Keeping Our Secrets? Designing Internet Technologies for the Public Good

Professor Ian Brown*

Senior Research Fellow and Associate Professor, Oxford Internet Institute, University of Oxford

Information technology; Mobile telephones; Personal data; Portable computers; Privacy; Public interest

Abstract

The ongoing development of computing, communications and storage technologies presents a challenge to privacy protection, given the increasing ease with which personal data can be collected, analysed, stored and shared. Computer scientists have developed "privacy by design" techniques such as data minimisation, which help to enforce the data protection and privacy safeguards contained in national legal frameworks and international human rights instruments. Such techniques provide a template for societies that wish to ensure the continued protection of core social values in an increasingly technology-mediated world.

Introduction

Sun Microsystems was one of the biggest companies in the Internet technology boom of the late 1990s. According to its adverts, Sun "put the dot in dot.com". When Sun's CEO Scott McNealy was asked at a press conference about the privacy features of some new software, he replied: "You have zero privacy anyway. Get over it."[1]

Was McNealy right? Does, and should, new technology have the potential to sweep away fundamental rights and societal values?[2] There are clearly challenges for privacy in the continuing development of Internet and related technologies—something that McNealy and many others have recognised. But there is also a significant amount of research into how these technologies can be designed in a way that better protects privacy.

After describing these challenges, this article presents the key elements of these design features, using the examples of targeted advertising for mobile phones and privacy-protective robots. From this, it draws broader lessons for how society can shape the evolution of new technologies in the public interest.

Moore's law and continuing advances in computing, communications and storage

Since the Second World War, computers have developed enormously: from specialised military equipment, to tools for big business and government agencies, then onto the desktops and increasingly into the pockets of an increasing percentage of the world's population. This integration into everyday life is likely to continue as the "Internet of Things" spreads, with sensors and computing increasingly built into everyday objects—biometric headphones, fitness-monitoring false teeth, Google Glass …

* This article is adapted from the 2014 Oxford London Lecture given by the author at Church House, Westminster, on March 18, 2014, supported by Oxford University's Romanes fund. The research it describes is supported by EPSRC grant EP/L00416X/1.

[1] Polly Sprenger, "Sun on Privacy: 'Get Over It'", *Wired*, January 26, 1999.

[2] H. Nissenbaum, "Values in the Design of Computer Systems" (March 1998) *Computers in Society* 38.

One of the main drivers of this rapid evolution was predicted in 1964 by Gordon Moore, father of the microprocessor and co-founder of Intel Corporation. After designing the earliest microchips, he predicted that the number of transistors you could fit on a chip at an efficient price would double every two years. The chip industry's research and development has kept to this pace ever since. Roughly speaking, this has resulted in a doubling of computer power every two years for the last four decades.

Alongside this, communications bandwidth and storage capacity have been growing just as quickly. This kind of exponential growth leads over time to an enormous increase in capability—as is obvious from today's smartphones. Computers can process data much faster, store much larger quantities of data and rapidly share that data using data networks, particularly now the Internet interconnects so many systems around the world.

When the data in question is about people, this can have a big impact on privacy. Much more data is being collected about people's day-to-day activities as they interact with digital technology, directly and via organisations. Many people are volunteering further data to social networking sites and other online services. And sensors—in smartphones, CCTV cameras and "Internet of Things" objects—are making the physical world as potentially trackable as the virtual.

People are very often unaware of how much data is being gathered about them, let alone the purposes for which it can be used. A study by Aleecia McDonald and Laurie Cranor in 2008 found that the privacy policies of the 75 most-visited websites take on average 10 minutes to read, and that the average Internet user visits 119 unique sites each year.[3] Very few people are spending 20 hours each year reading privacy policies.

