Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws

OMER TENE*

TABLE OF CONTENTS

I. INTRODUCTION

Privacy law is suffering from a midlife crisis. Despite well-recognized tectonic shifts in the socio-technological-business arena, the information privacy framework continues to stumble along like an aging protagonist in a rejuvenated cast. The framework's fundamental concepts are outdated; its goals and justifications in need of reassessment; and yet existing reform processes remain preoccupied with internal organizational measures, which yield questionable benefits to individuals. At best, the current framework strains to keep up with new developments; at worst, it has become irrelevant. More than three decades have passed since the introduction of the *OECD Privacy*

* Vice Dean of the College of Management Haim Striks School of Law, Israel; Affiliate Scholar at the Stanford Center for Internet and Society; Senior Fellow at the Future of Privacy Forum. I would like to thank Ruth Boardman, Peter Fleischer, and Christopher Kuner for their insightful comments. Research for this article was supported by the College of Management Haim Striks School of Law research fund and the College of Management Academic Studies research grant.

Guidelines; and fifteen years since the *EU Directive* was put in place and the "notice and choice" approach gained credence in the United States. This period has seen a surge in the value of personal information for governments, businesses, and society at large. Innovations and breakthroughs, particularly in information technologies, have transformed business models and affected individuals' lives in previously unimaginable ways. Not only technologies, but also individuals' engagement with the data economy have radically changed. Individuals now proactively disseminate large amounts of personal information online via platform service providers, which act as facilitators rather than initiators of data flows. Data transfers, once understood as discrete point-to-point transmissions, have become ubiquitous, geographically indeterminate, and typically "residing" in the cloud.

This Article addresses the challenges posed to the existing information privacy framework by three main socio-technological-business shifts: the surge in big data and analytics; the social networking revolution; and the migration of personal data processing to the cloud. The term *big data* refers to the ability of organizations to collect, store, and analyze previously unimaginable amounts of unstructured information in order to find patterns and correlations and draw useful conclusions. Big data creates tremendous value for the world economy, individuals, businesses, and society at large. At the same time, it heightens concerns over privacy, equality, and fairness, and pushes back against well-established privacy principles. *Social networking services* have revolutionized the relationship between individuals and organizations. Those creating, storing, using, and disseminating personal information are no longer just organizations, but also geographically dispersed individuals who post photos, submit ratings, and share their location online. The term *cloud computing* encompasses (at least) three distinct models of utilizing computing resources through a network—software, platform, and infrastructure as a service. The advantages of cloud computing abound and include, from the side of organizations, reduced cost, increased reliability, scalability, and security, and from the side of users, the ability to access data from anywhere, on any device, at any time, and to collaborate on a single document across multiple users; however, the processing of personal information in the cloud poses new privacy risks.

In response to these changes, policymakers in the Organization for Economic Co-operation and Development (OECD), EU and the United States launched extensive processes for fundamental reform of the information privacy framework. The product of these processes is set to become the second generation of information privacy law. Yet, as discussed in this Article, the second generation is strongly anchored in the existing framework, which in turn is rooted in an architecture dating back to the 1970s. The major dilemmas and policy choices of information privacy remain unresolved.

First, the second generation fails to update the definition of personal data,[1] the fundamental building block of the framework. Recent advances in re-identification science have shown the futility of traditional de-identification techniques in a big data ecosystem. Consequently, the scope of the framework is either overbroad, potentially encompassing every bit and byte of information, ostensibly not about individuals; or overly narrow, excluding de-identified information, which could be re-identified with relative ease. More advanced notions that have gained credence in the scientific community, such as differential privacy and privacy enhancing technologies, have been left out of the debate.

Second, the second generation maintains and even expands the central role of consent. Consent is a wild card in the privacy deck. Without it, the framework becomes paternalistic and overly rigid; with it, organizations can whitewash questionable data practices and point to individuals for legitimacy. The Article argues that the role of consent should be demarcated according to normative choices made by policymakers with respect to prospective data uses. In some cases, consent should not be required; in others, consent should be assumed subject to a right of refusal; in specific cases, consent should be required to legitimize data use. Formalistic insistence on consent and purpose limitation can impede data driven breakthroughs that benefit society as a whole.

Third, the second generation remains rooted on a linear approach to processing whereby an active "data controller" collects information from a passive individual, and then stores, uses, or transfers it until its ultimate deletion. The explosion of peer produced content, particularly on social networking services, and the introduction into the data value chain of layer upon layer of service providers, have meant that for vast swaths of the data ecosystem, the linear model has become obsolete. Privacy risks are now posed by an indefinite number of geographically dispersed actors, not least individuals themselves, who voluntarily share their own information and that of their friends and relatives. Despite much discussion of "Privacy 2.0," the emerging framework fails to account for these changes. Moreover, in many contexts, such as mobile applications, behavioral advertising, or social networking services, it is not necessarily the controller, but rather an intermediary or platform provider, that wields the most control over information.

Fourth, the second generation, particularly of European data protection laws, continues to view information as "residing" in a jurisdiction, despite the geographical indeterminacy of cloud storage and transfers. For many years, transborder data flow regulation has caused much consternation to global

---

[1] "Personal data" is the term of art under the European framework; the equivalent term in U.S. frameworks is "personally identifiable information" (PII). This Article uses both terms interchangeably. Although not identical, these terms are the basic building blocks for the respective information privacy frameworks. For differences between both terms, see Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. (forthcoming 2014) (manuscript at 5–11) (on file with authors).

businesses, while generating formidable legal fees. Unfortunately, this is not about to change.

While not providing solutions to these challenging problems, the Article sets an agenda for future research, identifying issues and potential paths towards a rejuvenated framework for a rapidly changing environment.

II. THE FIRST GENERATION

The current legal framework for information privacy and data protection is founded largely on instruments such as the 1980 *OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (the "*OECD Guidelines*");[2] the *European Union Data Protection Directive* 95/46/EC (the "*EU Directive*");[3] and sector-specific legislation in the United States.[4] While these regimes all bear substantial similarities, they also have unique features, which are briefly discussed in this Part. Specifically, the *OECD Guidelines*, while innovative in their statement of the now generally accepted fair information practice principles (FIPPs), lack specificity and enforcement mechanisms. The *EU Directive*, while surely the most detailed and influential legislation in the field, leaves much to be desired in terms of consistency, harmonization, and effective enforcement. The U.S. regime, while flexible and occasionally effectively enforced, is a quilt work of statutory islands connected by vast regulatory lacunae and sometimes based on tenuous legal mandate.[5]

---

[2] Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, OECD Doc. C(80)58/FINAL (Sept. 23, 1980) [hereinafter *OECD Guidelines*], *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[3] Council Directive 95/46/EC of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].

[4] *See, e.g.*, Fair Credit Reporting Act (FCRA) of 1970, 15 U.S.C. § 1681b (2012); Children's Online Privacy Protection Act (COPPA) of 1998, 15 U.S.C. §§ 6501–6506 (2012); Gramm–Leach–Bliley Act (GLBA) of 1999, 15 U.S.C. § 6809(4)(A) (2012); Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710 (2012); Family Educational Rights and Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g (2012); Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, 123 Stat. 226 (2009) (codified as amended in scattered sections of 42 U.S.C.); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936.

[5] The primary source of authority for the Federal Trade Commission's privacy enforcement is Section 5 of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." Federal Trade Commission (FTC) Act, 15 U.S.C. § 45(a)(1) (2012); *see also About: A Brief Overview of the Federal Trade Commission's Investigative and Law Enforcement Authority*, FTC, http://www.ftc.gov/ogc/brfovrvw.shtm. (last updated July 2008).

A. *The OECD Guidelines*

In 1980, the OECD adopted the *OECD Guidelines* to address information privacy concerns related to the increased use of personal data as well as the risk that member economies will impose restrictions on transborder data flows.[6] The *OECD Guidelines* contained the first internationally agreed-upon iteration of the FIPPs.[7] They have been highly influential in setting the context for national legislation and have had a clear impact on the Council of Europe Convention 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data ("*Convention 108*"),[8] which was negotiated and accepted around the same time as the *EU Directive*, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA),[9] and additional legislative instruments. They represented a consensus on basic principles that should govern the collection and use of personal data, and were framed in concise, technology-neutral language, which has proven quite resistant to change.

The main advantages of the *OECD Guidelines* include their definition of the term "personal data," broad scope, and statement of the FIPPs. The content-neutral definition of personal data as "any information relating to an identified or identifiable individual" preceded by more than a decade a similar definition used in the *EU Directive*, which, as discussed below, is one of the great artifacts of the current framework.[10] The scope of the *OECD Guidelines*, covering both public and private sector data processing, demonstrates that given the right level of abstraction, similar principles can apply to both businesses and governments, greatly simplifying the framework and reducing incentives for regulatory arbitrage.[11] The statement of the FIPPs in the *OECD Guidelines* remains compelling even today, more than three decades after its induction. Indeed, in its recent Consumer Privacy Bill of Rights, the Obama Administration refers

---

[6] *OECD Guidelines*, *supra* note 2.

[7] In fact, the first version of the FIPPs appeared in the United States in a 1973 report sponsored by the Department of Health, Education, and Welfare (HEW), *Records, Computers, and the Rights of Citizens*. SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS. OF THE U.S. DEP'T OF HEALTH, EDUC. & WELFARE (HEW), RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS 50 (1973).

[8] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *opened for signature* Jan. 1, 1981, E.T.S. No. 108 (entered into force Oct. 1, 1985).

[9] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (amended 2011) (Can.).

[10] *OECD Guidelines*, *supra* note 2.

[11] *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, 27–28 (2003); *see also* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 629–30 (2004); Jon D. Michaels, *All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 932 (2008).

back to the FIPPs as stated in the *OECD Guidelines*, including collection limitation, data quality, purpose specification, use limitation, security, openness, individual participation, and accountability.[12]

Yet the *OECD Guidelines* have their drawbacks too. To begin with, unlike the *EU Directive* or national data protection legislation, the *OECD Guidelines* are not binding in nature.[13] Second, the *OECD Guidelines* fail to provide (or even call) for an enforcement mechanism, leaving the matter largely to the good will of member countries.[14] Finally, what may be the greatest advantage of the *OECD Guidelines*, their clear, succinct, minimalistic prose, proves to be a liability at the stage of implementation. Principles such as "accountability" or the provisions on transborder data flows are not intuitively clear and require elaboration.

B. *The EU Directive*

Few would dispute that the *EU Directive* remains the most significant piece of data protection legislation in the world today. The *EU Directive* emerged in 1995 after years of negotiations[15] and more than two decades' worth of distinct, un-harmonized data protection legislation in multiple European jurisdictions.[16] As such, one of its primary purposes was to harmonize European data protection laws, removing a potential barrier to data flows among Member States. In addition, the *EU Directive* was premised on a conception of

---

[12] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 32 n.39 (Feb. 2012) [hereinafter THE WHITE HOUSE BLUEPRINT], *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. An annex to the Report includes a table comparing the Consumer Privacy Bill of Rights to the *OECD Guidelines* and other documents. *Id.* at 49–52.

[13] *OECD Guidelines*, *supra* note 2.

[14] This has been partly offset by the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy. ORG. FOR ECON. CO-OPERATION & DEV., RECOMMENDATION ON CROSS-BORDER CO-OPERATION IN THE ENFORCEMENT OF LAWS PROTECTING PRIVACY 6–7 (2007) [hereinafter OECD CROSS-BORDER RECOMMENDATION], *available at* http://www.oecd.org/internet/ieconomy/38770483.pdf.

[15] Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data*, 80 IOWA L. REV. 445, 445 (1995).

[16] Datenschutzgesetz, [Data Protection Act], Oct. 7, 1970, Gesetz- und Verordnungsblatt für das Land Hessen [BGBL. I] at 626, § 6 (Ger.) (West German state of Hesse data protection act); Loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Law 78-17 of January 6, 1978 Relating to Computers, Files and Freedoms], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, p. 227, arts. 6–13 (French data protection law); Lov om personen register av 9 June 2003, nr. 48, *available at* http://www.regjeringen.no/nb/dep/jd/dok/nouer/1997/NOU-1997-19/25.html?id=140995 (Norwegian personal data registers act); NORVÉGE, Norges lover: 1685–1985, at 2180 (Sjur Brækhus, Magnus Aarbakke, Universitetet I Oslo eds., 1986).

information privacy, or in the words of the West German Federal Constitutional Court "informational self-determination," as a fundamental human right.[17]

The *EU Directive* has reached its zenith as an influential legislative instrument based on several factors, including its sheer geographical scope, applying to the first or second largest economy in the world; its heavily bureaucratic requirements for organizations operating within the EU, which prompted multinational businesses to devote significant resources to compliance; and its unique mechanism to project power outside of the EU by subjecting transborder data flows to oversight and regulation.[18] Moreover, the *EU Directive* established a network of national regulators, typically referred to as the data protection authorities (DPAs), which separately and through their coordination mechanism (the Article 29 Working Party) created a locus for discussion, analysis, interpretation, and development of data protection law.[19]

The *EU Directive* has numerous advantages, including its definition of key terms and concepts; binding, enforceable nature; relative technological neutrality; and institutions for enforcement and legal development. The definition of personal data is similar to that in the *OECD Guidelines*, focusing on identifiability and impartial to content. The definition of "processing" is similarly elegant, covering "any operation or set of operations which is performed upon personal data," including collection, storage, use, disclosure or deletion. The definition of consent as "any freely given, specific and informed indication of . . . wishes" is compelling. And the introduction of the framework's main actors—controllers, processors, data subjects, and third parties—has for the most part been useful. In stark contrast to the *OECD Guidelines*, the *EU Directive* is a binding instrument, which has been transposed into the national legislation of each of the EU Member States and has established regulatory agencies with (admittedly inconsistent) enforcement powers.[20] The DPAs have become a center of knowledge and core for a community of professionals devoted to data protection,[21] and have made a

---

[17] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Dec. 15, 1983, 65 BVerfG 1, 68–69 (1984) (Ger.); *see* ANITA L. ALLEN, UNPOPULAR PRIVACY: WHAT MUST WE HIDE? 13 (2011); Edward J. Eberle, *The Right to Information Self-determination*, 2001 UTAH L. REV. 965, 978, 1004, 1006.

