New Directions in Surveillance and Privacy

Edited by
Benjamin J. Goold and Daniel Neyland

ROUTLEDGE

New Directions in Surveillance and Privacy

New Directions in Surveillance and Privacy

Edited by

Benjamin J. Goold and Daniel Neyland

Routledge
Taylor & Francis Group
LONDON AND NEW YORK

First Published by Willan Publishing 2009

This edition published by Taylor & Francis 2011

2 Park Square
Milton Park
Abingdon
OX14 4RN

Published simultaneously in the USA and Canada by

711 Third Avenue
New York
NY 10017

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

ISBN 978-1-84392-363-3 hardback

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library.

Project managed by Deer Park Productions, Tavistock, Devon
Typeset by GCS, Leighton Buzzard, Bedfordshire

Contents

Acknowledgements

Many thanks to the Oxford Institute for Science, Innovation and Society for their funding of the seminar series on which this book was based. The Institute was established in 2004 at the University of Oxford through the generosity of the James Martin Trust, and seeks to investigate how science and technology will shape society in the next century, and inform the education of business leaders and policy and decision makers worldwide. http://www.sbs.ox.ac.uk/research. We are also grateful to the University of Oxford Centre for Criminology for its support during the course of the seminar series.

Benjamin J. Goold and Daniel Neyland
2009

List of abbreviations

AC	Assistant Commissioner
ACLU	American Civil Liberties Union
APIG	All Party Parliamentary Internet Group
ATCSA	Anti-Terrorism, Crime and Security Act
CCTV	closed circuit television
CNIL	Commission Nationale de l'Informatique et des Libertés
CO19	Central Operations Specialist Firearms Unit (of the Metropolitan Police)
CRIS-E	Client-Registry Information System – Enhanced
DNA	Deoxyribonucleic acid
DRI	Digital Rights Ireland
DRM	Digital Rights Movement
DSL	digital subscriber line
ECHR	European Court of Human Rights
EDRI	European Digital Rights
EEA	European Economic Area
EHRR	European Human Rights Report
EWCA	England and Wales Court of Appeal
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FLOSS	Free/Libre/Open Source Software
FSA	Financial Service Authority
GCHQ	Government Communications Headquarters
GPS	Global Positioning System
HMSO	Her Majesty's Stationery Office

HMRC	Her Majesty's Revenue and Customs
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPCC	Independent Police Complaints Commission
IPS	Identity and Passport Service
ISSA	Information Systems Security Association
ITAA	Information Technology Association of America
LSE	London School of Economics
MEP	Member of the European Parliament
MPA	Metropolitan Police Authority
NAO	National Audit Office
NIR	National Identity Register
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
OGC	Office of Government Commerce
PACE	Police and Criminal Evidence Act
PDA	personal digital assistant
PETs	privacy enhancing technologies
PGP	pretty good privacy
PIN	personal identification number
PNR	passenger name record
P3P	platform for privacy preferences
QC	Queen's Counsel
RAE	Royal Academy of Engineering
RIPA	Regulation of Investigatory Powers
SAS	Special Air Service
SOCA	Serious Organised Crime Agency
SO12	Specialist Operations Department of the Metropolitan Police
TNIR	Temporary National Identity Register
TOR	The Onion Router (anonymity network)
UKIPS	UK Identity and Passport Service
VoIP	Voice over Internet Protocol

Notes on contributors

Ian Brown is a research fellow at the Oxford Internet Institute and an honorary senior lecturer at University College London. His research is focused on public policy issues around information and the Internet, particularly privacy, copyright and e-democracy. He also works in the more technical fields of information security, networked systems and healthcare informatics. His recent research grants include £2m from the Engineering and Physical Sciences Research Council to investigate individuals' conceptions of privacy and consent across a range of contexts and timeframes. During 2009 he is undertaking a study for the European Commission on updating the European data protection framework.

Benjamin J. Goold is a university lecturer in law and a fellow and tutor at Somerville College, and a member of the University of Oxford Centre for Criminology. His major research interests are in the use of surveillance technology by the police and the relationship between individual privacy rights and the criminal law. In recent years, he has served as a specialist legal advisor to the House of Lords Inquiry into Surveillance and Data Collection, and as an independent advisor to the UK Identity and Passport Service. He also writes on aspects of the Japanese criminal justice system and is a member of the Oxford University Faculty of Oriental Studies and an associate member of the Nissan Institute of Japanese Studies.

