specific certificates (Blaze, Feigenbaum, Ioannidis and Keromytis, 1999); long-lived multipurpose certificates (e.g., Anderson, 2001); certificates signed by multiple parties (Visa, 1995); a

Web of Trust (Garfinkle, 1994) and or a combination of these into a Web of Hierarchies. Yet other than the Web of Trust, few of the distributed trust mechanisms have been evaluated with respect to their ability to recognize an attack, reduce the damage of any attack, and subsequently recover. To design for trust, it is necessary to determine if, and under what conditions trust mechanisms are brittle.

4 A Design for Trust Application: The Case of Whois

Were whois to function as designed there would be no privacy considerations. Recall that the design goal of whois is to provide technical information in the case of technical errors or malicious action.

Yet the Internet has changed, and the administrative structures of the Internet have changed as well. whois is an example of a technology currently in use which was designed at a point in time with vastly different economics, norms, and politics.

whois was designed for the purpose of containing narrow technical contact information. whois was built for a relatively small Internet community consisting of predominantly technical users. Additional fields were added to whois, and the expansion of the function of whois occurred when the trust assumptions about the Internet began to fail. The additional fields include administrative and billing contacts. Had the trust model implicit in whois been recognized, the lack of wisdom in adding the additional field would have been obvious. A technical contact would be appropriately contacted if a server were taking part in a DDoS attack. Yet the webmaster or billing contact would be appropriately contacted if content in a web site were under dispute.

The additional fields in whois are useful primarily to content enforcement authorities. A significant problem with the traditional approaches to obtaining law enforcement information is that web sites cross jurisdictions. There already exist treaties and cooperation in terms of obtaining subscriber information form telephone companies across the borders of jurisdictions. Such policies, worked out over more than century, provide a basis for law enforcement to obtain information. These policies were worked out in a complex trust network that included issues of sovereignty and imbalances of power. As the Internet and traditional network services converge, the possible business and legal arrangements between a network service provider and content provider explode. The trust environment becomes more similar to the politicized environment of global competition and cooperation reflected in the governance of telephony.

By limiting whois information to technical contact and the appropriate registrar, motivation for incorrect contact information would be significantly decreased. Default automated access to whois information could reasonably be limited to those with network responsibilities. Feasible limitation of automated access to whois, and thus the ability to increase the integrity of the information, requires technical coordination at a level the holders of whois information have yet to achieve. A necessary first step for cooperation is trust. Trust may be enabled by removing the functionality that brought the enforcement spotlight to bear on whois. Reversing the unwise expansion of whois, and thus decreasing the resulting focus of intellectual property and other enforcement authorities on whois', could enable the trust necessary for cooperation.

In addition to the changes in community the domain name itself has changed. Originally simply a mnemonic the domain name is now commercial property, politi-

cal speech, personal expression or artistic moniker. As a result very different models of privacy apply. It is these differences in privacy models that 'are a core cause of the trust models in whois. It is unlikely that IBM.com considers the contact information in the domain registration as constraining institutional autonomy in the political domain. etoys.org was notoriously noncommercial (Mueller, 2002).

The trust failure is a function of the expansion of whois to include billing and administrative fields without reconsidering the core trust assumption: that all Internet users are created equally powerful. Billing and administrative contact became necessary as the use and users of the Internet, and thus the trust relationships on the Internet, were changing. The increased diversity of Internet users and the resulting decrease in trust was exacerbated by alterations of whois.

In this case the original design was narrow and suitable for the initial environment. Failing to expand the function and fields of whois beyond the minimal necessary technical requirements would both have served the whois system more effectively and allowed the trust assumptions to remain valid in the rapidly changing realm of the Internet. This is because the trust framing was for technical individuals empowered over some small section of the network. By limiting the fields to technical information, that trust model would have been more likely to remain consistent, and therefore the service was more likely to remain effective.

5 Design for Trust

At this point I have offered a concept of trust as consisting of privacy, reliability and security. Also there has been one small example, arguing that design for trust would have resulted in a more limited and possibly more reliable whois. In this section that modest core is expanded to a broad call for trust systems that are multidimensional, transitive, and aggregate.

Trust in today's Internet is based on all-or-nothing trust relationships. A network resource request is not trusted before authentication, and after authentication it is granted the full credentials of the corresponding user. Executable content from within a protected network is completely trusted, but content from outside the firewall is strictly disallowed. A network connection, once established, has equal priority with all other network connections on the system. These all-or-nothing trust relationships fail to match the expectations of users and the needs of next generation network applications. This mismatch promotes security breaches among users, as users undermine simplified trust models to meet their own complex resource-sharing needs. As for the specific example of executable content, it is one of the keys to providing advanced functionality in network applications, but is typically disallowed by firewalls. The firewall model of trust is too simple to distinguish secure sources of executable content. When sophisticated users find this exclusion unacceptable and use methods like tunneling to work around it the security of the entire protected network can be compromised. There is a need for distributed trust modes that will allow distinctions to be made in the trustworthiness of network entities. In order to do this it is necessary to provide a better match between peoples' intuitive notion of trust and the needs of next generation applications.