[18] Michael D. Birnhack, *The EU Data Protection Directive: An Engine of a Global Regime*, 24 COMPUTER L. & SECURITY REV. 508, 510–11 (2008). *See generally* Bartosz M. Marcinkowski, *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, 74 OHIO ST. L.J. 1167 (2013).

[19] Directive 95/46/EC, *supra* note 3, 1995 O.J. at 39.

[20] *Id.* at 34.

[21] The main annual meeting place for DPAs is the International Data Protection and Privacy Commissioners Conference, which was established in 1979. In recent years, the Conference has grown into a one week event, comprising an open session accessible to all privacy professionals, including industry, government, academia, and civil society representatives, and a closed session only accessible to data protection and privacy authorities, as well as several side meetings organized by international and non-governmental organizations, such as the OECD and Public Voice. For a history of all

formidable contribution to advancing the framework in both joint and national opinions, guidance documents, and enforcement notes.[22] Finally, while far more detailed than the *OECD Guidelines*, the *EU Directive* managed to remain relatively technology neutral and, for the most part, has survived the rigors of the technological land shifts that have occurred since its introduction, including the advent of the Internet, mobile, biometrics, and cloud.[23]

At the same time, the *EU Directive* has also had noticeable problems, which have led to a comprehensive reform effort currently debated among the centers of powers in Brussels, Strasbourg, and Member State capitals. First, despite its aspiration to harmonize data protection laws across the EU, the *EU Directive* left ample room for national implementation, yielding twenty-seven distinct and sometimes conflicting regimes. Second, the highly bureaucratic nature of some of its regulatory mechanisms, such as notification of or authorization for data processing, helped critics portray the *EU Directive* as an impediment to innovation and economic progress;[24] this was particularly evident with respect to transborder data transfers, which have given rise to an entire industry of contract-signing and form-filling professionals who generate little if any benefit to individuals' privacy. Third, there has been a noticeable gap between European data protection law on the books and on the ground;[25] enforcement has been fickle and sanctions weak. Finally, consistent with its source as "common market" measure of harmonization, the scope of the *EU Directive* explicitly excludes any activities in the zone of law enforcement or national security; meaning that precisely those activities which raise most concern from a fundamental rights perspective remain largely unaffected by the framework.[26]

---

conferences see *Conferences*, PRIVACYCONFERENCE.ORG, https://privacyconference2013.org/Conferences (last visited Oct. 27, 2013).

[22] *See Opinions and Recommendations*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation (last updated Oct. 11, 2013).

[23] As discussed below, while technology-neutral on the surface, the *EU Directive* represents a technological paradigm dating back to the age of mainframe computers. *See* Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J.L. & TECH. 24, 70 (2012).

[24] *See, e.g.*, AM. CHAMBER OF COMMERCE TO THE EUR. UNION, AMCHAM EU POSITION ON THE GENERAL DATA PROTECTION REGULATION 3, 6, 11 (2012), *available at* https://dataskydd.net/wp-content/uploads/2013/01/AmCham-EU_Position-Paper-on-Data-Protection-20120711.pdf.

[25] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 253 (2011).

[26] In transposing the *EU Directive* into national law, many EU Member States have applied the information privacy framework to law enforcement or national security authorities yet at the same time they have carved out broad exemptions for those same entities. *See, e.g.*, Data Protection Act, 1998, c. 29, §§ 28–29 (Eng.).

C. *The U.S. Framework*

The U.S. information privacy framework differs markedly from that in Europe. To begin with, the United States lacks comprehensive, omnibus information privacy legislation, relying instead on sector-specific piecemeal statutes covering certain types of data (health, financial, credit reporting, Federal government, children's, video rental, and more) while leaving others (for example, online browsing and location) largely unregulated.[27] Moreover, information privacy is not a constitutionally protected right in the United States; and even the constitutional status of privacy remains hotly debated.[28] Finally, unlike Europe, the United States does not have a dedicated privacy enforcement agency. While the Federal Trade Commission (FTC) has greatly raised its profile in this space, its authority rests on a tenuous legal mandate. It is restricted to protecting consumers (as opposed to employees or citizens) and, even in the consumer context, its authority does not apply across the board.[29] Furthermore, as a consumer protection and antitrust agency, the FTC is charged with a broader mandate than just the regulation of privacy, as are state attorneys general who are sometimes involved in privacy enforcement.

At the same time, as Ken Bamberger and Deirdre Mulligan demonstrated, in the United States, much like in Europe, privacy on the books differs markedly from privacy on the ground.[30] Based on extensive interviews with experts and professionals, Bamberger and Mulligan show that a confluence of factors contributes to the U.S. framework delivering greater information privacy protection than the sum of its parts.[31] Specifically, they point out the elevated profile of the FTC as an enforcement agency and its shift from the "deceptive" to the "unfair" strain of its legislative mandate;[32] the emergence of the role of the Chief Privacy Officer;[33] the introduction of security breach notification

---

[27] For recent criticism see Daniel Solove, *The Chaos of US Privacy Law*, LINKEDIN (Oct. 24, 2012), http://www.linkedin.com/today/post/article/20121024165918-2259773-the-chaos-of-us-privacy-law.

[28] There are two strains of privacy protection in the U.S. Constitution: Fourth Amendment protection against unreasonable search and seizure; and the uniquely American concept of "decisional privacy," protecting, for example, a "woman's decision whether or not to terminate her pregnancy." Roe v. Wade, 410 U.S. 113, 153 (1973); *see* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340, 1357, 1391.

[29] The FTC's Section 5 authority does not extend to financial institutions (which are subject to the jurisdiction of the Federal Reserve Board); common carriers (subject to the Federal Communications Commission); air carriers; insurance companies; and non-profit organizations. 15 U.S.C. § 45(a)(2) (2012).

[30] Bamberger & Mulligan, *supra* note 25, at 260.

[31] *Id.* at 251.

[32] *Id.* at 273.

[33] Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897 (2013).

statutes in nearly all states;[34] the activity of the press and privacy advocates in making consumer privacy a market reputation issue;[35] and the emergence of industry self-regulation and standards for best practices, partly as a plan to avert legislation.[36] Additional factors include the existence in the United States of potent avenues for individual enforcement, namely though class action lawsuits;[37] and the increasing engagement of the United States under the Obama Administration in international privacy fora, including the International Conference of Privacy and Data Protection Commissioners, the OECD, and the Asia-Pacific Economic Cooperation (APEC); one example of which is the creation of the Global Privacy Enforcement Network (GPEN), which was driven by the FTC in order to foster cross-border co-operation among privacy authorities.[38]

The U.S. framework has several advantages. First, certain parts of the U.S. framework were forward looking and innovative when introduced; consider the Federal Privacy Act of 1974,[39] which featured one of the first ever legislated versions of the FIPPs; or the HIPAA,[40] which introduced what at the time was a nuanced approach to the definition of personal data and the concept of de-identification. Second, when competent and authorized to act, the FTC is a formidable enforcement agency striking fear in the heart of any actor with a cavalier approach to privacy. Indeed, if the results of an investigation recently conducted by the FTC into the data practices of Facebook are compared with those of a similar investigation conducted under the *EU Directive* by the Irish data protection regulator, it is clear that the U.S. framework has punch. Finally, the elevation of privacy, particularly in the digital context, to a front-page news item,[41] speaking to the American ethos of insulation from power—if not to

---

[34] *See* Priscilla M. Regan, *Federal Security Breach Notifications: Politics and Approaches*, 24 BERKELEY TECH. L.J. 1103, 1120 (2009).

[35] *See, e.g.*, *What They Know Series*, WALL ST. J., http://online.wsj.com/public/page/what-they-know-digital-privacy.html (last visited Oct. 27, 2013).

[36] *See, e.g.*, DIGITAL ADVER. ALLIANCE, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 19 (2012), *available at* http://www.aboutads.info/obaprinciples; GSMA, MOBILE PRIVACY PRINCIPLES 3 (2012), *available at* http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacyprinciples2012.pdf; NETWORK ADVER. INITIATIVE, 2013 CODE OF CONDUCT 1 (2013), *available at* http://www.networkadvertising.org/2013_Principles.pdf.

[37] Peter Fleischer, *Privacy-Litigation: Get Ready for an Avalanche in Europe*, PETER FLEISCHER: PRIVACY . . . ? (Oct. 26, 2012, 10:00 AM), http://peterfleischer.blogspot.com/2012/10/privacy-litigation-get-ready-for.html. *But see* Eric Goldman, *The Irony of Privacy Class Action Litigation*, 10 J. ON TELECOMM. & HIGH TECH. L. 309, 310 (2012) (arguing against allowing class action lawsuits as enforcement mechanisms in privacy statutes).

[38] See GLOBAL PRIVACY ENFORCEMENT NETWORK, https://www.privacyenforcement.net (last visited Oct. 27, 2013).

[39] Privacy Act of 1974, 5 U.S.C. § 552a (2012).

[40] HIPAA, Pub. L. No. 104-191, 110 Stat.1936 (1996).

[41] Timothy B. Lee, *Report: NSA Asked Verizon for Records of All Calls in the U.S.*, WASH. POST BLOG (June 5, 2013, 9:14 PM), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/05/nsa-asked-verizon-for-records-of-all-calls-in-the-u-s/.

black letter law—has increased public scrutiny over privacy practices in the United States and enriched the public debate.[42] To a great extent, even fifteen years after its appearance, EU privacy law remains a top-down product of a Brussels bureaucracy, while U.S. privacy law is a bottom-up topic, featured in town hall meetings, academic conferences, and traditional news media.

Alas, it should come as no surprise that the U.S. framework has disadvantages and shortcomings. To begin with, the FTC's authority to enforce privacy rests on the narrowest of legal mandates; Section 5 of the FTC Act, which prohibits organizations from engaging in "unfair or deceptive acts or practices," is hardly a sufficient data protection law.[43] The "deceptive" strain of Section 5 enables the FTC, at most, to keep organizations true to their word; that is, to comply with their own set of privacy promises (also known as the "notice and choice" approach).[44] At the same time, organizations enjoy largely unfettered autonomy to craft privacy policies in exceedingly broad terms, covering any and every data activity. "Deceptive acts or practices," in other words, protects consumers against misrepresentation, not privacy violations. The "unfair" strain of Section 5, while ostensibly flexible enough to cover privacy, is so broad as to offer little guidance to organizations and regulators. In fact, in some legal systems it might be considered anathema to fundamental principles of jurisprudence (*nullum crimen sine lege*).[45] And while some have heralded an emerging "common law of [FTC] consent decrees,"[46] such common

---

[42] *See, e.g.*, *Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act*, PRIVACY & CIV. LIBERTIES OVERSIGHT BOARD (PCLOB), http://www.pclob.gov/9-July-2013 (last visited Oct. 27, 2013). The PCLOB meeting was streamed live by C-SPAN and is available for viewing online; as much as the NSA programs remained veiled in secrecy, one would be hard pressed to find European or other national security agencies publicly discussing their surveillance activities. *See Privacy Board Hosts Workshop on Surveillance Programs*, C-SPAN VIDEO LIBR. (July 9, 2013), http://www.c-spanvideo.org/event/221275.

[43] Federal Trade Commission (FTC) Act, 15 U.S.C. § 45(a)(1) (2012).

[44] *See* FTC, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE ii, 13, 20, 27 (2000), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (focusing on the principles of notice, choice, access and security).

[45] Omer Tene, *There Is No New Thing Under the Sun*, CONCURRING OPINIONS (July 30, 2012, 7:47 PM), http://www.concurringopinions.com/archives/2012/07/there-is-no-new-thing-under-the-sun.html.

[46] Christopher Wolf, Targeted Enforcement and Shared Lawmaking Authority as Catalysts for Data Protection 2 (presented at 32nd Annual International Conference of Privacy and Data Protection Commissioners, Oct. 27–29, 2010), *available at* http://www.justice.gov.il/NR/rdonlyres/8D438C53-82C8-4F25-99F8-E3039D40E4E4/26451/Consumer_WOLFDataProtectionandPrivacyCommissioners.pdf (FTC consent decrees have "created a 'common law of consent decrees,' producing a set of data protection rules for businesses to follow"); *see also* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. (forthcoming 2014) (manuscript at 62) (on file with authors); Julie Brill, Comm'r, FTC, Remarks to the Mentor Group Forum for

law leaves much to be desired as it is based on non-transparent negotiations behind closed doors, resulting in terse orders, which do not have precedential value.[47] As long as the United States fails to enact a comprehensive information privacy statute that will ground the FIPPs in "hard law," its information privacy regime will remain deficient, with entire swaths of the market unregulated and subject at best to a "notice and choice" regime.

