International Data Privacy Law Advance Access published November 3, 2010

Privacy: The New Generations

Omer Tene*

Privacy law in general, and informational privacy in particular, have always been closely linked to technological development. In their seminal 1890 article 'The Right to Privacy', Warren and Brandeis lament the '[i]nstantaneous photographs and newspaper enterprise [that] have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops" '.[1] The current legislative framework for privacy and data protection, founded largely on instruments such as the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the 'OECD Guidelines') and the European Union Data Protection Directive 95/46/EC (the 'EU Directive')[2] (together, the 'Current Framework'), harkens back to a technological landscape strikingly different than the one today.[3]

Innovations and breakthroughs, particularly in information and communications technologies, have created new business models and tools affecting individuals' lives and impacting the functioning of virtually every business process and government activity. Although modelled to be technologically neutral and apply across industries, the Current Framework is in danger of being unravelled by a new generation of users utilizing a new generation of technologies. The fundamental concepts underlying the Current Framework, including basic terms such as 'personal data', 'data controller', 'data processor', and 'data transfer', have been disrupted by shifting technological realities.

Not only technology has changed over the past 30 years; the individuals using it have changed too. This new generation of users consists of individuals who post and search for personal, often intimate, information online; communicate with friends and colleagues on social networks; and are accustomed to their location being tracked and broadcast in search of nearby friends or restaurants. Indeed, even the distinction between the private and public sphere has muddled, with users of social media broadcasting personal information to sometime strangers whom they label 'friends'. More pressing than before is the need for a 'right to oblivion', which would extricate individuals from the increasingly burdensome informational load they carry through different stages of their lives.

Key Points

- The current international legal framework for data protection and privacy is founded on instruments such as the 1980 OECD Guidelines and the European Union Data Protection Directive that date from the 1980s and 1990s.
- At the time these instruments were drafted, technologies that have become pervasive today (such as the Internet, social networking, biometrics, and many others) were virtually unknown. Moreover, a new generation of users has grown up in the last few years that has come to integrate online technologies into the fabric of their daily lives.
- Privacy legislation has not kept up with these developments and remains based on concepts developed in the mainframe era. Thus, we need a new generation of privacy governance to cope with the implications of the new generation of online technologies, and to protect the new generation of technology users.

* Associate Professor, College of Management School of Law, Rishon LeZion, Israel. The author would like to thank Christopher Kuner, Christopher Millard, Fred Cate and Chris Hoofnagle for their helpful comments. All web sites cited were last visited 8 September 2010.

1 Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31.

3 For a brief exposition of the technological landscape setting the stage for the Current Framework *see* Viktor Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Philip Agre and Marc Rotenberg (eds), *Technology and Privacy: The New Landscape* (MIT Press, Cambridge, MA 1997) 219–41.

Government entities around the world (including the European Commission,[4] the OECD,[5] and the US government)[6] are currently grappling with the fact that the new generation of technologies and of users calls for a new generation of data protection governance.

I. A new generation of technologies

I outline below some major examples of a new generation of technologies that are challenging the Current Framework and creating a need for innovative solutions.

The Internet

It seems awkward to talk about the Internet as a 'new technology' these days. After all, a new generation of users dubbed 'Digital Natives'[7] was born and has matured with the Internet already a driving force in society. E-commerce, e-government, search engines, and social networks are deeply rooted in today's politics, culture, economy, and academia. Yet, strikingly, the Current Framework, so dramatically impacted by the Internet, was conceived and put in place when the network was just in its infancy.[8] It is perhaps telling that the first major data protection case decided by the European Court of Justice (the *Bodil Lindqvist* case[9]) dealt with a 'transfer' of personal data online, in a manner so benign as to appear trivial in retrospect (the prosecution of a Swedish churchgoer for publishing a personal web page containing rather mundane information about her colleagues in the parish). Here are some noteworthy developments in the online sphere that have occurred in the last few years:

Cloud computing

Individuals and businesses are increasingly storing and processing data on remote servers accessible through the Internet rather than on local computers. 'Cloud services' include both business-to-consumer tools, such as e-mail, instant messaging, and photo sharing services; and business-to-business applications, such as customer relationship management (CRM) and enterprise resource planning (ERP) software (software as a service, or SaaS); computing platforms offered as a service to facilitate low cost, rapid development and hosting of third party web service applications (platform as a service, or PaaS); and infrastructure offerings, including low cost facilities for storage, computing and networking (infrastructure as a service, or IaaS).[10] The advantages of cloud computing abound and include reduced cost, increased reliability, scalability, and security. However, the storage, processing, and transfer of personal data in the cloud pose risks to privacy, as data changes hands, crosses borders, and may be accessed and used without the knowledge and meaningful consent of individuals.[11] Cloud computing challenges some of the fundamental concepts of the Current Framework, including the definition of controller and processor; the nature of data transfers; the meaning of individual consent; and the thorny question of applicable law.

Behavioural targeting

Behavioural targeting involves the tracking of individuals' online activities in order to deliver tailored advertising.[12] The more finely tailored the ad, the higher the conversion or 'clickthrough' rate (CTR), and thus the revenues of advertisers, publishers, and various inter-

4 See European Commission, Consultation on the legal framework for the fundamental right to protection of personal data, 31 December 2009, available at <http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm>; Article 29 Working Party, 'The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data' (WP 168), 1 December 2009, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp168_en.pdf>.

5 *See* OECD, 'The 30th Anniversary of the OECD Privacy Guidelines', 2010 (Roundtable Series and Report), available at <www.oecd.org/document/35/0,3343,en_2649_34255_44488739_1_1_1_1,00.html>.

6 FTC, 'Exploring Privacy: A Roundtable Series', 2009–2010, available at <www.ftc.gov/bcp/workshops/privacyroundtables>.

7 John Palfrey and Urs Gasser, *Born Digital: Understanding the First Generation of Digital Natives* (Basic Books, New York 2008).

8 In fact, the OECD Guidelines, as well as Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), Strasbourg, 28 January 1981, were put in place before the advent of the World Wide Web as a public network. *See* Tim Berners-Lee, *Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web* (Harper Collins, New York 2000).

9 Bodil Lindqvist (Case C-101/01) [2003] ECR I-12971.

10 For a good exposition, see Let it rise: A survey of corporate IT, The Economist, 23 October 2008, available at <www.economist.com/node/12411882> (registration may be needed); Tim Mather, Subra Kumaraswamy and Shahed Latif, *Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice)* (O'Reilly Media, Sebastopol, CA 2009).

11 See, e.g., Ann Cavoukian, 'Privacy in the Clouds: A White Paper on Privacy and Digital Identity—Implications for the Internet', 28 May 2008, available at <www.ipc.on.ca/images/Resources/privacyintheclouds.pdf>; Office of the Privacy Commissioner of Canada, 'Reaching for the Cloud(s): Privacy Issues related to Cloud Computing', 29 March 2010, available at <http://priv.gc.ca/information/pub/cc_201003_e.cfm>; William Robison, 'Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act' (2010) 98 Georgetown Law Journal 1195.