Security in today's Internet is focused on a centralized model where strong security requires a firewall. The firewall may be a formidable obstacle, but once it has been

compromised the entire network that it protects is compromised, making the firewall a single point of failure. The tunneling example demonstrates how this centralized approach can allow a single breach of security to compromise the security of the entire protected network.

The Microsoft/Verisign approach to regulating executable content is to centralize trust. In this approach, a presumably trustworthy third party uses a digital signature to verify the identity of an executable module. Although there is some commonality in purpose, their security model is the antithesis of most human approaches. It assumes that the same level of trust is appropriate for all approved content and gives a right of approval to some developers. Further, it requires users to manually examine the source of executable content to provide more subtle variations of trust. The parallel to the firewall example are clear.

Currently proposed cross-domain trust mechanisms seek to minimize computational costs and management overhead. For example, commerce systems minimize key generation by linking all attributes and rights to a single commerce-enabling certificate. These keys are validated by a single root. This creates a single point of failure for the entire system (the root) as well as a single point of failure for the consumer (the key). The only similar system in the United States is the currency system, where the failure of the US Treasury would yield complete collapse. In family systems, individual businesses, and even religions there are multiple levels and power points. In physical security, any key is a part of a key rings, so that the failure of the validity of one key does not destroy the strength of all electronic locks. .Net ("dot net") or Passport exacerbate this problem by allowing cross-domain failure from a single lost pass phrase.

SSH and SSL are used for securing Internet connections. SSH is commonly used to provide secure terminal connections, whereas SSL is commonly used to implement secure HTTP connections. The endpoints of these connections have to be ready to extend trust before the mechanism are called into play. They are extremely useful technologies for the prevention of snooping but are not useful for implementing organizational or individual trust across many dimensions (including time).

Yet in real life and in social networks the "security models" (including drivers licenses, check clearing, credit cards, etc.) distribute the resources that implement authentication and authorization. In network security there are still single roots, and control is often held in a centralized point of control.

A network service can be rendered unusable when the number of requests it receives exceeds the rate at which they can be served. This creates an important relationship between performance and security for Internet servers. Although users on today's Internet are accustomed to server failures due to overload, the the next generation of Internet-based applications will require better service guaranties. Decentralization is necessary to provide stable peak performance, even when a site as a whole is experiencing overload, until network capacity becomes the limiting factor. Decentralization provides defense against a large class of denial of service attacks. In contrast, overload in conventional systems typically results in thrashing behavior such as paging, leading to significant performance loss.

Decentralization requires utilizing processing power at the endpoints more effectively. Decentralized trust requires enabling users to be their own trust managers. There is a need for a peer-to-peer distributed trust mechanism that implements trust effectively in the ever-increasing scale of the network. The network needs to scale not only to an increasing number of devices but also in terms of complexity of tasks.

Yet as there are increasingly complex interactions and task on the network, simplicity is critical to user-managed resource-specific security.

In order to allow users to share information it is necessary both to communicate trust states and enable users manipulation their own trust states. Trust must support the complexity of life, in that users function in multiple dimensions. For example, a spouse will have access to all shared family and personal information. Yet a spouse should not have access to all company and employer information. Trust in these two dimensions is managed off-line because of the reality of physical space.

In addition to having multiple dimensions, users should be able to aggregate trust within a dimension. With aggregate trust the initial extension of trust is based on some introduction, which is provided by any entity or security mechanism. Any additional extension of trust is then based on aggregating different mechanisms (e.g., attaching value to different attribute-based certificates and summing) and/or extending trust to a machine based on interactions over time. Such a mechanism would be modeled more on observed social networks than on the strengths of cryptography. Users who find multiple independent paths to another user would increase the trust to that person accordingly, in a more generous manner than proposed in (Beth, Borcherding, and Klein, 1994).

An early example of a user-centered approach to distributed trust, the UNIX philosophy gives users responsibility for setting security controls on their own resources. For example, UNIX systems allow users to set file protection level. Yet this approach is not adequate for a number of reasons. First, for those using UNIX based system the security mechanism is hampered by its lack of simple mechanisms for authentication and resource sharing across domains. Second, the UNIX security system requires understanding the operating system and the distinction between listing, executing, and readings a file. Third, the interface violates the rules of good human-computer interaction (HCI) design. Truncated commands (e.g., chmod), a text line interface, and obscure error codes make this interface flawed. In addition the function has too many parameters, and these parameters are not clearly specified. For these reasons, even if there were well implemented cross-domain UNIX file protection mechanisms, this implementation would fail to meet the needs of the modern Internet user.

