2014

Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm

McKay Cunningham
Concordia University School of Law, mccunningham@cu-portland.edu

Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm

McKay Cunningham*

Keywords
INTERNET OF THINGS; PERSONAL INFORMATION; PRIVACY; PASSIVE DATA COLLECTION; DIRECTIVE

Abstract
The disparities inherent in various national privacy laws have come into sharper contrast as access to information grows and formerly domestic markets become international. Information flow does not adhere to national boundary lines. Increasingly, laws that seek to protect informational privacy do not either. The European Union took a bold approach by limiting access to its markets for those who failed to observe its strict law designed to protect personal information. The 1995 Directive (and 2014 Regulatory Amendment) embody this approach as they: (1) broadly define personal information; (2) broadly define those who process and control personal information; (3) restrict transfer of personal information to those who cannot demonstrate compliance. Tellingly, the Directive does not limit its scope to certain industries or practices, but requires privacy controls across the board, regardless of whether the processor is a healthcare provider, pastry chef or girl scout.

To many, the Directive has failed. While the global trend toward adopting laws similar to the Directive suggests that many States value privacy rights, commentators and empirical studies reveal significant shortcomings. The Directive outlaws harmless activities while allowing exceptions that threaten to swallow the rule. It is simultaneously over-inclusive and under-inclusive. National governments enjoy wide latitude to collect and use personal information under the guise of national security. Perhaps more concerning, technology continues to leapfrog. Information privacy is made continually more difficult with each new "app" and innovation. The Internet of Things is more probable than speculative. Radio-frequency identification is a predicate to computer identification and assimilation of everyday physical objects, enabling the use of these objects to be monitored and inventoried by computers. Tagging and monitoring objects could similarly be accomplished by other technologies like near field communication, barcodes, QR codes and digital watermarking, raising the legitimate argument that informational privacy—at least as envisioned in the 1995 Directive's absolute terms—is impossible.

Informational privacy cannot be accomplished by declaring it a fundamental right and outlawing all processing of personal information. To legally realise and enforce a privacy right in personal information, incremental, graduated, and practical legislation better achieve the goal than sweeping proclamations that have applications to actions unrelated to the harms associated with the absence of the right. With information privacy in particular, a capacious claim of right to all personal information undermines legal enforcement because the harms attending lack of privacy are too often ill-defined and misunderstood. As a result, legal realization of a claimed privacy right in the Age of Information should proceed incrementally and begin with the industries, practices, and

* Associate Professor, Concordia School of Law.

processes that cause the most harm by flouting informational privacy. Data mining and data aggregation industries, for example, collect, aggregate and resell personal information without express consent. A targeted prohibition of this industry would reduce financial incentives of the most conspicuous violators and alleviate some of the most egregious privacy infractions.

A graduated legal scheme also reduces undue and overbroad Internet regulation. While the right to privacy has been recognised and legally supported in one way or another for centuries, it has not faced the emerging and countervailing Age of Information until now. Current omnibus international legislation reflects the impossibility of legally protecting all privacy in the Age of Information; it also illustrates the need for a refined and practical legal scheme that gradually and directly targets the harms associated with privacy violations.

I. Introduction

Keeping our privacy is more unlikely than ever. Simply by moving from one place to another we exude data exhaust. This data exhaust, much of it personal, is valuable and increasingly collected without our knowing it. Everyday objects equipped with sensors that communicate to the Internet are commonplace and more are on the way. Over 200 billion worldwide are expected by 2020.[1]

Cisco projects that 'pretty much everything you can imagine will wake up.'[2] Already libraries tag and track every book in the collection,[3] dentists graft sensors into toothbrushes[4] and beer mugs with tilt sensors transmit consumption rates.[5] Smart phones, replete with apps that collect data exhaust, gather worlds of information like steps taken in a day, heartbeats per minute, driving logistics, hemoglobin, sleep habits and much more.[6] Rooftop video cameras, license plate readers, automobile GPS and smart phones log and report locational data by precise date and time.[7]

---

1 Time, Bajarin, T., *The Next Big Thing for Tech: The Internet of Everything*, 13 January 2014, available online at <time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/> (accessed 10 October 2014).

2 CISCO, *What is the Internet of Everything?*, available online at <cisco.com/web/tomorrow-starts-here/ioe/index.html> (accessed 10 October 2014).

3 Electric Engineering and Computer Science, Molnar, D., and Wanger, D., *Privacy and Security in Library RFID: Issues, Practices and Architectures*, 26–28 October 2004, available online at <cs.berkeley.edu/~daw/papers/librfid-ccs04.pdf> (accessed 11 October 2014).

4 Forbes, Clark, T., *At Mobile World Congress, A Connected Future Becomes Reality*, 27 February 2004, available online at <forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/> (accessed 10 October 2014).

5 Wired, Thompson, C., *No Longer Vaporware: The Internet of Things is Finally Talking*, 6 December 2012, available online at <wired.com/2012/12/20-12-st_thompson/> (accessed 11 October 2014).

6 San Jose Mercury News, Boudreau, J., *Your phone, your life: New apps change how you use mobile devices*, 13 March 2009, available online at <mercurynews.com/ci_11900793?IADID=Search-www.mercurynews.com-www.mercurynews.com> (accessed 11 October 2014); Zamani, D., "There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones", *Hastings Constitutional Law Quarterly*, vol. 38, 2010, 174–175; Wall Street Journal, Thurm, S. and Kane, Y. I., *Your Apps Are Watching You*, 17 December 2011, available online at <online.wsj.com/news/articles/SB10001424052748704694004576020083703574602> (accessed 11 October 2014).

7 Pell, S., and Soghoian, C., "Can You See Me Now: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact", *Berkeley Technology Law Journal*,

While technology leapfrogs, legislation flags. Few laws regulate the collection of data exhaust and fewer still address how that data can be used. Given the expansion of sensors and the emergence of the Internet of Things, it is increasingly unlikely that a person can know precisely how much of her data is captured, who controls it and for what purpose.

Policymakers seeking to protect informational privacy face a daunting task. Information flow does not adhere to national boundary lines. As a result, the most effective privacy laws do not either. The European Union boasts the paragon of privacy laws by limiting access to its markets for those who fail to observe its strict law designed to protect personal information. By so doing, it bends international law into conformity.[8]

The EU 1995 Directive (and 2014 Regulation) embody this approach as it: (1) broadly defines personal information; (2) broadly defines who processes and controls personal information; (3) restricts transfer of personal information to those who cannot demonstrate compliance with the law's strictures.[9] The Directive does not limit its scope to certain industries or practices, but requires privacy controls across the board,[10] regardless of whether the data processor is a hospital, pastry chef or girl scout.

While the Directive is laudable in its omnibus effort to protect privacy, it fails in several significant aspects. The Directive outlaws harmless activities while it allows harmful exceptions that threaten to swallow the rule. It is simultaneously over-inclusive and under-inclusive. For example, it includes an employer gathering her or his colleagues' lunch orders and excludes data collected for "national security", a fluid concept undefined by the Directive.[11] The "national security" exception arguably allowed the US global surveillance programs, data mining, and third party data collection unveiled by Edward Snowden's revelations.[12]

The EU Directive also fails to protect against an equally ominous threat, albeit a threat less publically acknowledged: the Internet of Things. Everyday devices—objects—talk to one another online. Sensors connect objects to the Internet and enable the object to send, receive and analyse data automatically without human intervention. Outfitting innumerable objects with identifying and transmitting technology could be fundamentally transforming.

Privacy laws fail to address the loss of privacy through data exhaust and the Internet of Things. The EU Directive, for example, hinges on providing individuals with notice and obtaining their consent before collecting data, but the Internet of Things collects data without user awareness, to say nothing of notice and consent. The Directive fails to countenance the proliferation of indirect data collection, instead relying on the faulty

---

vol. 27, 2012; Rice, K.P., "You Are Here: Tracking Around the Fourth Amendment to Protect Smartphone Geolocation Information with The GPS Act", *Seton Hall Legislative Journal*, vol. 38, 2013.

8 Greenleaf, G., "Global data privacy laws: 40 years of acceleration", *Privacy Laws & Business International Report*, vol. 112, September 2011, 11–17.

9 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 (EU 95/46/EC Directive).

10 *Ibid*.

11 Directive 95/46/EC, *supra* nt. 9, Article 3(2).

12 Lerner, J., Frank, M., Lee, M., and Wade, D., "The Duty of Confidentiality in the Surveillance Age", *Journal of Internet Law*, vol. 17, ed. 1, 2014; International New York Times, The Editorial Board, *Edward Snowden, Whistle-Blower,* 1 January 2014, available online at <nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0> (accessed 11 October 2014).

premise that users actively volunteer personal information and are aware when they divulge it.

This article posits that informational privacy cannot be accomplished by declaring it a fundamental right, outlawing all processing of personal information, and enforcing the law through notice and consent. To legally realise and enforce a privacy right in personal information, incremental, graduated, and practical legislation better achieve the goal than sweeping proclamations that have applications to actions unrelated to the harms associated with the absence of the right. With information privacy in particular, a capacious claim of right to all personal information undermines legal enforcement because the harms attending lack of privacy are too often ill-defined and misunderstood.

Regulating the *use* of sensitive data as it relates to particular risks or harms better comports with consumer law generally and allows needed adaptability to reflect context and changing technology. Calibrating the risk of harm from the use of data in a particular context reveals the value of that data and allows local regulatory regimes to incrementally adopt protective policies. An incremental risk-based approach is not a panacea and requires a normative taxonomy. But identifying and defining diverse data contexts and uses, and identifying the attendant risks or harms from the user's viewpoint are critical to successful implementation of contextual and harm-based personal data regulation.

In Part II, this article outlines the difficulty inherent in maintaining privacy in the Age of Information. Shortcomings stemming from the most prominent data privacy law are exposed, suggesting that the EU Directive is ineffective as both under and over-inclusive. Part III identifies an added difficulty, passive data collection and the Internet of Things. Personal data collected without user awareness is widespread now and will soon be ubiquitous. Current privacy laws, including the EU Directive, poorly address the collection and use of data generated without user awareness. Part IV urges policymakers to shift focus away from data collection and instead regulate data use. In particular, regulation should contextualise—from an individual's viewpoint—the privacy risks associated with an entity's purported use of that data. Legal realisation of a claimed privacy right in the Age of Information should proceed incrementally and begin with the industries, practices, and processes that cause the most harm by flouting informational privacy. Current omnibus international legislation reflects the impossibility of legally protecting all privacy in the Age of Information; it also illustrates the need for a refined and practical legal scheme that gradually and directly targets the harms associated with privacy violations.

II. Privacy in the Information Age

II.1. Deluge of Data

Never before has so much information been so readily available to so many.[13] In two decades from the commercialisation of the Internet in 1995[14] to today, Internet penetration has grown in exponential fashion.[15] From 2000 to 2012, Internet users grew from 360 million to 2.4 billion, a 566% growth rate.[16] As of 2012, 34% of the world population is connected.[17] In America, 66% of the adult population own at least one personal computer and 77% regularly use the Internet.[18]

While Internet penetration among many African nations ranks among the lowest, the growth rate—the rate of new Internet users in Africa—far eclipses the growth rates reported by the rest of the globe.[19] Some project that Internet traffic will grow by more than 50% in Latin America, the Middle East and Africa.[20] In one year alone, China added over 27 million Internet users.[21]

Not only is Internet access pullulating, the volume of information generated and transmitted is amplifying. One consultancy estimates that 2.8 zettabytes were created in 2012 and that by 2015 that number will double.[22] Facebook's 1.2 billion users generate an average of ninety pieces of content each month.[23] Wal-Mart reports more than one million transactions an hour, and YouTube estimates that every sixty seconds users

---

13 Mayer-Schönberger, V., and Cukier, K., *Big Data, A Revolution that Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt Publishing, 2013.