12 See Article 29 Working Party, 'Opinion 2/2010 on online behavioral advertising' (WP 171), 22 June 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp171_en.pdf>; FTC Staff Report, 'Self-Regulatory Principles for Online Behavioral Advertising', February 2009, available at <www.ftc.gov/os/2009/02/P085400behavadreport.pdf>.

mediaries. Behavioural targeting may of course have a positive effect on users' browsing experience, by providing relevant commercial and non-commercial content. Yet the collection and use of large amounts of data to create detailed personal profiles have clear privacy implications. Quite distressing in this respect is the fact that users are seldom aware of the data collection processes, prospective data uses, and identity of the myriad actors involved, including not only advertisers and publishers, but also ad networks, ad exchanges, analytics services, affiliate marketers, market researchers, and search engine optimizers.[13] As a result, behavioural targeting clearly challenges the Current Framework's principles of transparency and individual choice. In addition, the multitude of parties accessing user data complicates the delineation of duties among controllers and processors. Furthermore, the application of privacy laws to behavioural targeting platforms may strain the definition of 'personal data'. Most tracking technologies gather information through the use of 'cookies', which are stored on users' browsers and assigned random identifying numbers. Given that such identifiers are not connected in any way to users' offline identities or even IP addresses, it is not clear whether information stored on cookies constitutes 'personal data' at all. In recent years, online ad networks, and in some cases even Internet service providers,[14] have begun to implement a technique known as deep packet inspection (DPI), formerly restricted to national security organizations, to monitor the content of Internet communications for users' interests and preferences.[15] While DPI may have positive uses, such as cyber-security and network management, it also encroaches on users' privacy and raises the spectre of covert surveillance. Indeed, civil liberties groups have argued that such activity may run foul of wiretapping laws.[16] At the same time, companies that use DPI for ad targeting argue that the matching of random identifiers with user interests does not involve the use of personal data. Yet, this distinction has arguably become irrelevant, given that advertisers who can track users pervasively often do not care about and have no interest in knowing such users' names or specific identity.[17]

Analytics

Computerized information, which used to be measured in bits and bytes, is now measured in *teras*, *petas*, and *zetas*. This 'data deluge' has resulted in organizations looking for innovative ways to manage and analyse heaps of data being accumulated through various business processes.[18] To prevent identification of individual data subjects and violation of data protection obligations such as the principle of purpose limitation, controllers anonymize data sets, stripping data of personal identifiers such as individual names and social security numbers.[19] This allows analysts to process the data while at the same time preventing marketers and identity thieves from abusing personal information. However, behavioural targeting companies may collect anonymous data but then overlay it with other databases, in an attempt to bring the users' identity into clearer focus. As Paul Ohm recently observed, 'clever adversaries can often re-identify or de-anonymize the people hidden in an anonymized database. . . . Re-identification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization.'[20] Latanya Sweeney's groundbreaking research has shown that a mere three pieces of information—ZIP code, birth date, and gender—are sufficient to uniquely identify 87 per cent of the US population.[21] De-anonymization of seemingly anonymous databases was recently demonstrated by researchers who were able to identify a large proportion of anonymized Netflix subscribers by matching data in their movie ratings against an additional online

13 See informative graphic: 'Before You Even Click', *Future of Privacy Forum Blog*, 29 April 2010, available at <www.futureofprivacy.org/2010/04/29/before-you-even-click/>.

14 Eric Pfanner, 'Internet providers get a piece of ad income', NY Times, 15 February 2008, available at <www.nytimes.com/2008/02/15/business/worldbusiness/15iht-AD18.html>.

15 Comments of the Center for Democracy & Technology to the European Commission in the matter of the Consultation on the Legal Framework for the Fundamental Right to Protection of Personal Data, 31 December 2009, available at <http://ec.europa.eu/justice_home/news/consulting_public/0003/contributions/organisations_not_registered/center_for_democary_technology_en.pdf>.

16 See sources at Electronic Privacy Information Center, Deep Packet Inspection and Privacy, available at <http://epic.org/privacy/dpi/>.

17 See, eg, Solon Barocas and Helen Nissenbaum, 'On Notice: The Trouble with Notice and Consent', in *Proceedings of the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information*, October 2009, available at <www.nyu.edu/projects/nissenbaum/papers/ED_SII_On_Notice.pdf>.

18 *The Economist* recently reported that 'the amount of digital information increases tenfold every five years.' 'A special report on managing information: Data, data everywhere' (27 February 2010) The Economist, available at <www.economist.com/node/15557443> (registration may be needed); see discussion of government and private sector data mining in Ira Rubinstein, Ronald Lee, and Paul Schwartz, 'Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches' (2008) 75 University of Chicago Law Review 261.

19 See, eg, Henry T. Greely, 'The Uneasy Ethical and Legal Underpinnings of Large-Scale Genomic Biobanks', (2007) 8 *Annual Review of Genomics and Human Genetics* 343.

20 Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (forthcoming 2010) 57 UCLA Law Review.

21 Latanya Sweeney, 'Uniqueness of Simple Demographics in the U.S. Population' (2000) Laboratory for International Data Privacy Working Paper, LIDAP-WP4.

database.[22] In another case, two New York Times reporters were able to sparse out the identity of an AOL user, whose online search queries were anonymized and posted on an AOL research website.[23] The Netflix researchers, Narayanan and Shmatikov, conjecture that 'the amount of perturbation that must be applied to the data to defeat our algorithm will completely destroy their utility for collaborative filtering.' Hence, they argue that data are *either* useful *or* truly anonymous—never both.

Mobile data processing

With nearly 5 billion mobile subscriptions worldwide powering a growing variety of computing devices, including not only mobile phones but also smart phones, PDAs, netbooks, laptops, and portable gaming devices, mobile data processing ('mobile') is becoming the primary method of accessing the Internet. Beyond transforming the world of computing and communications, mobile raises unique privacy issues that pose further challenges to the Current Framework.

Location tracking

Mobile devices are able to detect, store, and broadcast their physical location, raising important questions as to users' expectation of privacy in both the public and private spheres. Location tracking technologies, including the Global Positioning System (GPS), triangulation by cell phone towers, wireless positioning, and IP location[24] pave the way for an exciting array of new applications and services, such as locating nearby friends, finding recommended restaurants in foreign cities, 'checking in' at venues to receive discounts and coupons, and obtaining up-to-date traffic reports.[25] However, many individuals may not be aware that the location of their mobile device is constantly being recorded regardless of their use or non-use of such device. Such a 'location trail' is, of course, of much interest to law enforcement and national security authorities, sparking the introduction of data retention requirements in the EU.[26] To be sure, the EU Directive on Privacy and Electronic Communications requires subscribers' opt-in consent for the collection and use of location data for the provision of value added services.[27] Yet the ubiquity of location data collection and the indispensable use of mobile devices render ineffective the existing notice and choice regime.[28] New rules are necessary to reinforce individual control over the collection and use of location data as well as third party access thereto.