Kevin D. Haggerty is editor of the *Canadian Journal of Sociology* and book review editor of *Surveillance and Society*. He is Associate

Professor of Sociology and Criminology at the University of Alberta and a member of the executive team for the New Transparency Major Collaborative Research Initiative. He has authored, co-authored or co-edited *Policing the Risk Society* (Oxford University Press, 1997), *Making Crime Count* (University of Toronto Press, 2001) and *The New Politics of Surveillance and Visibility* (University of Toronto Press, 2006).

Marie-Helen Maras is a recent graduate from the University of Oxford. At the University of Oxford, she completed her DPhil in Law in October 2008, MPhil in Criminology and Criminal Justice in November 2007, and MSc in Criminology and Criminal Justice in July 2006. She also has a Bachelor of Science in Psychology, a Bachelor of Science in Computer and Information Science, and a Masters in Industrial and Organisational Psychology. Marie has taught seminars at the University of Oxford on 'Security and the War on Terror' and the 'Burdens of Seeking Security' on the MSc in Criminology and Criminal Justice. In addition to her teaching and academic work, Marie served in the US Navy from 1997 to 2004. She gained extensive law enforcement and security experience from her posts in the military as a Navy Law Enforcement Specialist and Command Investigator. Her main research interests include terrorism, counter-terrorism, security and surveillance.

Mike Nellis is Professor of Criminal and Community Justice in the Glasgow School of Social Work, University of Strathclyde. He is a former social worker with young offenders, trained at the London School of Economics in 1977/8 and between 1990 and 2003 was himself closely involved in the training of probation officers at the University of Birmingham. He was awarded his PhD from the Institute of Criminology, University of Cambridge in 1991. He has written extensively on the changing nature of the probation service, the promotion of community penalties and the cultural politics of penal reform (including the educational use of prison movies and offenders' autobiographies). A longstanding interest in the electronic monitoring of offenders has taken him more deeply into the surveillance studies field.

Daniel Neyland works on a broad portfolio of projects focused on issues of governance and accountability (including surveillance technologies, the global textile trade, electronic waste, vaccines for neglected diseases, airports and security, traffic management, and household recycling). He has published widely including a 2006 book

entitled *Privacy, Surveillance and Public Trust* (Palgrave Macmillan, 2006) and a methodology text: *Organizational Ethnography* (Sage, 2007). He has a forthcoming book on *Mundane Governance*.

James B. Rule is Distinguished Affiliated Scholar at the Center for the Study of Law and Society, University of California, Berkeley. His first book on privacy and personal information was *Private Lives and Public Surveillance* (Allen Lane, 1973); his most recent is *Privacy in Peril* (Oxford University Press, 1997). In addition to these subjects, his writings include books and articles on the role of social science in the improvement of social conditions; the causes of civil violence; cumulation and progress in social and political thought; and computerisation in organisations. He also writes for *Dissent* magazine, on whose editorial board he serves. He lives in Berkeley, California and Aniane, France.

Edgar A. Whitley is Reader in Information Systems in the Information Systems and Innovation Group of the Department of Management at the London School of Economics and Political Science. He is the research co-ordinator of the LSE Identity Project and represented the project at the Science and Technology Select Committee review of the scheme. He has written extensively about the Identity Cards Programme for both academic and trade audiences and is a frequent media commentator on the scheme. He is also the co-editor for the journal *Information Technology & People* and an associate editor for the journal *MIS Quarterly*. His research draws on his interests in social theory and its application to information systems, and recent publications include work on FLOSS (Free/Libre/Open Source Software), international students and academic writing, and the technological and political aspects of the UK Identity Cards Scheme.

Introduction

Where next for surveillance studies? Exploring new directions in privacy and surveillance[1]

Daniel Neyland and Benjamin J. Goold

Surveillance is now so prevalent in modern society that it touches almost every aspect of our daily lives. Our homes, our workplaces and even the public spaces in which we socialise, play and shop, are now brimming with a multitude of sophisticated data collection systems and complex surveillance technologies. Although many people may not be fully aware of the extent to which they are being monitored, most now regard surveillance as an inescapable – if not necessarily desirable – part of life in the early twenty-first century. While we can argue about whether we are already living in a 'surveillance society', it is abundantly clear that the spread of surveillance has dramatically altered the way in which our societies function and are experienced by ordinary people.