Similarly peer to peer systems allow users to determine which files are be shared. Peer to peer systems are built to implement coordination and trust across administrative domains. Peer to peer systems allow for sharing trust across domains, yet are notoriously hampered by problems of accountability (e.g., Oram, 2001). Peer to peer systems allow users control over their own files in a more transparent manner than UNIX controls, but the P2P code itself is often untrustworthy (e.g., Borland, 2002).

Any optimal trust approach would benefit from experience with Pretty Good Privacy (PGP), which lets users increase trust in a transitive manner. Transitivity means that users select their own sources of validation; e.g. if A trusts B and B validates C, then A trusts C. There is no central server of tree-like hierarchy that validates users. PGP also lets users select their own sources of trust, and select a key length appropriate for the situation. PGP is specific to a single application, electronic mail. In PGP users select specific individuals to trust based on their ability to verify the identity/key carried in a PGP certificate. This research extends and enhances the distributed security model of PGP to the more generic problem of sharing resources.

PGP is weak in that there is a single dimension of trust. Regardless of the definition of trust, it is certain that there are different dimensions of trust. Social admonitions not to mix friendship and money illustrate this, as well as concepts of family

trust versus trusting in a business transactions. Trusting one's sister and trusting IBM are very different matters indeed. Users should be able to express trust in more dimensions, more richly, than with PGP. Yet unlike whois, PGP has maintained its efficacy by refusing to expand beyond its design base of email.

The attempt to minimize system management by concentration of trust management is a fundamental error, doomed to fail in a world of increasingly complex trust arrangements. Oversimplified security paradigms which limit implementations will result in users subversion. Security management should be distributed and simplified by automation, rather than simplified at by the administrative assumption of a single trusted entity. Humans are capable of managing quite complex tasks (consider in the abstract the task of driving an automobile) if enabled by an interface that provides adequate and useful feedback.

Rather than minimizing computational and management costs, future trust designs ideally will recognize the high value of distributed security and empower the resource owner to be a security manager. Security management must become more complex because peer-to-peer, international resource sharing is more complex than intra-network sharing. Peer to peer systems recognize the need to share resources, yet the trust problems in peer to peer systems have not been solved. In fact, in 2002 most trust systems require users trust a central software distributor or administrator. The trust problem has only begun to be solved.

In order to provide simple mechanisms to enable users to take responsibility for their own resources, the design must implement an understanding of trust based on an understanding of trust among human users and social networks. While such a design basis may appear initially too complex for implementation, such a model would inherently provide better scalability and better resistance to attacks than the current, popular, centralized model.

In short, trends in distributed system security computing are on a collision course with system survivability through the construction of brittle trust mechanisms. The lack of understanding of the human interface exacerbates this problem. If trust extensions are not effectively communicated to the very human users, those users cannot react effectively when and if the trust system fails.

6 Conclusions on Design for Trust

Experts focus on the considerable technological challenges of securing networks, building trust mechanisms, and devising security policies. Although these efforts are essential, that trust and security would be even better served if designs more systematically addressed the (sometimes irrational) people and institutions served by networked information systems. In order to address human concepts of trust, privacy must be a consideration and not an enemy or afterthought of the implementation.

Efforts at securing systems should involve not only attention to machines, networks, protocols and policies, but also a systematic understanding of how social agents (individuals and institutions) participate in and contribute to trust. Security is not a separable element of trust. An interdisciplinary perspective will enable protocols for trust over the network to be optimized for human trust.

That the human is a critical element in security systems has been recognized both from a usability point of view (Tygar and 'Whitten, 1999) and from the analysis of

systematic failures of security (Anderson, 1994). However, little work integrates methods from the social sciences, philosophy, and computer science to evaluate mechanisms for trust on-line. Previous work on integrating privacy and security (Friedman, Howe and Felton, 2002) has been complicated by the lack of a definition that can be used across disciplines. Efforts have been made to find a single definition of trust that can be used effectively within philosophy, computer security, and those social scientist embracing an operational definition of trust, as shown in (Camp, McGrath and Nissenbaum, 2001).

Design for trust requires examining all assumptions about a system and the user of the system. Sometimes those assumptions are based on class (e.g., the user has a credit card). Sometimes those assumptions are based on the capacities of the human (e.g., the user must select a large number of context-free random passwords). Sometimes the assumptions are necessary to enable a functioning design.

Design for trust requires enumerating the social assumptions and examining how those assumptions can function to put some user of the system at risk. In order to understand and design trust systems, acknowledgment of the social and human elements are required.

