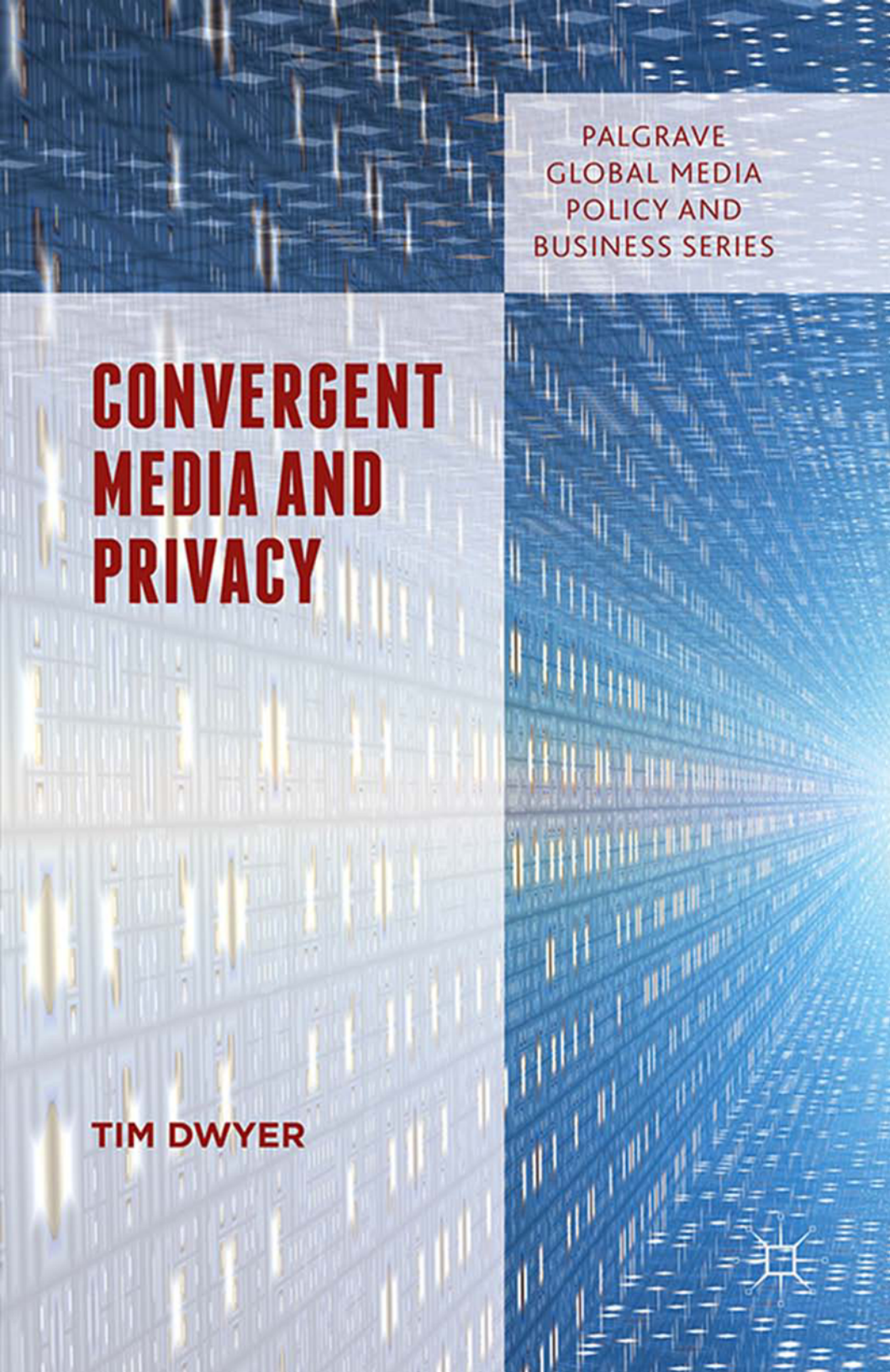

PALGRAVE
GLOBAL MEDIA
POLICY AND
BUSINESS SERIES
CONVERGENT
MEDIA AND
PRIVACY
TIM DWYER

Palgrave Global Media Policy and Business

Series Editors: **Professor Petros Iosifidis, Professor Jeanette Steemers** and **Professor Gerald Sussman**