14 Frischmann, B., "Privatization and Commercialization of the Internet Infrastructure: Rethinking Market Intervention into Government and Government Intervention into the Market", *The Columbia Science and Technology Law Review*, vol. 2, 2001, 1–70.

15 Internet Usage Statistics, available online at <internetworldstats.com/stats.htm> (accessed 11 October 2014).

16 *Ibid.*

17 *Ibid.*

18 *Ibid*.

19 Engineering News, Esterhuizen, I., *Internet Growth Strong in Africa*, 16 January 2012, available online at <engineeringnews.co.za/article/Internet-growth-strong-in-africa-2012-01-16> (accessed 11 October 2014); Citizen, *Africa Internet Use Hits 2,000 Per Cent Growth*, 17 January 2012, available online at <thecitizen.co.tz/Business/-/1840414/1813774/-/iwlyg2/-/index.html> (accessed 11 October 2014).

20 Global Pulse, Blog, *Big Data for Development: Challenges & Opportunities*, May 2012, available online at <unglobalpulse.org/BigDataforDevWhitePaper> (accessed 16 November 2014). Global Pulse is a United Nations project, initiated in 2009 by the Secretary General. The UN tasked Global Pulse with exploring opportunities deriving from digital data in order to help policymakers evaluate crises in real time for vulnerable populations.

21 PC World, Kan, M., *China Reaches 485 Million Internet Users as Growth Slows*, 19 July 2011 available online at <pcworld.com/businesscenter/article/235978/china_reaches_485_million_internet_users_as_growth_slows.html> (accessed 11 October 2014); 'There is now so much data stored in the world that we're running out of language to describe it. The only quantity bigger than a zettabyte is a yottabyte, a figure with 24 zeroes.' International Bar Association, IBA Global Insight, Lowe, R., *Me, Myself and I*, 14 October 2013, available online at <ibanet.org/Article/Detail.aspx?ArticleUid=B47A1361-16DD-4F04-B83D-ADD60898F213> (accessed 11 October 2014).

22 MIT Technology Review, Tucker, P., *Has Big Data Made Anonymity Impossible?*, 7 May 2013, available online at <technologyreview.com/news/514351/has-big-data-made-anonymity-impossible/> (accessed 11 October 2014).

23 Prasad, A., Mehta, K., Ventre, A., and Kearney, A. T., *Big Data: Understanding This New Normal*, 1107 PLI/Pat 411, 2012.

upload sixty hours of video.[24] Users send approximately 294 billion emails every day.[25] At 487 billion gigabytes, the world's digital content reduced to a stack of books would reach to Pluto ten times.[26] That is 'more than 1,000 gigabytes of data—twice the capacity of a standard laptop—of data for every person on earth in 2015.'[27] Given recorded human history, this near ubiquity of easy information over a mere twenty years is difficult to underestimate.

II.2. Threat to Privacy

This deluge of information threatens personal privacy, a fundamental right in many nations.[28] Ready access to individual's precise location,[29] tax returns,[30] Internet browsing history,[31] social interactions,[32] religious affiliation[33] and more carry a host of unwanted harms ranging from profiling by commercial marketers,[34] to undue governmental criminal investigation,[35] to health insurance rate increases,[36] to chilling political speech.[37]

One report from the 2014 World Economic Forum noted, 'The growth of data, the sophistication of ubiquitous computing and the borderless flow of data are all

---

24 *Ibid.*

25 *Ibid*.

26 The Guardian, Wray, R., *Internet data heads for 500bn gigabytes*, 18 May 2009, available online at <guardian.co.uk/business/2009/may/18/digital-content-expansion> (accessed 11 October 2013).

27 Liberty Global Policy Series, Boston Consulting Group, "The Value of Our Digital Identity", 2012, available online at <libertyglobal.com/PDF/public-policy/The-Value-of-Our-Digital-Identity.pdf> (accessed 10 December 2014).

28 Samuelson, P., "Privacy as Intellectual Property?", *Stanford Law Review*, vol. 52, 2000, 1125–1173; Loring, T. B., "An Analysis of the Informational Privacy Protection Afforded by the European Union and the United States", *Texas International Law Journal*, vol. 37, 2002, 423–460.

29 Yakowitz, J., "Tragedy of the Data Commons", *Harvard Journal of Law and* Technology, vol. 25, 2011, 1–67.

30 Schwartz, P. M., "The Future of Tax Policy", *National Tax Journal*, vol. 61, 2008, 883–900.

31 McIntyre, J. J., "Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information", *DePaul Law Review,* vol. 3, 2011 895–936, 913.

32 Stoddart, J., "Privacy in the Era of Social Networking: Legal Obligations of Social Media Sites", *Saskatchewan Law Review*, vol. 74, 2011, 263–274; Gunasekara, G., and Toy, A., "Myspace" or Public Space: The Relevance of Data Protection Laws to Online Social Networking", *New Zealand Universities Law Review*, vol. 23, 2008, 191–214.

33 Bergelson, V., "It's Personal But Is It Mine? Toward Property Rights In Personal Information"*, UC Davis Law* Review, vol. 37, 2003, 379–451.

34 DeMarco, D. A., Note, "Understanding Consumer Information Privacy in the Realm of Internet Commerce: Personhood and Pragmatism, Pop-Tarts and Six-Packs", *Texas Law Review*, vol. 84, 2006, 1013–1065, 1019; McClurg, A. J., "A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling", *Northwestern University Law Review,* vol. 98, 2003, 63–144, 90–91 .

35 Kline, C., "Security Theater and Database-Driven Information Markets: A Case for an Omnibus U.S. Data Privacy Statute", *University of Toledo Law Review*, vol. 39, 2008, 443–495; Cockfield, A. J., "Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance", *Queen's Law Journal*, vol. 29, 2003, 364–407.

36 Florencio, P. S., and Ramanathan, E.D., "Secret Code: the Need for Enhanced Privacy Protections in the United States and Canada to Prevent Employment Discrimination Based on Genetic and Health Information", *Osgoode Hall Law Journal*, vol. 39, 2001, 77–116.

37 Michelman, S., "Who Can Sue Over Government Surveillance?", *University of California Law* Review, vol. 57, 2009, 71.

outstripping the ability to effectively govern on a global basis.'[38] This point is worth emphasis: digital data knows no borders in the Internet age.[39] Metal file cabinets filled with paper dossiers and glossy photographs are of receding relevance. Digital data—including personal information—can be many places at once, travel thousands of miles in fractions of seconds from one nation to the next, and can be readily collected without notice or consent.[40] Digital data's fluid and borderless nature undermines national legislation aimed at regulating the collection and use of such information.[41] As one analyst put it, 'in the age of big data, those laws constitute a largely useless Maginot Line.'[42]

The difficulties inherent in national regulation of digital data are exacerbated by the diversity of data sources.[43] Digital data comes from everywhere: cell phone GPS signals, online browsing, cookies, digital purchases, social media pictures and posts, traffic videos and license plate cameras.[44] Emerging technologies like wearable devices will further the volume and variety of data input.[45] Google Glass, for example, collects, inventories, analyses and reports information that was previously intimate.[46]

Passive data sources are similarly emerging.[47] The Internet of Things—discussed in more detail below—imbues ordinary objects with in-product sensors that report activity through the Internet and relay usage data.[48] 'Automobiles, home appliances and energy meters are among the traditional product categories that have—or soon will have—integrated links to the internet,'[49] but this is only the beginning. In Europe, an additional seventy-five million objects will be connected to the Internet by 2015.[50] As the volume, variety and velocity[51] of digital data increases, so does the difficulty of implementing national legislation that effectively regulates it.[52]

---

38 World Economic Forum (WEF) prepared in collaboration with Kearney, A.T., *Rethinking Personal Data: A New Lens for Strengthening Trust*, May 2014, available online at <www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf> (accessed 13 October 2014); see Nguyen, C., and Haynes, P., "Rebalancing Socioeconomic Asymmetry in a Data-Driven Economy", *World Economic Forum Global Information Technology Report*, 2013.

39 Geist, M., "Cyberlaw 2.0", *Boston College Law Review*, vol. 44, 2003; Goldsmith J., and Wu, T., *Who Controls the Internet?: Illusions of a Borderless World*, Oxford University Press, 2006, 188.

40 *Ibid*.

41 Steward, M. G., "Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet", *The Business Lawyer*, vol.55, 2000.

42 Mayer-Schonberger and Cukier, *supra* nt. 13, 16.

43 Yakowitz *supra* nt. 29,'Today, data privacy practices are shaped by some combination of ambiguous statutory directives, inconsistent case law, industry best practices, whim, and self-serving discretionary preferences. The time is ripe for the creation of uniform data privacy policies, and there is much to fix'.

44 Mayer-Schonberger and Cukier, *supra* nt. 13, 16.

45 Schwartz, P. M., "Property, Privacy and Personal Data", *Harvard Law Review*, vol. 117, 2004.

46 Wagner, M. S., "Google Glass: A Preemptive Look at Privacy Concerns", vol. 11, *Journal on Telecommunications & High Technology Law*, 2013; Wall Street Journal, Wilson, J. W., *Wearable Gadgets Transform How Companies Do Business*, 20 October 2013, available online at <online.wsj.com/news/articles/SB10001424052702303796404579099203059125112> (accessed 11 October 2014).

47 WEF and Kearney, *supra* nt. 38.

48 Lowe, *supra* nt. 21.

49 The Value of Our Digital Identity, *supra* nt. 27.

50 *Ibid.*

51 *Ibid*.

52 Lowe, *supra* nt. 21.

The most effective legislation, like the data it seeks to regulate, is itself borderless. The most widely acclaimed example is the European Union's 1995 Directive.[53] The Directive seeks to ensure citizen's rights to their personal information by truncating access to European markets for those who fail to comply with the Directive's strictures.[54] The Directive's effectiveness in large part stems from its extra-jurisdictional reach.[55] But the law has not succeeded. Where the Directive confronts the operose task of capturing transnational data flow, it fails in several other critical respects. This article posits that the Directive, laudable in aspiration, fails in practice. It is at once fatally over-inclusive and under-inclusive.

II.3. Leading Global Privacy Regulation: The European Union Directive

II.3.1. The Directive's Broad Scope

The Directive seeks to regulate the collection, storage, use, and dissemination of personal data;[56] it treats the right to privacy as a fundamental right,[57] awarding individuals autonomy over the distribution of personal data.[58] The Directive casts a wide net, illustrated by three key definitions. The Directive applies to (1) personal data, that is (2) processed by (3) controllers or processors.[59] Personal data is defined in the Directive as

> Any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[60]

Personal data refers not just to names, national identification numbers, social security numbers and addresses but includes information that can lead to identification directly or indirectly.[61] This definition of personal data equates identified with identifiable.[62] Data is

---

53 Directive 95/46/EC, *supra* nt. 9; Lindsay, D., "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", *Melbourne University Law Review*, vol. 29, 2005, 154–59.