To date, academics and others interested in the nature and effects of surveillance have sought to understand this phenomenon through a variety of disciplinary lenses. Drawn together under the banner of surveillance studies, writers in sociology, philosophy, criminology, political studies, geography and urban studies have all offered their own unique insights into surveillance, and have together produced a diverse and impressive body of work on the subject. Indeed, to describe surveillance studies as multi-disciplinary is to do it something of a disservice: it is at its heart pragmatic and eclectic, and has shown an admirable willingness to embrace new and often divergent perspectives in its efforts to understand the complexities of surveillance.

It is in keeping with this spirit that the following volume – and the seminar series on which it was based – was conceived. Conscious

of the fact that as disciplines mature, there is always the danger of them being constrained by the emergence of an accepted orthodoxy or canon of key ideas, this book aims both to celebrate the diversity of the field and to provide a home for new and emerging ideas about surveillance and privacy. As even the most casual glance at the table of contents will reveal, this is not a book that embraces any single theme, or one which takes a narrow view of the nature or significance of surveillance. Instead, it seeks to provoke by presenting readers with a range of radically divergent yet sympathetic perspectives, ranging from the philosophical and legal to the literary and futurist. Here, the hope is that readers will find their assumptions about the field tested and their curiosity provoked. Furthermore, because the chapters in this collection all seek to anticipate how surveillance and our responses to it might develop, hopefully they will provide a rich source of ideas for future research and writing in the field of surveillance studies, and help to ensure that it retains its intellectual diversity and dynamism.

New directions

In order to provide a space for pushing current writing in new directions, this collection is organised around three main themes. The first of these investigates the possibility of regulating surveillance activities and offering privacy protection. This involves questioning the strength of current protections (Rule), the possibilities of developing regulation more suitable for rapidly expanding technological systems (Brown and Goold) and the justification and necessity of giving up civil liberties in return for apparent protection (Maras). The second theme of this collection focuses on technologies and techniques of surveillance. It investigates the possibilities of rendering surveillance accountable (Neyland) and newly emerging public configurations of opposition to surveillance (Whitley). Finally, the third theme of the collection is focused on the future of privacy and surveillance. Here we find an analysis of future-oriented surveillance fiction (Nellis) and a search for possible future directions in surveillance activities (Haggerty). The following sections will provide a brief analysis of why we as editors think these themes are provocative, challenging and relevant for surveillance and privacy scholars.

Regulation of surveillance and privacy protection

One trend in recent privacy and surveillance writing has been to focus on regulation. Questions have been raised regarding the possibility, likelihood, range, time frame and logistics of protecting privacy from surveillance. But regulation has not been narrowly conceived, with discussions ranging across, amongst many other things, codes of conduct, laws, policies and privacy enhancing technologies. Much of this discussion takes place simultaneously with suggestions that privacy has died (see for example, Garfinkel 2000), is dying (see for example, Sykes 1999; Whitaker 2000; Rosen 2001) and/or that we already live in a transparent society (Brin 1998).

Claims regarding the death, end or destruction of privacy are frequently founded on one of the following arguments. First, it is claimed that an interconnected global flow of data, people and technology has emerged in recent years that has shifted 'us' into an era of so many privacy concerns that the term itself has become defunct. There are just too many variations on what a privacy concern could be for the term privacy to be able to cope (Sykes 1999). Second, it is suggested that the same flows have led to a situation where there are no longer any spaces, actions or forms of information which can be considered immune from collection, storage, analysis and further mobilisation. In this sense privacy as a concept is dead (or dying) as traditional material boundaries prove to be an insufficient impediment to activities of data scrutiny and management (Brin 1998). Detailed consideration of these claims suggests a variety of problems.

First, the proposal that society is now characterised by an interconnected mass of people, technology and flows of information, what Castells (1996) refers to as the network society, offers a socio-technical gloss to a range of complex and ongoing relations. These relations involve the plaiting and bounding of social and technical entities for the production, mobilisation and direction of forms of information. For example, in a CCTV system we can find staff, monitors, radios, police officers, pens, paper, regulations, codes of practice and fibre optic connections drawn together. Much effort goes into both building and maintaining these relations between people and things. However, it is not straightforwardly the case that such interconnection is all-encompassing. There are breakdowns in relations between people and technologies, and there is a great deal of work done to constitute boundaries that prevent potential relationships between people and technologies from emerging. For example, local

populations could be invited to engage with CCTV cameras through opening up systems of surveillance. In practice, local populations do not receive such an invitation. Furthermore, these relations do not stand still. New technologies are frequently introduced, along with new ways of working, new subjects of focus, and new ways to use old data.