III. THE SECOND GENERATION

More than three decades have passed since the advent of the *OECD Guidelines* and more than fifteen years since the EU enacted the *EU Directive* and the United States adopted a notice and choice approach.[48] This period has seen a surge in the value of personal data for governments, businesses, and individuals. Innovations and breakthroughs, particularly in information and communications technologies, have created new business models and tools affecting individuals' lives and impacting the functioning of virtually every business process and government activity. Not only technologies have changed; the individuals using them have changed too. Individuals now volunteer massive amounts of information via platform service providers that act as facilitators rather than initiators of data flows. Even the distinction between the private and public sphere has muddled, with users of social media broadcasting personal information to sometime strangers whom they call "friends."

The following Parts address the challenges posed to the existing frameworks by three significant socio-technological-business shifts: the surge in big data and analytics; the social networking revolution; and the migration of personal data processing to the cloud. The *first shift* concerns *big data,* a term referring to the ability of organizations to collect, store, and analyze previously unimaginable amounts of unstructured data in order to find patterns and correlations and draw useful conclusions.[49] This trend is accentuated by reduced costs of storing information and moving it around in conjunction with an increased capacity to instantly analyze heaps of unstructured data using modern experimental methods, observational and longitudinal studies, and large scale simulations. It is boosted by the enhanced value derived from so-called "meta-

---

EU–US Legal-Economic Affairs (Apr. 16, 2013), *available at* http://www.ftc.gov/speeches/brill/130416mentorgroup.pdf.

[47] *But see* Solove & Hartzog, *supra* note 46, at 62.

[48] *OECD Guidelines*, *supra* note 2.

[49] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 245, 253 (2013); *see also* WORLD ECON. FORUM, UNLOCKING THE VALUE OF PERSONAL DATA: FROM COLLECTION TO USAGE 3 & n.1 (2013), *available at* http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage; Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 74 (2013).

data," a derivative of personal data, perhaps not defined as such, but often no less revealing, and even bigger, more obscure, and harder to control.[50]

The *second shift* concerns *social networking services*, which have revolutionized the relationship between individuals and organizations. Those creating, storing, using, and disseminating personal data are no longer just organizations but rather geographically dispersed individuals who take photos and videos and stream them online; submit ratings about movies and restaurants; and share on social networking sites geo-location markers and rich descriptions of their friends and social interactions. The explosion in peer-produced content, particularly in the social networking ecosystem, has led to the production of an enormous amount of identity-centric content. This shift is dramatic and has serious implications for both information privacy and digital identity.

The *third shift* entails the arrival of *cloud computing*, a term encompassing (at least) three distinct models of using computing resources through a network: (1) software as a service, or SaaS, which includes both business-to-consumer tools, such as e-mail, instant messaging, and photo-sharing services, and business-to-business applications, such as customer relationship management (CRM) and enterprise resource planning (ERP) software; (2) platform as a service, or PaaS, computing platforms offered as a service to facilitate low cost, rapid development, and hosting of third party web service applications; and (3) infrastructure as a service, or IaaS, infrastructure offerings, including low cost facilities for storage, computing, and networking. The advantages of cloud computing abound and include reduced cost, increased reliability, scalability, and security.[51] However, the storage, processing, and transfer of personal data in the cloud means that the location of data becomes indeterminate, indeed unimportant, from a technological point of view, posing new risks to privacy and data security.

To respond to these changes, policymakers in charge of each of the three frameworks launched processes for fundamental legal reform. The product of these processes is poised to become the second generation of information privacy law. Yet as discussed in this Part, the second generation is set to end up strongly anchored in the existing framework; this means more high level pronouncements by the OECD; bureaucratic processes by the EU; and notice and choice by the United States. This is unfortunate, given that fundamental

---

[50] Matt Blaze, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, WIRED (June 19, 2013, 9:30 AM), http://www.wired.com/opinion/2013/06/phew-it-was-just-metadata-not-think-again. *See generally* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071 (2013).

[51] *See, e.g.*, ANN CAVOUKIAN, PRIVACY IN THE CLOUDS: A WHITE PAPER ON PRIVACY AND DIGITAL IDENTITY—IMPLICATIONS FOR THE INTERNET 7 (May 28, 2008), *available at* www.ipc.on.ca/images/Resources/privacyintheclouds.pdf. *But see Reaching for the Cloud(s): Privacy Issues Related to Cloud Computing*, OFF. PRIVACY COMMISSIONER CANADA (Mar. 2010), http://priv.gc.ca/information/pub/cc_201003_e.cfm.

aspects of the current framework are already significantly challenged by technological and business developments on the ground, not to mention changes expected in the near future.

A. *OECD Reform*

The review of the *OECD Guidelines* arises out of the *Seoul Declaration for the Future of the Internet Economy* (the "*Seoul Declaration*"), which was adopted by the ministers of the OECD member countries in June 2008.[52] The *Seoul Declaration* called for the OECD to assess the application of certain instruments, including the *OECD Guidelines*, in light of "changing technologies, markets and user behavior and the growing importance of digital identities."[53] In 2010, in the context of the thirtieth anniversary of the *OECD Guidelines*, the OECD launched a comprehensive review of its framework.[54] Building on this preparatory work and the June 2011 *Communiqué on Principles for Internet Policy-Making*,[55] the OECD Working Party on Information Security and Privacy (WPISP) developed Terms of Reference to serve as a roadmap for the review.[56] It expanded a Volunteer Group of Privacy Experts, initially formed to work on the 2007 OECD Recommendation on Enforcement, to include experts from governments, privacy enforcement authorities, academics, business, civil society, and the Internet technical community (the "Expert Group").[57] The Expert Group, chaired by Jennifer Stoddart, Privacy Commissioner of Canada, focused on three main themes identified by the Terms of Reference: the roles and responsibilities of key actors; geographic restrictions on transborder data flows; and proactive implementation and enforcement.[58] The approach that emerged from the work of the Expert Group suggested that, although the technological and business

---

[52] Org. for Econ. Co-operation & Dev., The Seoul Declaration for the Future of the Internet Economy 9 (presented at the OECD Ministerial Meeting on the Future of the Internet Economy, June 17–18, 2008), *available at* http://www.oecd.org/internet/consumer/40839436.pdf.

[53] *Id.* at 10.

[54] Org. for Econ. Co-operation & Dev., Terms of Reference 2 (presented at Global Forum on Transparency and Exchange of Information for Tax Purposes, Sept. 1–2, 2009) [hereinafter OECD *Terms of Reference*], *available at* http://www.oecd.org/internet/consumer/40839436.pdf.

[55] Org. for Econ. Co-operation & Dev., Communiqué on Principles for Internet Policy-Making (presented at the OECD High Level Meeting on the Internet Economy: Generating Innovation and Growth, June 28–29, 2011), *available at* http://www.oecd.org/dataoecd/40/21/48289796.pdf.

[56] OECD Terms of Reference, *supra* note 54, at 2.

[57] The author was hired to serve as *rapporteur* for the Expert Group.

[58] Org. for Econ. Co-operation & Dev., Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [C(80)58/FINAL], as amended on 11 July 2013 [C(2013)79] [hereinafter OECD Recommendation].

environment has significantly changed, an update to the *OECD Guidelines* was preferred over a fundamental rethinking of its core principles.[59] This is reflected in the ensuing Recommendation of the OECD Council (the "OECD Recommendation"),[60] which posits that the articulation of the FIPPs in Part 2 of the *OECD Guidelines* was sound and should remain intact.

Although the OECD Recommendation introduced a number of new concepts to the *OECD Guidelines*, such as privacy management programs, security breach notification, national privacy strategies, education and awareness, and global interoperability, its revisions are limited to subtle adjustments to the existing framework rather than comprehensive reform. Specifically, most of the amendments implement the principle of accountability, which already appears in the *OECD Guidelines*, through the new concept of a "privacy management program."[61] The addition of a security breach notification requirement, which also fits into this mold, is recognition of the regulatory *zeitgeist* not only in most U.S. states but also in the EU.[62]

Two of the changes introduced by the OECD Recommendation are particularly important, namely the explicit reference to a "privacy enforcement authority" and the simplification of the provision on transborder data flows. The reference to privacy enforcement authorities is new in the OECD context, although the 2007 OECD Recommendation on Enforcement assumes their existence and recommends their endowment with effective powers and authority.[63] The revised Part on "National Implementation" calls on member countries to "establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis."[64] This formulation, which steered clear of the *EU Directive*'s contentious requirement of "independence," is more a recognition of the current state of affairs in almost all OECD member countries than a forward looking measure.[65] The original transborder data flows provision in the *OECD Guidelines* was based on an "adequacy" rationale, similar to (though more loosely stated than) that in the *EU Directive*.[66] A regulatory approach based exclusively on country-specific assessments has proven difficult to implement and enforce due to the challenges of assessing the efficacy of an entire country's

---

[59] *Id.* at 22.

[60] *Id.*

[61] *Id*. art. 15(a).

[62] Council Directive 2009/136/EC of 12 July 2002 on Privacy and Electronic Communications, art. 2(4)(c), 2009 O.J. (L 337) 11, 29–30 [hereinafter e-Privacy Directive].

[63] OECD CROSS-BORDER RECOMMENDATION, *supra* note 14, at 6–7.

[64] OECD Recommendation, *supra* note 58, art. 19(c).

[65] Chile, Korea, Japan and Turkey are the only OECD member countries that do not have a DPA.

[66] *OECD Guidelines*, *supra* note 2, at 29.

privacy framework not only on the books but also on the ground.[67] The new language represents a shift to an accountability model, requiring organizations to remain accountable for personal data under their control without regard to their location. This move, while novel, draws from existing accountability-based regimes, such as the Canadian PIPEDA.[68]

Overall, the reform of the *OECD Guidelines* introduces useful concepts that have gained credence in data protection circles over the past decade or so, yet does not break new ground.

B. *EU Reform*

In November 2010, the European Commission released a "Communication" titled: *A Comprehensive Approach on Personal Data Protection in the European Union*.[69] The Communication recognized that "rapid technological developments and globalization have profoundly changed the world around us, and brought new challenges for the protection of personal data."[70] It concluded that, while the core principles of the *EU Directive* remain valid, the *EU Directive* required revision "with the objective of strengthening the EU's stance in protecting the personal data."[71] The Commission then launched an extensive multi-stakeholder consultation, which led to the submission in January 2012 of a legislative package aimed at reforming the *EU Directive*.

The legislative package consists of a draft Regulation (the "Draft EU Regulation"), which would replace the *EU Directive* with an instrument that has direct legal effect in all EU Member States, thereby greatly increasing harmonization; as well as a Directive, specifying rules with respect to the

---

[67] It is doubtful, for example, that Argentina and Israel, which have both gained adequacy status under the *EU Directive*, have more robust privacy protection on the ground than the United States or Australia, which have not been certified "adequate." *See Commission Decision of 30/06/2003 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data in Argentina*, COM (2003) 1731 final (June 30, 2003), *available at* http://ec.europa.eu/justice/policies/privacy/docs/adequacy/decision-c2003-1731/decision-argentine_en.pdf; Commission Decision 2011/61/EU of 31 January 2011 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequate Protection of Personal Data by the State of Israel with Regard to Automated Processing of Personal Data, 2011 O.J. (L 27) 39.

[68] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, Schedule 1, Principle 4.1.3 (amended 2011) (Can.).

[69] *A Comprehensive Approach on Personal Data Protection in the European Union*, COM (2010) 609 final (Nov. 4, 2010) [hereinafter *A Comprehensive Approach*], *available at* http://ec.europa.eu/health/data_collection/docs/com_2010_0609_en.pdf.

[70] *Id.* at 2. Another important driver for legislative reform was the entry into force of the Treaty of Lisbon, which includes explicit mention of a fundamental right to data protection (Article 16(1) of the Treaty on the Functioning of the European Union (TFEU)) and eliminates the EU's "pillar" structure, thereby requiring the application of similar legal protections to all forms of processing. Consolidated Version of the Treaty on the Functioning of the European Union art. 16(1) & (2), Mar. 30, 2010, 2010 O.J. (C 83) 47.

[71] *A Comprehensive Approach*, *supra* note 69, at 18.

processing of personal data by law enforcement authorities.[72] The Draft EU Regulation is a dense legal document more than 100 pages long. It introduces numerous changes to the existing framework, some of which have been applauded by businesses[73] while others have been decried as unworkable[74] or even calamitous.[75] The legislative reform addresses matters of both principle and implementation.[76] On principle, some of the main amendments include significantly restricting the use of consent for legitimizing data processing; introducing a new "right to be forgotten"[77] and "right to data portability;" and requiring the use of data protection "by design" and "by default."[78] Important amendments on implementation include the introduction of the concept of a lead regulator and "one stop shop;"[79] enhancing internal processes such as privacy "impact assessments," documentation of data processing, and appointment of "data protection officers;"[80] requiring security breach notification; and "greatly enhancing the enforcement powers and sanctions available to data protection authorities."[81]

Despite much anticipation, the Draft EU Regulation did not significantly alter the definition of "personal data" and the related concept of anonymization;[82] nor did it fundamentally overhaul the adequacy model

---

[72] *Proposal for a Directive of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and the Free Movement of Such Data*, COM (2012) 10 final (Jan. 25, 2012).