54 "International Privacy Issues", 23 No. 3 *International Human Rights Journal*, Article 4, 2014.

55 Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000.

56 Murray, P. J., "The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?" *Fordham International Law Journal*, vol. 21, ed. 3, 1998, 932–1018, 933.

57 Sotto, L. J., *Privacy and Data Security Law Deskbook*, Aspen Publishers, New York, 2010, Section 18.02[A], '[t]hus the Data Protection Directive is based on internationally recognized fundamental human rights, specifically, the fundamental human right to privacy'.

58 Directive 95/46/EC, *supra* nt. 9, the Directive provides data subjects with a number of rights with respect to their personal data, including but not limited to: (1) the right of access to data; (2) the right to withhold permission to use data; (3) the right to have inaccurate data rectified; and (4) the right of recourse in the event of unlawful processing of data.

59 *Id.,* Articles 2, 6, 7.

60 *Id.,* Article 2(a).

61 *Ibid*.

62 Schwartz, P. M., and Solove, D. J., "The PII Problem: Privacy and a New Concept of Personally Identifiable Information", *New York University Law Review*, vol. 86, ed. 6, 2011, 1814–1894, 1819, arguing that information privacy regulations rest on an unstable and ill-defined concept of personally identifiable information.

considered personal when it enables anyone to link information to a specific person, even if the person or entity holding that data cannot itself make the link.[63] As one EU authority stated, data is considered "personal" when, 'although the person has not been identified yet, it is possible to do it.'[64] Thus, information need not identify an individual directly to constitute "personal data", the mere fact that the information is related to an individual capable of being identified results in the data being "personal data" under the Directive.[65]

The Directive couples this broad definition of personal data with a broad definition of data "processing," defined as

> [A]ny operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.[66]

Any collection, use and transfer of personal data—even the redaction and deletion thereof—constitutes "processing".[67] This definition purposefully includes data processed automatically as part of a filing system.[68] The Directive defines those deemed to have "processed" personal data as either data controllers or data processors. A data controller is 'the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.'[69]

Under these definitions, it is difficult to imagine commercial use of the Internet without processing personal information of some ilk. Given the law's broad reach and the significant restrictions levied on those that process personal information, policymakers anticipated that many organisations would sooner relocate or transfer processing functions overseas than comply.[70] The European Commission Website concedes the same: 'Without such precautions, the high standards of data protection established by the Data Protection Directive would quickly be undermined, given the ease with which data can be moved around in international networks.'[71]

The Directive's "precautions" include mechanisms that effectively legislate outside the jurisdiction of the European Union.[72] 'Because of its potential effect on other nations that interact with or do business in Europe, it may be the most controversial feature of the

---

63 *Id.*, 1817.

64 European Commission, Article 29 Data Protection Working Party, *Opinion 4/2007 on the Concept of Personal Data*, 20 June 2007, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf> (accessed 17 October 2014).

65 Sotto, *supra* nt. 57, Section 18.02[A].

66 Directive 95/46/EC, *supra* nt. 9, Article 2(b).

67 *Ibid.*

68 *Id.*, Article 5, Recital 15.

69 *Id.*, Article 2(d).

70 Assey, J. M. Jr. and Eleftheriou, D. A., "The EU-U.S. Privacy Safe Harbor: Smooth Sailing or Troubled Waters?" *CommLaw Conspectus*, vol.9, ed. 2, 2001, 145–158, 146.

71 European Commission, *Transferring your personal data outside the EU*, 20 May 2014, available online at <ec.europa.eu/justice/data-protection/data-collection/data-transfer/index_en.htm> (accessed 17 October 2014).

72 Sotto, *supra* nt. 57, Section 18.02[A]1[c].

Directive.'[73] One mechanism that forces international compliance does so through the use of "equipment" located in the EU.

> Each Member State shall apply … this Directive to the processing of personal data where: (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[74]

An EU company trying to avoid compliance with the Directive by relocating to Canada could not successfully do so if the personal data involved the computer, smart phone, or other such equipment of an EU resident. This provision not only dissuades EU companies from relocating, it also imposes the Directive's requirements on a host of non-EU entities. Many organisations headquartered in countries outside the European Union have been surprised to learn of their obligation to comply with EU law.[75]

The Directive's reach does not stop with data processing that uses EU-based "equipment",[76] it specifically targets data transfers to "third countries".[77] Article 25 prohibits the transfer of personal data to a third country (any Non-EU or EEA country) unless the European Commission deems that country "adequate".[78] The Commission currently recognises only twelve countries as adequate: Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay.[79] Given the broad definition of "personal information", the global economy and the free flow of data over the Internet, restricting data flow to twelve countries appears unmanageable at best.

Three principal avenues—outside a finding of nationwide adequacy—allow non-EU entities to receive and process EU personal data: (1) binding model contracts,[80] (2) binding corporate rules,[81] (3) Safe Harbor self-regulation.[82] The Directive also contains

---

73 Salbu, S. R., "Regulation of Borderless High-Technology Economies: Managing Spillover Effects", *Chicago Journal of International Law*, vol. 3, ed. 2, 2002, 137–153, 137; see also Kuner, C., "Beyond Safe Harbor: European Data Protection Law and Electronic Commerce", *The International Lawyer*, vol., 35, 79, 87.

74 Directive 95/46/EC, *supra* nt. 9, Article 4.

75 Salbu, *supra* nt. 73, 137.

76 Directive 95/46/EC, *supra* nt. 9, Article 25.

77 *Ibid*.

78 *Ibid*.

79 European Commission, *Commission decisions on the adequacy of the protection of data in third countries*, 24 June 2014, available online at <ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm> (accessed 17 October 2014), providing the requirements for "adequacy" and listing the few countries whose national laws meet the requirements.

80 Directive 95/46/EC, *supra* nt.9, Article 26(4); The Directive allows transfers of personal data even to third countries that fail to ensure an adequate level of protection if the data controller erects 'sufficient safeguards' via 'certain standard contractual clauses' consistent with a 'Commission's decision'. Under this approach, the contractual clauses incorporate by reference the data protection law of the Member State in which the data exporter is established. See Leathers, D. R., "Giving Bite to the EU-US Data Privacy Safe Harbor: Model Solutions for Effective Enforcement" *Case Western Reserve Journal of International Law* vol. 41, ed.1, 2009, 193–242, 199–200.

81 Directive 95/46/EC, *supra* nt.9, Article 29, binding corporate rules track EU data protection standards and allow multinational organisations to conduct business with EU counterparts without having to draw up model contract language for every transaction. The relevant Member State's Data Protection Agency must approve binding corporate rules, which can be an arduous and lengthy process. As a

situational exceptions and derogations that allow processing of personal data and often undermine the law's broad definitions and extra-jurisdictional reach.[83] The Directive, despite its worthy aspiration, contains significant shortcomings. It is both over and under-inclusive.

II.3.2. The Directive's Over-Inclusiveness

By most accounts, protecting personal information is a deserving goal. The Directive's extra-jurisdictional reach, penalties for non-compliance, and expansive definition of those who process personal information reflect sincerity in reaching that goal.[84] Ironically, by purporting to protect all personal information from almost all processing, the Directive undermines its central objective; its over-inclusiveness debilitates its effectiveness.

II.3.2.1.Restricting Harmless Data Processors

Privacy scholar, Fred Cate, notes that children recording orders for Girl Scout cookies, individuals organising their business contacts, and students operating websites that require registration all qualify as data controllers under the Directive.85 A co-ed collecting names for intramural flag football in Boise, Idaho is likely a "controller" who "processes" "personal information". Perhaps more commonly,

> anyone who posts personal information about another person on his or her own social networking profile or uses personal information from another

---

result, relatively few binding corporate rules have been approved. See Sotto, *supra* nt. 57, Section 18.02[B].

82 US Department of Commerce, *Welcome to the U.S.-EU & U.S.-Swiss Safe Harbor Frameworks*, 4 August 2014, available online at <export.gov/safeharbor/> (accessed 17 October 2014).

83 Directive 95/46/EC, *supra* nt. 9, art. Article26(1), the Directive's Article 26(1) authorises a number of other exceptions to legally transmit personal data outside of Europe even to a 'third country' that fails to offer an 'adequate level of protection'. A data controller or processor can legally send personal data outside of Europe to the United States, or any other country, if:

(a) the data subject has [freely] given his consent unambiguously to the proposed transfer [to be enforceable, a consent must indeed be unambiguous and freely given; EU data authorities take the position that a consent must specifically list the categories of data and the purposes for the processing outside the EU; in the employment context, consents may be deemed presumptively not freely given, merely because of the imbalance in bargaining power between employer and employee]; or

(b) the transfer is necessary [not merely convenient] for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or

(c) the transfer is necessary [not merely convenient] for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or

(d) the transfer is necessary [not merely convenient] or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims; or (e) the transfer is necessary [not merely convenient] in order to protect the vital interests of the data subject; or

(f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.

84 Directive 95/46/EC, *supra* nt. 9.

85 Cate F. H., "The Changing Face of Privacy Protection in the European Union and the United States" *Indiana Law Review*, vol., 33, 1999, 173–232, 183.

> person's profile could be deemed a 'data controller' subject to the data protection obligations of the Directive.[86]

Seemingly innocuous data like the nine-digit numerical label assigned to each device that participates in a computer network amounts to personal data.[87] The Working Party on data privacy for the European Commission confirmed that IP addresses and cookies are "personal data",[88] a finding echoed by the US Federal Trade Commission in its proposed revisions to COPPA.[89]

In short, the Directive's broad reach captures an uncomfortably high percentage of "data processors" whose use of "personal information" is disassociated from the harm that the Directive seeks to alleviate.[90] As noted above, "personal information" under the Directive includes information that identifies a person and information that could lead to identifying a person. The EU Directive is not alone in using such a broad definition. The US Health Insurance Portability and Accountability Act defines identifiable health information as including information 'with respect to which there is a reasonable basis to believe the information can be used to identify the individual.'[91] In fact, the clear majority of nations that have enacted universal privacy laws regulate information that could lead to identification.[92]

This definition has proven increasingly problematic because most information that relates to a person—even when scrubbed to create "anonymity"—can be decoded.[93] 'The emergence of powerful re-identification algorithms demonstrates … the fundamental inadequacy of the entire privacy protection paradigm based on "de-identifying" the data.'[94]

Companies that collect personal information, like online retailers or social networking entities, often promise to share only customer information that is non-personally

---

86 Bennett, S. C., "The "Right to be Forgotten": Reconciling E.U. and U.S. Perspectives", *Berkeley Journal of International Law*, vol., 30, ed., 1, 2012, 161–195, 186.

87 McIntyre, J. J., "Comment, Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information", *DePaul Law Review*, vol. 60, ed. 3, 2011, 895–936, 897.

88 European Commission, Article 29 Data Protection Working Party, *Opinion 1/2008 on Data Protection Issues Related to Search Engines*, 00737/EN/WP148, 4 April 2008, 3, 8, available online at <ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_en.pdf> (accessed 17 October 2014) (WP148).

89 Black J. E. Jr., "Privacy Liability and Insurance Developments in 2012*", Journal of Internet Law*, vol. 16, ed. 9, 2013, 3–13.