References

Anderson, R.: Security Engineering, Wiley, New York (2001).

Axelrod, R.: The Evolution of Cooperation, Harper Collins, USA (1994).

Beth, T. , Borcherding, M., Klein, B.: Valuation of Trust in Open Networks. D. Gollman, ed., Computer Security – ESORICS '94 Lecture Notes in Computer Science. Springer-Verlag Inc., Berlin (1994) 3–18.

Blaze, M., Feigenbaum, J. , Ioannidis, J. , and Keromytis, A.:The role of trust management in distributed systems security" Secure Internet Programming, Vol. 1603. Lecture Notes in Computer Science. Springer-Verlag Inc. Berlin (1999) 185-210.

Bloustein, A. :Privacy as an aspect of human dignity: an answer to Dean Prosser. New York University Law Review 39: (1968) 962-970.

Borland, J.: Stealth P2P network hides inside Kazaa. CNET Tech News, April, 2002. http://news.com.com/2100-1023-873181.html (2002)

Camp, L. J. : Trust and Risk in Internet Commerce, MIT Press, Cambridge, MA (2001).

Camp, L. J and Chien, Y.T. :The Internet as Public Space: Concepts, Issues and Implications in Public Policy, Readings in Cyberethics. eds. R. Spinello and H Tavani, Jones and Bartlett Pub., Sudbury , MA (January 2001). Previously published in ACM Computers and Society, September (2000).

Camp, L. J., McGrath C. and Nissenbaum H.: Trust: A Collision of Paradigms. Proceedings of Financial Cryptography, Lecture Notes in Computer Science. Springer-Verlag Inc. Berlin (2001).

Camp, L. J. and Osorio, C. :Privacy Enhancing Technologies for Internet Commerce. Trust in the Network Economy. Springer-Verlag, Berlin (2002).

Cohen, J. :A Right to Read Anonymously: A Closer Look at Copyright Management in Cyberspace. Conn. L. Rev. Vol. 28 (1996).

Compaine B. J. :Issues in New Information Technology. Ablex Publishing, Norwood, NJ (1998)

Friedman, B., Howe, D. C., and Felten, E.: Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Proceedings of the Thirty-Fifth Annual Hawaii's International Conference on System Sciences. IEEE Computer Society: Los Alamitos, CA. (2002).

Fukuyama F. :Trust: The Social Virtues and the Creation of Prosperity. Free Press, NY, NY (1996).

Golberg, Hill and Shostack: Privacy Ethics and Trust. Boston University Law Review, Vol. 81, N. 2 (2001) 407 -422.

Garfinkle, S.: Pretty Good Privacy, O'Reilly Publishing, Cambridge, MA. (1994).

Kahan, D. :Trust, Collective Action, and Law. Boston University Law review, Vol. 81, N. 2 (2001) 333-347.

Lawler, E. J. :Coercive Capability in Conflict: A Test of Bilateral versus Conflict Spiral Theory. Social Psychology Quarterly, Vol. 50 (1988) 93-96.

Mell, P.:Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness. Berkeley Technology Law Journal 11(1).
(http://www.law.berkeley.edu/journals/btlj/index.html) (1996)

Morgan, M. G.,Bostrom, A., Fischhoff, B., Atman, C. J.: Risk Communication : A Mental Models Approach. Cambridge University Press, Cambridge, UK (2002).

Mueller, M.: Ruling the Root. MIT Press, Cambridge, MA (2002).

Nissenbaum, H. and Introna, L. :Sustaining the Public Good Vision of the Internet: The Politics of Search Engines. The Information Society, Vol. 16, No. 3 (2000).

Olson: The Logic of Collective Action: Public Goods and the Theory of Groups. Harvard University Press. Cambridge, MA (1965).

A. Oram, ed.: Peer-to-Peer Harnessing the Power of Disruptive Technologies. O'Reilly and Associates, Cambridge, MA (2001).

Prosser W.L.: Handbook of the Law of Torts, West Publishing Co., St. Paul, MN (1941).

S. Shapiro: Places and Space: The Historical Interaction of Technology, Home, and Privacy. The Information Society, No. 14, Vol. 4, (1998) 275-284.

Titmuss R. M. :The Gift Relationship: From Human Blood to Social Policy, Expanded and revised edition. Ann Oakley and John Ashton (eds.) The New Press, New York (1997).

Trublow, G.: Privacy law and practice. Times Mirror Books, New York (1991).

Tygar, J.D. and Whitten, A., : WWW Electronic Commerce and Java Trojan Horses, Second USENIX Electronic Commerce Workshop, Berkeley, CA (1996).

Tyler, T. :Why People Obey the Law. Yale University Press, New Haven, NH (1990).