Third party applications

Third party applications are programs written to work within a given operating system by individuals or companies other than the provider of that operating system. Recent years have seen an explosion in the market for online and mobile applications, better known simply as 'apps', paving the way for innovative functionality for end users. However, users often lack a complete understanding of who is responsible for the applications they download and the personal data such applications use. The service and licence agreements as well as privacy policies of equipment manufacturers, mobile operators and app developers, are highly technical, vague, and written in dense legalese. Many of the data sharing transactions happen behind the scene, between computers, far from human oversight or control. Consequently, users have little ability to choose an application based on its privacy or security

22 Arvind Narayanan and Vitaly Shmatikov, 'Robust De-anonymization of Large Sparse Datasets' (2008) *IEEE Symposium on Security and Privacy* 111.

23 Michael Barbaro and Tom Zeller, Jr., 'A Face is Exposed for AOL Searcher No. 4417749' (9 August 2006) NY Times.

24 I refer to mobile location tracking. Additional location tracking technologies include smart transportation systems, such as mass transit cards and electronic tolling systems, electronic swipe cards, and RFID enabled devices.

25 See, eg, Foursquare, <http://foursquare.com>; Gowalla, <http://gowalla.com>; and Loopt, <http://www.loopt.com>.

26 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC [2006] OJ L105/54. See generally Francesca Bignami, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive' (2007) 8 Chicago Journal of International Law 233; Article 29 Data Protection Working Party, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC', 25 March 2006, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf>.

27 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37, amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 [2009] OJ L337/11; see Article 29 Data Protection Working Party, 'Opinion on the use of location data with a view to providing value-added services' (WP115), 25 November 2005, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf>.

28 See, eg, Center for Democracy & Technology Policy Post, 'The Dawn of the Location-Enabled Web', 6 July 2009, available at <http://www.cdt.org/policy/dawn-location-enabled-web>; Electronic Frontier Foundation, 'On Locational Privacy, and How to Avoid Losing it Forever', August 2009, available at <www.eff.org/files/eff-locational-privacy.pdf>.

practices.[29] Indeed, even highly trained experts often labour to fully understand which platform providers and application developers do what with users' personal data, where they store it, and who may have access to it. Compounding the picture is the fact that app platforms are increasingly global, creating multi-jurisdictional patterns where, for example, a user in Country A uses equipment made in Country B, operated by a mobile operator in Country C, to download an application developed in Country D, which stores and processes data in Country E, transmitting it through routers in Country F. The multitude of parties involved in the 'app stack'; automated computer to computer data sharing; cross border data flows; and opaque privacy policies all mean the app economy poses novel challenges to the Current Framework.

A smart new world

Not only computers are connected to the Internet these days, but also an increasing array of objects communicate with each other to create the so-called 'internet of things'. Whether it is inventory on the shelves of a supermarket, cars on a highway, suitcases in an airport, clothes, passports, or electric appliances, more and more objects are connected to information networks, effectively filling up our environment with billions of insect-size networked computers. This brings substantial benefits to government, business, and consumers, yet also generates novel privacy risks.

RFID

Radio-frequency identification (RFID) enables wireless data collection by readers from electronic tags attached to or embedded in objects, and potentially also people.[30] RFID systems give objects a unique identity, providing identification or location information and increasing efficiencies, such as by reducing warehousing and distribution costs, improving forecasting and planning, minimizing time to payment, or reporting patients' medical conditions without intrusive procedures. At the same time, RFID facilitates pervasive tracking, including monitoring individuals' location; enables the collection of personal data without data subject awareness; and may allow surreptitious tag scanning and use of data for purposes adverse to the interests of data subjects.[31]

Smart grid

The 'smart grid' delivers electricity from suppliers to consumers using two-way digital technology to carry both electricity and information to and from consumers' homes.[32] It is used by electricity providers to save energy, reduce costs, increase transparency, and even control appliances at consumers' homes, notifying them when a refrigerator is underperforming or water heater left on. It can help increase efficiency through network management and peak load reduction, monitor power outages, prevent costly blackouts and brownouts, and identify unauthorized or unmetered electricity draws. At the same time, it allows for the monitoring of individuals' activities in their home, collecting data regarding their waking hours, vacation time, laundry and personal hygiene, TV usage, and even caffeine consumption.[33] Moreover, as plug-in hybrid electric vehicles are deployed and customers engage in electricity sales on the grid outside of their homes, information from smart transportation systems will be matched against smart grid data to create detailed user profiles.

Robotics[34]

Bill Gates predicted in 2006 that the consumer market for robots is now at a similar stage to that of the market for personal computers in the 1970s.[35] Given that there are currently billions of PCs in use by individuals all over the world, we can expect robots—reprogrammable multifunctional devices designed to perform tasks on their own—to become an increasingly common feature of our daily lives. In the near future, we may rely on robots to drive us to work, clean our homes, keep our children and pets company, help people with disabilities and perform complex medical operations. Now, we clearly do not want a robot to waste valuable energy on

29 But cf. <https://whatapp.org/>, a project by Stanford law professor Ryan Calo, allowing users and experts to review online and mobile apps and platforms for privacy, security, and openness.

30 Marisa Anne Pagnattaro, 'Getting Under Your Skin—Literally: RFID in the Employment Context', (2008) University of Illinois Journal of Law, Technology and Policy 237.

31 See Article 29 Data Protection Working Party, 'Opinion 5/2010 on the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications' (WP 175), 13 July 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp175_en.pdf>; Article 29 Data Protection Working Party, 'Working document on data protection issues related to RFID technology' (WP 105), 19 January 2005, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf>.

32 See Elias Leake Quinn and Adam Reed, 'Envisioning the Smart Grid: Network Architecture, Information Control, and the Public Policy Balancing Act' (2010) 81 University of Colorado Law Review 833.

33 Ann Cavoukian, 'SmartPrivacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation' (November 2009), available at <www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf>.

34 I address the privacy risks inherent in robotics without expanding the discussion to the world of artificial intelligence, which presents an additional set of ethical issues. For the seminal exposition see Joseph Weizenbaum, *Computers Power and Human Reason: From Judgment to Calculation* (W.H. Freeman and Company, 1976).

35 Bill Gates, 'A robot in every home' (January 2007) Scientific American 58–65.

blow drying a dry floor, but rather to spring into action once a child spills a glass of water. Hence, a unique and attractive feature of robots is that they not only perform tasks assigned to them, but also have the ability to sense, process, and record the world around them. As Ryan Calo recently put it, 'robots can go places humans cannot go [and] see things humans cannot see'.[36] Yet with the power to observe and process information comes the ability to survey.[37] The introduction into the home environment of surveillance tools with computer wired brains, perfect memory, online connectivity and GPS location awareness, has disturbing privacy implications. Furthermore, Calo points out a novel risk to privacy presented by robots that are built to resemble humans.[38] These humanoid robots may be anthropomorphized and allowed to enter into the truly intimate, personal sphere historically reserved for solitude and reflection.[39] Indeed, one researcher goes so far as to predict that by the year 2050, humans will love, marry, and have sex with robots.[40] In this case, the privacy harm can be nuanced, subtle, and restricted to the realm of feeling or even the subconscious. It therefore challenges not only the notion of harm under the Current Framework, but also Isaac Asimov's all-famous enunciation of the 'First Law of Robotics': 'A robot may not harm a human being'.[41]

The human body

Breakthroughs in medical science and genetics present some of the most perplexing dilemmas involving privacy and data protection.