90 Yakowitz, *supra* nt. 29, noting unintended costs like preventing use of personal data to confront public health issues, create economic value, and prevent fraud); MIT Technology Review, Simonite, T., *Business Report—Big Data Gets Personal: Smartphone Tracker Gives Doctors Remote Viewing Powers*, 17 May 2013, available online at <technologyreview.com/news/514756/smartphone-tracker-gives-doctors-remote-viewing-powers/> (17 October 2014); MIT Technology Review, Talbot, T., *Business Report—Big Data Gets Personal: African Bus Routes Redrawn Using Cell-Phone Data*, 30 April 2013, available online at <technologyreview.com/news/514211/african-bus-routes-redrawn-using-cell-phone-data/> (accessed 17 October 2014)

91 Health Insurance Portability and Accountability Act, United States of America, 1996 as in force on 23 March 2010, US Code Title 42 Chapter 7(XI) Part C Section1320d (6)(B)(ii), available online at <law.cornell.edu/uscode/text/42/1320d> (accessed 17 October 2014).

92 Greenleaf, *supra* nt. 8, 11.

93 Ohm, P., "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization", *UCLA Law Review*, vol. 57, ed. 6, 2010, 1701–1777.

94 Narayanan, A. and Shmatikov, V., "Privacy and Security Myths and Fallacies of "Personally Identifiable Information", *Communications of the ACM*, vol. 53, ed. 6, 2010, 24–26.

identifiable.[95] Such promises will soon be illusory: 'They fundamentally rely on the fallacious distinction between "identifying" and "non-identifying" attributes.'[96]

By illustration, hackers recently employed content search queries to re-identify AOL customers. Location data, commercial transactions and web browsing history readily populate de-anonymising algorithms. Even movie-viewing histories have been shown to effectively re-identify users.[97] Combining the vast continuum of human characteristics and activities with the quantity and specificity of information already available, suggests that re-identification is inevitable and, more importantly, that 'any attribute can be identifying in combination with others.'[98]

Despite a high likelihood of re-identification, the concept of 'personally identifiable information' remains central to existing privacy regulations,[99] leading many to decry the use of 'personally identifiable information' as a regulatory lynchpin.[100] As discussed in more detail below, emerging technologies stretch the already broad applicability of such laws to near universality, revealing the over-inclusiveness and also arguably, the ineffectiveness of the EU Directive.

Moreover, enforcement of laws, that incriminate a disproportionately large ratio of those individuals governed by it, or that are so broad as to capture the entire body politic have historically been declared invalid. Criminalising those who speak in an "annoying" way,[101] or outlawing "vagrancy",[102] confer upon government *carte blanche* enforcement authority. Officials can arbitrarily choose to prosecute disfavoured parties. The Directive attracts similar criticism.[103]

Upset by lacklustre enforcement in the United States, for example, European Union officials chastised their US counterparts,[104] issuing a working paper noting that 'less than half of organisations post privacy policies' and that most failed to observe 'the expected

---

95 Ohm, *supra* nt. 93; Wall Street Journal, Steel, E. and. Fowler, G. A*., Facebook in Privacy Breach*, 18 October 2010, available online at <online.wsj.com/news/articles/SB10001424052702304772804575558484075236968> (accessed 17 October 2014).

96 Narayanan and Shmatikov, *supra* nt. 94.

97 *Ibid*.

98 *Ibid*.

99 Greenleaf, *supra* nt. 8.

100 Word Press, Taylor, L., *Hacking a Path Through the Personal Data Ecosystem*, 12 December 2013, available online at <linnettaylor.wordpress.com/2013/12/12/hacking-a-path-through-the-personal-data-ecosystem/> (accessed 17 October 20).

101 *People v Raphael Golb*, 2014 NY Slip Op 03426, Decided on May 13, 2014 Court of Appeals Abdus-Salaam, J. Published by New York State Law Reporting Bureau pursuant to Judiciary Law, Section 431; *People v Dietze* 75 NY2d 47 (1989), striking down a similar harassment statute, former Penal Law, Section 240.25, which prohibited the use of abusive or obscene language with the intent to harass, annoy or alarm another person; NY Times, Leland, J., *Top Court Champions Freedom to Annoy*, 13 May 2014, available online at <nytimes.com/2014/05/14/nyregion/top-court-champions-freedom-to-annoy.html?_r=0> (accessed 17 October 2014).

102 *Papachristou v Jacksonville*, 405 US 156 (1972); *Kolender v Lawson* 461 US 352 (1983), striking laws against vagrancy for unconstitutional vagueness; in restricting activities like 'loafing', 'strolling', or 'wandering around from place to place', the law gave arbitrary power to the police and, since people could not reasonably know what sort of conduct is forbidden under the law, could potentially criminalize innocuous everyday activities.

103 Leathers, *supra* nt. 81, 195–200.

104 *Ibid*, '[s]ince the Safe Harbor's inception, the program has been subject to heavy criticism from privacy advocates and an EU oversight committee. The heaviest criticism is levied against the Safe Harbor's inadequate internal and external enforcement mechanisms.'; US Federal Trade Commission, *Court Halts U.S. Internet Seller Deceptively Posing as U.K. Home Electronics,* PRESS RELEASE, *6 August 2009*, available online at <ftc.gov/opa/2009/08/bestpriced.shtm> (accessed 17 October 2014).

degree of transparency as regards their overall commitment or as regards the contents of their privacy policies.'[105] Indeed, the FTC waited nine years before bringing a data privacy enforcement action;[106] the ambitious and over-inclusive nature of the Directive invites its arbitrary enforcement.

The Directive's over-inclusive model implicates another topic of note—data security. Security breaches from malware, hackers, netbots, viruses and all manner of cyber threats plague individuals and organisations alike. In April 2011, Sony suffered a massive breach in its video game online network.[107] Volumes of customer data were compromised, including names, addresses, and possibly credit card data associated with over seventy-seven million user accounts.[108] In 2005, America's major newspapers headlined the following: "Info Theft Slams Chain: 1.4 Million Card Numbers Stolen"; "Poll Says Identity Theft Concerns Rose After High-Profile Breaches"; "Data Security Breaches Alarm Consumers".[109] Data security experts recorded 403 million variants of malware in 2011.[110] As one commentator notes, '[s]cholars, government officials, journalists, and computer scientists all agree that inadequate security is an emerging threat—perhaps a catastrophic one…'.[111] Data that cannot be protected cannot be private.

Even so, the Directive includes no exception allowing data to be processed solely for security purposes.[112] Modern security protocols require analysis of massive data sets.[113] Anomalies in data usage often reveal cyber attacks.[114] In 2011, for example, a firm specialising in international money transfers notified authorities when it spotted a slight abnormality in Discover Card transactions originating in New Jersey.[115] Individually, the transactions appeared pedestrian, but viewed together and in context with large data sets,

---

105 European Commission, Commission Staff Working Paper, The Application of Commission Decision 520/2000/EC of 26 July 2000 Pursuant to Directive 95/46 of the European Parliament and of the Council on the Adequate Protection of Personal Data Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce, SEC (2002) 196, 13 February 2002, available online at <ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf> (accessed 17 October 2014)

106 Leathers, *supra* nt. 80, 195–196.

107 Kuhlmann, S., "Do Not Track Me Online: The Logistical Struggles Over the Right "To Be Let Alone" Online", *De Paul Journal of Art, Technology & Intellectual Property Law*, vol. 22, 2011, 242–245.

108 *Ibid*.

109 Barnes, M. E., "Falling Short of the Mark: The United States Response to the European Union's Data Privacy Directive", *Northwestern Journal of International Law & Business*, vol. 27, ed. 1, 2006, 171–198.

110 Symantec, *Internet Security Threat Report: 2011 Trends*, 12 April 2012, available online at <symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf> (accessed 29 October 2014).

111 Bambauer, D. E., "Conundrum", *Minnesota Law Review*, vol. 96, 2011, 584–674.

112 Data Protection Directive, *supra* nt. 8; but see Proposal for a 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, COM, 2012, 11 final, 25 January 2012. (Recital 39 of the new Regulation suggests there will be more room for security providers to process data).

113 Symantec, *Technology: Defense in Depth*, available online at <symantec.com/about/profile/star_technology.jsp> (accessed 29 October 2014), 'Network-based protection is a set of technologies designed to block malicious attacks before they have a chance to introduce malware onto a system. Unlike file-based protection, which must wait until a file is physically created on a user's computer before scanning it, network-based protection analyzes all incoming data streams before they can processed by the computer's operating system and cause harm'.

114 *Ibid*.

115 Mayer-Schonberger and Cukier, *supra* nt. 13, 27–28.

the irregularities revealed that the transactions came from the same criminal organisation. 'The only way to spot the anomaly was to examine all the data'.[116]

But those providing data security must comply with the Directive if the security measures require the "processing" of "personal data."[117] Given the massive data sets required by modern security programs, the likelihood of processing personal information is high.[118] For example, in 2012 Microsoft announced plans to publish a real-time intelligence feed drawn from its extensive data security protocols.[119] However, because the intelligence feed distributed IP addresses of systems infected by malware, the Directive posed a substantial obstacle.[120] Analysing and sharing large amounts of information is critical to data security, a task made onerous by the Directive's sweeping application. In choosing an ambitious scope, EU policymakers failed to account for the fact that safeguarding networks from hacking and cyber threats is itself a form of privacy protection.

II.3.3. The Directive's Under-Inclusiveness

While the Directive's over-inclusive scope encircles those whose use of "personal information" is removed from the harm that the Directive seeks to alleviate, it is simultaneously under-inclusive, ignoring many of privacy's worst offenders. Several exceptions and derogations threaten to outstrip the law's prime objective.[121] As a preliminary matter, the Directive does not have literal effect on Member States but only requires them to pass legislation that tracks the Directive in spirit and result.[122] Each Member State retains discretion as to form and implementation of the national privacy law that each ultimately enacts and enforces.[123] 'A margin for manoeuvre' potentially subverts the Directive by allowing disparate and inconsistent laws among Member States.[124]

More to the point, the Directive itself allows for specific exceptions, some of which are generally identified without limiting language. This article does not attempt to address them all. Two exceptions sufficiently reflect the Directive's failure to regulate many of the most harmful offenders: (1) the National Security and Criminal Proceedings exception;[125] and (2) the Safe Harbor exception.[126]

---

116 *Ibid*.

117 Cunningham, M, "Privacy in the Age of the Hacker: Balancing Global Privacy and Data Security Law", *George Washington International Law Review*, vol. 44, 2012, 643–696, 681–685.

118 *Ibid.*

119 Network World, Neagle, C., *Microsoft to Launch Real-Time Threat Intelligence Feed*, 12 January 2012, available online at <networkworld.com/news/2012/011212-microsoft-intelligence-254846.html> (accessed 29 October 2014).

120 Cunningham, *supra* nt. 117, 643–696.

121 Directive 95/46/EC, *supra* nt. 9, Articles 13, 26.

122 Directive 95/46/EC, *supra* nt. 9, Articles 22–23.

123 Sotto, *supra* nt. 57, Section 18.02.

124 Ritter, J. B., Hayes B. S. and Judy H. L., "Emerging Trends in International Privacy Law"*, Emory International Law Review*, vol. 15, 2001, 87–92, nt. 11.

125 Directive 95/46/EC, *supra* nt. 9, Articles 3(2), 13.

126 European Commission, 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, available online at <http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32000D0518> (accessed 25 November 2014).