Hence, we need to pay close attention to the kinds of relations in play between people and surveillance systems, and to what those relations open up and what they close down. Rapidly adopting metaphors of the network society, as if everyone and everything is now related and that all relations are equal and operate smoothly, risks a socio-technical gloss which opens up the space for making grand claims such as privacy is dead. Indeed rather than heralding a death of privacy, these relations, their openings and closures, inspire many new ideas, discussions and demands of privacy.

A second problematic feature of the death of privacy arguments relates to the 'we' or 'us' which, it is claimed, is now experiencing a global flow of information, ending boundaries to data collection, storage and analysis. Who is the 'we' that might be experiencing such a phenomenon? As in Bennett and Raab (2003), both Haggerty and Maras argue in their respective chapters that our social experiences of privacy are not evenly distributed. Those in need of state welfare are involved in the submission, collection and use of information that otherwise would not be required. Those with credit cards and those who have access to the internet and telephones, as well as those who pay bills, shop in areas covered by CCTV, and are required to carry ID cards, may each engage in a range of observable activities, the traces of which are collected, stored, analysed and further mobilised. However, these are by no means global experiences and are by no means universally experienced even by those who do participate. The claim that everyone participates in such activities and that these participants share the same experiences is simplistic. Research on technology (see for example Bijker, Hughes and Pinch 1989; Bijker and Law 1992; Grint and Woolgar 1997 amongst others) provides multiple examples of the variety of experiences which engagement with the 'same' technology can bring. In light of this, careful consideration is required of what is meant by privacy in relation to specific technological systems, when and for whom.

A third feature of death of privacy arguments involves the claim that the rise in number and scope of systems designed to collect, store, categorise and analyse information on the population has led to an explosion of privacy concerns so diverse that the term privacy is

no longer appropriate or meaningful. This implies that at a previous time there was a universal, agreed-upon definition of privacy that has now somehow become obsolete. This does not appear to be the case. Privacy has consistently formed a focus for questions. What might be an appropriate form of privacy? What types of information should be held on the population? Which freedoms should the population be expected to concede in order to meet the demands of the state? These questions constituted the basis for the (successful) 1952 challenge to abandon the use of wartime identity cards in the UK, and have been reiterated on every occasion since when successive governments have proposed some new identity card system.

In this sense privacy has always been a focus for multiple concerns and, although there are more technologies available to gather information, it is not clear that the types of privacy concern have significantly altered or become obsolete. Indeed, Rule in this collection makes the case that a liberal democratic consensus on privacy protection principles is broadly recognisable. Although experiences of privacy invasion may be highly variable across different contexts, we can still find much discussion of the appropriate means to protect privacy against surveillance. According to Whitley (this volume) we may only now be witnessing the emergence of a popular, public uptake of privacy issues. Hence in place of the dissolution of privacy, we find instead a mounting discussion of privacy and the development of new modes of privacy legislation. For Rule, this has led to the development of a consensus of privacy protection principles (although this consensus is not without problems, notably that the diverse experiences of privacy may not match a narrowly constituted consensus, see below). This may now mean that privacy – at least in policy terms – has greater coherence and resonance than ever before. For example, although the Human Rights Act (1998) is subject to multiple interpretations, it does for the first time establish a right to privacy in the United Kingdom.

This suggests current writing on privacy and surveillance displays a combination of both scepticism (that privacy might already be dead or at least on its way out) and hope (that there might be a form of regulation which could be more effective in protecting privacy from surveillance). How then, can we tackle this simultaneous scepticism and desire for change? Rule takes us through a natural history of privacy as a topic of controversy. In line with some of the sceptics, Rule suggests that privacy is an intractable problem. The lack of any natural limit to innovation in the technologies of information collection, mobilisation and techniques of utilisation, suggests

the problem of privacy is not about to be solved in any single, straightforward manner. At the same time, privacy does not die. Instead, it is continuously subject to change in line with technological developments, new and imaginative ways to exploit existing data, and in response to changes in legislation.