Genetics and personalized medicine

New developments in pharmacogenomics and medical research, including genetic testing and the use of biological samples to develop personalized medicines, offer unique benefits not only for the health of individuals but also for medical research and public health.[42] They can help achieve breakthroughs in the eradication of disease, detection of genetic predispositions to certain ailments, and the development of personalized cures.[43] At the same time, such practices may reveal critical personal information not only about individual patients but also about their family and ancestry.[44] Medical and genetic information is of course highly sensitive and may have potential implications for discriminatory practices in employment, insurance, and the relations between citizen and state. A critical issue for both patients and industry is how to strip the health data of personal identifiers in order to eliminate or reduce privacy concerns, while at the same time retaining information that is useful for research.[45] Yet, as we have seen, the prospect of re-identification of de-identified data looms large over any attempt at effective anonymization. In addition, warehousing genetic data for research purposes raises the risk of its use for purposes not envisioned by the donors, including secondary research.[46] Additional quandaries concern the ownership of genetic samples; cross-border transfer of samples or data; and reporting to the donor on the outcomes of the research.

Biometrics

The human body is being used to harness data not only for genetic testing but also for authentication and

36 M. Ryan Calo, 'Robots and Privacy', in Patrick Lin, George Bekey, and Keith Abney (eds), *Robot Ethics: The Ethical and Social Implications of Robotics* ((MIT Press, Cambridge, MA forthcoming 2011).

37 See, eg, Rafe Needleman, 'Flying surveillance robots coming soon from Aeryon' (29 July 2009) Cnet News, available at http://news.cnet.com/8301-19882_3-10299166-250.html; also see Noah Shachtman, 'Petagon's Cyborg Beetle Spies Take Off' (28 January 2009) Wired, available at www.wired.com/dangerroom/2009/01/pentagons-cybor/ (reporting on a Pentagon plan to inject surveillance technology into live insects making them remotely controllable audio devices—essentially 'bugging the bugs').

38 See generally Isaac Asimov and Karen A. Frenkel, *Robots: Machines in Man's Image* (Harmony Books, 1985); the classic of course is Mary Shelley, *Frankenstein* (Bantam Classic, 2003), first published in 1818.

39 Calo, see n 36 above, at pp. 10–14; also see M. Ryan Calo, 'People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship' (2010) 114 Penn State Law Review 809; Ian Kerr, 'Bots, Babes, and the Californication of Commerce' (2004) 1 University of Ottawa Law & Technology Journal 285.

40 David Levy, *Love + Sex with Robots: The Evolution of Human-Robot Relationships* (Harper Perennial, 2008).

41 More accurately, Asimov's first law reads: 'A robot may not injure a human being or, through inaction, allow a human being to come to harm'. Isaac Asimov, *Runaround* in *I, Robot* (Gnome Press, 1950); also see Roger Clarke, 'Asimov's Laws of Robotics: Implications for Information Technology', (December 1993) 26 IEEE Computer 53–61 (Part I) and (January 1994) 27 IEEE Computer 57–66 (Part II), available at <www.rogerclarke.com/SOS/Asimov.html>.

42 The discussion here sets aside other genetic databases, notably ones established by law enforcement authorities to help investigate crimes and apprehend criminals. See S. and *Marper v The United Kingdom* 30562/04 [2008] ECHR 1581 (4 December 2008).

43 Teresa Kelton, 'Pharmacogenomics: The Re-Discovery of the Concept of Tailored Drug Therapy and Personalized Medicine' (2007) 19(3) Health Lawyer 1.

44 Berrie Rebecca Goldman, 'Pharmacogenomics: Privacy in the Era of Personalized Medicine' (2005) 4 Northwestern Journal of Technology and Intellectual Property 83; Jennifer Gniady, 'Regulating Direct to Consumer Genetic Testing' (2008) 76 Fordham Law Review 2429.

45 Center for Democracy & Technology, 'Encouraging the Use of, and Rethinking Protections for De-Identified (and "Anonymized") Health Data', June 2009, available at <www.cdt.org/files/pdfs/20090625_deidentify.pdf>.

46 See, eg, Amy Harmon, 'Indian Tribe Wins Fight to Limit Research of Its DNA' (21 April 2010) NY Times, available at <www.nytimes.com/2010/04/22/us/22dna.html>. The article describes how members of a small Native-American tribe had given DNA samples to university researchers in the hope that they might provide genetic clues to the tribe's high rate of diabetes. But they learned that their blood samples had been used to study many other things, including mental illness and theories of the tribe's geographical origins that contradict their traditional stories.

identification by governments, employers, and service providers. The concept of identifying people using unique biometric features is not new; fingerprints were used as far back as ancient Egypt and Babylon. Yet recent years have seen a proliferation of biometric identification in both the public and private sector, including iris and retina scans, hand geometry, ear shape, and recently voice, odor, scent, and sweat pore analysis. Perhaps most troubling from a privacy perspective is facial recognition technology. The increasing ubiquity of surveillance cameras (CCTV)[47] and integration of face recognition into social media[48] raise the spectre of pervasive surveillance. In addition, unique behavioural traits are increasingly being used for identification ('behaviometrics'), including signature verification, typing rhythm and keystroke analysis, and the study of gait. The use of biometrics raises privacy risks, including identity theft, function creep, and government surveillance.

II. A new generation of users

In the 1980s, when the Current Framework entered into force, people still used fixed line telephones and postal mail to communicate. They searched for information for research and recreation in public libraries; and purchased flight tickets in travel agencies, music in (vinyl) record stores, and second hand products in flea markets. They watched TV shows and were obliged to wait an entire week between episodes. Most of them did not have personal computers, and the ones that did had models named Commodore 64 and IBM XT.

The changes undergone by users are reflected in more than just the new technologies they use. Information, including personal data, has emerged from being a side product of economic activity to become the fuel and driving force of the new economy. Businesses today, in financial services, telecom, health, and online services, often stand to gain more from the data and meta-data they accumulate than from their core economic activities.

I outline below the major characteristics of a new generation of users that challenge the Current Framework and require innovative solutions.