II.3.3.1.National Security Exception

Although national security and criminal investigations often require efficiency and secrecy, the Directive's drafters declined to define the scope of these exceptions.[127] National security is a fluid concept. The Directive predates the attacks of September 11, 2001 and the subsequent and ongoing war on terror.[128] Edward Snowden's revelations about US global surveillance programs, data mining, interception projects, third party data collection and complex analytic schemes unveiled privacy violations on a scale previously unknown.[129] The war on terror catalysed these invasive and covert programs, and the Directive's generalised exceptions for "national security", facilitate these open-ended and continuing privacy violations.[130]

The United States is not alone in its use of national security to boost data collection, analysis and retention. Many States have documented pervasive deprivation of privacy rights justified, in part, by national security.[131] A report given at the World Economic Forum noted the atmosphere of anxiety and agitation that often prevails, leaving a 'one-dimensional debate…where the interest of privacy are traded off against public safety and security'.[132] A better balance is required. The first data protection commissioner in the German State of Hesse argued that an individual's right to access should 'never be totally excluded, but rather can at most be partially restricted or temporarily suspended in a series of unequivocally defined and exhaustively listed cases'.[133] The Directive offers no such parameters, leaving government surveillance unregulated.

II.3.3.2.Safe Harbor Exception

The other notable exception is the Directive's Safe Harbor provision.[134] Unique to the United States and perhaps owing to its singular economic status at the time, the European Commission fashioned a heavily diluted version of the Directive for application to US entities that chose it.[135] The hope was to construct a streamlined channel for US entities to roughly comply with the Directive's strictures.[136] The watery version reflects US resistance to omnibus privacy legislation and ultimately signals to US entities that pro forma compliance suffices.[137]

Importantly, Safe Harbor facilitates hollow compliance because it is voluntary, self-certifying, and largely unenforced.[138] US businesses that process EU personal data

---

127 Directive 95/46/EC, *supra* nt. 9, Article 3(2), 13.

128 Directive 95/46/EC, *supra* nt. 9.

129 International Bar Association, IBA Global Insight, Mulrenan, S., *Snowden NSA Revelations Make Mockery of Hong Kong Resolve on Privacy*, August 2013.

130 Fitzgerald, E. O., "The Globalized Rule of Law and National Security: An Ongoing Quest for Coherence", *University of New Brunswick Law Journal*, vol. 65, 2014, 40–85.

131 *Ibid.*

132 WEF and Kearney, *supra* nt. 38; Nguyen, C. and Haynes, P., "Rebalancing Socioeconomic Asymmetry in a Data-Driven Economy", *in*: Bilbao-Osorio, B., Dutta, S. and Lanvin, B. eds., *Global Information Technology Report 2014: Rewards and Risks of Big Data*, Insight Report, World Economic Forum and INSEAD, 2014.

133 The Value of Our Digital Identity, *supra* nt. 27, 10.

134 European Commission 2000/518/EC Decision, *supra* nt. 126.

135 *Ibid*.

136 Cunningham, M., "Diminishing Sovereignty: How European Privacy Law Became International Norm", *Santa Clara International Law Journal*, vol. 11, 2013, 421–452.

137 *Id.*, 440.

138 Wang, M.-L., "Information Privacy in a Network Society: Decision Making Amidst Constant Change", *National Taiwan University Law Review*, vol. 5, 2010, 127–154, 133 nt. 23.

regulate their own adherence to Safe Harbor privacy principles.[139] No government official reviews and then authorises whether any given company in fact complies with Safe Harbor principles before awarding certification.[140] An entity need only notify the US Department of Commerce that it intends to comply with Safe Harbor and publicly declare compliance on its website.[141] A US organisation that self-certifies through Safe Harbor is then afforded automatic approval from data processing authorities in the European Union.[142] Among US companies, this approach does not foster recognition and adherence to the privacy principles laid out in the Directive.[143] Neither does the relaxed approach incent US businesses to self-certify, as many view self-certification as creating unnecessary liability and oversight.[144] Professor Joel R. Reidenberg concludes that 'self-regulation is not an appropriate mechanism to achieve the protection of basic political rights. Self-regulation in the US reduces privacy protection to an uncertain regime of notice and choice.'[145]

Moreover, Safe Harbor certification shifts the jurisdiction from EU authorities to the US Department of Commerce and the Federal Trade Commission (FTC).[146] Although implemented in 2000, the FTC did not bring an enforcement action under Safe Harbor until 2009.[147] As one commentator notes, 'The heaviest criticism is levied against the Safe Harbor's inadequate internal and external enforcement mechanisms.'[148] In light of the large numbers of US organisations engaged in e-commerce or otherwise processing large amounts of data, the Safe Harbor "exception" effectively insulates a significant faction of privacy offenders.

The Directive aspires to protect privacy as a fundamental right regardless of industry, sector or other such context.[149] In so doing, it propagates a disconnect between the law and the harm it seeks to mitigate. By including almost all data processors irrespective of whether they cause privacy harms and by excluding those data processors that in fact harm individuals by misusing their private data, the Directive undermines its central objective.

---

139 Leathers, *supra* nt. 80, 196; Vitale, A., "The EU Privacy Directive and the Regulating Safe Harbor: The Negative Effects on U.S. Legislation Concerning Privacy on the Internet", *Vanderbilt Journal of Transnational Law*, vol. 35, 2002, 321–357, 339.

140 *Ibid.*

141 *Ibid.*; Sotto, *supra* nt. 57 , Section 18.02 [A], 2010.

142 *Ibid*; Rubinstein, I. S., "Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes", *I/S: A Journal of Law and Policy for the Information Society*, vol. 6, ed. 3, 2011, 355–423.

143 Reidenberg, J. R., "Setting Standards for Fair Information Practice in the U.S. Private Sector", *Iowa Law Review*, vol. 80, 1995, 497–551, 500, 'Despite the growth of the Information Society, the United States has resisted all calls for omnibus or comprehensive legal rules for fair information practice in the private sector. Legal rules have developed on an ad hoc, targeted basis, while industry has elaborated voluntary norms and practices for particular problems. Over the years, there has been an almost zealous adherence to this ideal of narrowly targeted standards.'

144 Nijhawan, D. R., "The Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States", *Vanderbilt Law Review*, vol. 56, ed. 3, 2003, 940–996, 975–976, noting that 'in order to comply, companies must incur substantial costs to ensure that their data management processes meet threshold requirements'.

145 Reidenberg, J. R., "E-commerce and Trans-Atlantic Policy", *Houston Law Review*, Vol. 38, 2001, 717–750.

146 Cunningham, *supra* nt. 117, 681.

147 Sotto, *supra* nt. 57, Section 18.02[B].

148 Leathers, *supra* nt. 80, 195–196.

149 Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, 1–88.

III. Next Generation Privacy

Protecting privacy through omnibus legislation like the EU Directive is unlikely to succeed.[150] Even universal international accord memorialised by a treaty purporting to protect informational privacy would likely fail because it misperceives the current era of big data—one that is firmly rooted and not easily upended by absolutist privacy legislation.[151]

III.1. Commercialisation and Ubiquity of Personal Data

The enormous amount of information already available allows easy re-identification; 'any attribute can be identifying in combination with others'.[152] A 2,000% increase in global data is expected by 2020.[153] The more data there is, the less that any of it can be said to be private.[154] Users continue to reveal personal data through social networking sites.[155] Such websites are growing three times faster than the overall Internet rate, and currently represent the fourth most popular online activity.[156] In other words, active data sharing is not slowing and those who seek privacy are often those who broadcast personal information in the digital world.[157] Perhaps fooled by the myth of online anonymity,[158] users continuously divulge bits of themselves when searching Google, purchasing items online, posting pictures, "liking" restaurants and browsing vacation spots.

These online actions appear free; they are not.[159] As computer scientist, Jaron Lanier writes: 'the dominant principle of the new economy, the information economy, has lately been to conceal the value of information'.[160] Google receives more than three billion search inquiries every day—and saves them all.[161] A recent study predicts 'the Big Data market is on the verge of a rapid growth spurt that will see it top the USD50 billion mark

---

150 Wang, *supra* nt. 138, 133 nt. 23.

151 Foreign Affairs, Mundie, C., *Privacy Pragmatism,* March-April 2014, available online at <foreignaffairs.com/articles/140741/craig-mundie/privacy-pragmatism> (accessed 29 October 2014), 'Today, the widespread and perpetual collection and storage of personal data have become practically inevitable.'

152 Narayanan and Shmatikov, *supra* nt. 94.

153 Tucker, *supra* nt. 22, 2–3.

154 *Ibid.,* quoting Princeton University computer scientist, Arvind Narayanan; Mundie, *supra* nt. 151; but see Yakowitz, *supra* nt. 29, arguing that re-identification is not easy and that the digital commons is beneficial to scientific research.

155 Nielesen Online, *Social Networks & Blogs Now 4th Most Popular Online Activity, Ahead of Personal Email, Nielson Reports,* NEWS RELEASE, 9 March 2009, available online at <nielsen-online.com/pr/pr_090309.pdf> (accessed 29 October 2014) (Nielsen News Release); see also Neilsen Online, *Social Networking and Blog Sites Capture More Internet Time and Advertising*, Newswire, 24 September 2009, available online at <nielsen.com/us/en/insights/news/2009/social-networking-and-blog-sites-capture-more-internet-time-and-advertisinga.html> (accessed 29 October 2014); Nunziato, D. C., "Romeo and Juliet Online and in Trouble: Criminalizing Depictions of Teen Sexuality (c u l8r: g2g 2 jail)", *Northwestern Journal of Technology and Intellectual Property*, vol. 10, ed. 3, 2012, 57–92, 58.

156 *Ibid.*

157 Waldman, A. E., "Durkheim's Internet: Social and Political Theory in Online Society", *New York University Journal of Law and Liberty*, vol. 7, ed. 2, 2013, 345–440.

158 *Ibid*.

159 Lowe, *supra* nt. 21.

160 Lanier, J., *Who Owns the Future?*, Simon and Schuster, New York, 2013, 15.

161 Mayer-Schonberger and Cukier, *supra* nt. 13, 2.

worldwide within the next five years.'[162] Acxiom, a data wholesaler, maintains an average of 1,500 pieces of information on more than 500 million consumers across the globe.[163] 'Data collection is the dominant activity of commercial websites. Some 92% of them collect personal data from web users, which they then aggregate, sort, and use.'[164]

Facebook's value is not the number of people it can reach for advertisements but the volume and specificity of personal information it has on each Facebook user.[165] One Facebook user, after repeatedly asking Facebook to remit his personal data, eventually received more than 1, 220 pages of his personal information after only three years using Facebook.[166] 'Pictures uploaded from smartphones included precise global positioning system coordinates, the identities of anyone tagged in the photos and the moment—down to the second—when the shutter clicked. Information that users thought they had deleted survived in Facebook files.'[167]

Data analytics was an estimated USD25.1 billion industry in 2004 and a USD105 billion industry in 2010.[168] A 2010 study by IBM reveals that 83% of business leaders identify analytics as a top priority for their businesses.[169] The revenues of the largest data-mining companies exceed USD1 billion annually,[170] suggesting that the data collection and retention infrastructure is far-reaching, diverse and entrenched. Data and personal information were described in the World Economic Forum as 'the new oil'.[171]

The commercialisation of personal data, the myth of anonymity and the public's habitual reliance on the Internet stand in the way of omnibus privacy reform. Even in the unlikely event that users stop actively divulging personal information, and that legislation can uproot businesses whose revenue flow from collection and dissemination of personal data, "passive" data transmission and collection continue to grow with emerging technologies.