Most privacy risks are highly probabilistic, cumulative and difficult to calculate. A student sharing a photo of over-exuberant exam celebrations might not be thinking clearly about the risk that the photo could be seen by a future interview panel. Or that the heart rate data they share today from a fitness gadget might later reveal a higher risk of future heart problems. Or that combined, this data might fit the profile of a high risk-taker, with all the implications that could have for future employment, insurance and financial services decisions.[4]

These are low probability but high-impact risks. Four decades of behavioural economics research has shown that most people are bad at making decisions trading immediate benefits—like polishing your reputation with your university friends or running club—against uncertain, delayed costs, such as future difficulties getting a mortgage.[5]

Even individuals with strong privacy concerns have limited options when it comes to finding privacy-friendly alternative Internet services. New software is expensive to write, but almost free to run. It can be difficult for users to transfer their data from one service to a competitor. And if all of your friends are on one social networking service, you probably want to be there too. These effects all tend to favour incumbents in information industries.[6] Indeed, in Europe, Google has around 90 per cent of the search market, while 71 per cent of online Americans use Facebook.[7]

Finally, there are the extraordinary lengths that some organisations will go to for access to data about people of interest to them. Those might be celebrities, or ordinary people suddenly involved in big news stories, as in the phone-hacking cases revealed by *The Guardian*.[8] The Information Commissioner's Office and National Crime Agency are investigating corrupt staff in public and private sector organisations, who

[3] A. McDonald, and L. Cranor (2008) "The Cost of Reading Privacy Policies", *I/S: A Journal of Law and Policy for the Information Society* (Privacy Year in Review issue).

[4] I. Brown, "The Economics of Privacy, Data Protection and Surveillance" in J.M. Bauer and M. Latzer (eds), *Research Handbook on the Economics of the Internet* (Cheltenham: Edward Elgar, 2014).

[5] Brown, "The Economics of Privacy, Data Protection and Surveillance" (2014).

[6] I. Brown and C. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age* (Cambridge, MA: MIT Press, 2013).

[7] Pew Research (2013), *Social Media Update*, *http://www.pewinternet.org/2013/12/30/social-media-update-2013/* [Accessed July 21, 2014].

[8] See archive of articles, *http://www.theguardian.com/media/phone-hacking* [Accessed July 24, 2014].

have been found to be selling access to data on phone use, car registrations and even criminal records, to private investigators and their clients in the media, local authorities and the City of London.[9]

Or given much greater resources, it could be the data about hundreds of millions of Internet users scooped up by the US and UK intelligence agencies, in the hope that these haystacks can be winnowed down to information useful for national security programmes.[10] The multi-billion-pound surveillance systems revealed by Edward Snowden have the potential to make our digital lives almost transparent to GCHQ and the US National Security Agency.

Privacy-enhancing technologies

Since the 1980s, computer scientists have been developing methods for designing privacy into new technologies and systems—rather than waiting for something to go wrong, then spending large amounts of time and money trying (and often failing) to fix privacy problems.[11]

One of the most important principles they have developed is data minimisation. This means very carefully limiting the collection of personal data to that needed to provide a service, rather than storing everything that can be conveniently retrieved. Additionally, access to data should be limited within organisations. It should be under distributed control, ideally held by the individuals it relates to and restricted using encryption. And once personal data is no longer needed, it should be deleted or anonymised.

This approach protects against a number of risks. It limits the impact of data losses and breaches. It protects against corrupt staff with authorised access to data—a practice that an investigation by the UK Information Commissioner's Office showed was widespread.[12] The price list of one investigator is shown in the following table, with the amount paid to the corrupt insider (or "blagger") for the information, and the amount clients were charged for that data:

Information required	**Price paid to "blagger"**	**Price charged**
Occupant search	not known	£17.50
Telephone reverse trace	£40	£75
Friends and family	£60–£80	not known
Vehicle check at DVLA	£70	£150–£200
Criminal records check	not known	£500
Locating a named person	not known	£60
Ex-directory search	£40	£65–£75
Mobile phone account	not known	£750
Licence check	not known	£250

Privacy by design[13] also protects against function creep. When an organisation has invested significant time and resources to collect personal data for one reason, it can be very attractive for them to use it for other purposes. While this is limited in the EU by data protection law, government agencies are in a good position to push for changes to national laws if they wish, bypassing such "purpose limitations". Nor do these rules tend to apply to intelligence agencies.

[9] House of Commons Home Affairs Committee (2013), *Private Investigators: follow-up, oral and written evidence*, available at: *http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/524/524.pdf* [Accessed July 21, 2014]

[10] Ian Brown (2013), Witness Statement for *Big Brother Watch, Open Rights Group, English PEN and Constanze Kurz v United Kingdom* (App. No.58170/13) ECtHR.