Editorial Board: **Sandra Braman, Peter Dahlgren, Terry Flew, Charles Fombad, Manuel Alejandro Guerrero, Alison Harcourt, Robin Mansell, Richard Maxwell, Toby Miller, Zizi Papacharissi, Stylianos Papathanassopoulos, Caroline Pauwels, Robert Picard, Kiran Prasad, Marc Raboy, Chang Yong Son, Miklos Suksod, Kenton T. Wilkinson, Sugmin Youn**

This innovative series examines the wider social, political, economic and technological changes arising from the globalization of the media and communications industries and assesses their impact on matters of business practice, regulation and policy. Considering media convergence, industry concentration, and new communications practices, the series makes reference to the paradigmatic shift from a system based on national decision-making and the traditions of public service in broadcast and telecommunications delivery to one that is demarcated by commercialization, privatization and monopolization. Bearing in mind this shift, and based on a multi-disciplinary approach, the series tackles three key questions: To what extent do new media developments require changes in regulatory philosophy and objectives? To what extent do new technologies and changing media consumption require changes in business practices and models? And to what extent does privatization alter the creative freedom and public accountability of media enterprises?

Steven Barnett & Judith Townend (*editors*)
MEDIA POWER AND PLURALITY
From Hyperlocal to High-Level Policy

Abu Bhuiyan
INTERNET GOVERNANCE AND THE GLOBAL SOUTH
Demand for a New Framework

Benedetta Brevini
PUBLIC SERVICE BROADCASTING ONLINE
A Comparative European Policy Study of PSB 2.0

Karen Donders, Caroline Pauwels and Jan Loisen (*editors*)
PRIVATE TELEVISION IN WESTERN EUROPE
Content, Markets, Policies

Tim Dwyer
CONVERGENT MEDIA AND PRIVACY

Tom Evens, Petros Iosifidis and Paul Smith
THE POLITICAL ECONOMY OF TELEVISION SPORTS RIGHTS

Manuel Guerrero and Mireya Márquez-Ramírez (*editors*)
MEDIA SYSTEMS AND COMMUNICATION POLICIES IN LATIN AMERICA

Petros Iosifidis
GLOBAL MEDIA AND COMMUNICATION POLICY
An International Perspective

John Lent and Michelle Amazeen
KEY THINKERS IN CRITICAL COMMUNICATION SCHOLARSHIP
From the Pioneers to the Next Generation

Michael Starks
THE DIGITAL TELEVISION REVOLUTION
Origins to Outcomes

Peggy Valcke, Miklos Sükösd, Robert Picard
MEDIA PLURALISM AND DIVERSITY
Concepts, Risks and Global Trends

Palgrave Global Media Policy and Business
Series Standing Order ISBN 978–1–137–27329–1 (hardback) 978–1–137–36718–1 (paperback)
(*outside North America only*)

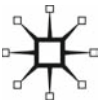
You can receive future titles in this series as they are published by placing a standing order. Please contact your bookseller or, in case of difficulty, write to us at the address below with your name and address, the title of the series and one of the ISBNs quoted above.

Customer Services Department, Macmillan Distribution Ltd, Houndmills, Basingstoke, Hampshire RG21 6XS, England

Convergent Media and Privacy

Tim Dwyer
University of Sydney, Australia

palgrave
macmillan



Softcover reprint of the hardcover 1st edition 2015 978-1-137-30686-9

First published 2015 by
PALGRAVE MACMILLAN

Palgrave Macmillan in the UK is an imprint of Macmillan Publishers Limited, registered in England, company number 785998, of Houndmills, Basingstoke, Hampshire RG21 6XS.

Palgrave Macmillan in the US is a division of St Martin's Press LLC, 175 Fifth Avenue, New York, NY 10010.

Palgrave Macmillan is the global academic imprint of the above companies and has companies and representatives throughout the world.