Information consumers

The advent of online search engines has revolutionized access to information, putting nearly infinite amounts of data, including third parties' personal data, at our fingertips. Google, the undisputed king of online search, enjoys access to vast amounts of personal data, creating a privacy problem dubbed by Princeton computer scientist Edward Felten as 'perhaps the most difficult privacy [problem] in all of human history.'[49]

Search engine privacy comes in two flavours.[50] First, there is the privacy interest of the search *object*. The power of search has significantly reduced the transaction costs of compiling digital dossiers profiling a person's activities. Before the arrival of search engines, we enjoyed a degree of 'practical obscurity', protecting our privacy interest in issues such as litigation, asset ownership, past employment, and political opinion. Although such information has always been in the public sphere, it was invisible *de facto* to all but skilled investigators or highly motivated researchers, due to the practical difficulty and costs involved in uncovering and compiling the data. Today the search for such information has become instant and costless.[51] Moreover, not only have other people's data become easy to find, search, and retrieve, but they are also increasingly persistent and difficult to discard. Jeffrey Rosen recently described this problem as 'a challenge that, in big and small ways, is confronting millions of people around the globe: how best to live our lives in a world where the Internet records everything and forgets nothing—where every online photo, status update, Twitter post and blog entry by and about us can be stored forever.'[52]

Background searches and the compilation of detailed personal profiles are no longer restricted to the realm of security agencies, private investigators or data warehouses; they can be performed individually by curious neighbours, prospective employers, or hopeful dates. Indeed, US Supreme Court Justice Antonin Scalia

47 See, eg, Ting Shan, Shaokang Chen, Conrad Sanderson, and Brian Lovell, 'Towards Robust Face Recognition for Intelligent-CCTV based Surveillance using One Gallery Image' (2007) IEEE Conference on Advanced Video and Signal Based Surveillance 470–75.

48 Roi Carthy, 'Face.com Brings Facial Recognition To Facebook Photos' (24 March 2009) Techcrunch available at <http://techcrunch.com/2009/03/24/facecom-brings-facial-recognition-to-facebook-photos-we-have-invites>.

49 The Economist, 'Inside the Googleplex', 30 August 2007, available at <www.economist.com/node/9719610>.

50 Omer Tene, 'What Google Knows: Privacy and Internet Search Engines' (2008) Utah Law Review 1433; Article 29 Data Protection Working Party, 'Opinion 1/2008 on data protection issues related to search engines', (WP 148),4 April 2008, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf>.

51 See, eg, Daniel Solove, 'Justice Scalia's Dossier: Interesting Issues about Privacy and Ethics', Concurring Opinions Blog, 29 April 2009, available at <www.concurringopinions.com/archives/2009/04/justice_scalias_2.html>.

52 Jeffrey Rosen, 'The Web Means the End of Forgetting' (21 July 2010) NY Times, available at <www.nytimes.com/2010/07/25/magazine/25privacy-t2.html>; Michael Fertik and David Thompson, *Wild West 2.0: How to Protect and Restore Your Online Reputation on the Untamed Social Frontier* (American Management Association, 2010).

recently received a stark reminder of the powers of amateur search: after having publicly made the comment that treating much of the information available online as private was 'silly', Justice Scalia was incensed when students from a Fordham Law School Information Privacy Law class assembled a 15-page digital dossier ripe with information about him and his family. That the information was compiled from publicly available online sources did little to alleviate Justice Scalia's privacy harm.[53] Viktor Mayer-Schönberger believes this challenge can only be met by setting an 'expiration date' for personal data, effectively enforcing a 'right to oblivion' through technological means.[54]

The second problem afflicting Internet search engines concerns the privacy interest of the *user conducting the search*. Search engines maintain comprehensive logs detailing each user's search history. Every day, hundreds of millions of users provide Google with unfettered access to their interests, needs, desires, fears, and pleasures. In doing so, they often divulge information that is medical, financial, sexual, or otherwise intimate in nature. Many users are already aware today that virtually all of this information is digitally logged and stored in a form which may facilitate their identification for various purposes, including not only behavioural targeting but also prosecution by the government[55] or pursuit by private litigants.[56] As John Battelle memorably put it, '[l]ink by link, click by click, search is building possibly the most lasting, ponderous, and significant cultural artifact in the history of humankind: the Database of Intentions.'[57] There has never quite been an offline equivalent to this individual and collective 'mental X-ray' of users online.[58] By consuming massive amounts of information in a scope and scale unimaginable just a few years ago, users have become the 'transparent citizens' foretold by David Brin,[59] subject to profiling and commodification. 'You are what you eat' has given way to 'you are what you read' online. And while search engines epitomize this phenomenon, they are by no means the sole actors engaged in monitoring and analysing their users' interests and tastes. Covertly and overtly, illicitly and with user consent, using tools as sophisticated as semantic analysers and as simple as cookies, intelligence agencies, law enforcement authorities, Internet service providers, Web publishers, advertisers and ad networks—are all engaged in close observation of the new information consumer. The newest playing grounds for analytics algorithms are online social networks and the 'social graphs' they create.[60]

Information producers

One of the most significant developments in the online environment over the past few years has been the meteoric rise of user generated content and social media. Facebook, first launched in 2004, had 100 million users in late 2008 and had quintupled that amount two years later to become the second most popular website online.[61] Twitter, created in 2006, had 100 million registered users in 2010, and was rated by Alexa as the eleventh most popular web site, five places ahead of online giant Amazon. The third most popular web site after Google and Facebook, YouTube, is an outlet for user generated content.

Online users can benefit from posting information online, including significant amounts of personal data, such as photos and videos; friends lists; political, ideological, and artistic tastes; social relationships and sexual interests. And while throngs of middle aged and older users are joining the bandwagon, it is the younger generation that is blazing the path to the creation and development of a digital persona.[62] No matter how hard you try, your kids will typically have

53 Daniel Solove, 'Justice Scalia's Dossier: Interesting Issues about Privacy and Ethics' (29 April 2009) Concurring Opinion Blog, available at <www.concurringopinions.com/archives/2009/04/justice_scalias_2.html>.

54 Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, 2009).

55 See *Gonzales v Google, Inc.*, 234 F.R.D. 674 (N.D.Cal. 2006) (US government subpoenas AOL, Google, Microsoft, and Yahoo, for the addresses of all web sites indexed by the search engines as well as every search term entered by search engine users during a period of two months.)

56 *Cohen v Google, Inc.*, No. 100012/09, 2009 WL 2883410 (N.Y. Sup. Ct. 17 August 2009) (plaintiff seeks court order to force Google to unmask the real identity of a party named 'Anonymous Blogger'); Civ. App. 1622/09 *Google Israel v Brokertov* (1 July 2010) (Israeli Supreme Court refuses to order Google to unmask anonymous defendant).

57 John Battelle, *The Search: How Google and its Rivals Rewrote the Rules of Business and Transformed our Culture* ((Portfolio, 2005).

58 See, eg, Google Flu Trends, available at <www.google.org/flutrends/>; Google follows online searches for flu symptoms and keywords related to the flu (such as muscle aches, coughing, chest pain, thermometer, and others), to detect regional outbreaks of the flu even before they are reported by the Centers for Disease Control and Prevention.

59 David Brin, *The transparent society: will technology force us to choose between privacy and freedom?* (Perseus Books, 1998).

60 'Social graphs' are defined by Brad Fitzpatrick as 'the global mapping of everybody and how they're related'. Brad Fitzpatrick, 'Thoughts on the Social Graph' (17 August 2007) Bradfitz Blog, available at <http://bradfitz.com/social-graph-problem/>; see 'Untangling the social web' (2 September 2010) The Economist, available at <www.economist.com/node/16910031> (registration may be required).