[11] S. Spiekermann and L.F. Cranor, "Engineering Privacy" (2009) 35(1) IEEE Transactions on Software Engineering.

[12] Information Commissioner's Office, *What Price Privacy?* (2006) HC 1056.

[13] S. Gürses, C. Troncoso and C. Diaz, "Engineering", *Privacy by Design*, Computers, Privacy & Data Protection (2011).

Another key aspect of putting users in control of their personal data is making sure they know what data is being collected and how it is being used—and ideally being asked for their consent.

There have been some interesting experiments with privacy interfaces for small screens. Figure 1 shows an example from Imperial College and the Open University, which helps smartphone users understand who is asking for their location data.

Figure 1: **L. Jedrzejczyk et al., (2010) "'Privacy-shake': A Haptic Interface for Managing Privacy Settings in Mobile Location Sharing Applications, *Conference on Human-Computer Interaction with Mobile Devices and Services* (2010), pp.411–412**

It might be a friend or a family member that a user always wants to give access. Or it might be someone from work they would be willing to share your location with occasionally in office hours, but not several times in one week. This interface helps people understand what data has been recently shared with specific individuals.

Smartphones have quite enough storage and computing capacity to do some tasks, such as showing users adverts relevant to their known interests, without sharing any personal data with third parties. Figure 2 shows our efficient system to distribute targeted adverts to phones in a privacy-friendly way. Software on the phone selects adverts to show to users based on their previous browsing behaviour, without notifying advertisers of individual interests.