If the problem of privacy is intractable and ever changing, what are the prospects for protection? The authors in this volume posit a range of possible responses. For Brown, the massive expansion of communication technology provides a compelling need for privacy protection to keep up. Brown suggests that policies have slipped behind the social, political and technological landscape. Writing in a similar vein, in his chapter Goold questions the effectiveness of regulatory regimes that rely solely on legal rules and sanctions, and argues instead for an approach that embeds organisational restraint and a respect for privacy via privacy enhancing technologies (PETs). Finally, for Maras, concerns over privacy protection in relation to data retention suggest a profound change in social order. We are now called upon to sacrifice civil liberties and need to ask what we might receive in return, whether or not our sacrifices are necessary and on what grounds our sacrifices might be justified. Privacy protection appears some distance from cognisance of these issues. For Rule the lack of any natural limit to privacy invasion requires a normative stance. Questions to ask include what kinds of information should different organisations collect, and what ought organisations be allowed to do with information?

This suggests both that privacy has not died, and that protection against surveillance has not become any less poignant a matter of social and political interest. However, as Goold reminds us, identifying the most appropriate means of privacy protection is neither straightforward nor universal. Furthermore, Rule's critique of liberal democratic privacy protection principles is an apt demonstration of the limitations of universality. A single set of privacy protection principles suitable for all occasions is unlikely to prove adequate. Lee (1999) refers to this as the tension between the general and the particular. The general refers to those sets of principles, codes and laws which might be deemed relevant to any incident. The particular refers to the work done to translate the general into something relevant for each specific incident where the general is invoked. For Lee (1999), this translation can lead to a tension whereby disputes follow on from any particular translation of a general principle. In relation to privacy, how might general privacy protection principles be enacted in particular situations, who would decide on whether

or not a particular translation of a general principle is suitable and what might the consequences be of movement between the general and the particular?

These are all questions considered by authors in the first section of the collection. Rule suggests that the current liberal democratic consensus on privacy protection principles (what we might term the general) run into a multitude of problems across specific incidents (the particular) when they are applied. For Brown the general lags behind the particular. For Goold, (general) privacy protections must be designed into (particular) surveillance systems, as well as mandated by law. For Maras the general have unexplored and problematic social consequences when translated into particular instances of policy implementation. A challenge set down by these authors is how we might sidestep or get beyond some of these tensions.

Technologies and techniques of surveillance

A second trend in privacy and surveillance writing in recent years has been a detailed analysis of the technologies and techniques of surveillance. Arguments have been put forward regarding the need to get close to what goes on in surveillance systems, to generate further insights into public understanding of surveillance, and to explore the extent to which such detailed explorations can aid in the development of normative understandings of privacy and surveillance. Getting closer to the activities of surveillance has involved up-close, often ethnographic, studies of, for example, CCTV control rooms (see for example, Norris and Armstrong 1999; and Goold 2004). This has provided a rich and nuanced picture of what surveillance in practice looks like and has initiated debates regarding the extent, likelihood, threats to and prospects for privacy protection.

Within this focus on the techniques and technologies of surveillance, developing a public understanding of surveillance has been hitherto a somewhat neglected concern both practically and theoretically. Firstly, in the UK there has been a lack of clear public participation in debates regarding privacy and surveillance (with the exception of the proposed ID card scheme). Where consultation does happen, for example in the introduction of new CCTV systems, it seems to be on a small scale and without clear consequences. Secondly, this absence of participation and consultation seems to have evinced very little interest in the privacy and surveillance studies community. These notable absences tie in with research in the field of public

understanding of science and technology which has frequently involved a focus on what have been termed deficit models (see for example Irwin 1995). The first deficit model suggested that policy-makers treated knowledge held by members of the public as inferior to that held by apparent experts.[2] The focus for these models has shifted more recently to a deficit in participation or trust (that there are too few opportunities for public participation in scientific and technological debates and an absence of trust in science, Gregory 2001), and to a deficit in legitimacy of public engagement (that science is afforded a licence to operate beyond, despite or regardless of public participation, Gregory 2001).

Each of these deficit models could be said to apply to public participation in surveillance and privacy debates. For example, it is not clear that public consultation on potentially privacy-infringing technologies treats public knowledge as having potentially equal status with expert knowledge. This suggests a frequent policy buy-in to deficit in public knowledge models. It is also not clear that public participation in the introduction of new technology such as CCTV systems in the UK operates to the same extent as the introduction of other technologies, such as new ID cards. This signals a deficit in opportunities for participation in relation to some technologies. It might also be said that such participatory activities lack legitimacy, with consultations, for example, carried out in order to adhere to government guidelines, rather than with a view to incorporating a strong public voice into developments.