Visa: Secure transaction technology specifications. Version 1.1, Visa International, New York (1995).

Warren S. and Brandeis L.: The right to privacy. Harvard Law Review, Vol. 4 (1890) 193-220.

[2]

The Digital Persona and Its Application to Data Surveillance

ROGER CLARKE

Australian National University
Department of Commerce
Canberra, Australia

The digital persona is a model of the individual established through the collection, storage, and analysis of data about that person. It is a useful and even necessary concept for developing an understanding of the behavior of the new, networked world. This paper introduces the model, traces its origins, and provides examples of its application. It is suggested that an understanding of many aspects of network behavior will be enabled or enhanced by applying this concept. The digital persona is also a potentially threatening, demeaning, and perhaps socially dangerous phenomenon. One area in which its more threatening aspects require consideration is in data surveillance, the monitoring of people through their data. Data surveillance provides an economically efficient means of exercising control over the behavior of individuals and societies. The manner in which the digital persona contributes to an understanding of particular dataveillance techniques such as computer matching and profiling is discussed, and risks inherent in monitoring of digital personae are outlined.

Keywords Internet, agent, network behavior, behavior monitoring, personality projection, computer matching, profiling, data quality

The marriage of computing and telecommunications brought us networks. This led to connections among networks, most importantly the Internet. With the networks has come a new working environment, popularly called "the net," "cyberspace," or "the matrix." Individuals communicate by addressing electronic messages to one another and by storing messages that other, previously unknown people can find and access. For a review of applications of the Internet to the practice of research, see Clarke (1994).

People exhibit behavior on the network that other people recognize. Some of it is based on name; for example, people who use a pseudonym like "Blackbeard" create different expectations in their readers than people who identify themselves using a name like "Roger Clarke." Other aspects of the profile of people on the net are based on the promptness, frequency, and nature of their contributions, and the style in which they are written.

Over a period of time, the cumulative effect of these signals results in the development of something that approximates personality. It is a restricted form of personality, because the communications medium is generally restricted to standard text; at this early stage of developments, correspondents generally do not see pictures or sketches, or even handwriting, and do not hear one another's voices. The limitations of the bare 26 letters,

Received 20 August 1993; accepted 20 January 1994.

Address correspondence to Roger Clarke, The Australian National University, Dept. of Commerce, Canberra, ACT 0200 Australia. Email: Roger.Clarke@anu.edu.au.

10 digits, and supplementary special characters of the ASCII character set have spawned some embellishments, such as the commonly used "smiley" symbol :-), the frowning symbol, :-(, and the wink ;-). Some variations are possible, of course; for example, (:-|) could imply a boring, bald person with a beard, and {&-() could be someone with a hangover. Generally, however, the symbol set is anything but expressively rich. Moreover, its use originated in and is by and large limited to particular net subcultures.

Net-based communications give rise to images of the people involved. These images could be conceptualized in many different ways, such as the individual's data shadow, or his or her alter ego, or as the "digital individual." For reasons explained below, the term "digital persona" has some advantages over the other contenders. This paper's purpose is to introduce and examine the notion of the digital persona.

Introduction to the Digital Persona

In Jungian psychology, the *anima* is the inner personality, turned toward the unconscious, and the *persona* is the public personality that is presented to the world. The persona that Jung knew was that based on physical appearance and behavior. With the increased data intensity of the second half of the twentieth century, Jung's persona has been supplemented, and to some extent even replaced, by the summation of the data available about an individual.

The digital persona is a construct, i.e., a rich cluster of interrelated concepts and implications. As a working definition, this paper adopts the following meaning:

> The digital persona is a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual.

The ability to create a persona may be vested in the individual, in other people or organizations, or in both. The individual has some degree of control over a *projected* persona, but it is harder to influence *imposed* personae created by others. Each observer is likely to gather a different set of data about each individual, and hence to have a different gestalt impression of that person. In any case, the meaning of a digital persona is determined by the receiver based on his or her own processing rules. Individuals who are aware of the use of data may of course project data selectively in order to influence the imposed digital persona that is formed (e.g., on arriving in the United States, immigrants may take out an unnecessary loan simply to create a credit record).

It is useful to distinguish between *informal* digital personae based on human perceptions, and *formal* digital personae constructed on the basis of accumulations of structured data. The data intensity of contemporary business and government administration results in vast quantities of data being captured and maintained, and hence considerable opportunity to build formal digital personae. These data range from credit and insurance details, through health, education, and welfare, to taxation and licensing. The extent of interchange of data holdings among organizations is increasing, both concerning groups (e.g., census and other statistical collections) and about identified individuals (e.g., credit reference data and ratings, insurance claims databases, consumer marketing mailing lists, telephone, fax and email address directories, electoral rolls, and license registers). Later sections of this paper also distinguish between *passive, active,* and *autonomous* digital personae. A schematic representation of the formal, passive digital persona is shown in Figure 1.