61 Caroline McCarthy, 'Facebook's half-billion milestone is official' (21 July 2010) CNET News, available at <http://news.cnet.com/8301-13577_3-20011227-36.html?tag=nl.e496>.

62 'Looking across the range of items we queried, internet-using Millennials were much more likely than older cohorts to report that at least five pieces of information were available online for others to see.'

more Facebook friends than you do (you are not one of them, of course), and communicate with several of them at the same time at any given time.

The tide of user posted personal information is constantly rising. For example, in November 2007, Facebook launched Beacon, a service allowing users to share with their friends their purchasing habits on affiliated websites. Buy a book, a DVD, or tickets to a concert online—and your friends get notified, with a link to the merchandise. Friend brings friend advertising is considered to be highly effective, given that users often trust their friends' taste and choices more than they do Hollywood celebrities appearing in multi-million dollar ad campaigns.[63] In just a few weeks, however, Facebook hurried to withdraw the service in the face of online petitions and user outrage over the privacy infringement.[64] In addition, Facebook had to settle a consequent class action law suit paying an amount of $9.5 million (minus $3 million for legal fees), to create a 'digital trust fund' dedicated to studying online privacy.[65] Yet not long after the demise of Facebook Beacon, new websites emerged, such as Swipely[66] and Blippy,[67] providing essentially the same service and drawing a significant number of users.[68] Other popular newcomer sites encourage users to enter into webcam-based video chats with randomly selected strangers.[69] The most significant recent trend, meanwhile, is of location based social networking services and mobile applications, which allow users to broadcast their precise geographical location to the digital world.[70]

The information posted to social media may be detrimental to users' privacy and reputation. Numerous media stories report the loss of jobs, college admissions, or relationships due to the posting of photos taken in different states of intoxication.[71] A recent Pew report finds that Internet users are now more likely to search for social networking profiles than they are for information about someone's professional accomplishments or interests.[72] This means that a Facebook profile and information posted therein may be more conducive to one's finding a job (or date) than one's resume or bio on an employer website. This is exacerbated for young people, since by the time they are 30 or 40 they will have formed comprehensive digital identities spanning decades of information uploads by themselves and third parties. As John Palfrey and Urs Gasser note: 'Time, in this sense, is not on the side of those who are born digital. No one has yet been born digital and lived into adulthood. No one has yet experienced the aggregate effect of living a digitally mediated life over the course of eighty or ninety years.'[73]

Browsing through Facebook profiles and status updates, Twitter tweets, and Foursquare 'check ins' of youngsters today, one might get the impression that youths simply do not care about privacy. Yet this would be a misconception. In fact, empirical research consistently proves the contrary. The Pew Report, for example, shows young adults (aged 18–29) are more likely than older users to limit the amount of information available about them online. Moreover, it finds that among users of social networking sites, young adults are the most proactive in customizing their privacy settings and restricting who can see various updates.[74] Similar results have been reported by a group of Berkeley researchers, suggesting 'that young-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.'[75] Alessandro Acquisti and Ralph Gross

Mary Madden and Aaron Smith, Reputation Management Online: How people monitor and maintain their identity through search and social media, (26 May 2010) Pew Internet & American Life Project,available at <www.pewinternet.org/Reports/2010/Reputation-Management.aspx> (hereinafter Pew Report).

63 Louise Story, 'Facebook Is Marketing Your Brand Preferences (With Your Permission)', NY Times, 7 November 2007, available at <http://www.nytimes.com/2007/11/07/technology/07adco.html>.

64 Louise Story, 'Apologetic, Facebook Changes Ad Program' (6 December 2007) NY Times, available at <www.nytimes.com/2007/12/06/technology/06facebook.html>.

65 *Lane v Facebook, Inc.*, Case No. 5:08-CV-03845-RS (N.D. Cal. 12 August 2008).

66 Available at <http://swipely.com/>.

67 Available at <http://blippy.com/>.

68 Brad Stone, 'For Web's New Wave, Sharing Details Is the Point' (22 April 2010) NY Times, available at <http://dealbook.blogs.nytimes.com/2010/04/23/for-webs-new-wave-sharing-details-is-the-point>.

69 See, eg, Chatroulette, available at <http://chatroulette.com/>; see Brad Stone, 'Chatroulette's Creator, 17, Introduces Himself' (13 February 2010) NY Times, available at <http://bits.blogs.nytimes.com/2010/02/13/chatroulettes-founder-17-introduces-himself/>.

70 See Foursquare, available at <http://foursquare.com>; Gowalla, available at <http://gowalla.com>; Loopt, available at <http://www.loopt.com>. Facebook recently launched its own location based service, Places; see Maggie Shiels, 'Facebook launches Places location based service' (19 August 2010) BBC available at <www.bbc.co.uk/news/technology-11020795>.

71 Stephanie Goldberg, 'Young job-seekers hiding their Facebook pages' (29 March 2010) CNN, available at <http://edition.cnn.com/2010/TECH/03/29/facebook.job-seekers/index.html>.

72 Pew Report, see n 62 above.

73 Palfrey and Gasser, see n 7 above.

74 Also see danah boyd and Eszter Hargittai, 'Facebook Privacy Settings: Who Cares?' (2 August 2010) 15(8) First Monday, available at <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086/2589>.

75 Chris Hoofnagle, Jennifer King, Su Li, and Joseph Turow, 'How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies?' (14 April 2010), available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864>.

found that undergraduate Facebook users ranked privacy as an extremely important public issue, more so even than the threat of terrorism.[76]

What accounts for this apparent discrepancy? If users care so much about privacy why do they keep posting sensitive data online? Part of the answer is that young people do not conceive social media as a 'public' space, reflecting a shift in our understanding of the delineation of what is public and private.[77] Facebook is where they exchange information and communicate with their peers. Enter a parent or a teacher, and the party is over. Not communicating online is not really an option; it means acting like a hermit. As Kate Raynes-Goldie observes, 'the mass adoption of Facebook, especially among younger users in North American urban centers, makes it increasingly important for one's social life to be on the site.'[78]

What complicates matters even more is the fact that while not 'public', Facebook is clearly not a 'private' space, at least not in the traditional sense. While apparently a closed network of friends, the concept of 'friend' on a social network is quite distinct from that in the offline world. danah boyd explains that 'because of how these sites function, there is no distinction between siblings, lovers, schoolmates, and strangers. They are all lumped under one category: Friends'.[79] Moreover, certain information posted on social networking sites is publicly available to users and non-users alike, and is even searchable by search engines such as Google.[80] Through the information, photos, comments, and videos they post, as well as 'friend' selections, users intend to project an image to a real or imagined audience. They 'are rewarded with jobs, dates, and attention for displaying themselves in an easily-consumed public way using tropes of consumer culture.'[81] Indeed, some users may attain a degree of celebrity (or micro-celebrity)[82] in the process.[83]

This blurring of boundaries between private and public resonates in Helen Nissenbaum's theory of 'contextual integrity'.[84] Nissenbaum argues that '[a] central tenet of contextual integrity is that there are no arenas of life not governed by norms of information flow, no information or spheres of life for which 'anything goes'.[85] Hence, the crucial issue is not whether the information posted on a Facebook profile is 'private' or 'public', but whether Facebook's actions on such information breaches contextual integrity. This, in turn, may be assessed by reverting to the celebrated decision of the US Supreme Court in *Katz v United States*, [86] which rules that a right to privacy exists where an individual has a 'reasonable expectation of privacy'.[87] It is the thwarting of user expectations through changes in privacy defaults[88] or unexpected uses of data[89] that creates what danah boyd coined a 'privacy FAIL'.[90] A recent case in point is the Google Buzz affair. Google mistakenly interspersed users' wholly-private (Gmail, an email service) and semi-public (Buzz, a social network) networks, stirring a privacy maelstrom which

76 Alessandro Acquisti and Ralph Gross, 'Imagined communities: Awareness, information sharing, and privacy on the Facebook' (2006) Privacy Enhancing Technologies (PET) Workshop, Lecture Notes in Computer Science 4258, Springer, 36–58, available at <www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf>.