[73] These include increased harmonization toward the application of a single set of rules across the EU; establishing a "one-stop-shop" system whereby a single DPA is responsible for a company operating in several countries; abolishing some of the unnecessary bureaucratic requirements such as notification obligations; and simplifying transborder data flows. AM. CHAMBER OF COMMERCE TO THE EUR. UNION, *supra* note 24, at 4, 14, 17.

[74] With respect to consent, see Omer Tene & Christopher Wolf, The Draft EU General Data Protection Regulation: Costs and Paradoxes of Explicit Consent 3, 8 (presented at The Future Privacy Forum, Jan. 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Consent-January-201310.pdf.

[75] *See* Jeffrey Rosen, *The Right To Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89–90 (2012).

[76] *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 (General Data Protection Regulation)*, at 7, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *General Data Protection Regulation*], *available at* http://ec.europa.eu/justice/dataprotection/document/review2012/com_2012_11_en.pdf.

[77] *Id.* at 9.

[78] *Id.* at 9–10.

[79] *Id.* at 12.

[80] *Id.* at 4–5.

[81] *Id.* at 14.

[82] Except that it is now integrated into the definition of "data subject." *General Data Protection Regulation*, *supra* note 76, at 7.

governing transborder data flows.[83] More generally, the EU reform process, while no doubt comprehensive and of grand scale,[84] would leave the core of the existing framework intact, including the FIPPs and the concepts of personal data, processing, consent, controller-processor, and data "location."

C. *U.S. Reform*

Both the FTC and the U.S. Commerce Department undertook steps in 2010 to review the information privacy framework. The Commerce Department Internet Policy Task Force[85] conducted a series of multi-stakeholder consultations, including the publication of *Information Privacy and Innovation in the Internet Economy Notice of Inquiry*.[86] These discussions led to the adoption of a Green Paper in December 2010 titled: *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[87] The release of the Green Paper was followed by another round of consultations, which included the submission of more than 100 position papers from multiple stakeholders, leading to the release in February 2012 of the final White House Report: *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (the "White House Blueprint").[88]

Concurrent with the process led by the Commerce Department, the FTC launched a series of public roundtables to explore privacy challenges associated with the new technological and business landscape.[89] The Preliminary FTC

---

[83] Some strides forward have been made with respect to formal recognition of Binding Corporate Rules, for controllers and processors, as a preferred mechanism. Viviane Reding, Vice-President, Eur. Comm'n, EU Justice Comm'r, Binding Corporate Rules: Unleashing the Potential of the Digital Single Market and Cloud Computing (Nov. 29, 2011), *available at* http://europa.eu/rapid/press-release_SPEECH-11-817_en.htm; *see also* LOKKE MOEREL, BINDING CORPORATE RULES: CORPORATE SELF-REGULATION OF GLOBAL DATA TRANSFERS 118 (2012); Rolf H. Weber, *Transborder Data Transfers: Concepts, Regulatory Approaches and New Legislative Initiatives*, 3 INT'L DATA PRIVACY L. 11–14 (2013); Miriam Wugmeister, Karin Retzer & Cynthia Rich, *Global Solution for Cross-border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 GEO. J. INT'L L. 449, 480 (2007).

[84] Christopher Kuner called it a "Copernican revolution." Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, BLOOMBERG BNA (Feb. 6, 2012).

[85] *Internet Policy Task Force*, NAT'L TELECOMMS. & INFO. ADMIN., http://www.ntia.doc.gov/category/internet-policy-task-force (last updated Aug. 9, 2013).

[86] Notice of Inquiry, 75 Fed. Reg. 21226-31 (Apr. 23, 2010).

[87] *See* INTERNET POLICY TASK FORCE, DEP'T OF COMMERCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK i (2010).

[88] *See* THE WHITE HOUSE BLUEPRINT, *supra* note 12, at 7.

[89] For a description of the roundtables and issues they surfaced, see FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED

Report, which was issued in December 2010, proposed a new framework for "commercial entities that collect or use consumer data that can be reasonably linked to a specific consumer, computer, or other device," centered on principles of privacy by design, simplified choice and greater transparency.[90] Significantly, the FTC initiated discussion of a "do not track" standard, intended to provide consumers with a simple centralized mechanism to opt out of online behavioral advertising.[91] The Preliminary Report included a number of questions for public comment to assist and guide the FTC in developing its final report. The FTC received more than 450 comments, from a wide variety of stakeholders, addressing these questions.[92] In March 2012, the FTC issued its final report, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (the "FTC Report").[93]

The White House Blueprint recommends that Congress enact legislation to implement a "Consumer Privacy Bill of Rights" based on the FIPPs.[94] In addition, the White House Blueprint calls for a multi-stakeholder process to determine how to apply the Consumer Privacy Bill of Rights in different business contexts through enforceable codes of conduct.[95] As part of the sought-after consumer privacy legislation, the Administration calls on Congress to endow the FTC and state attorneys general with specific authority to enforce the Consumer Privacy Bill of Rights.[96] Finally, in a nod to the evolving global privacy frameworks, the White House Blueprint calls for "improving global interoperability" through mutual recognition and enforcement cooperation.[97]

The FTC Report clarifies the scope of the information privacy framework and the term "personal data" by proposing a de-identification safe harbor effective where an organization (1) takes reasonable measures to ensure that the data is de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data.[98] The FTC Report also sets boundaries for the scope of individual control and consent, stating that organizations do not need to provide choice before collecting and using personal data for practices that are consistent with the context of a transaction or with an organization's relationship with an individual, or as authorized by law.[99] The FTC Report further calls for specific

---

FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[90] *Id.* at 42.

[91] *Id.* at 66.

[92] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 1 (Mar. 2012) [hereinafter FTC REPORT].

[93] *Id.*

[94] THE WHITE HOUSE BLUEPRINT, *supra* note 12, at 1.

[95] *Id.* at 2.

[96] *Id.*

[97] *Id.*

[98] FTC REPORT, *supra* note 92, at 21.

[99] THE WHITE HOUSE BLUEPRINT, *supra* note 12, at 38–39.

legislation addressing the practices of information brokers;[100] for implementation of an effective do not track solution;[101] and for the development of enforceable sector-specific codes of conduct, similar to those mentioned in the White House Blueprint.[102]

To be sure, if Congress heeded the White House's call for legislation codifying the FIPPs, U.S. privacy law would be radically reformed. In its second term, the Obama Administration remains committed to pursuing privacy legislation based on the White House Blueprint. Such legislation is currently being drafted by the Administration with supporters in Congress such as Senator John Rockefeller.[103] Yet observers are skeptical that omnibus privacy legislation can gain critical political mass. And this means that the reforms introduced by the White House Blueprint may boil down to the multi-stakeholder process.[104] As recognized by the FTC in the FTC Report, the record for industry self-regulation has been less than satisfactory.[105] One recent example, the tracking protection working group of the W3C, which is debating the do not track initiative, has been rife with controversy and bellicose rhetoric and constantly appears to be on the verge of imploding, or worse, becoming irrelevant in retrospect.[106] Indeed, many commentators believe that the parties

---

[100] *Id.* at iv; *see also The Big Picture: Comprehensive Online Data Collection*, FED. TRADE COMMISSION, http://www.ftc.gov/bcp/workshops/bigpicture/ (last visited Oct. 28, 2013).

[101] The do-not-track process has proceeded sluggishly for the past two years at the World Wide Web Consortium Tracking Protection Working Group. *See Tracking Protection Working Group*, W3C, http://www.w3.org/2011/tracking-protection (last visited Oct. 28, 2013); *see also* Thomas Roessler, *The State of Do Not Track*, W3C BLOG (Apr. 26, 2012), http://www.w3.org/QA/2012/04/the_state_of_do_not_track.html; Peter Swire, *Sunnyvale DNT Meeting: Overcast with Skies Clearing*, W3C BLOG (May 13, 2013), http://www.w3.org/QA/2013/05/sunnyvale_dnt_meeting_overcast.html.

[102] *See* FTC REPORT, *supra* note 92, at 6.

[103] Natasha Singer, *Senator Seeks More Data Rights for Online Consumers*, N.Y. TIMES BITS (Feb. 28, 2013, 3:53 PM), http://bits.blogs.nytimes.com/2013/02/28/senator-seeks-more-data-rights-for-online-consumers.

[104] The first NTIA-convened privacy multi-stakeholder process regards mobile application transparency. "On June 15, 2012, NTIA announced that the goal of the first multi-stakeholder process is to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data." *Privacy Multistakeholder Process: Mobile Application Transparency*, NAT'L TELECOMMS. & INFO. ADMINISTRATION, http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency (last updated July 25, 2013).

[105] Peter P. Swire, *Markets, Self-regulation, and Government Enforcement in the Protection of Personal Information*, *in* PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U.S. Dep't of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm; Ira S. Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 ISJLP 355, 355 (2011).

[106] Natasha Singer, *Do Not Track? Advertisers Say "Don't Tread on Us,"* N.Y. TIMES, Oct. 14, 2012, at BU3; *see also* ARI SCHWARTZ, CTR. FOR DEMOCRACY & TECH., LOOKING

have moved beyond do not track to unilateral cookie blocking on the part of browser makers,[107] countered by server side monitoring and device fingerprinting[108] on the part of ad intermediaries.[109] In other words, if the White House Blueprint's legacy is restricted to a sluggish multi-stakeholder self-regulatory process, it will be quite limited in scope.

The FTC Report, meanwhile, constructively engages with important issues such as privacy by design, de-identification safe harbors and the limits of consent. At the same time, as a practical matter, so long as the United States does not legislate the FIPPs, the FTC's grounds for enforcement remain limited to sanctioning companies for not complying with self-imposed standards, which could be set quite low. To be sure, in recent enforcement actions the FTC has begun to embrace a broader notion of privacy based on "consumer expectations."[110] This means that rather than just enforcing agreements between companies and individuals, the FTC increasingly questions the reasonableness of underlying data practices.[111] Yet even this strain of FTC activity remains grounded in companies' promises. For example, in the *Sears* case, a company failed to disclose the scope of personal information that its software application would monitor, a failure that the FTC held was material enough to mislead consumers.[112] Had Sears been more straightforward about its practices, the FTC's options would have been limited.[113]

To sum up, even after the significant reforms proposed this past year by the White House and the FTC, the U.S. framework remains grounded on a "FIPPs-

---

BACK AT P3P: LESSONS FOR THE FUTURE (Nov. 2009), *available at* http://www.cdt.org/files/pdfs/P3P_Retro_Final_0.pdf.

[107] Megan Geuss, *Firefox Will Block Third-Party Cookies in a Future Version*, ARS TECHNICA (Feb. 23, 2013, 10:00 PM), http://arstechnica.com/business/2013/02/firefox-22-will-block-third-party-cookies.

[108] *See, e.g.*, *Panopticlick*, ELECTRONIC FRONTIER FOUND., https://panopticlick.eff.org (last visited Oct. 28, 2013).

[109] Peter Swire, *How To Prevent the "Do Not Track" Arms Race*, WIRED (Apr. 24, 2013, 8:00 AM), http://www.wired.com/opinion/2013/04/do-not-track/.

[110] Solove & Hartzog, *supra* note 46, at 62.

[111] Bamberger & Mulligan, *supra* note 25, at 273–74; *see, e.g.*, *In re* Gateway Learning Corp., 138 F.T.C. 443, 450 (2004) (failing to notify consumers of changes to the company's privacy policy was found to be deceptive).

[112] Sears Holdings Mgmt. Corp., No. C-4264, FTC File No. 0823099, at *3 (Aug. 31, 2009), *available at* http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf. Sears settled the case before the filing of a formal complaint by accepting the terms of a consent agreement.

[113] Yan Fang, *The Death of the Privacy Policy?: Effective Privacy Disclosures After In Re* Sears, 25 BERKELEY TECH. L.J. 671, 691 (2010); Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J. TECH. & INTELL. PROP. 1, 3 (2009).

lite"[114] approach revolving around the much discredited model of notice and choice.

D. *Other Frameworks*

While drawing most of the academic and public attention, the EU and U.S. frameworks are far from being the only information privacy laws around. Over the past few years, nearly 100 countries all over the world adopted information privacy statutes, many of them integrating the FIPPs and customizing the template of the *EU Directive*.[115] This is the case particularly in Latin America, where countries have rapidly adopted legislation, established regulatory agencies, and even hosted the last two Annual International Conferences of Privacy and Data Protection Commissioners;[116] and Asia, with countries such as Australia, Korea, Hong Kong, and New Zealand actively taking part in the Asia-Pacific Economic Cooperation (APEC) privacy framework.[117] Assessing the robustness of these regulatory frameworks exceeds the scope of this Article; suffice it to say that information privacy laws are not restricted to the EU and United States.

IV. PRIVACY LAW'S MIDLIFE CRISIS: NEW REALITY; OLD BAG OF TRICKS

The existing information privacy frameworks appear sluggish in dealing with rapidly evolving technologies and business models. Indeed, given the existing technological, business, and social conditions, it is not clear that the information privacy framework delivers much privacy protection at all. This Part discusses the shortcomings of the existing frameworks in addressing a world of big data, social networking services, and cloud computing. In particular, even after their impending reform, the existing frameworks remain grounded in concepts of identifiability; consent; linear processing; and location—all of which have been subject to far-reaching change. More generally, even after decades of adherence to FIPPs-based information privacy

---

[114] Ira S. Rubinstein & Nathaniel Good, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents*, 28 BERKELEY TECH. L.J. (forthcoming 2013), *available at* http://lsr.nellco.org/nyu_plltwp/347.