There is something innately threatening about a persona constructed from data and used as a proxy for the real person. It is reminiscent of the popular image of the voodoo

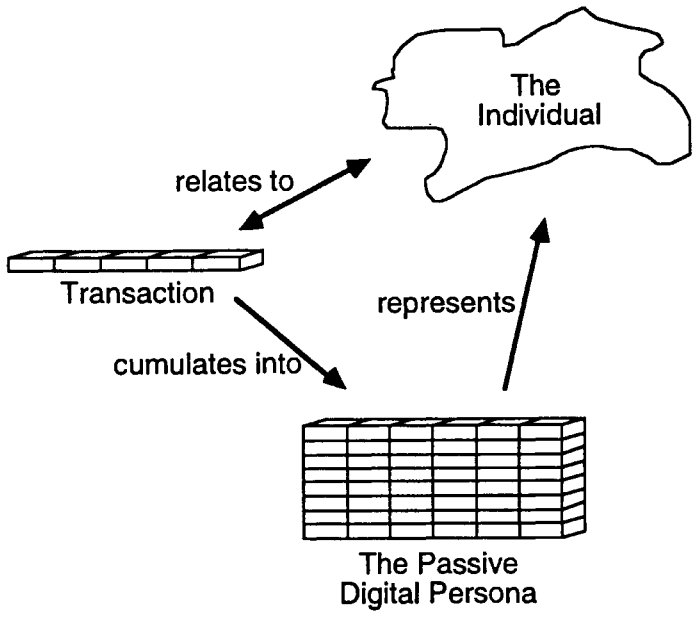

Figure 1. The passive digital persona.

doll, a (mythical) physical or iconic model, used to place a magical curse on a person from a distance. Similar ideas have surfaced in "cyberpunk" science fiction, in which a "construct" is "a hardwired ROM cassette replicating a. . . man's skills, obsessions, knee-jerk responses" (Gibson, 1984, p. 97). Some people may feel that such a construct is demeaning, because it involves an image rather than a reality. Others may regard it as socially dangerous. This is because the person's action is remote from the action's outcome. This frees the individual's behavior from his or her conscience, and hence undermines the social constraints that keep the peace.

The digital persona offers, on the other hand, some significant potential benefits. Unlike a real human personality, it is digitally sense-able, and can therefore play a role in a network, in real time, and without the individual being interrupted from work, play, or sleep. Leaving aside the normative questions, the notion has descriptive power: Whether we like it or not, digital personae are coming into existence, and we need the construct as an element in our understanding of the emerging network-enhanced world. The following sections investigate the nature of the digital persona, commencing with a simple model and progressively adding further complexities in order to build up a composite picture of the notion.

The Passive Digital Persona

A digital persona is a model of an individual and hence a simplified representation of only some aspects of the reality. The efficacy of the model depends on the extent to which it captures those features of the reality that are relevant to the model's use. As with any modeling activity, it suffers the weaknesses of the reductionist approach: Individuals are treated not holistically, but as though a relatively simple set of data structures were

adequate to represent their pertinent characteristics. Some aspects of the person's digital persona and of the transactions that create and maintain it can be represented by structurable data, such as the times of day when the person is on the net, the frequency and promptness with which he or she communicates, and the topics he or she discusses. Other aspects are more subjective and depend on interpretation by message recipients of such factors as the degree of patience or tolerance shown, the steadiness of expression, the appreciation of the views of others, and the consistency of outlook. There is a trade-off between the syntactic consistency with which structured data can be processed and the semantic depth and tolerance of unusual cases associated with less formal communications.

An individual may choose to use more than one projected digital persona. People may present themselves differently to different individuals or groups on the net, or at different times to the same people, or at the same time to the same people. One projection may reflect and provide close insight into the person's "real personality," while other personae may exaggerate aspects of the person, add features, omit features, or misrepresent the personality entirely. Reasons why people may wish to adopt multiple personae include the following:

- Maintenance of a distinction between multiple roles (e.g., prison warder, psychiatrist or social worker, and spouse/parent; employed professional and spokesperson for a professional body; and scoutmaster and spy)
- Exercise of artistic freedom
- Experimental stimulation of responses (e.g., the intentional provocation of criminal acts, but also the recent instance of a male impersonating a physically impaired female)
- Willing fantasy (as in role-playing in multiuser dungeons and dragons, or MUDDs)
- Paranoia (i.e., to protect against unidentified and unlikely risks)
- Fraud and other types of criminal behavior