ISBN 978-1-349-55719-6 ISBN 978-1-137-30687-6 (eBook)
DOI 10.1007/978-1-137-30687-6

This book is printed on paper suitable for recycling and made from fully managed and sustained forest sources. Logging, pulping and manufacturing processes are expected to conform to the environmental regulations of the country of origin.

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

Library of Congress Cataloging-in-Publication Data

Dwyer, Tim.
Convergent media and privacy / Tim Dwyer, University of Sydney, Australia.
pages cm. — (Palgrave global media policy and business)
1. Mass media policy. 2. Mass media – Social aspects. 3. Mass media – Law and legislation. 4. Mass media – Moral and ethical aspects. I. Title.

P95.8D89 2014
302.23—dc23 2015021868

Contents

List of Illustrations

Acknowledgements

My first thanks go to Felicity Plester for her support of the book from the outset in suggesting a title in this area of new media and privacy, and for the invitation to be involved in the series from the editors of the Global Media Policy and Business Series at Palgrave Macmillan. I am grateful to colleagues in the Department of Media and Communications at the University of Sydney, for various kinds of assistance enabling me to undertake this writing project. In particular, I am indebted to research colleagues who were working with me on other projects and who helped in a variety of ways: Fiona Martin, Gerard Goggin, Jonathon Hutchinson, Damien Spry, Virginia Nightingale, Monika Bednarek, Aidan Wilson, and from the IT School, James Curran and Joel Nothman. Various international researchers generously assisted me in developing my ideas for the book while I was attending conferences, and especially while I was visiting Denmark in 2014. My thanks to Danish colleagues Anja Bechmann at the Digital Footprints Centre at the University of Aarhus, and Niels Ole Finneman at the Royal School of Library and Information Science at the University of Copenhagen for their conversations. The Faculty of Arts and Social Sciences at the University of Sydney made it all possible through supporting my research and approving the study leave to write the book.

Frontispiece: Cartoon on Metadata by Reg Lynch used with permission. First published in the Sun-Herald, Fairfax Media.

1
Introduction

> Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual ... the right 'to be let alone' ... Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops'.[1]

A key focus of this book is to examine the way that our ideas about privacy change constantly in response to their technological, and therefore their socio-cultural contexts. In this sense, the valorisation of 'privacy' is an historical construct shaped through the evolution of particular media and other technologies, usage forms, media practices and discourses. We are all familiar with the extraordinary way that media technologies (and scientific developments more generally) become so quickly naturalised in society. As with traditional media, the new media industries are themselves embedded in political economic contexts, and these tend to mandate their platform arrangements, underlying business patterns and unfolding trends.

The broader canvas of this exploration of the dynamic relations between the media and privacy is a narrative about modernity itself. My argument is that histories of the media inevitably are linked with social and cultural change, and the way in which media have both shaped and are shaped by people's everyday lives.

From the public's perspective, the cascading events, print media disclosures and televisual circus that followed from *The Guardian's* original revelation in July 2011 that News Corporation's *News of the World* had hacked the mobile phone of murdered teen Milly Dowler became synonymous with 'the media and privacy'. From this point on there was no turning back for the media or journalism. The Leveson Inquiry into the culture, practices and ethics of the press would then systematically excavate, on an unprecedented scale, the evidence that revealed the grossly unethical dimensions of this species of newspaper journalism's modus operandi.[2] Yet the intrusion into people's private lives afforded by mobile phone technologies was, at the same time, simply the latest episode in the longer history of print mediated 'news' journalism that began on an industrial scale in the 18th century.

Layered over the top of these events, convergent media are dynamically interacting with this complex environment, and the mobile Internet is to the fore of this ongoing change. There are seemingly endless varieties of software applications for business and pleasure. Indeed, mediatisation itself varies along with the purpose of the application, their networks and definitions of 'sociality'. These differences include whether media applications include locative affordances; the categories of data new media platforms generate; and, increasingly, the way in which mobile and wearable media, including embedded sensors in the 'Internet of Things', are figured in new media practices.