[115] Graham Greenleaf, *"Modernising" Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?*, 29 COMPUTER L. & SECURITY REV. 430, 431 (2013); Graham Greenleaf, *The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108*, 2 INT'L DATA PRIVACY L. 68, 68 (2012).

[116] *See, e.g.*, Graham Greenleaf, *Uruguay Starts Convention 108's Global Journey with Accession: Toward a Global Privacy Treaty?*, 122 PRIVACY L. & BUS. INT'L REP. 20, 20 (2013).

[117] *See generally Privacy Framework*, APEC, http://publications.apec.org/publication-detail.php?pub_id=390 (last visited Oct. 28, 2013). *But see* Chris Pounder, *Why the APEC Privacy Framework Is Unlikely To Protect Privacy*, OUT-LAW.COM (Oct. 15, 2007), http://www.out-law.com/default.aspx?page=8550.

frameworks, it remains far from clear that individual privacy has been well-served by existing regulation.

A. *Identifiability*

For many years, the concept of "personal data," the most basic building block of information privacy laws, appeared to be operational under both the OECD and European frameworks. Based on identifiability of individual "data subjects" and agnostic to content, the definition—"any information relating to an identified or identifiable individual"[118]—proved adaptable to a digital reality where aggregation of innocuous, insensitive facts could result in a detrimental privacy impact.[119] Unlike the U.S. sector-based approach, which protected certain categories of information, such as health (HIPAA), financial (GLBA), credit history (FCRA), video rentals (VPPA), or children (COPPA), the OECD and European model triggered privacy protections when *any* type of data was implicated concerning an "identified or identifiable natural person."[120]

Of course, if identifiability subjects data to the information privacy framework, then lack of identifiability extricates data from such obligations. Anonymization or de-identification were perceived as a silver bullet, allowing organizations to "have their cake and eat it too;" that is, to retain information, repurpose, and analyze it while at the same time preserving individuals' privacy.[121] Alas, over the past decade it has become clear that in a world of big data collection, storage, and analysis, de-identification is increasingly strained by re-identification techniques. Today, examples of re-identification of apparently de-identified data abound.

The classic case study was published by Latanya Sweeny in 1999. Sweeney showed that 87% of the U.S. population could be identified using just three items of innocuous data—zip code, birthdate, and gender; and she did so provocatively, by exposing the health records of William Weld, then governor of Massachusetts.[122] In 2006, two *New York Times* reporters parsed out the

---

[118] This is the OECD version; the *EU Directive* refers to "any information relating to an identified or identifiable natural person." *OECD Guidelines*, *supra* note 2.

[119] Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES MAG., Feb. 16, 2012, http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html. Solove characterized this privacy harm as "aggregation." Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 507 (2006).

[120] Schwartz & Solove, *supra* note 1, at 7.

[121] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1736 (2010).

[122] Latanya Sweeney, *Simple Demographics Often Identify People Uniquely* 16 (Laboratory for Int'l Data Privacy, Working Paper No. 3, 2000); *cf.* Daniel C. Barth-Jones, *The "Re-Identification" of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now* 2–3 (July 24, 2012) (pre-publication working paper), *available at* http://dx.doi.org/10.2139/ssrn.2076397; *see also* Latanya Sweeney, Akua Abu & Julia Winn, *Identifying Participants*

identity of an AOL user whose online search queries were anonymized and posted on an AOL research website. This privacy snafu cost the company's CTO her job.[123] In 2008, University of Texas researchers (then) Arvind Narayanan and Vitaly Shmatikov re-identified anonymized movie recommendations made available as part of the "Netflix challenge"[124] by crossing the de-identified database with another data resource which was available online.[125] Narayanan and colleagues have since demonstrated various other re-identification attacks, including on Amazon's collaborative filter mechanism ("Customers Who Bought This Item Also Bought . . .").[126] Simply stated, they show that it is impossible to scrub data to prevent its re-identification in a foolproof way without also sacrificing its utility. In other words, data are either robustly de-identified or useful, but not both.[127]

Paul Ohm drew on this literature to "blow the whistle" on de-identification. In an influential paper published in 2010, he warned that "[r]e-identification science disrupts the privacy policy landscape by undermining the faith that we have placed in anonymization."[128] He argued that by collecting apparently de-identified nuggets of information and matching them against additional information, adversaries incrementally create a "database of ruin," chewing away bit by byte on individuals' privacy until their profiles are completely revealed.[129]

De-identification science has also made noticeable strides. A line of work by Cynthia Dwork and others has shown how privacy can be maintained, even mathematically proven, by calibrating noise into datasets in amounts large enough to mask individual users yet small enough to maintain data accuracy.[130]

---

in the Personal Genome Project by Name 2 (Harvard Coll., Data Privacy Lab, White Paper No. 1021-1, Apr. 24, 2013), *available at* http://dataprivacylab.org/projects/pgp/1021-1.pdf.

[123] Michael Barbaro & Tom Zeller, Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A7.

[124] Kate Greene, *The $1 Million Netflix Challenge*, MIT TECH. REV. (Oct. 6, 2006), http://www.technologyreview.com/news/406637/the-1-million-netflix-challenge.

[125] Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* PROCEEDINGS OF THE 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111, 111–12 (May 19, 2008), *available at* http://www.senyt.dk/bilag/netflix2.pdf.

[126] Joseph A. Calandrino et al., *"You Might Also Like": Privacy Risks of Collaborative Filtering*, *in* PROCEEDINGS OF THE 2011 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 232 (May 24, 2011), *available at* http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5958032&tag=1.

[127] Ohm, *supra* note 121, at 1704.

[128] *Id.*

[129] *See* Paul Ohm, *Don't Build a Database of Ruin*, HARV. BUS. REV. (Aug. 23, 2012, 10:00 AM), http://blogs.hbr.org/cs/2012/08/dont_build_a_database_of_ruin.html.

[130] *See generally* Cynthia Dwork, Differential Privacy (presented at 33rd International Colloquium on Automata, Languages and Programming, July 7, 2006), *available at* http://research.microsoft.com/pubs/64346/dwork.pdf; Cynthia Dwork et al., *Calibrating Noise to Sensitivity in Private Data Analysis*, *in* PROCEEDINGS OF THE 3RD THEORY OF CRYPTOGRAPHY CONFERENCE 265 (2006); *see also* Ed Felten, *Protecting Privacy by Adding Noise*, TECH@FTC (June 21, 2012, 10:31 AM), https://techatftc.wordpress.com/2012/06/21/

Differential privacy avoids the ailments of de-identification by allowing data sharing in a way that maintains data quality while at the same time preserving individuals' privacy.[131] It enables data controllers to share derivative data without subjecting any individual to more than a minimal risk of harm from the use of his or her data in computing the values to be released, even when those values are combined with other data that may be reasonably available.[132] In other words, it allows data controllers and third parties to draw lessons and derive valuable conclusions from a data set, without being able to determine whether or not such conclusions are based on the personal data of any given individual. Hence, differential privacy emphasizes not whether an individual can be directly *associated* with a particular revealed value, but rather the extent to which any revealed value *depends* on an individual's data.

At the same time, differential privacy does not solve all potential privacy problems. It does not provide protection *vis-à-vis* a data controller who is in possession of the data set containing the raw (or micro-) data and it could leak information where positive correlations exist between individuals whose data reside in a given data set.[133] Critics argue that it is limited in scope and difficult to operationalize.

Policymakers appear to be sitting on the sidelines of the escalating arms race between anonymizers and attackers, where every de-identification tit meets its re-identification tat. Which policy lessons should lawyers draw from the de-identification discussion? One possible conclusion would be that all data should

---

protecting-privacy-by-adding-noise. Stated (a bit) more technically, differential privacy requires that when one person's data is added or removed from a database, the output distribution of the database access mechanism changes very little. In other words, a randomized function of a database is differentially private if its output distribution is insensitive to the presence or absence of any particular record in the database. Put yet another way, with differential privacy an attacker does not learn more about an individual than what can be deduced from the data of everyone else in the database.

[131] Dwork et al., *supra* note 130, at 265.

[132] *Id.*

[133] *See, e.g.*, Andreas Haeberlen, Benjamin C. Pierce & Arjun Narayan, *Differential Privacy Under Fire*, *in* PROCEEDINGS OF THE 20TH USENIX SECURITY SYMPOSIUM 2 (Aug. 12, 2011), *available at* http://www.cis.upenn.edu/~ahae/papers/fuzz-sec2011.pdf. Another group of scientists introduced "crowd-blending privacy," a method involving limiting how a data set can be analyzed to ensure that any individual record is indistinguishable from a sizeable crowd of other records, and removing a record from the analysis if this cannot be guaranteed. Johannes Gehrke et al., *Crowd-Blending Privacy*, *in* PROCEEDINGS OF THE 32ND INTERNATIONAL CRYPTOLOGY CONFERENCE 1 (Aug. 22, 2012), *available at* http://cs.colgate.edu/~mhay/pdfs/gehrke2012crowd.pdf (positing that "k-crowd blending private sanitization of a database requires that each individual *i* in the database 'blends' with *k* other individuals *j* in the database, in the sense that the output of the sanitizer is 'indistinguishable' if *i*'s data is replaced by *j*'s"); *see also* Tom Simonite, *How To Share Personal Data While Keeping Secrets Safe*, MIT TECH. REV. (Aug. 7, 2012), http://www.technologyreview.com/news/428733/how-to-share-personal-data-while-keeping-secrets.

be treated as personal and subject to the information privacy framework.[134] Indeed, the European e-Privacy Directive has given up pretext of distinguishing personal from non-personal information.[135] Yet such a result would create perverse incentives for organizations to forgo de-identification altogether and therefore increase, not alleviate, privacy and data security risks.[136] A further pitfall is a vastly expanded definition of personal data would render the information privacy framework all but unworkable, detaching it from its strong nexus to individuals' privacy and converting it to a framework of general application. Difficult enough to comply with and enforce today, the framework may well be unmanageable if it extends to every piece of information.[137] Finally, critics of this approach argue that the issue should not be the identifiability of data *per se*, but rather the level of *risk* inherent in the identifiability of data.[138]

The Draft EU Regulation introduces new language on de-identification that is at best cryptic, stating "identification numbers, location data, online identifiers or other specific factors as such need not necessarily be considered as personal data in all circumstances."[139] Without entering the fray of the de-identification debate, the Draft EU Regulation posits that "[t]he principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable."[140] This definition of personal data is outmoded not only in its perception of de-identification but also in its view of personal data as a static concept, referring to "an individual." This notion of data, sometimes referred to as "microdata," fails to account for the fact that data that are ostensibly not about "an individual," such as metadata, social grid

---

[134] Ohm, *supra* note 121, at 1742.

[135] Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, 00909/10/EN WP 171 (June 22, 2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf ("Article 5(3) applies to 'information' (stored and/or accessed). It does not qualify such information. It is not a prerequisite for the application of this provision that this information is personal data within the meaning of Directive 95/46/EC.").

[136] ANN CAVOUKIAN & KHALED EL EMAM, DISPELLING THE MYTHS SURROUNDING DE-IDENTIFICATION: ANONYMIZATION REMAINS A STRONG TOOL FOR PROTECTING PRIVACY 3 (2011), *available at* http://www.ipc.on.ca/images/Resources/anonymization.pdf.

[137] For example, according to a 2010 report by the EU Agency for Fundamental Rights, even in Europe, data protection authorities lack sufficient independence and funding; impose few sanctions for violations of data protection laws; and are often not equipped with full powers of investigation and intervention or the capacity to give legal advice or engage in legal proceedings. EUR. UNION AGENCY FOR FUNDAMENTAL RIGHTS, DATA PROTECTION IN THE EUROPEAN UNION: THE ROLE OF NATIONAL DATA PROTECTION AUTHORITIES 6 (2010).

[138] CAVOUKIAN & EL EMAM, *supra* note 136, at 14.

[139] *General Data Protection Regulation*, *supra* note 76, at recital 24.

[140] *Id.* at recital 23.

analysis, or stylometry (analysis of writing style),[141] may have unambiguous privacy impact.[142]

Another approach is to delineate a middle category between personal and fully de-identified information. Such a category of information, titled "identifiable," "pseudonymous," or "yellow stage" (as opposed to personally identified "red" or fully de-identified "green"),[143] would be subject to some but not all of the FIPPs. This is the approach advanced by the European Parliament's Rapporteur for the data protection reform, MEP Jan Philipp Albrecht.[144] Yet, the definition of the term "pseudonymous data" in the Rapporteur's Report is vague; and more importantly, the Rapporteur's approach fails to provide organizations with sufficient (if any) incentive to pseudonymize data.[145] Specifically, the Rapporteur's revisions to the framework's consent requirements determine that consent to the processing of pseudonymous data "may be given by automated means using a technical standard with general validity in the Union . . . without collecting identification data." Yet other obligations attached under the Draft EU Regulation to the strict new consent requirements render the collection of consent from unauthenticated users theoretically appealing but realistically impractical.[146]

The three state solution has gained traction in academia. Paul Schwartz and Dan Solove propose a distinction between identified and identifiable information, applying the full thrust of the information privacy framework to the former but only a subset of obligations to the latter.[147] For example,

---

[141] Arvind Narayanan et al., *On the Feasibility of Internet-Scale Author Identification*, *in* PROCEEDINGS OF THE 2012 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 300 (May 22, 2012), *available at* http://www.cs.berkeley.edu/~dawnsong/papers/2012%20On%20the%20Feasibility%20of%20Internet-Scale%20Author%20Identification.pdf.