Beyond these deficit models, it has also been argued (Neyland 2006) that public participation in privacy and surveillance debates could be characterised by a deficit of concern. It is often the case that local residents living near CCTV systems in the UK assume that the system is operating for their benefit (or at least is not operating to their detriment), and that there is some notable authority overseeing CCTV on their behalf (Neyland 2006). However, this deficit of concern may be slowly changing. In his chapter on ID cards in this collection, Whitley suggests that attempts to introduce ID cards in the UK have shifted the tenor of the public debate around privacy and the limits of surveillance. According to Whitley, media stories of ID cards and their associated challenges have coincided with an increase in other stories of privacy and surveillance, including breaches, challenges and their social consequence. This increase in media attention might be a signal that the deficit of concern is diminishing. It could also signal a move toward greater public engagement in normative debates over the appropriate extent of surveillance and the value of privacy.

Normative questions are also helpful insofar as they challenge our belief in the straightforward utility of detailed, empirical studies of surveillance technologies and techniques, and can instead inform our understanding of what surveillance and privacy protection ought to look like. The tension generated by such normative questioning has been noted over many years of philosophical and social scientific work, and is traceable (at least) as far back as the work of Hume (1740). Hume famously argued that there is no logical connection between questions regarding the nature of what something is and questions regarding the nature of what something ought to be. This division between 'is' and 'ought' later became known amongst philosophers as Hume's guillotine (Black 1964). For philosophers, the cut of the guillotine is a matter of logic. For social scientists, however, the cut presents more of a practical challenge: namely, how to develop policies and practical solutions to problems from our empirical observations of the social world? (Woolgar and Neyland forthcoming).

In surveillance studies, the work required to get from observation to prescription requires us to translate up-close studies of the features of surveillance in practice into recommendations for possible remedial action. Here Neyland looks at two aspects of this challenge in relation to the accountability of surveillance systems. Neyland argues that legal processes aimed at ensuring surveillance actors and systems are held to account are inevitably complex and messy. This suggests that establishing what happened in a particular instance of surveillance – the 'is' in Hume's dichotomy – is far more challenging than it may first appear. Furthermore, beyond determining what has happened and who has done what to whom in a particular surveillance episode (in this case, the mistaken police shooting of Jean Charles de Menezes in London as a suspected terrorist), there are numerous questions concerning who should be held to account for those actions, and with what outcomes. This latter question of 'ought' is made more complex by continuing disputes regarding what has happened, whether or not the form of accountability is appropriate, and multiple interpretations of the outcome of the accountability process.

Whitley and Neyland's chapters offer insight into the challenge of getting close to the technologies and techniques of surveillance, and of using that closeness to engage with normative debates. Whitley's chapter could, for example, be read as an illustration of the advantages of greater public participation in surveillance debates, while Neyland's chapter demonstrates some of the limitations (and need to get beyond) current accountability dependencies. However, as

Latour (2004) has cautioned, moving from matters of fact to matters of concern is not straightforward. Normative engagements do not get any easier when we turn our attention to the future.

Futures of privacy protection

A third focus for surveillance studies introduced by the chapters of this book is that of the future. We can find a broad range of future-oriented writing across the social sciences from futurology to scenario planning. The purposes of this future orientation may vary from concerns with planning and strategising, through mapping, to concerns with the present and a desire to invoke questions such as how can we know more about what to do now, given what we think might happen next? This appears to be an under-explored area in surveillance studies. However, its potential utility is clear. Engaging with possible futures of privacy and surveillance enables a continuation of normative challenges (how should we engage with the future of surveillance, what would we want the future of privacy to look like?) and epistemological challenges (how could we know what the future holds?). Beyond normativity and epistemology, we are also faced with a methodological challenge: how might we research people, events, places, policies and technologies which are not happening yet (and may never come to fruition)?