Critical understanding of contemporary networked privacy needs rethinking as we shift to leading more of our lives in emerging mediatised mobile and online spaces. *Convergent Media and Privacy* therefore seeks to contextualise privacy historically, socially, culturally and technologically. The book seeks to tease out the nuance of these meanings of privacy contexts of evolving new media industries, technologies, forms, applications and practices. The approach is a multidisciplinary one, being located at the intersection of media and cultural studies, political economy, legal studies, information industries, communication and network studies.

Populations and individuals are being tracked, monitored and surveilled by corporations and governments in ways that were unimaginable only a few decades earlier. The privacy implications of the ubiquitous Internet are quite literally changing how we live.

Algorithmically mediatised living

In this second decade of the 21st century, the sweeping power of national governments to legislate, and to take unilateral privacy invasive measures on a grand scale in the guise of homeland security, has emerged as emblematic of a 'big data' surveillance and privacy zeitgeist. These security policies and surveillance practices are now dialectically embedded in our complex digital media landscapes. Certainly, our evolving media privacy is inevitably shaped by the contested platform politics of vested political, economic-technological, and socio-cultural interests, and the shift to what has been called 'algorithmic living'.[3]

The privileging of predictive data ways of thinking and knowing is central to this shift. As Mark Andrejevic argues, 'The promise of automated data processing is to unearth the patterns that are far too complex for any human analyst to detect and to run the simulations that would generate the emergent patterns that would otherwise defy our predictive power'.[4] Digital media convergence has become the fertile breeding ground for the predictive mode of thinking and knowing. Computer analytics, scaled-up data mining and visualisations can all operate in the service of this mode of thinking. Yet it's interesting to note that there's a fundamental contradiction at the heart of this shift: simultaneously a promise of democratic digital media empowerment for individuals goes hand in glove with the reality of elitist access, and the finely-tuned skill set to make use of and interpret database-derived information. Using the alternative qualitative research term of 'thick data' rather than 'big data', Langlois and Elmer argue that studying communications acts on social media platforms to expose corporate power, requires an ontological unveiling of technical, corporate and media logics.[5] Their approach to analysing 'thick' digital objects (acting interdependently at the 'media', 'network' and 'phatic' layers) has much to offer those concerned with the uses of personal data on social media platforms such as Facebook. They argue:

> The articulation of participatory and corporate logics can be examined through identifying the different kinds of informational logics and layers, phatic moments, media processes and their interactions. The analysis of a digital object, even if it takes

> place within a small sample, can thus yield greater knowledge and awareness as to how corporate social media logics enter into participatory processes.[6]

Some uses of large-scale personal datasets are much less ambiguous. Following the unprecedented surveillance vortex created by the Snowden-National Security Agency (NSA) revelations in 2013, a federal judge from the U.S. District Court for the Southern District of New York scrutinised the legality of the NSA metadata surveillance activities. In his deliberations Judge William Palley III sided with the Obama administration in dismissing a challenge to the legality of the NSA's bulk metadata program brought by the American Civil Liberties Union. In his ruling Judge Palley, while acknowledging that 'robust discussions' were underway across the nation, including in the Congress and White House, nonetheless found that the government's bulk telephony metadata program was lawful. The judgement makes the point that the Obama Administration began its bulk metadata collection program in the post-9/11 context so it could 'find and isolate gossamer contacts among suspected terrorists in an ocean of seemingly disconnected data. This blunt tool works because it collects everything. Such a program, if unchecked, imperils the civil liberties of every citizen'.[7] The judge further observed that if the metadata was 'plumbed', the data was capable of revealing a rich profile of any individual and a detailed record of their associations. I will discuss these questions further in Chapter 5 when we consider the way in which state secrecy is traded off against personal privacy. The idea of being able to 'identify' individuals in the crowd ('a needle in a haystack') remains at the core of what it means to breach hard won rights to privacy, and as a corollary, what might be at stake in the steps taken to preserve personal privacy.