[142] *See* Letter from Salil Vadhan et al., Professor, Harvard Univ., to The Dep't of Health & Human Servs., Office of the Sec'y, & Food & Drug Admin. (Oct. 26, 2011), *available at* http://dataprivacylab.org/projects/irb/Vadhan.pdf.

[143] Shane Wiley, A Deidentification Approach to DNT: A Path Forward to Creating a W3C DNT Standard (presented at W3C TPWG Presentation, June 21, 2013), *available at* http://lists.w3.org/Archives/Public/public-tracking/2013Jun/att-0406/W3C_DeID_Presentation_20130625.pdf.

[144] *See generally* JAN PHILLIP ALBRECHT, DRAFT REPORT ON THE 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 (2012) [hereinafter RAPPORTEUR'S DRAFT].

[145] OMER TENE & CHRISTOPHER WOLF, THE DEFINITION OF PERSONA DATA: SEEING THE COMPLETE SPECTRUM 3 (2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-De-Id-January-201311.pdf.

[146] *Id.*

[147] Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1817 (2011); *see also* Omer Tene, *The Complexities of Defining Personal Data: Anonymisation*, DATA PROT. L. & POL'Y, Aug. 2011, at 6.

organizations would not be required to re-identify information solely for the purpose of satisfying a subject access request.[148]

Another approach would delineate legislative safe harbors to allow data use even with a lingering risk of re-identification. Already a decade ago, the HIPAA set forth two such alternative safe harbors;[149] one based on removing from a dataset a list of eighteen data fields that could identify an individual (the so called "safe harbor method");[150] the other on having a statistical expert certify that risk of re-identification is very small (the "statistical method").[151] In its Final Report, the FTC proposed a safe harbor based on a combination of technological and legal measures;[152] namely a given data set will be exempt from the scope of the information privacy framework as long as it is "not reasonably identifiable; the company publicly commits not to re-identify it; and the company requires any downstream users of the data to keep it in de-identified form."[153] Technologists criticize this approach, claiming that organizational mechanisms are inherently weak and ultimately rely on the good will of businesses.[154] A more sophisticated safe harbor would be based on differential privacy, allowing organizations to respond to queries without revealing whether the results depend on the personal data of any given individual.

In a sense, lawyers dealing with the de-identification problem are saying: "don't bother us with the facts; we'll just tell you what the law is." This result is unsatisfactory. It creates legal uncertainty for organizations contemplating use of apparently de-identified data. It is incompatible with the existing technological reality, in which with sufficient incentive and effort, nearly every piece of data can be linked to an individual. It clings to an outdated framework, which has proven ill-suited to provide clarity and guidance in a big data world. As Michael Birnhack recently wrote:

> [T]he definition of personal data is rooted within a digital technological paradigm, for good or for bad. The good part is that it is more advanced than the previous, analogue, content-based definition; the bad part is that the

---

148 Schwartz & Solove, *supra* note 147, at 1880–81.

149 CTR. FOR DEMOCRACY & TECH., ENCOURAGING THE USE OF, AND RETHINKING PROTECTIONS FOR DE-IDENTIFIED (AND "ANONYMIZED") HEALTH DATA 5 (June 2009), *available at* https://www.cdt.org/files/pdfs/20090625_deidentify.pdf.

150 45 C.F.R. § 164.514(b)(2)(i) (2013).

151 *Id.* § 164.514(b)(1).

152 For another proposal in this vein, coming from the masters of re-identification, see Arvind Narayanan & Vitaly Shmatikov, *Privacy and Security: Myths and Fallacies of "Personally Identifiable Information*," 53 COMMUNICATIONS OF THE ACM, June 2010, at 24, 26 (arguing that "any system for privacy-preserving computation on sensitive data must be accompanied by strong access control mechanisms and non-technological protection methods such as informed consent and contracts specifying acceptable uses of data").

153 FTC REPORT, *supra* note 92, at 22.

154 Claudia Diaz, Omer Tene & Seda Gürses, *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923 (2013).

> concept of non-identification is about to collapse, if it has not already done so.[155]

Unfortunately, even if it will collapse, a reinvigorated concept is unlikely to emerge from the reformed framework.

B. *Consent*

Consent, or individual control, is a wild card in the privacy deck. On the one hand, if consent is taken out, the framework becomes paternalistic and overly rigid; after all, assuming consent is *truly* voluntary and informed, who is to say one should not negotiate one's privacy rights? Unlike organ selling or slavery, an invasion of privacy is not a *mala in se*. On the other hand, it is an open secret that consent to data uses, which almost always implies relationships of power, is seldom meaningful, voluntary, and fully informed. Individuals cannot be bothered to educate themselves about the increasingly complex data ecosystem, and they would typically have little bargaining power even if they did.[156]

Alan Westin's canonical conceptualization of privacy depicts it as individual control over personal information.[157] Accordingly, the existing information privacy framework is heavily preoccupied with consent. Most data processing operations in Europe and even more so in the United States rely on consent for legitimacy.[158] While the *EU Directive* enumerates alternative legal bases for processing, including compliance with a legal obligation; or fulfilling the controller's "legitimate interest," which must be balanced against the privacy risk to individuals; consent is often the fallback.[159]

This is unlikely to change under the revised framework. As discussed above, the United States clings to a model based on enforceable promises made by companies to respect individual choices. In Europe, if anything, the Draft EU Regulation would increase reliance on explicit consent as the primary means of legitimizing data processing.[160] The Draft EU Regulation's emphasis on explicit consent reflects an underlying assumption that an opt-in mechanism delivers greater protection for individuals. This assumption is misplaced. In many instances, opt-in consent is neither more voluntary nor informed than implied consent; particularly where implied consent is properly assumed from the

---

[155] Birnhack, *supra* note 23, at 77.

[156] Daniel J. Solove, *Introduction: Privacy Self-management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1898–99 (2013).

[157] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1966).

[158] Article 29 Data Protection Working Party, *Opinion 15/2011 on the Definition of Consent*, at 4–6, 01197/11/EN, WP 187 (July 13, 2011).

[159] Directive 95/46/EC, *supra* note 3, at 40–41.

[160] *General Data Protecton Regulation*, *supra* note 76, art. 4(8) (defining "the data subject's consent" as "any freely given specific, informed and explicit indication of his or her wishes").

context of a relationship and accompanied by transparency and opt-out rights. Excessive reliance on opt-ins would disrupt user interfaces and encumber individuals with repetitive prompts, which they will be eager to click through to reach their destination. Indeed, the EU e-Privacy Directive,[161] a grand scale experiment with an opt-in model, has left the field in disarray with little benefit to users.

While intended to empower individuals, the privacy-as-choice model in fact leaves them confused and impoverished.[162] As often used in practice, consent is a red herring. Fred Cate explained that "[n]otice and consent requirements often create the illusion, but not the reality, of meaningful consumer choice."[163] Individuals cannot be bothered to read privacy policies; nor would they understand them if they had. The data ecosystem has become too complex even for experts to keep up. Improving the notice mechanism, meanwhile, runs into a paradox—if information is simplified, individuals will not be fully informed; if information is detailed, individuals will not understand.[164]

The heated debate over default rules illustrates the cynical use of "consent" to legitimize data use.[165] All sides know that users are unlikely to sway from the default, regardless of whether it is privacy protective or embraces data sharing. Dan Ariely explained that the reason that individuals rest with the default is not that a decision is inconsequential and of little interest, but rather the opposite, that a decision is important, multifaceted, and requires contemplation and thought.[166] Thus, the binary nature of the default setting crystallizes an ideological divide about the social desirability of a given activity.[167] Whether tracking protection on a browser is turned "on" or "off" by default reflects a

---

[161] *See generally* e-Privacy Directive, *supra* note 62.

[162] Julie Cohen explains:

> Even assuming perfect information about all contemplated reuses of data, however, consumer freedom is relative. Individual consumers are free to accept or reject the terms offered, but it is the vendor who is free to decide what terms to offer in the first place. Thus, consumers may discover that the surrender of personal information is nonnegotiable or prohibitively priced.

Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1397 (2000) (footnote omitted).

[163] Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341, 364 (Jane K. Winn ed., 2006).

[164] Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 688 (2011).

[165] Wendy Davis, *IAB: One in Five Users Send Do-Not-Track Request*, MEDIA POST (July 8, 2013, 11:52 AM), http://www.mediapost.com/publications/article/204016/iab-one-in-five-users-send-do-not-track-request.html.

[166] Dan Ariely, *3 Main Lessons of Psychology*, DAN ARIELY BLOG (May 5, 2008), http://danariely.com/2008/05/05/3-main-lessons-of-psychology.

[167] Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J. L. SCI. & TECH. 281, 334–35 (2012).

value judgment as to whether the underlying activity is socially beneficial, given that only a few users will adjust their settings.

A further complicating factor is that the exchange of personal data, while now a primary feature of almost any online or mobile transaction, is seldom the driving transactional force for individuals. Individuals acquire goods or services online, often at no monetary cost, in return for their personal information.[168] For the most part, they have little knowledge or understanding of the potential value of this economic exchange; nor do they know what will become of their information or the full implications of its release.[169] They are eager to complete a transaction in order to download an app, view a video, order a book, or pay a bill online. In their view (though not in the vendor's view), the data exchange is a byproduct, a side deal to the main transaction. They simply want to click through. In certain contexts, such as in monopolistic or oligopolistic markets, this reality detracts from even the most fully informed and premeditated consent. Individuals simply have no choice.

In a big data reality, insistence on individual consent and the attendant principle of purpose limitation raises an additional problem. It may hinder innovation and thwart highly beneficial uses of data. More generally stated, the radical increase in opportunities to derive great value from unanticipated uses of data presents stark policy choices between privacy and individual autonomy, on the one hand, and a multitude of big data benefits in scientific research, public health, national security and law enforcement, and efficient energy use, on the other hand. In a recent paper, Jules Polonetsky and I claim that finding the right balance between privacy risks and big data rewards may very well be the biggest public policy challenge of our time.[170] Many scientific breakthroughs would simply not occur if individuals were asked to pre-approve data use.[171] Where anticipated benefits to society are compelling and risks to individuals small, consent may be the wrong tool to legitimize data flow.

In order to maintain a zone of individual empowerment while not stifling beneficial data uses, the role of consent should be demarcated according to normative choices made by policymakers. In some cases, consent should not be

---

[168] Ai-Mei Chang et al., *The Economics of Freebies in Exchange for Consumer Information on the Internet: An Exploratory Study*, 4 INT'L J. ELECTRONIC COM., Fall 1999, at 85, 86; M.J. van den Hoven, *Privacy and the Varieties of Moral Wrong-Doing in an Information Age*, 27 COMPUTERS & SOC'Y, Sept. 1997, at 33, 35.

[169] *See, e.g.*, Aleecia M. McDonald, *Cookie Confusion: Do Browser Interfaces Undermine Understanding?*, *in* CONFERENCE PROCEEDINGS AND EXTENDED ABSTRACTS OF THE 28TH ANNUAL CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 4393, 4395 (2010), *available at* http://dl.acm.org/citation.cfm?doid=1753846.1754159.

[170] Tene & Polonetsky, *supra* note 49, at 239; *see also* Rubinstein, *supra* note 49, at 78.

[171] *See, e.g.*, Nicholas P Tatonetti et al., *A Novel Signal Detection Algorithm for Identifying Hidden Drug–Drug Interactions in Adverse Event Reports*, 19 J. AM. MED. INFORMATICS ASS'N 79, 79–80 (2012) (discovery of harmful drug interaction through analysis of individuals' health records). *But see* Paul Ohm, *The Underwhelming Benefits of Big Data*, 161 U. PA. L. REV. ONLINE 339 (2013), http://www.pennlawreview.com/online/161-U-Pa-L-Rev-Online-339.pdf.

required; in others, consent should be assumed subject to a right of refusal; in specific cases, explicit consent should be required to legitimize data use. The classification of data uses into the relevant category should be based on a cost–benefit analysis, weighing the risk of a given data use to individuals' privacy against its expected value, and distinguishing between uses that benefit an individual, organization, community, or society at large.

To some extent, the EU framework enables such collective determination through its "legitimate interests" clause.[172] However, the legitimate interests test is not fully developed; is applied inconsistently in various EU jurisdictions;[173] and fails to provide organizations with the legal certainty and predictability required to establish business models and transactions. This, in turn, drives organizations to fall back on individuals' consent.

C. *The Controller Model*

Not only technologies but also individuals' engagement with the data economy have radically changed over the past decades. Individuals now proactively disseminate large amounts of personal information online via platform service providers, which act as facilitators rather than initiators of data flows. Data transfers, once understood as discrete point-to-point transmissions, have become ubiquitous, geographically indeterminate, and frequently "residing" in the cloud. The transition from a closed network environment to an open network environment has made it increasingly difficult to identify a single party responsible for all data flows. It has radically changed the relationships between individuals, organizations, and platform providers. Yet, the existing framework continues to envisage an environment of mainframe computers and centralized databases, where a "data controller" (typically a government, business, or research institution) actively collects personal data from passive "data subjects," sometimes using a third party ("processor") to process the information (the "controller model").[174] This too is unlikely to change under the reformed framework.