III.2. Emerging Technology and Passive Data Transmission

Broad privacy laws that regulate the collection and retention of personal information fail to account for new technologies and expanding sources of passive data generation. National privacy laws like the Directive presume the individual's voluntary participation, including the opportunity to consent to the collection of their personal information.[172]

---

162 Wikibon, Kelly, J., *Big Data Market Size and Vendor Revenues*, 3 January 2014, available online at <wikibon.org/wiki/v/Big_Data_Market_Size_and_Vendor_Revenues> (accessed 29 October 2014).

163 Tucker, *supra* nt. 22, 2–3.

164 Peppet, R. S., "Unraveling Privacy: The Personal Prospectus and the Threat of a Full-Disclosure Future", *Northwestern University Law Review*, vol. 105, 2011, 1153–1204, 1164.

165 New York Times, Sengupta, S. and Rulsi, E., *Personal Data's Value? Facebook Is Set to Find Out,* 31 January 2012, 'More than the world's largest social network, it is a fast-churning data machine that captures and processes every click and interaction on its platform'.

166 The Washington Post, Tmberg, C., *Austrian student challenges Facebook's use of personal data*, available online at <independent.co.uk/news/world/europe/austrian-student-challenges-facebooks-use-of-personal-data-8219155.html> (accessed 29 October 2014).

167 *Ibid*.

168 McClurg, *supra* nt. 34, 71–72.

169 Economic Times, *IBM Sees Biz Analytics Market Growing Sharply*, 11 May 2010, available online at <articles.economictimes.indiatimes.com/2010-05-11/news/27589148_1_business-analytics-information-integration-ibm-software-group> (accessed 29 October 2014).

170 McClurg, *supra* nt. 34, 71.

171 Lowe, *supra* nt. 21.

172 Directive 95/46/EC, *supra* nt. 9, Article 14(b), requiring that individuals 'be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing, and to be

But our data exhaust is increasingly collected without our awareness.[173] The proportion of personal data passively generated is growing and may even surpass personal data that is "actively" produced or volunteered by individuals.[174] Passively generated personal data can be further broken down into observed and inferred data.[175]

Observed data that is passively generated refers to data captured by recording individuals' activities.[176] Observed data is often, though not always, accompanied by the individual's unawareness of data collection.[177] While an individual may be aware that a browser cookie collects personal information, other forms of observational data elude awareness like rooftop security cameras and event data recorders that are found in most automobiles. In both instances, however, the individual does not proactively volunteer the information.[178] Importantly and perhaps ironically, the individual's lack of awareness and voluntariness tends to shift "ownership" and consequently control of the data to the entity that captured it.[179]

Inferred data, while similar to observed data, is differentiated by synthesis or analysis.[180] Through analysis of varying data, larger institutions create inferred data at a higher expense for predictive purposes.[181] Aggregation and analysis of multiple data points characterise inferred data.[182] Like observed data, inferred data suggests that it is the entity rather than the individual who exercises ownership and control. Especially given the novelty of the analysis, and the time and expense incurred creating it.[183]

Mobile phones provide a good example of passively generated data. Mobile phone companies track and record the location of the world's six billion mobile phone users.[184] Users do not voluntarily and constantly log and submit locational data. Locational data is intensely powerful.[185] On a micro level, for example, doctors can track the movement of diabetes patients, raising alarms for unusual or lethargic locational patterns.[186] On a

---

expressly offered the right to object free of charge to such disclosures or uses'; Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, 1–88.

173 UN Global Pulse, *supra* nt. 20.

174 WEF and Kearney, *supra* nt. 38.

175 *Ibid.,* noting a lack of and increasing need for a workable taxonomy.

176 *Ibid*.

177 *Ibid*.

178 Mueller, P. R., Comment, "Every Time You Break, Every Time You Make—I'll Be Watching You: Protecting Driver Privacy in Event Data Recorder Information", *Wisconsin Law Review*, 2006, 135–189.

179 WEF and Kearney, *supra* nt. 38.

180 *Ibid*.

181 *Ibid*.

182 *Ibid*.

183 *Ibid*.

184 MIT Technology Review, Talbot, D., *Big Data from Cheap Phones*, 23 April 2013, available online at <technologyreview.com/featuredstory/513721/big-data-from-cheap-phones/> (accessed 20 October 2014).

185 The Wall Street Journal, Hotz, R. L., *The Really Smart Phone*, 23 April 2011, available online at <online.wsj.com/news/articles/SB10001424052748704547604576263261679848814> (accessed 20 October 2014).

186 Diabetes Health, Silberstein, N., *Mobile Technology and Blood Glucose Monitoring, Diabetes Health*, 24 June 2007, available online at <diabeteshealth.com/read/2007/06/24/5286/mobile-technology-and-blood-glucose-monitoring/> (accessed 20 October 2014); The New York Times, Wayner, P., *Monitoring Your Health with Mobile Devices*, 22 February 2012, available online at <nytimes.com/2012/02/23/technology/personaltech/monitoring-your-health-with-mobile-devices.html?_r=0> (accessed 20 October 2014).

macro level, large-scale locational data reveal where populations go in the midst of a pandemic, even suggesting 'early warning systems' that far outpace traditional warning methods.[187] Researchers at IBM analysed data and proscribed more efficient bus routes based on people's movements derived from millions of cell phone users in the Ivory Coast.[188]

When sharing location data, mobile companies often aver that they anonymise data before transferring it, either for profit or charitable purposes.[189] Blacking out user names and phone numbers before selling locational data however, fails to satisfy privacy advocates. MIT researchers Cesar A. Hidalgo and Yves-Alexandre de Montjoye demonstrated that four data points about a phone's location can usually identify the user.[190] In fact, with a little more data, researchers divined information about a person's "future" location. One study predicted a person's approximate location up to eighty weeks in the future—with 80% accuracy.[191]

Mobile phone locational data is only one example. Passively generated data and the concomitant dilution of the individual's ownership thereof is accelerating.[192] Individuals exude "data exhaust": actions, choices, locations, and preferences as they go about their daily lives. Proliferating sensors digitally track, store, and communicate these actions to the Internet.[193] 'From 2012 to 2017, machine-to-machine traffic will grow an estimated 24 times to 6 x 1017 bytes per month'.[194] Cisco projects fifty billion devices will connect to the Internet by 2020,[195] but other valid estimates reach up to 200 billion by the same year.[196] Even today, more things are connected to the Internet than there are people in the world.[197] Like locational data from mobile phones, the data generated in an "Internet of Things", will be largely passive.

---

187 Mayer-Schonberger and Cukier, *supra* nt. 13.

188 Talbot, *supra* nt. 90.

189 MIT Technology Review, Leber, J., *How Wireless Carriers are Monetizing Your Movements*, 12 April 2013, available online at <technologyreview.com/news/513016/how-wireless-carriers-are-monetizing-your-movements/> (accessed 20 October 2014).

190 MIT News, Hardesty, L., *How hard is it to 'de-anonymize' cellphone data?,* 27 March 2013, available online at <newsoffice.mit.edu/2013/how-hard-it-de-anonymize-cellphone-data>; see also de Montjoye, Y. A., *Projects*, available online at demontjoye.com/projects.html (accessed 20 October 2014).

191 Tucker, *supra* nt. 22.

192 WEF and Kearney, *supra* nt. 38.

193 Mundie, *supra* nt. 151.

194 WEF and Kearney, *supra* nt. 38, 16.

195 Ericsson, *Ericsson White Paper: More than 50 Billion Connected Devices* , February 2011, available online at <akos-rs.si/files/Telekomunikacije/Digitalna_agenda/Internetni_protokol_Ipv6/More-than-50-billion-connected-devices.pdf> (accessed 20 October 2014).

196 Bajarin, *supra* nt. 1.

197 *Ibid*.

III.3. Internet of Things

The Internet of Things avoids precise definition.[198] In layman's terms, everyday devices—objects—talk to one another online. Connecting objects to a mobile or wired network enables the object to send and receive data automatically without human intervention.[199] Outfitting innumerable objects with tiny identifying and transmitting technology could be radically transforming. One commentator, perhaps dramatically, avers that 'no technology breakthrough since the introduction of telephone networks themselves, with the possible exception of the Internet itself, puts as massive and fundamental changes on the table as the Internet of Things'.[200]

With billions of passive sensors communicating to the Internet already,[201] the Internet of Things is more science than science fiction. From home to the car to work, the Internet of Things captures passive data about individuals and transmits them to the Internet.

III.3.1. Internet of Things at Home

Consider smart meters. Meaningful efficiencies attend electronic sensors that identify, analyse and communicate electricity use from an individual residence to a utility company.[202] Instead of employing workers to walk neighbourhoods reading each resident's meter every six months and then estimating monthly usage from prior history, smart meters provide real time granular data.[203] As of 2012, approximately thirty-six million smart meters record and transmit energy use in the US,[204] and over 200 million smart meters will be installed in the EU by 2020.[205]

A recent eighty-five-page White House report notes the benefits of smart meters, but also admits that they can 'show when you move about your house'.[206] The Report cites

---

198 Dr.Vermesan, O., Dr. Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Dr. Bassi, A., Jubert, I. S., Dr. Mazura, M., Dr. Harrison, M., Dr. Eisenhauee, M., Dr. Doody, P., "Internet of Things Strategic Research Roadmap", *in*: Vermesan, O. and Friess, P., eds., *Internet of Things—Global Technological and Societal Trends*, River Publishers, Denmark, 2011, 9–52, 10, defining the Internet of Things as 'an integrated part of Future Internet including existing and evolving Internet and network developments and could be conceptually defined as a dynamic global network infrastructure with self configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network'.

199 The Value of Our Digital Identity, *supra* nt. 27.

200 IT Business Edge, Weinschenk, C., *Impossible to Overestimate Impact of the Internet of Things*, 30 June 2014, available online at <itbusinessedge.com/blogs/data-and-telecom/impossible-to-overestimate-impact-of-the-internet-of-things.html> (accessed 20 October 2014); see also RFID Journal, Ashton, K., *That Internet of Things' Thing*, 22 July 2009, available online at <rfidjournal.com/articles/view?4986> (accessed 20 October 2014), 'The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so'.

201 Bajarin, *supra* nt. 1.

202 Balough, C. D., "Privacy Implications of Smart Meters", *Chicago Kent Law Review*, vol. 86, ed. 1, 2011, 161–191; Stern, S. M., "Smart-Grid and the Psychology of Environmental Behavior Change", *Chicago Kent Law Review*, vol. 86, ed. 1, 2011, 139–160.

203 *Ibid*.

204 US Energy Information Administration, *Smart Meter Deployments Continue to Rise*, 1 November 2012, available online at <eia.gov/todayinenergy/detail.cfm?id=8590> (accessed 20 October 2014).

205 Navigant Research, *Smart Meters in Europe*, available online at <navigantresearch.com/research/smart-meters-in-europe> (accessed on 20 October 2014).