In this book I argue that with the rise of web-based media, social networking and the rapid take-up of mobile devices and apps, notions of privacy are being modified at a commensurate rate for media audiences. It's important to realise at the outset that powerful market dominating new media corporations such as Google (the owner of YouTube), Facebook, LinkedIn and Twitter have made it clear that it is their avowed intention to reconfigure people's understanding of the meanings of personal privacy. This usually incremental change process can be witnessed in continuous website terms

of service and software updates by these corporations, developments to handset design and operations, and in the changing ways that people privately use media devices on the move in public spaces.[8]

Lori Andrews argues that 'Facebook is unilaterally redefining the social contract – making the private now public and making the public now private'.[9] She observes that public institutions, for example, such as the police, now routinely use data gleaned from social networks to assist them in their investigations, in ways that would have previously often required a court order to obtain the information.

For Jose van Dijck this can be expressed as 'the Devil is in the Default'. She argues 'Platform owners have a vested interest in complete openness on the side of users; the more they know about users the more information they can share with third parties'.[10] Similarly, new mobile media when viewed as assemblages of hardware, software and usage practices are actively implicated in a process of redefining the social and cultural meanings of the concepts we generically label as concerning 'privacy'. In this sense, then, there is a power imbalance regarding our personal information on the owner-design side of these interactive platforms. The extension of digital media affordances to gather, stockpile, and to track and monitor people's usage data in online mobile spaces is pushing out our understandings of privacy in uncharted directions.

New frontiers in privacy

One of the emerging frontiers of new digital media technologies arises from the convergence of mobile media and locative media. Many of the privacy concerns that relate to locative media overlap with those of online mobile media by dint of their common transmission infrastructures and access devices. The growth of Location-Based Services (LBS) has been linked with the rise in smartphone ownership and people getting location-based directions and information for purchasing goods or services, or using them to 'check-in' on social media applications while they're on the move.[11] Smartphone ownership is now part of mainstream media. Market research company *eMarketer* predicted that by the end of 2014 there would be 4.55 billion users of a mobile phone. Globally the smartphone audience had reached around 1.75 billion and more than 2.23 billion

people worldwide, or 48.9% of mobile phone users, went online via mobile at least monthly in 2014. By 2017, 'smartphone penetration among mobile phone users globally will near 50%'.[12] This general pattern of 'leapfrogging', where people gain access to the Internet, perhaps for the first time, using a mobile device, bypassing more conventional device access, is being repeated around the world in both developing and developed nations.[13]

However, these conceptions of privacy linked to the use of location aware services, apps and mobile devices should be considered as a serious policy issue arising from the broader social and cultural implications of 'networked locality'.[14] Developments in privacy and the use of personal information are highly consequential as populations increasingly conduct their lives in and through online mobile media transaction spaces, for entertainment, news, information and services, for banking and shopping, and for social interactions. Arising from these developments, policymakers need to be alert to the shifting categories of mediatised practices involving personal information, and be prepared to specifically identify and ring-fence these for priority interventions. As people depend more and more on global positioning systems (GPS) to 'pull' and have information 'pushed' to their geo-location, the risks to personal privacy arising from these practices will only increase. Community research in Australia indicates that the majority of people have only a poor level of awareness of the way in which their personal data is shared when they use LBS. Yet this greater use of LBS 'does not equate to a greater understanding' about what personal data is collected and shared and with whom, how it was collected, where data is sent, stored or compiled, or indeed who is in control of their personal data.[15] I will consider more specific privacy concerns raised by LBS in Chapter 4. But in the meantime it's important that we have an understanding of the new industrial and social contexts in which these emerging technologies and their associated cultural forms are embedded. It's also important to reflect on ideas regarding privacy and convergent and 'morphing' media, and the wider impacts of promotional or selling cultures.

Drones, wearables and the Internet of Things

According to one recent account, during Obama's time as President, to date there have been 349 drone strikes in Pakistan, and these have

killed around 4000 people, with 'an estimated quarter of them being innocent civilians'.[16]

Drones (or unmanned aerial vehicles) have become a standard weapon in contemporary warfare, and they have also made their way into a number of areas of everyday life, for business (including media practices) and recreational purposes. Digital cultures researcher Chris Chesher has explored the application of humanities research traditions for analysing robot technologies such as drones, including media studies. He argues, 'Humanities researchers have competencies that may support collaborations with engineers, independent uses of robotic technologies, or critical attention to the practices of research and deployment of robotic technologies'.[17]