Indeed, perhaps the most conspicuous addition to the reformed framework is the elaboration of the OECD principle of accountability, a cornerstone of the controller model, which encompasses an intricate set of procedures, including

---

[172] Directive 95/46/EC, *supra* note 3, at 40.

[173] For example, the UK Information Commissioner's Office issued guidance encouraging controllers to look to the "legitimate interest" test before any of the other legal bases for processing. *See The Conditions for Processing*, U.K. INFO. COMMISSIONER'S OFF., http://www.ico.org.uk/for_organisations/data_protection/the_guide/conditions_for_processing (last visited Sept. 4, 2013). Spain failed to even adopt the "legitimate interest" language into its national data protection law. *See* Ariane Mole, *The European Court of Justice Finds Spain in Breach of Article 7*, INT'L ASS'N PRIVACY PROFS. (Nov. 28, 2011), https://www.privacyassociation.org/publications/the_european_court_of_justice_finds_spain_in_breach_of_article_7.

[174] Directive 95/46/EC, *supra* note 3, at 38–39.

maintaining a privacy compliance program; appointing a chief privacy officer; establishing a records retention policy; conducting privacy impact assessments; reporting data security breaches; documenting internal data operations; and more.[175] As beneficial to privacy as these measures may be, they address neither of the two fundamental developments discussed in this Part, namely the rise of social media and the emergence of platform providers as powerful arbiters of data ecosystems. The inadequacy of the controller model in this context was recognized by Jonathan Zittrain, who—addressing "Privacy 2.0," a term he coined to refer to privacy in a Web 2.0 environment—suggested: "Effective solutions for the problems of Privacy 2.0 have more in common with solutions to other generative problems than with the remedies associated with the decades-old analytic template for Privacy 1.0."[176]

The arrival of social media (which includes not only social networking services, but also microblogs, reputation systems, and ambient social location apps) has brought an explosion of peer-produced identity-centric content; i.e., content about individuals of which individuals are both the producers and consumers. While privacy issues associated with processing of personal data by governments and businesses remain important, they are increasingly dwarfed by threats to privacy that do not fit the standard analytical mold of the controller model.[177] The central problem is that those creating, storing, using, and disseminating personal data are no longer just organizations, but rather geographically dispersed individuals who take photos and stream them online; submit ratings about lecturers, movies, and restaurants; and share on social networking sites photos, geo-location markers, and rich descriptions of their friends and interactions.[178] And while social media services have become as powerful as traditional databases, governments cannot possibly impose on individuals the same type of administrative burdens that are reasonably placed on businesses or governments. The EU framework, for example, generally exempts individuals from legal obligations under the so-called "household exemption."[179] A recent narrow judicial interpretation of the exemption by a

---

[175] *OECD Guidelines*, *supra* note 2, ¶ 14.

[176] Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 72.

[177] Omer Tene & Jules Polonetsky, A Theory of Creepy: Technology, Privacy and Shifting Social Norms (unpublished manuscript) (on file with the author); *see also* Diana I. Tamir & Jason P. Mitchell, *Disclosing Information About the Self Is Intrinsically Rewarding*, 109 PROC. NAT'L ACAD. SCIS. 8038, 8038, 8041 (2012).

[178] *See* Kashmir Hill, *Oops. Mark Zuckerberg's Sister Has a Private Facebook Photo Go Public*, FORBES (Dec. 26, 2012, 8:52 AM), http://www.forbes.com/sites/kashmirhill/2012/12/26/oops-mark-zuckerbergs-sister-has-a-private-facebook-photo-go-public. *See generally* Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307 (2013).

[179] *See* Article 29 Data Prot. Working Party, *Opinion 5/2009 on Online Social Networking*, at 5–7, 01189/09/EN, WP 163 (June 12, 2009) (discussion on the scope of the exemption).

UK court notwithstanding,[180] the household exemption makes clear that the legislative framework does not impact individual-to-individual relations.[181]

Several commentators have addressed the challenges presented by "Privacy 2.0." Zittrain suggested harnessing code-backed norms, such as data tagging or respect for the robots.txt protocol (preventing data from being indexed by search engines);[182] enabling "reputation bankruptcy" (allowing individuals to express a choice "to deemphasize if not entirely delete" existing information about them);[183] and contextualizing data with rejoinders or complementary information posted by data subjects (similar to drowning a noisy nuisance with "white noise").[184] Woodrow Hartzog and Fred Stutzman advocated a legal concept of "online obscurity," which they interpret as a state where information "exists in a context missing one or more key factors that are essential to

---

[180] Law Soc'y v. Kordowski, [2011] EWHC (QB) 3185 (Eng.). Also known as the "Solicitors from Hell" case, this case involved a website used by disgruntled individuals to post negative, often defamatory, comments about lawyers and law firms. *Id.* By 2011, the website contained more than 900 separate posts and received more than one million visitors every month. Eddie Craven, *Case Law:* Law Society v Kordowski*, "Solicitors from Hell" Shut Down*, INT'L F. FOR RESPONSIBLE MEDIA BLOG (Dec. 20, 2011), http://inforrm.wordpress.com/2011/12/20/case-law-law-society-v-kordowski-solicitors-from-hell-shut-down-eddie-craven/. The Law Society submitted a formal complaint about the website's compliance with the UK Data Protection Act to the Information Commissioner. Relying on the "household exemption," the Information Commissioner declined to intervene, writing:

> I am strongly of the view that it is not the purpose of the DPA to regulate an individual right to freedom of expression—even where the individual uses a third party website, rather than his own facilities, to exercise this. . . . The situation would clearly be impossible were the Information Commissioner to be expected to rule on what it is acceptable for one individual to say about another be that a solicitor or another individual.

Kordowski [2011] EWHC (QB) at [96]. The Court disagreed, holding:

> I do not find it possible to reconcile the views on the law expressed in the Commissioner's letter with authoritative statements of the law. The DPA does envisage that the Information Commissioner should consider what it is acceptable for one individual to say about another, because the First Data Protection Principle requires that data should be processed lawfully.

Id. at [100].

[181] Directive 95/46/EC, *supra* note 3, at 39.

[182] Zittrain, *supra* note 176, at 106–09. Lauren Gelman similarly proposes tools, such as metatags, to allow users to express and exercise privacy preferences over uploaded content. Lauren Gelman, *Privacy, Free Speech, and Blurry-Edged Social Networks*, 50 B.C. L. REV. 1315 (2009); *see also* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009); Lilian Edwards & Ian Brown, *Data Control and Social Networking*: *Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 202, 225–26 (Andrea M. Matwyshyn ed., 2009).

[183] Zittrain, *supra* note 176, at 109–10.

[184] *Id.* at 110–13.

discovery or comprehension."[185] Specifically, they stress the importance of search visibility, unprotected access, identification, and clarity, as indices for obscurity or lack thereof.[186] Short of anonymity or secrecy, obscurity surrounds individuals with a cloak of "fuzziness" sufficient to blur their identity.[187] Lior Strahilevitz too used the concept of obscurity to develop a notion of "social networks privacy."[188] Strahilevitz argues that privacy law should focus not on the "abstract, circular, and highly indeterminate question of whether [an individual] reasonably expected . . . information about himself [to] remain 'private,' but rather on the more objective . . . question of what extent of dissemination [an individual] should have expected to follow his disclosure of [such] information to others."[189] He concludes that liability for a privacy infringement should arise where one actor "materially alters the flow of otherwise obscure information through a social network, such that what would have otherwise remained obscure becomes widely known."[190]

Unfortunately, innovative thinking about social media privacy is hardly reflected in the reformed framework, which remains strongly rooted in the controller model. Perhaps the sole response to these issues is the European Commission's proposal of a new "right to be forgotten," allowing individuals to scrub their digital record clean.[191] Partially a concretization of Zittrain's reputation bankruptcy, partially a reformulation of the existing requirement to delete data after initial use, the right to be forgotten imposes a weighty obligation on platform providers "to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data."[192] Here again, the regulatory obligations befall on platform providers as opposed to individuals themselves. Yet, while platform providers can remedy certain privacy risks, such as those associated with their harnessing data for targeted

---

[185] Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 32 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 397 (2013); *see also* Fred Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, *in* CSCW'12: PROCEEDINGS OF THE ACM 2012 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 769, 773 (2013), *available at* http://dl.acm.org/citation.cfm?id= 2145320&bnc=1.

[186] Hartzog & Stutzman, *The Case for Online Obscurity*, *supra* note 185, at 2.

[187] *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 764 (1989) (holding that "[t]he very fact that federal funds have been spent to prepare, index, and maintain these criminal-history files demonstrates that the individual items of information in the summaries would not otherwise be 'freely available' either to the officials who have access to the underlying files or to the general public. . . . [T]he issue here is whether the compilation of otherwise hard-to-obtain information alters the privacy interest implicated by disclosure of that information.").

[188] Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 925–26 (2005).

[189] *Id.* at 921.

[190] *Id.* at 988.

[191] *General Data Protection Regulation*, *supra* note 76, at 51–53.

[192] *Id.* at 9.

ads, they should not bear responsibility for voluntary actions of consenting adults who choose to share information about themselves and others.[193] As has become clear in other legal arenas, such as copyright and defamation, imposing intermediary liability for user-generated content risks stifling innovation and free speech.[194] To prevent undesirable content monitoring and censorship and refrain from an unrealistic expectation that platform providers disentangle complex webs of individual rights, a more nuanced approach to the right to be forgotten is needed. Such an approach would be based on relevant distinctions, for example, between data collected from passive individuals; data actively shared by them; and data about them posted by third parties.[195]

Thus, while addressing privacy in social media, the right to be forgotten is yet another legislative proposal grounded in the controller model. It fails to address a reality where decision-making power is distributed among hundreds of millions of individuals dispersed around the globe; where a single individual's decision to download an app or use a photo auto-tagging tool may have a significant impact on the privacy of others.[196]

The existing framework's overreliance on the controller model is manifest in other contexts, such as the role of platform providers. An increasing number of business models revolve around central platform providers, which enable the development of tools, applications, and additional services directly or through an application programming interface (API). Consider, for example, Apple's iOS mobile operating system or Google Android. As of June 2013, Apple's App Store contained more than 900,000 iOS applications ("apps"), which have collectively been downloaded more than fifty billion times;[197] Android's figures

---

[193] CTR. FOR DEMOCRACY & TECH., ON THE "RIGHT TO BE FORGOTTEN": CHALLENGES AND SUGGESTED CHANGES TO THE DATA PROTECTION REGULATION 7–8 (May 2, 2013), *available at* https://www.cdt.org/files/pdfs/CDT-Free-Expression-and-the-RTBF.pdf.

[194] *See, e.g.*, Jeff Kosseff, *Defending Section 230: The Value of Intermediary Immunity*, 15 J. TECH. L. & POL'Y 123, 125 (2010); Rebecca Tushnet, *Power Without Responsibility: Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 1006 (2008); *see also* Jeffrey Rosen, *The Delete Squad: Google, Twitter, Facebook and the New Global Battle over the Future of Free Speech*, NEW REPUBLIC (Apr. 29, 2013), http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules#. *See generally* Thomas Margoni & Mark Perry, *Deep Pockets, Packets, and Harbors*, 74 OHIO ST. L.J. 1195 (2013); Tal Z. Zarsky & Norberto Nuno Gomes de Andrade, *Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum*, 74 OHIO ST. L.J. 1335 (2013).

[195] Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PETER FLEISCHER: PRIVACY . . . ? (Mar. 9, 2011, 8:59 AM), http://peterfleischer.blogspot.co.il/2011/03/foggy-thinking-about-right-to-oblivion.html; Peter Fleischer, *The Right To Be Forgotten, or How To Edit Your History*, PETER FLEISCHER: PRIVACY . . . ? (Jan. 29, 2012, 6:57 AM), http://peterfleischer.blogspot.co.il/2012/01/right-to-be-forgotten-or-how-to-edit.html; *see also* Jef Ausloos, *The "Right To Be Forgotten"—Worth Remembering?*, 28 COMPUTER L. & SECURITY REV. 143, 151–52 (2012).

[196] *See* Hill, *supra* note 178.

[197] Press Release, Apple, Apple's App Store Marks Historic 50 Billionth Download (May 16, 2013), *available at* http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html.

are similar.[198] Facebook, the dominant social networking provider, fulfills a similar gatekeeping role in its market segment. Some platforms are open, leaving developers with a great deal of control within a set of ground rules determined by the platform providers; others are closed, walled-gardens, where platform providers act like true gatekeepers.

The allocation of responsibilities among various links in the mobile (or social networking) value chain, including hardware manufacturers, platform makers, app developers, mobile operators, advertising networks, and location providers, has been the subject of intense debate.[199] The controller model, with its linear view of data processing, is clearly ill-suited to navigate this terrain.[200] Who should be charged with providing individuals with notice and choice? Against whom should individuals assert their rights of access, rectification, and erasure? Should privacy law recognize an intermediary role, which is neither controller nor processor, for platform providers?[201] Or, conversely, is it perhaps the platform providers, as parties generally trusted by consumers, who should bear the brunt of privacy law? In which case, is it sufficient for platform providers to contract out liability to app developers through bilateral agreements (excluding consumers) such as the iOS Developer Program License Agreement or the App Store Review Guidelines? Or must platform providers actively monitor, police, and sanction untoward practices by apps?