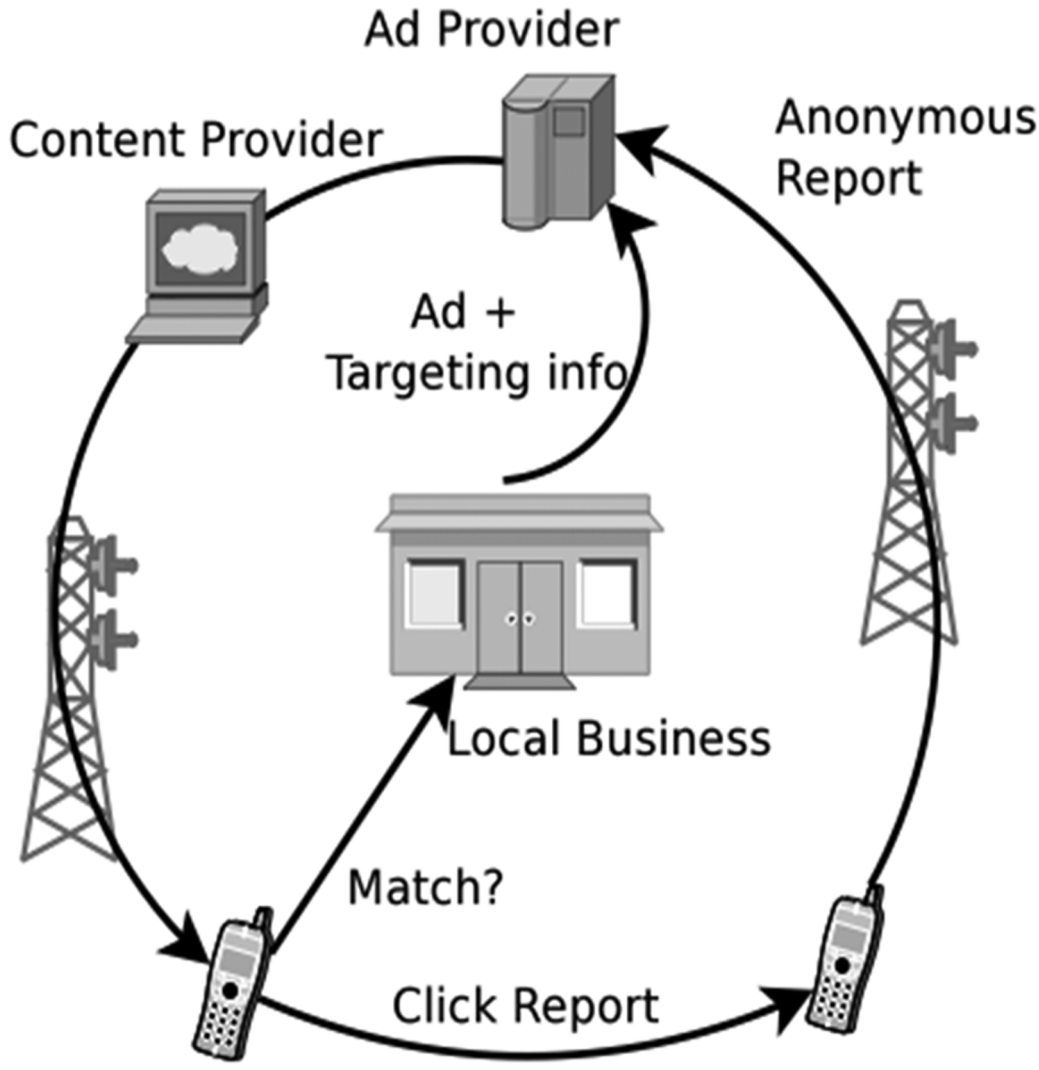

Figure 2: **H. Haddadi et al., "Targeted Advertising on the Handset: Privacy and Security Challenges" in J. Müller, F. Alt and D. Michelis (eds), *Pervasive Advertising* (Heidelberg: Springer, 2011), pp.119–137.**

The system works especially efficiently for location-targeted adverts, for example offering a discount at a local shop. And when a user clicks on an advert, an anonymous report is sent back to the advertising network which can claim payment from the advertiser without identifying the user. Unlike existing behavioural advertising systems, users' profiles are kept under their direct control.

This kind of user-controlled data storage and processing has all kinds of applications, for example with smart electricity meters[14] and congestion charging for roads.[15]

[14] G. Danezis et al., *Smart Meter Aggregation via Secret-Sharing* (ACM Smart Energy Grid Security Workshop, 2013).
[15] J. Balasch et al., *PrETP: Privacy-preserving Electronic Toll Pricing* (19th USENIX Security Symposium), pp.63–78.

Another example of our research in this area is in human-robot interfaces. When people begin to interact with more human-like computing devices, their expectations and assumptions shift, bringing in questions of our trust and emotional relationship with these devices. Can we design robots to gather only the information they need to interact with humans and carry out tasks, rather than risk them being seen as CCTV cameras with legs?

Conversely, how does it affect trust and other psychological variables if a robot makes full use of the information it can access about us, such as recognising our smartphone's identifiers and automatically looking us up online? At what point does "too much information" come as an unpleasant surprise?

Protecting the public interest in technology design

Having described the challenges that technology brings to privacy, but also the ways in which technology can be designed to deal with some of those challenges, what broader lessons can be drawn about shaping technologies for the public good?

The first obvious question is: what is the public good? Who gets to define it? One option is to look at opinion polling about public concerns and values over long periods of time. The European Commission does regular polls across the EU on social concerns (see figure 3). In most countries in Europe, including the UK, people have had significant concerns about data privacy for decades:

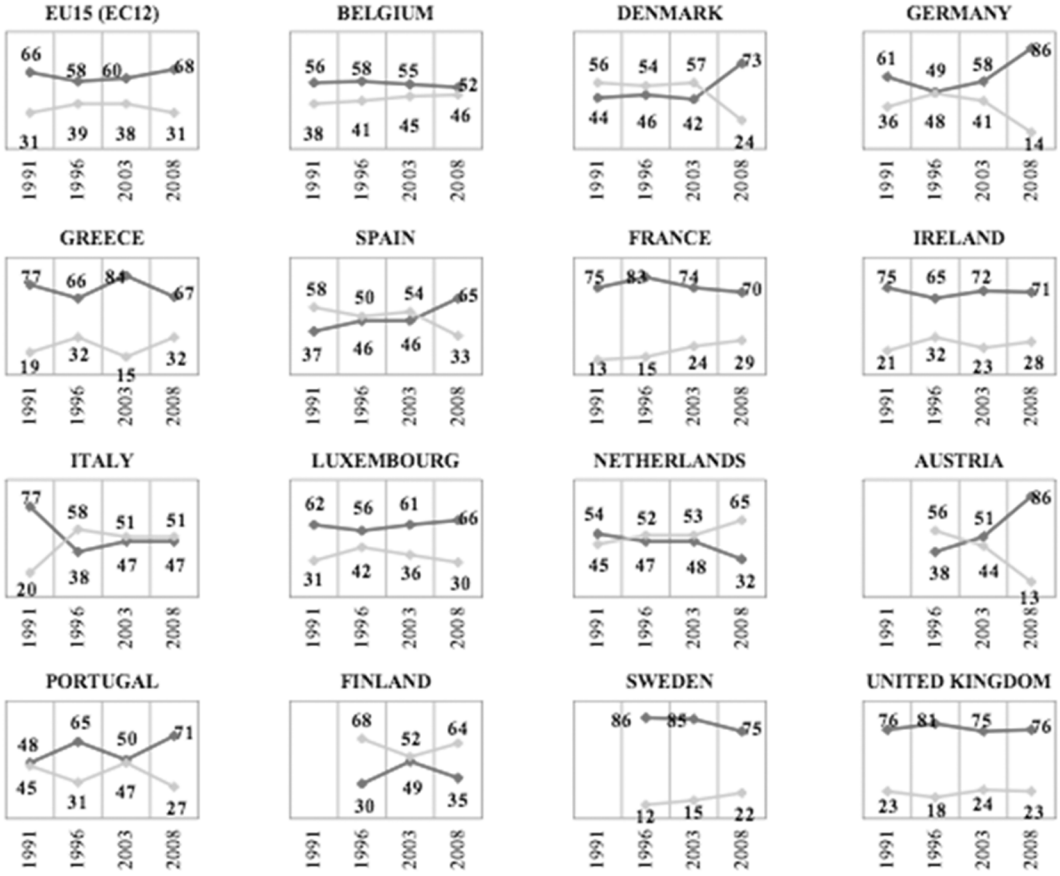

***Figure 3: Eurobarometer 225: Data Protection in the EU*, February 2008, p.8**

A more fundamental view of core social values can be found at the national level in constitutions, and between nations in human rights treaties. As courts interpret these legal instruments over time, they come to cover new technologies such as the Internet.

As well as the protection of private life and correspondence in art.8 of the European Convention on Human Rights, the freedom of thought, expression, association and assembly rights in arts 9–11 (and their equivalents in the US Bill of Rights, and the International Covenant on Civil and Political Rights) are also relevant. The freedom to say unpopular things, or associate with unpopular people, is discouraged if there is a perception that speech or association may be noted and have a negative effect. Similarly, people may be reluctant to go on a public demonstration if they fear that data may be recorded about their mobile phone, or that police photographers will add them to their national database of "extremists".

ECHR, 1950	**US Bill of Rights, ratified 1791**
Reaffirming their profound belief in those fundamental freedoms which are the foundation of justice and peace in the world…	…extending the ground of public confidence in the Government, will best insure the beneficent ends of its institution…
§8 Everyone has the right to respect for his private and family life, his home and his correspondence.	I: 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.
§9 Everyone has the right to freedom of thought, conscience and religion.	
§10 Everyone has the right to freedom of expression.	
§11 Everyone has the right to freedom of peaceful assembly and to freedom of association with others.	IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.

Internationally, the US Constitution is particularly important given the geography of the Internet. The table above shows excerpts from the First Amendment, protecting free speech and assembly, and the Fourth Amendment, interpreted over time by the Supreme Court to protect privacy against the government.

This national and international law restricts how states use technology to infringe human rights, even for national security purposes. There are several US legal challenges to the constitutionality of NSA communications surveillance, with a federal court in Washington DC finding that bulk access to phone records is against the Fourth Amendment[16] (but another court in New York finding the opposite[17]). The UK campaign groups Big Brother Watch, Open Rights Group and English PEN have taken a case to the European Court of Human Rights, arguing that UK law in this regard is incompatible with the Human Rights Convention.[18]

The independent review panel set up by President Obama to consider the NSA programmes concluded that providing such "bulk" access was not in the long-term interests of the US:

> "Although we might be safer if the government had ready access to a massive storehouse of information about every detail of our lives, the impact of such a program on the quality of life and on individual freedom would simply be too great … We recommend that the US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection."[19]

[16] *Klayman v Obama* , WL 6571596 (D.D.C. 2013).
[17] *ACLU v Clapper* , No.13-3994 (S.D. New York, December 28, 2013).
[18] See fn.10 above.
[19] *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies*, December 12, 2013, p.115/173.