77 danah boyd argues that '[i]t's easy to think that "public" and "private" are binaries. . . . But this binary logic isn't good enough for understanding what people mean when they talk about privacy. What people experience when they talk about privacy is more complicated than what can be instantiated in a byte.' danah boyd, 'Making Sense of Privacy and Publicity' (13 March 2010) SXSW, available at <www.danah.org/papers/talks/2010/SXSW2010.html>.

78 Kate Raynes-Goldie, 'Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook' (2010) 15 (1) First Monday, available at <http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432>.

79 danah boyd, 'Friends, Friendsters, and MySpace Top 8: Writing Community Into Being on Social Network Sites', (December 2006) 11 (12) First Monday, available at <www.firstmonday.org/issues/issue11_12/boyd/index.html >.

80 See Kevin Bankston, 'Facebook's New Privacy Changes: The Good, The Bad, and The Ugly' (9 December 2009) Electronic Frontier Foundation Blog, available at <www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>; Michael Zimmer, ' "But the Data is Already Public": On the Ethics of Research in Facebook' (4 June 2010) Ethics and Information Technology.

81 Alice E. Marwick and danah boyd, 'I Tweet Honestly, I Tweet Passionately: Twitter Users, Context Collapse, and the Imagined Audience' (7 July 2010) New Media Society, available at <http://nms.sagepub.com/content/early/2010/06/22/1461444810365313>.

82 Clive Thompson, 'The Age of Microcelebrity: Why Everyone's a Little Brad Pitt' (27 November 2007) Wired Magazine, available at <www.wired.com/techbiz/people/magazine/15-12/st_thompson>.

83 Theresa M. Senft, *Camgirls: Celebrity and Community in the Age of Social Networks* (Peter Lang 2008).

84 Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford University Press 2009).

85 Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79 Washington Law Review 101. Nissenbaum points out that 'public and private define a dichotomy of spheres that have proven useful in legal and political inquiry. Robust intuitions about privacy norms, however, seem to be rooted in the details of rather more limited contexts, spheres, or stereotypic situations' *Ibid*, at p. 119.

86 *Katz v United States*, 389 U.S. 347 (1967).

87 *Ibid*, at pp. 360–61 (Harlan, J., concurring).

88 For two recent examples, including the December 2009 changes in Facebook's privacy policy and the launch of Google Buzz as a social network automatically opting-in Google Mail users, see Kevin Bankston, 'Facebook's New Privacy Changes: The Good, The Bad, and The Ugly' (9 December 2009) *Electronic Frontier Foundation Blog*, available at <www.eff.org/deeplinks/2009/12/facebooks-new-privacy-changes-good-bad-and-ugly>; Miguel Helft, 'Anger Leads to Apology From Google About Buzz' (14 February 2010) NY Times, available at <www.nytimes.com/2010/02/15/technology/internet/15google.html>.

89 Jacqui Cheng, 'Facebook reevaluating Beacon after privacy outcry, possible FTC complaint' (29 November 2007) ArsTechnica, available at <http://arstechnica.com/tech-policy/news/2007/11/facebook-reevaluating-beacon-after-privacy-outcry-possible-ftc-complaint.ars>.

90 boyd, see n 77 above.

cost the company at least $8.5 million—the sum of a class action settlement.[91]

An additional problem is that users often hurry to adopt new social media tools with little consideration of providers' back-end capability to record and track their activity over time, and little foresight into the long-term aggregation and reuse of their personal information.[92] Thus, users enthusiastically adopt new technologies, and in the process unwittingly create permanent records of their online activities or geographical whereabouts. Indeed, the Berkeley researchers conclude that 'young adults . . . are more likely to believe that the law protects them both online and off. This lack of knowledge in a tempting environment, rather than a cavalier lack of concern regarding privacy, may be an important reason large numbers of them engage with the digital world in a seemingly unconcerned manner.'[93] Such cognitive failures, certainly when associated with young users, necessitate regulatory response.

When revising the Current Framework, policy makers must account for changes in the delineation of what is private and public. Understanding that private and public are not binaries; that 'what people experience when they talk about privacy is more complicated than what can be instantiated in a byte';[94] is the first step toward addressing the perplexing challenges presented to privacy by a generation of users who think, reflect, communicate—indeed live—online. Social media must convey to users the essence and consequences of their choices, and clarify the tradeoff between publicity and privacy, in order to enable them to make free and informed choices.

III. A new generation of governance

Where do these changes leave us? The Current Framework is clearly straining to keep up with the technology locomotive. Indeed, the most fundamental concept in the Current Framework, that of personal data, has become fuzzy, and the distinction between it and non-personal data muddled. Could personal data, defined as data relating 'to an identified or identifiable natural person', continue to be the focal point for legal protection in a landscape where even anonymized data could have significant privacy consequences? The use of cookies, deep packet inspection, RFID, and key-coded genetic data, together with enhanced analytic capacities, further clouds the Current Framework's fundamental term. The ability of behavioural targeting firms to pervasively track users without deciphering their specific identities seems to have made the 'identifiability' aspect of the definition of personal data obsolete.

Moreover, the fundamental distinction between what is public and private is eroding, requiring a new paradigm that protects privacy in public or semi-public spaces. This is evident in the streets of megacities such as London, once the epitome of privacy and anonymity, which are now increasingly monitored by an intricate web of surveillance cameras backed up by face recognition software.[95] It arises in the context of social media sites, where information is partially broadcast to the world, partially shared with friends; and the defaults of what is public and what is private are inversed—public by default, private by choice. The Current Framework, established in a black and white era where the private and public spheres rarely coincided, often overlooks such shades of gray. Lawmakers must now be ready to accord users a degree of privacy in public, setting limits on what may be done with personal information disclosed in the 'semi-public' sphere.[96]

The notice and choice paradigm in the United States, or transparency principle in EU parlance, has been stripped of meaning by lengthy, complex privacy policies of little use to individuals.[97] In addition, the promises made in a privacy policy often ring hollow given the right reserved by service providers to unilaterally

91 Tom Krazit, 'Google settles Buzz lawsuit for $8.5M' (3 September 2010) Cnet News, available at http://news.cnet.com/8301-30684_3-20015620-265.html. This episode clearly cost Google more than the out of pocket settlement sum, given the dent in user trust for a company which depends on almost unfettered access to user data. See, eg, Miguel Helft, 'Critics Say Google Invades Privacy with New Service' (12 February 2010) NY Times, available at <http://www.nytimes.com/2010/02/13/technology/internet/13google.html?_r=1>. Also see danah boyd, 'Making Sense of Privacy and Publicity' (13 March 2010) SXSW, available at <http://www.danah.org/papers/talks/2010/SXSW2010.html>.