There are many instances in which multiple projected personae may be used constructively. In conventional e-mail, recipients may be unaware that multiple user names are actually projections of the same person, and the sender may thereby feel free to express a variety of ideas, including mutually contradictory ones. Anonymity is particularly useful in alleviating problems associated with power differentials, such as the fear of retribution by one's superiors or of derision by one's peers. Even where the mapping of digital personae to person is known to the recipients, the sender's choice of persona enhances the semantic richness of the conversation. In contexts beyond e-mail, the idea has even greater power. In the decision support literature, techniques such as brain-storming and Delphi encourage the pooling of know-how and the stimulation of new ideas. The existing choice among comments being anonymous, temporarily anonymous, or identified can be supplemented by participation in the event of more personae than people. This enables advantage to be taken of the power and complexity of intellectually prodigious individuals.

The Active Digital Persona

In the preceding section, the digital persona was described as a passive notion, comprising data alone. It is important to relax that simplification. The concept of an "agent" has been current in computer science circles for some years. This process acts on behalf of the individual, and runs in the individual's workstation and/or elsewhere in the net. A trivial implementation of this idea is the "vacation" feature in some e-mail servers, which

returns a message such as "I'm away on holiday until <date>" to the senders of messages. (Where the sender is a mailing list, this may result in broadcast of the message to hundreds or thousands of list members.)

More useful applications of projected active digital personae are mail filterers (to intercept incoming mail and sort it into groups and priority sequences), news gatherers (to search news groups, bulletin boards, and electronic journals and newsletters in order to identify items of interest to the individual and compile them into personal news bulletins), and "knowbots" (to undertake relatively intelligent searches of network sources in order to locate and fetch documents on a nominated topic). For a review of some of these capabilities, see Loch and Terry (1992).

The agent concept derives from two ideas. One is the long-standing, spookily named "daemon," i.e., a program that runs permanently in order to perform housekeeping functions (such as noticing the availability of files to be printed and passing them in an orderly manner to the printer). The other ancestor idea is the "object," which refers to the combination of data with closely associated processing code. Although this term should be understood in its technical sense, it is unavoidable that people who are fearful of the impacts of ubiquitous networking will draw attention to how the very word underlines the mechanistic dangers inherent in the idea.

The active digital persona has all of the characteristics of the passive: It can be projected by the individual or imposed by others and it can be used for good or ill. The difference is in the power that the notion brings with it. It enables individuals to implement filters around themselves, whereby they can cope with the increasing bombardment of data in the networked world. These need not be fixed barriers, because they can self-modify according to feedback provided by the person or compiled from other sources; and they can contain built-in serendipity, by letting through occasional lowly weighted communications, and hence provide the network equivalent of bookshop browsing.

People's digital behavior may be monitored (e.g., their access to their mail and the location they accessed it from, and their usage of particular databases or records). This may be done with the agreement of the individual, as a contribution to community welfare and efficiency (see, for example, Hill & Hollan, 1994), or without the individual's knowledge or consent, in which case it may be used sympathetically or aggressively.

In the extreme case, an active agent may be capable of autonomous behavior. It may be unrecallable by its originator (as was the case with the Cornell worm). It may, by accident or design, be very difficult to trace to its originator. A familiar analogy is to short-duration nuisance telephone and fax calls.

Public Personae

Individuals can exercise a degree of control over their projected passive and active personae, but much less influence over those personae imposed by others upon them. Although there are likely to be considerable differences among the various personae associated with an individual, there are also commonalities. With some individuals, there is so much in common among the images that it is reasonable to abstract a shared or public persona from the many individual personae.

Examples abound of public personae developed through conventional media. The public images of Zsa Zsa Gabor, Elizabeth Taylor, Pierre Trudeau, Donald Trump, and Ross Perot are public property. The idea of any of them successfully suing in defamation a person who criticized their public image, on the grounds that this misrepresented their

real personality, seems ludicrous. Similar limitations confront personalities of the Internet, such as Cliff Stoll, Peter Neumann, Richard Stallman, and Phiber Optik.

A public persona may arise in and be restricted to a particular context. For example, a person's digital shadow may be well known within an electronic community such as that associated with a mailing list or bulletin board. Archetypal public personae include the inveterate sender of worn-out jokes and clichés, the practical joker, the sucker who always takes practical jokers' bait, the wild idea generator, the moral crusader, and the steadying influence who calls for calm and propriety when the going gets rough.

With the immediacy of the net, many people play these roles without the realization that they are predictable. But they can be adopted quite consciously and constructively, e.g., where a respected persona reinforces the need for appropriate behavior and, conversely, where a normally placid respondent replies vigorously, implying that his or her patience is stretched to the limit. In such contexts, there is once again no reason why an individual should be restricted to a single public persona.