One UK political party has decided that intelligence agencies should embrace data minimisation, with Deputy Prime Minister Nick Clegg stating:

> "[O]ur current framework assumes that the collection of bulk data is uncontroversial as long as arrangements for accessing it are suitably stringent. I don't accept that … [S]trong access controls are vital to prevent employees from going on 'fishing expeditions' once a store of data exists. But the case for collection itself has to be made, not assumed."[20]

Can technology development be shaped more broadly to reflect such constitutional values? One of the best-known attempts is the EU's data protection framework. Privacy is a core European political value, not least because of the horrors of the Nazi and Communist regimes of the 20th century. Germany, France and Sweden all developed data protection laws in the 1970s in response to the development of automated systems for processing personal data, followed by most other European countries. The EU's Data Protection Directive (95/46/EC) harmonises these laws, and has provisions that encourage organisations to use technical measures to protect personal data.

An update of this Directive, which the European parliament has been debating over the last year, more explicitly includes this type of regulation by technology. Under this General Data Protection Regulation, organisations that are processing personal data will have to implement appropriate technical measures to protect Regulation rights. By default, organisations should only collect the minimum personal data they need, and allow individuals to control the distribution of their personal data[21]—encouraging the use of the data minimisation procedures described earlier.

The Regulation is currently being negotiated by the Member States. But a complementary option is stronger requirements on dominant technology companies to make their systems interoperate with competitor services. If it is easier for people to move from, for example, one social networking service to another if they are unhappy with the privacy protection available, that should apply competitive pressure to increase privacy protection.[22]

The Data Protection Regulation would require companies to make it easier for users to download all of their data, so that it could be uploaded to a competitor service. This data portability would reduce the switching costs associated with moving between services.

However, users have a strong incentive to be on the same social networking services as their friends, family, and colleagues since those are the people they want to communicate with. This makes it much harder for new services to break into an existing market. A potential remedy would be to require dominant services to interconnect with their competitors in the same way as telephone companies do so customers do not have to be on the same network to call a friend. Technically, there is no reason why online services like social networking sites should not provide similar functionality. Similar issues are raised when online services partner with dominant companies in a related sector, such as the telecoms industry.[23]

This type of technology regulation is not uncontroversial. The European Commissioner responsible for the Data Protection Regulation, Viviane Reding, has said that she had seen unprecedented and "absolutely fierce" lobbying against some of its provisions.[24]

Legislators would clearly be foolish to try and micro-manage the development of new technology. But the EU's principles-based approach to privacy has been internationally influential, with over 100 countries

[20] *Security and Privacy in the Internet Age*, Royal United Services Institute, London, March 4, 2014.

[21] Unofficial consolidated version about LIBE Committee vote provided by the rapporteur October 22, 2013, Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), *http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf* [Accessed July 21, 2014]

[22] See fn.6 above.

[23] See fn.6 above.

[24] Matt Warman, "EU Privacy Regulations Subject to 'Unprecedented Lobbying'", *Daily Telegraph*, February 8, 2012.

in total now having adopted the Data Protection Directive or similar laws.[25] If the EU can find the right balance in its Regulation, it has the opportunity to set the new global standard for privacy-protective technologies—a very significant opportunity indeed in the global marketplace.

Conclusion

Technical developments are clearly having a significant impact on privacy—unsurprisingly, given how quickly the underlying capabilities of computing, storage and networking technologies are increasing. But societies in turn have the opportunity to shape those developments towards positive social ends.

This article has described a number of ways that privacy-protective technologies can be designed, for a range of applications, such as targeted advertising and human-robot interfaces. If democracies around the world continue to believe that privacy is a foundational human right, the question is how they persuade companies and governments to put these techniques into practice.

Many technologists, policymakers and privacy regulators are more optimistic than Scott McNealy that this can be done, using laws such as the Data Protection Regulation, and more traditional human rights protections. Rather than "getting over it", privacy will ultimately only disappear if societies allow it to.

[25] G. Greenleaf, "Sheherezade and the 101 Data Privacy Laws: Origins, Significance and Global Trajectories" (2014) *Journal of Law, Information and Science*, forthcoming.