92 See, eg, Michael Zimmer, '41% of Facebook Users Share Personal Information with a Frog' (19 August 2007) Michael Zimmer.org blog, available at <http://michaelzimmer.org/2007/08/19/41-of-facebook-users-share-personal-information-with-a-frog/>.

93 Hoofnagle *et al.*, seen 75 above.

94 boyd, see n 77 above.

95 See Information Commissioner's Office, *A Report on the Surveillance Society* (September 2006), available at <www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf>.

96 Consider the recent attempt in Germany to limit employers' use of Facebook for screening job applicants. David Jolly, 'Germany Plans Limits on Facebook Use in Hiring' (25 August 2010) NY Times, available at <www.nytimes.com/2010/08/26/business/global/26fbook.html>.

97 For a new approach, see Corey Ciocchetti, 'The Future of Privacy Policies: A Privacy Nutrition Label Filled with Fair Information Practices' (2009) 26 John Marshall Journal of Computer and Information Law 1.

modify or amend its terms at will. Indeed, some commentators argue that the illusion of control affects individuals' propensity to disclose sensitive information even when the objective risks associated with such disclosures do not change or, in fact, worsen.[98] At the same time, businesses find themselves in a quandary concerning the level of specificity and granularity appropriate for privacy policies. Facebook, for example, has recently experienced a case of 'damned if you do, damned if you don't', where users first complained that its privacy policy is vague and overly broad, only to argue later that changes made it so granular as to become tedious and incomprehensible.[99]

The allocation of obligations among 'controllers' and 'processors' is another fundamental concept in distress.[100] As has been made evident by the SWIFT case,[101] the increasingly collaborative manner in which businesses operate precludes a neat dichotomy between controllers and processors. Many decisions involving personal data have become a joint exercise between customers and layers upon layers of service providers. With the rise of cloud computing and the proliferation of online and mobile apps, not only the identity but also the location of data controllers have become indeterminate. Meanwhile, in the arena of social media, it is not clear who should be considered data controller, the user who posts information voluntarily and makes privacy choices, or the social network service which stores the data, processes and secures it, and sets privacy defaults?[102] This, in turn, complicates the allocation of governing law and personal jurisdiction, which have traditionally hinged on the main place of establishment of the controller.[103]

The torrent of personal data collected and retained by telecom operators, online service providers, social networks, and financial institutions, hampers our ability to forget past transgressions and go on with our lives. Photos posted online by teenagers may return to haunt them decades later as they search for jobs. Missing a mortgage payment or failing to pay a bill may irreversibly taint one's credit history. The ease and low cost of data retention, coupled with government interest in private sector data retention, necessitate a new policy towards what has become known as 'the right to oblivion'.[104]

Perhaps the most contentious of all provisions of the EU Directive are the restrictions on global data transfers.[105] These restrictions set the stage for the development of a vast industry of legal services meant to overcome regulatory burdens, including through the use of the US Safe Harbor system, binding corporate rules, model contractual clauses, and the solicitation of data subject consent. More than any other provision in the Current Framework, these requirements have proven unrealistic, overly bureaucratic, costly and ineffective.[106] They were developed at a time when data transfers occurred in bulk between stand-alone computers typically housing the massive databases of government or large corporate organizations.

All this calls for a fundamental reshuffle of the Current Framework; for the application of a legal regime attuned to a risk of harm continuum,[107] rather than a dichotomy between personal and non-personal data, or

98 Laura Brandimarte, Alessandro Acquisti, and George Loewenstein, 'Misplaced Confidences: Privacy and the Control Paradox', in *Ninth Annual Workshop on the Economics of Information Security (WEIS)*, 7–8 June 2010, Harvard University, available at <http://weis2010.econinfosec.org/papers/session2/weis2010_brandimarte.pdf>.

99 'Facebook Privacy: A Bewildering Tangle of Options (Illustration)' (12 May 2010) NY Times, available at <www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html>.

100 Article 29 Data Protection Working Party, 'Opinion 1/2010 on the concepts of "controller" and "processor" ' (WP 169), 16 February 2010, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp169_en.pdf>.

101 Article 29 Data Protection Working Party, 'Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)' (WP 128), 22 November 2006, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp128_en.pdf>.

102 See, eg, Rebecca Wong, 'Social networking: A conceptual analysis of a data controller', (2009) 14 (5) *Communications Law* 142; Article 29 Data Protection Working Party, 'Opinion 5/2009 on Social Networking' (WP 163), 12 June 2009, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp163_en.pdf>.

103 Article 4(1)(a) of the Directive. See Christopher Kuner, 'Internet Jurisdiction and Data Protection Law: An International Legal Analysis' (2010) 18 (2) International Journal of Law and Information Technology 176 .

104 Mayer-Schönberger, see n 54 above; also see David Reid, 'France ponders right-to-forget law' (8 January 2010) BBC, available at <http://news.bbc.co.uk/2/hi/programmes/click_online/8447742.stm>.

105 Articles 25–26 of the Directive. Most pertinently, Article 25(1) provides that 'The Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection.' See generally, Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (2nd edn Oxford University Press, Oxford 2007) 151–232.

106 See recent discussion in Article 29 Data Protection Working Party, 'Opinion 3/2010 on the principle of accountability' (WP 173), 13 July 2010, paragraphs 55–57, available at <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2010/wp173_en.pdf>.

107 Requiring proof of harm to establish a privacy cause of action is highly contentious, given the difficulty individuals often face when trying to prove or assess the non-pecuniary damages associated with privacy infringements. See recently M. Ryan Calo, 'The Boundaries of Privacy Harm' (forthcoming, 2011) 86 Indiana Law Journal. The discussion of privacy harms exceeds the scope of this paper. The 'risk of harm continuum' I refer to in the text should be read broadly to include not only objective, monetary damages but also subjective infringement of dignity and personal autonomy. See generally Ruth Gavison, 'Privacy and the Limits of Law' (1980) 89 Yale Law Journal 421.

private and public spheres; for a new approach to notice and choice emphasizing user awareness and understanding, rather than corporate disclaimers of liability; for an allocation of responsibility according to data use and risks to data subjects, rather than a formal dichotomy between controllers and processors; for a sensible balance between data retention needs and individuals' '*droit à l'oubli*'; and for cross border data transfers governed by accountability and ongoing responsibility, rather than arbitrary barriers and bureaucratic form filling.

doi:10.1093/idpl/ipq003