Potential Applications

There is a range of uses to which individuals might put projected, passive digital personae. It may simply be to express their personality, or a facet of it, or an exaggeration of some feature of it, or a feature that the person would like to have. It may be a desire to free themselves of normal constraints in order to express different thoughts or the same thoughts differently. There is the well-known activity of "flaming" on the net, in which people express themselves to others with a vigor that would be socially and perhaps physically risky if done on a face-to-face basis. The freedom to project a digital persona can be used creatively, constructively, entertainingly, intemperately, in a defamatory manner, or criminally.

Projected, active digital personae are, on the other hand, a relatively recent development, and it is too early to be able to appreciate and analyze the scope of the potential applications. There is no reason, however, why an agent has to run on one's own workstation or be limited to input filtering. For example, so-called "program trading" agents can issue buy/sell orders if the price of nominated commodities fall/rise beyond a nominated (or computed) threshold; and updates to key records in remotely maintained statistical databases can be monitored. It is also possible to conceive of the "active" role being extended to, for example, conducting a nuisance campaign against an opponent, by bombarding his or her e-mail and/or fax letterbox or countering such a campaign that has been directed against oneself (e.g., by diverting the calls to another address).

Passive digital personae may be imposed by other individuals and organizations for a variety of reasons. Typical among these is the construction of a consumer profile in order to judge whether to promote the sale of goods, services, or ideas to each particular individual, and if so, then to indicate the suitability of each a palette of promotional media and devices should be used.

Similarly, imposed, active digital personae offer considerable prospects. People's interests or proclivities could be inferred from their recent actions, and appropriate goods or services offered to them by the supplier's computer program using program-selected promotional means. Another application might be a network "help desk" program to detect weak or inefficient database search strategies, and to offer advice as a service to network users. A network control mechanism could provide warnings to subscribers when they use foul language or exceed traffic or storage quotas. As with other forms of monitoring of the workplace and the public, questions of law, contract, image, and morality arise.

Aficionados of science fiction are aware of ample sources of inspiration for more futuristic uses of the concept. In John Brunner's *The Shockwave Rider* (1975), personae are used primarily by the State as an instrument of repression, but also secondarily by the few individuals capable of turning features of the net against the ruling clique, as a means of liberation. In "cyberpunk" literature, people adopt preprogrammed personae in a manner analogical to their usage of psychotropic drugs (see, in particular, Gibson's *Neuromancer* [1984], and the collection of short stories edited by Sterling [1986]). In Bear's *Eon* (1985), digital personae have become so comprehensive that they are routinely detached from individuals: Disembodied "partials" are created to perform specific tasks on their owners' behalf, and "ghosts" of biologically dead people are rejuvenated from the city databank.

As with all imaginative fiction, plugging into the net, partials, and ghosts should not be understood as predictions, but as investigations of extreme cases of contemporary ideas, as speculations of what might be, and as inspiration for more practicable, restricted applications. As virtual reality graduates from the laboratory, the digital persona idea will doubtless be embodied in some of its applications.

To provide a deeper appreciation of the power of the digital persona, the remaining sections of the paper investigate its application to one specific area: the monitoring of people.

Dataveillance

Data surveillance, usefully abbreviated to dataveillance, is the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons. In the past, the monitoring of people's behavior involved physical means, such as guards atop observation towers adjacent to prison yards. In recent times, various forms of enhancement of physical surveillance have become available, such as telescopes, cameras, telephoto lenses, audio recording, and directional microphones. In addition, electronic surveillance has emerged in its own right, in such forms as telephone bugging devices and the interception and analysis of telex traffic. Dataveillance differs from physical and electronic surveillance in that it involves monitoring not of individuals and their actions, but of data about them. Two classes need to be distinguished:

- Personal dataveillance, in which a previously identified person is monitored, generally for a specific reason
- Mass dataveillance, which is of groups of people, generally to identify individuals of interest to the surveillance organization

Dataveillance is much cheaper than conventional physical and electronic surveillance. The expense involved in physical and even electronic monitoring of the populace acted as a constraint on the extent of use. This important natural control has been undermined by the application of information technology to the monitoring of data about large populations. The development is perceived by philosophers and sociologists as very threatening to freedom and democracy.

The increasing information intensity of modern administrative practices has been well described by Rule and colleagues (Rule, 1974; Rule et al., 1980). Foucault (1975) used Bentham's concept of the "panopticon" to argue that a prison mentality is emerging in contemporary societies. Smith (1974 et seq.), Laudon (1986b), OTA (1986), and Flaherty (1989) deal with dataveillance generally. The role of information technology in dataveillance is discussed in detail in Clarke (1988). A political history of dataveillance measures in one country are in Clarke (1987, 1992a).