While the mediatisation of warfare 'content' certainly warrants closer scrutiny of drones, their use by police, private investigators and other law enforcement agencies is clearly pushing our ideas of privacy in novel directions. Similarly, when drone operators (oftentimes journalists) looking to collect information for a media story hover their machine over a private residence, or near some gathering of people in a public location, will they have an unalloyed sense of their activities as constituting 'media practice'? For Mark Andrejevic there is a sense in which the aerial robot is 'droning' digital media. At the level of the imaginary, drones have come to represent a convergent media device is some very significant ways. He argues, 'It encapsulates the emerging logic of portable, always-on, distributed, ubiquitious, and automated information capture'.[18] But it's more than this, he says; it concerns monitoring, sensing, and is an icon of locative media. It's the materiality and intrusiveness of the drone that redirects attention back: 'on the interface device that serves as mediator for both information collection and a certain type of automated action or response at a distance'.[19] The privacy concerns, then, are closely related to these material features of the drone being miniaturised, mobile and equipped with 24-hour sensing and digital interactivity.

The privacy implications of drones are only beginning to be assessed under relevant laws. For example, in Australia, the Federal Privacy Commissioner, who administers the *Privacy Act 1988*, when interviewed in 2012 noted that the act did not apply to individuals who were responsible for using drones, and he called on governments to review their privacy and surveillance legislation. Civil

Aviation authorities issue guidelines and these advise Drone owners to observe and be aware of privacy laws.[20]

In their 2014 report *Serious Invasions of Privacy in the Digital Era* the Australian Law Reform Commission (ALRC) argued that drones were becoming 'cheaper and more advanced'. They recommended that surveillance legislation needed to be technology neutral to embrace the full spectrum of emerging devices, software and networks.[21] The inquiry also recognised that as well as drones fitted with listening and optical functionality, other privacy intrusive categories of technology such as 'wearable surveillance devices' were earmarked as requiring attention within the scope of amended surveillance laws.[22]

With the continuing take-up of drones in the US there is speculation about the future of drones for media practice, after an unmanned, two-foot-wide quad copter crashed on the White House lawns at three in the morning. Inevitably, such an event became escalated as a security issue, and it comes at a time that 'media organisations are trying to convince skeptical regulators and law makers to allow them to use drones equipped with small cameras for gathering news and images'.[23] It was reported that the US Federal Aviation Authority had recently awarded CNN a licence to test camera-equipped drones for reporting. Journalism is one of the areas which is most strongly pushing for the use of drones, claiming that 'unmanned aircraft could transform the coverage of natural disasters, environmental spills or even wars'.[24] In the meantime, regulation of this potentially privacy intrusive activity is mainly covered by aviation authority guidelines.

Perhaps the arrival of Google's Glass signalled a new turn in the 'intimisation' of privacy and surveillance debates. It was a moment when it was possible to envisage significant societal shifts. The wearable computing device combines the functions of a smartphone, to search, image match, take photos, film and live stream that content to the net, without people in the vicinity of the user being aware of these activities. Arguably, too, it was one starting point for the trend that is all about integrating these devices into our lives.

Seen as part of an anticipated push into the wearables and 'Internet of Things' based on its Android software, Google Glass has divided community opinion in relation to privacy. Releasing its software developers' toolkit in order to accelerate the development of apps

for watches, fitness trackers, jackets and other items of clothing with embedded sensors, is a key first step as seen previously with smartphone application development. Undeniably though, Glass has been controversial, even to the extent of being banned in some US cinemas, cafes, casinos and bars.[25] The backlash needs to be considered in relation to previous privacy transgressions by Google, including the highly intrusive 'street view' search functionality, which escalated to full international scandal status when the company was also found to be copying unencrypted Wi-Fi data from the homes they filmed. The Glass device, paired with the geo-locative features of an Android compatible smartphone, or using similar in-built GPS functionality, were that to be introduced, is challenging regulators' ability to craft privacy protections.[26] In response to a letter from a group of privacy regulators requesting information as to how Google would be dealing with concerns over the misuse of personal data, the company advised that they would be developing the technology first, and assumed that regulatory and social norms would adapt as Glass was used more widely.[27]