Nellis strides out on a new and distinct methodological path by engaging with future-oriented writing about surveillance. What worlds are imagined and have been imagined by writers of fiction? Nellis takes us on a tour of the different genres and conventions for surveillance-based fiction, and surveys the fictional portrayals of future surveillance societies. Through Nellis' work, we are provided with a rich normative backdrop beyond our conventional contemplations, through which we are confronted with various new and provocative questions. This offers an alternative take on Leavis' work which suggests the importance of the arts and literature as having a critical function in opposing dominant views of our time. Leavis (1962: 28) argues that society needs a 'creative response to the challenges of our time' and that literature is essential in 'maintaining the critical function' (1962: 29). Hence we have the opportunity to ask whether writing about futures of surveillance can be seen as one of the sets of resources through which readers of texts orient their contemplation of surveillance activities? Through fiction can we see the ways in which surveillance concepts are becoming part of the world?

Haggerty also explores possible futures in a different but equally distinctive manner. In place of a focus on writing about the future, Haggerty instead focuses on current practices and tries to extrapolate from them and imagine what the future of surveillance might look like. Some of the futures suggested by Haggerty appear alluringly straightforward. For example, Haggerty suggests the current expansion of surveillance activities, technologies, information storage capabilities and capacities, is likely to continue and lead to more surveillance in the future. However, we should caution against any counter expectation that knowing the future of surveillance is simply a matter of extrapolation from today's newspapers. That there might be more surveillance tells us nothing of the modes, effects or consequences of expansion. For Haggerty, examining and predicting possible modes of future surveillance also involves an exploration of cognitive issues, conditional choices and stigmatisation. Each of these has a contemporary counterpart. It is through tracing out the bases for these contemporary actions that we might find traces of likely future consequences. Coming to terms with the epistemologies of surveillance (the nature of knowledge production and usage through surveillance) might give us a basis for navigating through the (at least in theory) limitless bounds of possible future actions.

In this sense, the future cannot be determined in a straightforward manner, but neither should it be left beyond our consideration. The future instead becomes a malleable boundary object (Star and Griesemer 1989), an object that is a locus for multiple representative practices that move through a more focussed passage point. As Star and Griesemer (1989: 387) argue: 'Scientific work is heterogeneous, requiring many different actors and viewpoints. It also requires co-operation … Boundary objects are both adaptable to different viewpoints and robust enough to maintain identity across them'. Hence the futures of privacy and surveillance can be seen as boundary objects, or as organising focal points around and through which a range of entities are gathered, occasionally producing incompatible renderings of our likely future and occasionally producing interpretations wildly off target. That our capacity to predict may be limited should not, however, limit our attempts to engage with the possible futures that may lie ahead of us.

Conclusion

The field of surveillance studies continues to expand at a rapid pace,

and with it so too does academic interest in questions of privacy and the limits of surveillance. This collection aims to provide a home for innovative new thinking and perspectives on surveillance, and to introduce new themes into existing discussions and debates. It also hopes to act as a guard against the emergence of any premature or comfortable consensus within the surveillance studies community. As the community continues to expand it becomes increasingly important to defend the eclecticism and intellectual curiosity that has helped to make surveillance studies so interesting, important and relevant. Put simply, we believe that one of the great strengths of the discipline is the fact that it operates as a broad church, and in providing a forum for new and challenging writing in the field, we hope this collection will help to keep the doors of that church as wide open as possible.

Notes

1 Many thanks to Inga Kroener for her helpful and insightful comments on an earlier version of this chapter.
2 This kind of model has been challenged by assertions that lay knowledge could be seen as a useful input to debates even if predicated upon a distinct epistemology (Wynne 1996).

References

Bennett, C. and Raab, C. (2003) *The Governance of Privacy – Policy Instruments in Global Perspective.* Hampshire: Ashgate.

Bijker, W. and Law, J. (eds) (1992) *Shaping Technology/Building Society: Studies in Sociotechnical Change*. London: MIT Press.

Bijker, W., Hughes, T. and Pinch, T. (1989) *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology.* London: MIT Press.

Black, M. (1964) 'The gap between "is" and "should"', *The Philosophical Review*, 73(2): 165–181.

Brin, D. (1998) *The Transparent Society: Will Technology Force Us To Choose Between Privacy and Freedom?* New York: Addison-Wesley.

Castells, M. (1996) *The Rise of the Network Society*. Oxford: Blackwell.

Garfinkel, S. (2000) *Database Nation: The Death of Privacy*. Sebastopol, CA: O'Reilly.

Goold, B.J. (2004) *CCTV and Policing: Public Area Surveillance and Police Practices in Britain*. Oxford: OUP.