206 Executive Office of the President, The White House Report, *Big Data: Seizing Opportunities, Preserving Values*, May 2014, available online at

Cornell Professor, Stephen Wicker, who is a bit more specific, noting that electrical devices have unique signatures, and some metering can 'distinguish the microwave from refrigerator, or even the light bulb in the bathroom from the light bulb in the dining room'.[207] Instead of simply knowing a resident's approximate monthly electricity use, smart meters reveal when a person is home, cooking, showering, watching television or on vacation.[208] The information can be used to infer whether the resident is wealthy, clean, healthy or sleep deprived.[209] One illustrative study showed with 96% accuracy that the exact television show or movie being watched could be divined solely from the electrical signal coming from an individual's home.[210]

In addition to smart meters, "smart homes" infuse sensors throughout the home to track resident behaviour and alter home conditions autonomously.[211] Google recently paid USD3.2 billion for Nest, a company that sells thermostats that track residential behaviour in order to adjust home temperature more efficiently.[212] Why spend so much for a self-adjusting thermostat? Nest's value resides in the connections it generates among its devices.[213] In other words, Nest's thermostat does more than cool a room when the resident returns home from work. 'Over time, as the Nest Learning Thermostat uses its sensors to train itself according to your comings and goings, the entire network of Nests in homes across the country becomes smarter'.[214] It is not the thermostat itself that boosts Nest's value, but the interconnectedness of all those thermostats. As the devices talk to each other, they construct an aggregate picture of human behaviour, and predict or anticipate what users want before they know it.[215]

Other home apps or devices use sensors to detect water leaks, open doors, energy use and home security.[216] Sensors can send a text message alerting you that the garage door is open, the bathroom light is on, or that the plants need watering.[217] While the home

---

<whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf> (accessed 20 October 2014).

207 Cornell University, Wicker, S., and Thomas, R., *A Privacy-Aware Architecture For Demand Response Systems*, Proceedings of the 44th Hawaiian Conference on System Science (HICSS-44), Kauai, Hawaii, January 2011 available online at <wisl.ece.cornell.edu/wicker/SWicker_RThomas_HICSS.pdf> (accessed 20 October 2014); see also Computerworld, Thibodeau, P., *The Internet of Things could encroach on personal privacy*, 3 May 2014, available online at <computerworld.com/article/2488949/emerging-technology/the-internet-of-things-could-encroach-on-personal-privacy.html> (accessed 20 October 2014).

208 *Ibid*.

209 *Ibid*.

210 Enev, M. *et al.*, "Inferring TV Content from Electrical Noise", 2011, available online at <miro.enev.us/papers/EMI_CCS_2011.pdf> (accessed 25 November 2014); see also Naked Security, Wisniewski, C., *Smart meter hacking can disclose which TV shows and movies you watch*, 8 January 2012, available online at <nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/> (accessed 20 October 2014).

211 Balough, *supra* nt. 202.

212 Wired, Wohlsen, M., *What Google Really Gets Out of Buying Nest for $3.2 Billion*, 14 January 2014, available online at <wired.com/2014/01/googles-3-billion-nest-buy-finally-make-internet-things-real-us/> (accessed 20 October 2014).

213 *Ibid*.

214 *Ibid*.

215 *Ibid*.

216 Postscapes, Rushing, K., *Wireless Home Sensor Systems*, available online at <postscapes.com/home-wireless-sensor-systems> (accessed 9 December 2014).

217 HGTV, *11 Smart Apps for Your Home*, available online at <hgtv.com/remodel/mechanical-systems/11-smart-apps-for-your-home> (accessed 9 December 2014).

applications of the Internet of Things have been growing and evolving, the user privacy implications have been largely ignored.

III.3.2. Internet of Things in the Car

Walk from the house to the car and the Internet of Things will follow. Toll tags, for example, include radio-frequency identification (RFID) technology that communicates with receptors at toll gantries in order to detect and record when a car passes.[218] While toll agencies routinely protect billing information associated with toll tags, few policies, if any, protect the personal information gathered. Indeed, in New York, toll tags reveal the driver's location in many part of the city regardless of toll gantries. Unbeknownst to users, New York traffic officials designed other uses for toll tags by erecting receptors throughout the city in order to better understand traffic flow in real time.[219] While improving traffic in New York seems innocuous (if unlikely) the technology allows constant automobile tracking without the driver's awareness or any assurance that the information will not be used or sold for other purposes.[220]

Don't use toll tags? License plate readers are proliferating among both private[221] and public organisations.[222] License plate readers capture license plate numbers, as well as the date, time and location of every scan.[223] Policing agencies across the United States collect and often pool this information, retaining the data for unspecified terms.[224] One civil rights group conducted a lengthy investigation among thirty-eight states and 600 local police departments before concluding that 'the documents paint a startling picture of a technology deployed with too few rules that is becoming a tool for mass routine location tracking and surveillance'.[225]

In one Texas city, police scanned an average of 14,547 license plates per day, and retained the information on almost two million license plates in its database.[226] Private entities also track automobiles using license plate readers and then sell the information to third parties, like repossession debt collectors and insurance companies.[227] Two private companies in the US recently collected 'tens of millions of pieces of geo-located information from thousands of license plate readers, mounted on tow trucks, mall

---

218 Forbes, Hill, K., *E-ZPasses Get Read All Over New York (Not Just At Toll Booths),* 12 September 2013, available online at <forbes.com/sites/kashmirhill/2013/09/12/e-zpasses-get-read-all-over-new-york-not-just-at-toll-booths/> (accessed 20 October 2014).

219 *Ibid.*

220 *Ibid.*

221 NBC News, Aegerter, G., *Licence Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, 1919 July 2013, available online at <nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677> (accessed 20 october 2014).

222 Center for Investigative Reporting, Winston, A., *Plans to Expand Scope of License-Plate Readers Alarm Privacy Advocates*, 17 June 2014, available online at <cironline.org/reports/plans-expand-scope-license-plate-readers-alarm-privacy-advocates-6451> (accessed 20 October 2014).

223 Merola, L. M. and Lum, C., "Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition (LPR) Technology", *Judicature*, vol. 96, 2012, 119–126.

224 American Civil Liberties Union, *You Are Being Tracked: How License Plate Readers Are Being Used to Record American's Movements*, 17 July 2013, available online at <aclu.org/alpr> (accessed 20 October 2014).

225 *Ibid*.

226 *Ibid*.

227 NBC News, Aegerter, G., *Licence Plate Data Not Just for Cops: Private Companies Are Tracking Your Car*, 19 July 2013, available online at <nbcnews.com/news/other/license-plate-data-not-just-cops-private-companies-are-tracking-f6C10684677> (accessed 20 October 2014).

security vehicles, police cars, at the entrances to store parking lots, on toll booths or along city streets and highways'.[228]

Combined with other data about an individual, license plate tracking becomes especially troubling because it reveals an impressive depth of field.[229] One California maker of license plate readers plans to fuse locational information from license plate trackers with public record data and eventually facial recognition technology by comparing real time snapshots with photographs from the local department of motor vehicles database.[230]

In contrast to toll tags and license plate readers, several devices *inside* the car collect and disseminate data. "Black boxes" or event data recorders log and retain driving data in most cars sold in the US in the past twenty years.[231] These sensors typically archive speed, revolutions per minute, brake usage, and the sequence of speed and braking immediately before and after a wreck or sudden stop.[232] Insurance companies urge customers to install similar devices that monitor and report speed, miles travelled, acceleration and braking.[233] Presumably, a continuous real-time data feed from thousands of automobiles allows underwriters to better assess risk.[234]

Of course, most cars carry their own GPS systems, with newer cars boasting more sensors and Internet connections, allowing for services ranging from voice activated restaurant recommendations nearby,[235] to automated searches for parking spots across twenty European countries.[236] A majority of industry experts project that connectivity will soon be the principle factor in car purchasing.[237] The consistent and unanswered question remains: How will this data be stored, transferred and used?

III.3.3. The Internet of Things at Work

The Internet of Things does not disappear when leaving the car and entering the workplace. Apart from ubiquitous upper corner video cameras, new data devices in the workplace capture and communicate employees' location, duration of breaks, productivity in completing discrete tasks and more.[238] Identification badges loaded with sensors measure employees' tone of voice, rapidity of speech and social interactions.[239]

---

228 *Ibid*.

229 *Ibid*.

230 Center for Investigative Reporting, Winston, A., *Plans to Expand Scope of License-Plate Readers Alarm Privacy Advocates*, 17 June 2014, available online at <cironline.org/reports/plans-expand-scope-license-plate-readers-alarm-privacy-advocates-6451> (accessed 20 October 2014).

231 National Highway Traffic Safety Administration, "Event Data Recorders", *Federal Register*, vol. 69, 14 June 2014, 32932–32954, 32932–32933.

232 Mueller, *supra* nt. 179.

233 *Id*., 155–160.

234 *Ibid*.

235 See Ford Webpage, *Explore Navigation by Voice*, available online at <support.ford.com/sync-technology/navigation-by-voice-sync-myford-touch> (accessed 20 October 2014).

236 See Parkopedia Webpage, *Parkopedia*, available online at <en.parkopedia.com/> (accessed 20 October 2014).

237 Forbes, Clark, T., *At Mobile World Congress, A Connected Future Becomes Reality*, 27 February 2014, available online at <forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/> (accessed 20 October 2014).

238 MIT Technology Review, Waber, B., *Augmenting Social Reality in the Workplace*, 15 May 2013, available online at <technologyreview.com/news/514371/augmenting-social-reality-in-the-workplace/> (accessed at 20 October 2014).

239 *Ibid*; Wall Street Journal, Wilson, J. H., *Wearable Gadgets Transform How Companies Do Business*, 20 October 2013, available online at <online.wsj.com/articles/wearable-gadgets-transform-how-companies-do-business-1382128410?tesla=y> (accessed 25 November 2014).

One company found that more socially engaged employees performed better,[240] leading a CEO to claim that he can predict 'from a worker's patterns of movement whether that employee is likely to leave the company, or score a promotion'.[241]

Another company seeks to use data sensors and analytics to augment social interactions in the workplace.[242] Analytical software set to optimise productivity determines which employees should be talking or socialising with certain other employees.[243] To repeat, software—in the interest of productivity—determines which employees should be interacting.[244] Actual workplace walls, coffee machine locations and other commons areas robotically move based on this algorithm to encourage specific employees to interact at specific times.[245] 'Unlike augmented reality, which layers information on top of video or your field of view to provide extra information about the world, augmented social reality is about systems that change reality…'.[246]

All of these sensors—at home, in the car, or at work—generate terabytes of data, much of it personal and most of it unregulated. Libraries affix RFIDs to every book in their collections.[247] Dentists graft sensors into toothbrushes that measure how you brush, identify problem areas, and send the bad news to the cloud for virtual check-ups.[248] Thousands of other examples range from tilt sensors in beer mugs that record how much someone consumes[249] to ingestible pharmaceuticals that measure and transmit internal bodily functioning.[250]

We generate much of this passive data simply by moving from one place to another; it is nearly impossible not to emit data exhaust. Everyday objects equipped with sensors that communicate with the Internet already exist and more are on the way.[251] Over 200 billion worldwide are expected by 2020.[252] For the cost of a few pennies each, RFIDs have the capability to track just about anything.[253] It is entirely feasible, if not likely, that most retail products will soon carry RFID tags that transmit data to a computer when it

---

240 *Ibid.*

241 Wall Street Journal, Silverman, R. E., *Tracking Sensors Invade the Workplace*, 7 March 2013, available online at <online.wsj.com/articles/SB10001424127887324034804578344303429080678> (accessed 25 November 2014).

242 Waber, *supra* nt. 238.

243 *Ibid*.

244 *Ibid*.

245 *Ibid*.

246 *Ibid.*

247 Molnar and Wanger, *supra* nt. 3, the study suggests that readers set up at airport security could identify those with "hotlisted" books and detain them for additional screening.