The promise of making our everyday lives easier, and at the same time figuring out how to make money from the transition to the global take-up of wearables, and other sensor-connected 'Internet of Things' apps and devices is the main driver of these technical innovations.[28] Adding sensors to everyday objects to make them 'smart', and enabling machines to talk with other machines, inevitably means aggregating usage data and being connected to the Internet. At the 2015 Las Vegas Consumer Electronics Show (CES), patrons gathered to survey how the latest snowboard can record and track the rider's weight distribution, how monitors can check that your dog is getting enough exercise, or how apps can allow you to light up or heat your home before you make it to the front door.[29]

The revenue implications for data-gathers in the data economy are potentially very lucrative, and their motives, therefore, easy to comprehend. Using personal data and on-selling it to third parties is now a tried and proven business model. As this *Financial Times* piece argues:

> Users will benefit from understanding more about their health or how to manage the risks they run in their everyday lives – but the same information will also be exceedingly valuable to healthcare

> providers and insurance companies, not to mention sellers of nutritional products, safety equipment, exercise machines and many other goods and services.[30]

Privacy issues arise at many points along these value chains where the commercial interests of Internet media giants and health tech firms are converging around the Internet of Things. First, what data will be collected, who exactly will our personal data be onsold to, and what will those third-party corporations then do with the data? Second, where will the data be sent, how secure will the cloud storage of this data be, and will there be procedures in place to update or amend data, assuming that consumers are even aware that these corporations have acquired and are controlling our data.

Chinese tech giants Xiaomi and Baidu have both announced smartphone-connected blood pressure monitors in partnership with specialist health technology firms. Baidu's 'Mumu BP 2' allows users to wirelessly monitor their blood pressure data in real-time and record it on a Baidu cloud server. It's reported that the device will include data on systolic blood pressure, diastolic blood pressure, and heart rate. There is backwards compatibility to older phones and Bluetooth software (for the elderly users). Apparently the commercial logic stacks up: 40% of Chinese people aged 45 or over have hypertension issues.[31]

Corporate buy-ups are, of course, a reasonably accurate indicator of the intention of media companies, and Google's acquisition of Nest, a smart thermostat and fire alarm maker, is obviously positioning itself to be a major player in the connected home hub of the Internet of Things. Google also announced smart contact lenses, their latest wearables, which are able to monitor the glucose levels of diabetics.[32]

The Internet of Things has been on the radar for at least a decade, and includes everything from connected cars and homes to wearables. Its accelerating growth has prompted the main privacy regulator, the Federal Trade Commission (FTC) to request that companies limit the quantity of personal data they collect. Edith Ramirez, the chairwoman advised the attendees at the CES that her agency would be examining the emerging Internet of Things for privacy issues.[33]

Smart TV brands monitor the programmes you watch and the websites you browse to offer personalised recommendations for TV shows - but this information can be passed on to advertisers to target viewers more accurately

Figure 1.1 Smart TV

Major branded television manufacturers including Samsung, LG, Sony, Sharp, TP Vision (Philips), Toshiba and Panasonic have produced so-called 'Smart TVs' for some years. Google Cast and Samsung's 'Tizen', and Apple's Airplay software operating systems are competitors in this Internet of Things and TV streaming space. There is mounting evidence that these Internet connected TVs are breaching privacy laws. The source of the controversy is the ability of the sets to transmit personal data back to the manufacturer and to related

Figure 1.1 Continued

third-party providers. Firstly, the problem is the categories of personal data being collected from the viewers and their viewing context, and then transmitted: not only are the choice of programs and Internet viewing habits being tracked and logged, but sound and vision are also being recorded. In some smart TVs (e.g. Samsung's) the camera is linked with facial recognition software, and cookies are used to monitor use of particular content, including email messages.[34] Their new global privacy policy for Smart TVs advises: 'Please be aware that if your spoken words include personal or other sensitive information, that information will be among the data captured and transmitted to a third party through your use of Voice Recognition'.[35] Secondly, these data recording activities are reproducing practices that have been available in Microsoft's X-Box Kinect since 2010, adding weight to the proposition that various online audiences are being exposed to