248 Forbes, Clark, T., *At Mobile World Congress, A Connecctd Future Becomes Reality*, 27 February 2014, available online at <forbes.com/sites/sap/2014/02/27/at-mobile-world-congress-a-connected-future-becomes-reality/> (accessed 20 October 2014).

249 Wired, Thompson, C., *No Longer Vaporware: The Internet of Things is Finally Talking*, 6 December 2012, available online at <wired.com/2012/12/20-12-st_thompson/> (accessed 20 October 2014).

250 See e.g., Proteus Digital Health, *Digital Health Feedback System*, available online at <proteus.com/technology/digital-health-feedback-system/> (accessed 20 October 2014).

251 WEF and Kearney, *supra* nt. 38.

252 Bajarin, *supra* nt. 1.

253 Schmidt, J. M., "RFID and Privacy: Living in Perfect Harmony", *Rutgers Computer and Technology Law Journal*, vol. 34, 2007, 247–272, 250–252.

is within twenty feet of a reader.[254] 'Pretty much everything you can imagine will wake up.'[255]

Given the expansion of sensors and the emergence of the Internet of Things, it is becoming increasingly unlikely that a person could know precisely how much of their data is captured, who controls it and for what purpose.

IV. Privacy Regulation Through Risk Management

The leading law on privacy, the EU's 1995 Directive, attempts to protect a user's personal information in a number of ways. Primarily, the law requires those who process personal information to give notice to the user and then allow the user to opt out.[256] The user must consent, in other words, before an entity can collect personal data.[257] The law also allows users to access and correct their personal data after it has been collected by another.[258]

Apart from the problematic and overbroad concept of "personal information",[259] the law fails to account for the Internet of Things. It fails to countenance the proliferation of passive data collection, and instead relies on the faulty premise that users actively volunteer all personal information.[260] Notice and consent obligations, like those in the Directive, apply poorly to passive data collection.[261]

How do businesses and governments issue notice and obtain consent from every person strolling on the sidewalk, whose images are captured by rooftop cameras? Must toll tag and license plate readers notify and obtain consent before every scan? Can residents withhold their consent to data gathering when a municipal government requires them to use smart meters? For those municipalities that do allow residents to opt-out of smart metering, does the notice provide clarity with regard to the amount of data collected and if so, can a resident access and correct that data? (*I was using the microwave, not the shower at 10:50pm on 11 August 2014.*) Does the notice include notice of potential or future uses of such data, including sale or transfer to third parties?

Requiring employers to provide notice and obtain consent before monitoring employee location, productivity and behavior poses similar difficulties. Even if a single global consent sufficed rather than requiring employers to obtain consent each time an employee's behavior is monitored, that consent is often illusory; no consent, no job.[262] Even in the home, users who purchase and install a Nest thermostat are likely consenting

---

254 *Ibid*; Kobelev, O., "Recent Development, Big Brother on a Tiny Chip: Ushering in the Age of Global Surveillance Through the Use of Radio Frequency Identification Technology and the Need for Legislative Response", *North Carolina Journal of Law & Technology*, vol. 6, ed. 2, 2005, 325–342.

255 Cisco, *What is the Internet of Everything*, available online at <cisco.com/web/tomorrow-starts-here/ioe/> (accessed 25 November 2014).

256 Directive 95/46/EC, *supra* nt. 9, Article 14(b), requiring that individuals 'be informed before personal data are disclosed for the first time to third parties for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses'; Shaffer, G., "Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards", *Yale Journal of International Law*, vol. 25, 2000, 1–88.

257 *Ibid.*

258 *Ibid.*

259 Taylor, *supra* nt. 100.

260 WEF and Kearney, *supra* nt. 38, 16.

261 *Ibid.*

262 Levin, A., "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada", *Canadian Journal of Law and Society*, vol. 22 ed. 2, 2007, 197–230; Willborn, S. L., "Consenting Employees: Workplace Privacy and the Role of Consent", *Louisiana Law Review*, vol. 66, ed. 4, 2006, 975–1008.

to the use of their personal information in order to optimise the home's temperature.[263] But does this consent extend to sharing that information with countless other automated thermostats and using aggregated information to predict future behavior? Does their consent cover neighbours or other invitees to the home?

One report from the 2014 World Economic Forum put it this way: 'With an increasing proportion of personal data now being passively collected by sensors or synthetically generated by algorithms, engaging individuals for consent to use data they know nothing about (and for purposes which are yet to be defined) remains problematic.'[264] Notice, consent, access and correction, while arguably useful tools regulating a user's voluntary divulgence of personal information, fall short when personal data is passively obtained. Current privacy laws miscarry when data 'originates at a distance from the immediate perception of individuals and where consent, participation and awareness are seldom feasible'.[265]

Instead of a broad privacy law that declares all personal data to be protected and that requires notice and consent before data collection, privacy laws should narrowly target specific harms that attend specific informational privacy violations. Regulating the *use* of sensitive data as it relates to particular risks or harms better comports with consumer law generally and permits the needed adaptability to reflect context and changing technology.[266]

This is not a novel idea.[267] Some in the privacy community liken this proposed regulatory approach to the field of risk management.[268] Calibrating the risk or the harm from the individual's viewpoint in using data in a particular way reveals the value of that data and allows local regulatory regimes to adopt protective policies incrementally.[269] It requires a normative taxonomy regarding data usage.[270] How is particular data used in a particular context? Sector or Industry-specific uses may provide a starting point; educational uses differ from healthcare uses or advertisement uses.

Within a given context or sector, a particular use would include parameters on who is authorised to process the data and for what purposes. Depending on context, user preferences could be factored in. Identifying and defining diverse data contexts and uses, and identifying the attendant risks or harms from the user's viewpoint are critical to successful implementation of contextual and harm-based personal data regulation.

License plate readers, for example, are sporadically and sparsely regulated throughout the United States.[271] Identifying the benefits of license plate readers, the privacy risks or harms from the individual's viewpoint, and the various uses that gleaned data may have, strengthens the likelihood of creating concrete policy and pragmatic regulation—much

---

263 Nest, *Terms of Service*, available online at <nest.com/legal/terms-of-service/> (accessed 20 October 2014).

264 WEF and Kearney, *supra* nt. 38, 10.

265 *Ibid.*

266 Spina, A., "Risk Regulation of Big Data: Has the Time Arrived for a Paradigm Shift in EU Data Protection Law?", *European Journal of Risk Regulation,* vol. 5, ed. 2, 2014, 248–252.

267 *Ibid*; Centre for Information Privacy Leadership, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice*, 19 June 2014, available online at <hunton.com/files/upload/Post-Paris_Risk_Paper_June_2014.pdf> (accessed 20 October 2014) (Post Paris Risk Paper).

268 Centre for Information Privacy Leadership, *Privacy Risk Framework and Risk-based Approach to Privacy*, 2014, available online at <informationpolicycentre.com/privacy_risk_framework/>; see also Post Paris Risk Paper, *supra* nt. 267.

269 *Ibid*; Spina, *supra* nt. 266.

270 WEF and Kearney, *supra* nt. 38.

271 American Civil Liberties Union, *supra* nt. 224.

more so than a global prohibition on collecting almost all personal information unless each individual is given notice and then consents. Policymakers might recognise the benefit to law enforcement and allow license plate readers for the specific purpose of pursuing certain criminal investigations. The harms or risks to individuals, however, might lead policymakers to outlaw storage of license plate data about innocent people as well as sharing that data with third parties. By addressing data collection from the individual's viewpoint, institutions can better identify privacy risks and create usage policies to minimise the same.[272]

Institutions gathering or using sensitive data can prioritise risk and use by asking: What is the intended use? What risks to the individual attend that use and how likely is it for that harm to occur? How severe is the harm: loss of property, physical injury or reputational damage?[273] Prioritisation based on seriousness or likelihood of harm borrows from traditional risk management protocols and allows policymaking that is tailored to context. 'Risk management can be applied across the data value chain to more granularly access systemic reliability, codes of conduct and legal compliance.'[274]

Of course, this approach is not a panacea. Different individuals perceive privacy harms differently. Many have suggested that generally, Americans are far less concerned about certain privacy matters than Europeans.[275] Moreover, individuals, regardless of residence, may have dramatically different privacy sensibilities. To one person, cookies that remember past Internet purchases are harmless; to another they are abhorrent. But the law has long accepted and regulated diverse individual perceptions of harm and risk.[276]

Effective regulation that protects individual privacy while facilitating innovation is a Gordian knot,[277] especially in light of the deluge of easily accessible data combined with rapidly changing technology. The proliferation of data, elaborate analytical capabilities and borderless flow of digital information befog regulatory efforts. Compounding the problem, data increasingly originates passively from sensors and analytic compilations, rendering individuals less aware and more distant from decisions regarding the use of their data.

For these reasons, and others not mentioned, global privacy regulation will remain formidable. But the bedeviling attributes plaguing data privacy also suggest that omnibus privacy laws like the Directive undermine privacy as much as protect it. Laws that provide blanket prohibitions and that hinge on an expansive understanding of personal information and that call for individuals' notice and consent cannot be fairly applied or enforced. A risk of harm-based legal framework that turns on the use of information contextualises potential privacy violations and allows institutions and governments to customise policies relevant to the risk of harm.

---

272 Post Paris Risk Paper, *supra* nt. 267.

273 *Ibid*.

274 WEF and Kearney, *supra* nt. 38, 18.

275 See e.g., Whitman, J. Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal*, vol. 113, 2004, 1151–1221, 1194; Walker, R. K., "The Right to Be Forgotten", *Hastings Law Journal*, vol. 64, 2012, 257–286.

276 Spina, *supra* nt. 266.

277 Encyclopedia Britannica, *Gordian Knot*, available online at <britannica.com/EBchecked/topic/239059/Gordian-knot> (accessed 25 November 2014).

V. Conclusion

Legacy privacy laws, like the EU Directive, seek to protect privacy in the Age of Information. They are failing. To some degree, they undermine privacy by restricting all processing of personal information—even processing that would ensure that data remains secure and therefore private. They cast a wide net; the laws include almost any data pertaining to a person. With burgeoning de-anonymising algorithms, efforts to scrub identifying data prove fruitless, resulting in an ever-expanding reach. As a result, the Directive and laws like it capture a great ocean of data processing, which foments uncertainty and uneven enforcement, rather than harmonising data processing regulation. The laws' laudable goal in principle, is reduced to platitude and bureaucracy in practice.

The Internet of Things sharpens this dysfunction. The Directive rests on the faltering presumption that individuals voluntarily divulge personal information, when the growing trend indicates a wide lacuna between user awareness and data collection. Users do not voluntarily post GPS locational data every few seconds or record and transmit automobile acceleration and braking events.

Privacy laws that turn on personal information and that require notice and consent before data collection poorly reflect the technological landscape and remain impractical at best. Privacy laws should focus on data use, not collection. Privacy laws should identify and address the specific harm or risk associated with the use of sensitive data in particular contexts. Among the privacy community, this approach is likened to the field of risk management. It allows contextualisation among privacy laws and encourages incremental and adaptable regulation based on specific risks associated with potential misuse of sensitive data.

Informational privacy is ominously fleeting. We have already passed the point and missed the opportunity of effectively regulating the collection of personal data. Rather than persist in vain to try regulating the collection of personal data, policymakers should consider regulating its use based on risk of harm.

*