Intermediary liability raises conflicting legal impulses in the online environment. On the one hand, few parties are as well-positioned as platform providers to effect significant control over the widely dispersed ecosystem. On

---

198 Hugo Barra, *Android@I/O: Just Press Play*, ANDROID: OFFICIAL BLOG (May 15, 2013), http://officialandroid.blogspot.com/2013/05/androidio-just-press-play.html.

199 *Compare* FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY i–iii (2013) (focusing on open and transparent communication between all parties), *and* KAMALA D. HARRIS, ATTORNEY GEN. CAL. DEP'T OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM 2 (2013), *with* Article 29 Data Prot. Working Party, *Opinion 02/2013 on Apps on Smart Devices*, at 27, 00461/13/EN, WP 202 (Feb. 27, 2013) (focusing suggestions on app developer responsibilities), *and* FUTURE OF PRIVACY FORUM & CTR. FOR DEMOCRACY & TECH., BEST PRACTICES FOR MOBILE APPLICATION DEVELOPERS: APP PRIVACY GUIDELINES BY THE FUTURE OF PRIVACY FORUM AND THE CENTER FOR DEMOCRACY & TECHNOLOGY 1 (2012) (saying app developers are best equipped to address problems).

200 W. Kuan Hon, Christopher Millard & Ian Walden, *Who Is Responsible for "Personal Data" in Cloud Computing?—the Cloud of Unknowing*, 2 INT'L DATA PRIVACY L. 3, 6 (2012).

201 In his report to Parliament on the Draft EU Regulation, the Rapporteur introduces a new role of "producer," applying to "person[s] . . . or . . . bod[ies] which create[] automated data processing or filing systems [to be used] by data controllers and data processors." RAPPORTEUR'S DRAFT, *supra* note 144, amend. 88. According to the Rapporteur, producers, including both makers of hardware and software, will need to comply with privacy by design and privacy by default requirements, even if they do not process personal data themselves. *Id.* amend. 71. The Rapporteur states: "This is especially relevant for widely used standard applications, but also should be respected for niche products." *Id.*; *see also id.* amends. 88, 98, 178.

the other hand, enhancing the control of already powerful central actors seems unwise from a competition law perspective and raises concerns over censorship and freedom of speech and occupation. A future-proof information privacy framework will have to conceive of a new model to address the allocation of responsibility and inherent limitations of key players in the ecosystem, including individuals.

D. *Location*

The second generation of information privacy laws, particularly the European framework, continues to view information as "residing" in a jurisdiction, despite the geographic indeterminacy of online transfers and cloud storage.[202] For many years, transborder data flow regulation has caused much consternation to businesses on both sides of the Atlantic.[203] These tensions have reached a zenith with the recent revelations about the scope of NSA access to data on the cloud.[204] Unfortunately, this approach is not likely to change.

There is inherent tension between the two primary objectives of the OECD and EU frameworks: the facilitation of transborder data flows, on the one hand,[205] and the protection of individuals' privacy on the other hand.[206] In trying to craft a careful balance between these goals, the frameworks have become fixated on data location. The EU framework in particular erected an entire legal edifice around the control of transborder data flows. An enormous amount of resources is spent attending to the requirement of the *EU Directive* to execute countless boilerplate agreements ("model clauses"); corporate codes of conduct ("binding corporate rules"); and national legal assessments ("adequacy" decisions; and the U.S. and Swiss Safe Harbor arrangements)—all geared at "legitimizing" data flows.[207] Alas, with the development of information communication technologies, the link between transborder data flow rules and realities on the ground has become tenuous at best.

---

[202] *See* Michael A. Geist, *Is There a There There? Toward Greater Certainty for Internet Jurisdiction*, 16 BERKELEY TECH. L.J. 1345, 1349–50 (2001); Dennis D. Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74 OHIO ST. L.J. 1029, 1036–37 (2013).

[203] Geist*, supra* note 202, at 1347–49.

[204] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 6, 2013, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[205] *OECD Guidelines*, *supra* note 2, ¶ 21.

[206] Directive 95/46/EC, *supra* note 3, at 38.

[207] *See id.* at 45–47. Certain improvements have been made with the European adequacy model and more are on the way, including flexible standard contractual clauses, binding corporate rules for processors, and a greater emphasis on binding corporate rules. *See* Reding, *supra* note 83.

If not already technologically obsolete when put in place in the 1990s, the rules on transborder data flows certainly appear so now.[208] Conceived in a day and age when data transfers consisted of postage of back-up tapes and floppy disks, these rules struggle to deal with the always connected world of online, mobile, and cloud computing.[209] Today, information zips across the globe at the speed of light; is accessed simultaneously from multiple locations; and "resides" on servers distributed in remote countries based on considerations such as latency or thermal control.[210] In a world where individuals freely carry powerful pocketsize devices across borders, the concept of a "data transfer" has become outmoded. As Christopher Millard and colleagues recently note: "[W]hat matters most is not where information is stored, but who can read it."[211]

Ironically, the first data protection case ever to be decided in the European Court of Justice (ECJ) already demonstrated the futility of regulating data transfers online. In the *Bodil Lindqvist* case, the ECJ contemplated whether the posting of personal information to a website constitutes a transborder data transfer, given that such information immediately becomes accessible to the entire world.[212] This question arose in the context of a mundane data transaction, long before the intense traffic velocity of social media sites.[213] The ECJ recognized that:

> If Article 25 of Directive 95/46 were interpreted to mean that there is "transfer [of data] to a third country" every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application . . . . The Member States would be obliged to prevent any personal data being placed on the internet.[214]

While limited to its facts, which involved the posting of data to a website "established" in the EU, the *Lindqvist* decision clearly struggled to contain the concept of a data transfer.[215] The *Lindqvist* ruling raised difficult questions, which have yet to receive an adequate response: Does it matter whether an individual or organization posting data online *intended* it to be accessed in a

---

[208] Omer Tene, *Privacy: The New Generations*, 1 INT'L DATA PRIVACY L. 15, 15–16 (2011).

[209] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 1–11, 25–59 (2013).

[210] Tene, *supra* note 208, at 16.

[211] W. Kuan Hon & Christopher Millard, Data Export in Cloud Computing—How Can Personal Data Be Transferred Oustide the EEA? 27 (Apr. 4, 2012) (unpublished manuscript), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1925066.

[212] Case C-101/01, *In re* Lindqvist, 2003 E.C.R. I-12971, ¶ 18.

[213] *Id.* ¶¶ 12–18.

[214] *Id.* ¶ 69.

[215] *See id.* ¶¶ 56–71.

certain jurisdiction? Does it matter whether the data were *in fact* accessed in such jurisdiction?

Over the decade since *Lindqvist*, additional questions arose, such as whether transborder data flow rules have conferred any benefits to individuals. Do individuals in the EU benefit from greater privacy protection than individuals in the United States due to transborder data flow restrictions? Are data stored, for example, in a highly secured, state of the art outsourcing center in India less "safe" than data maintained by a negligent contractor in Poland?

If these questions were complex in a traditional online environment, they have become daunting with the arrival of cloud computing. In cloud, data held by a service provider is typically replicated on multiple servers for reasons of performance, availability, and backup.[216] Copies are stored across different virtual and physical borders, often in different jurisdictions. Techniques such as "sharding" and "partitioning" enable the storage of fragments of data across a range of machines, logically linked and reassembled on demand, rather than as a single contiguous set.[217] Control over various parts of the cloud "stack" is distributed across a range of software (SaaS), platform (PaaS), and infrastructure (IaaS) providers, including multiple sub-providers and sub-sub-providers, each of which may be established in a different jurisdiction. In this ecosystem, merely figuring out where the data *are* is nontrivial. And even if a service provider can pinpoint a customer's data fragment to a specific data center, in most cases, such information will not be disclosed to the customer, who nevertheless remains the "data controller" under the EU framework.

Certain aspects of the data location paradigm are downright bizarre. For example, a U.S. entity storing data about U.S. persons with a U.S. cloud storage service provider with a data center in the EU may not be permitted to access its own data from the United States, given that such access is regarded as a "re-export" under EU law.[218] This will be the case regardless of the fact that the data originated in the United States, concerns U.S. individuals, is managed by U.S. entities, and more generally has no geographic (or other) nexus to the EU besides residing on EU-based hardware.[219] And while the rule imposing liability under EU law is about to be replaced as part of the reformed framework, the amended provision is no less grandiose in extraterritorial

---

[216] W. Kuan Hon, Christopher Millard & Ian Walden, *The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated?—The Cloud of Unknowing*, 1 INT'L DATA PRIVACY L. 211, 221 (2011).

[217] *Id.*

[218] Hon & Millard, *supra* note 211, at 32. This is the result of Article 4(1)(c) of the *EU Directive*, the "making use of equipment" test. Directive 95/46/EC, *supra* note 3, at 39.

[219] Certain EU Member States have either law or guidance that softens this aspect of the *EU Directive*, perhaps due to its illogicality or to avoid harming the local data processing industry. *See Sending Personal Data Outside the European Economic Area (Principle 8)*, U.K. INFO. COMMISSIONER'S OFF., http://www.ico.org.uk/for_organisations/data_protection/the_guide/principle_8 (last visited Sept. 5, 2013).

ambition; indeed it may be broader, ostensibly applying EU law to the entire Internet.[220]

When discussing transborder data flow regulation, the elephant in the room is lawful access or intercept by foreign governments. Even before the recent NSA revelations, EU policymakers have repeatedly voiced concerns over access to data concerning European citizens by law enforcement and national security agencies in the United States.[221] These concerns erupted into diplomatic bouts in connection with access to EU passengers' passenger name record (PNR) information by the U.S. Department of Homeland Security[222] and to records of financial transactions maintained by Belgium-based SWIFT by the Federal Bureau of Investigation.[223] The revelations about the striking scope and depth of data collection by the NSA directly from the servers of the largest global online service providers with little or no guarantees for the rights of non-U.S. persons, underscore the gravity of privacy risks in this brave new world of data transfers. It is doubtful, however, that transborder data flow regulation that is based on *ex ante* formalistic border controls can remedy these concerns. It has failed to do so in the past,[224] and given the ubiquity of data flows on the Internet, mobile, and cloud, it will fail to do so the future.

---

[220] Article 3(2) of the Draft EU Regulation extends the application of European law to the processing of personal data by a controller not established in the EU, "where the processing activities are related to: (a) the offering of goods or services to such data subjects in the Union; or (b) the monitoring of their behaviour." *General Data Protection Regulation*, *supra* note 76, at 41. This extension of extraterritorial application constitutes a dramatic shift from a country of origin to a country of destination approach, and portends general application of the regulatory framework to the entire Internet. Arguably, any website visited by a European end user and deploying monitoring tools (as nearly all websites do, for a wide range of purposes) meets one or both of the strains of Article 3(2). *See* OMER TENE & CHRISTOPHER WOLF, OVEREXTENDED: JURISDICTION AND APPLICABLE LAW UNDER THE EU GENERAL DATA PROTECTION REGULATION 3–4 (Jan. 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/FINAL-Future-of-Privacy-Forum-White-Paper-on-Jurisdiction-and-Applicable-Law-January-20134.pdf.

[221] *See generally* 2 INT'L DATA PRIVACY L. No. 4 (Nov. 2012), http://idpl.oxfordjournals.org/content/2/4.toc (special issue surveying systematic government access to private-sector data in nine countries).

[222] Letter from Jacob Kohnstamm, Chairman of the Article 29 Data Prot. Working Party, to Members of the LIBE Comm. of the Eur. Parliament (Jan. 6, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120106_letter_libe_pnr_en.pdf.

[223] Article 29 Data Protection Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, at 27–28, 01935/06/EN, WP 128 (Nov. 22, 2006).

[224] In its first report on transposition of the European Data Protection Directive, the European Commission noted that, "[M]any unauthorised and possibly illegal transfers are being made to destinations or recipients not guaranteeing adequate protection. Yet there is little or no sign of enforcement actions by the supervisory authorities." Comm'n of the Eur. Cmtys., *First Report on the Implementation of the Data Protection Directive (95/46/EC)*, at 19, COM (2003) 265 final (May 15, 2003).

A better policy would be based on clarifying the notoriously intricate rules on applicable law and jurisdiction; finding ways for the existing information privacy frameworks to interoperate in order to reduce international tensions over government access; and most importantly, using techniques like encryption and other privacy enhancing technologies to prevent unauthorized access with or without collaboration by service providers.[225]

E. *Harm*

Privacy harm is a concept that has not yet been fully explored by academics, regulators, and policymakers. What precisely is the information privacy framework trying to protect? This question, of course, touches on the contours of the right to privacy, an issue to steer clear from if one desires practical conclusions.[226] But without a better mapping of privacy harms, class action law suits in the United States will continue to fail,[227] and steep sanctions proposed under the reformed EU framework will appear draconian.[228] What harm is caused by a data spill if none of the concerned individuals suffer from identity (or credit card credentials) theft? And what harm does use of clickstream information for ad targeting cause, even without any transparency and user choice? Are individuals harmed when persistently monitored by a government or private actor even if they are never aware of being subject to surveillance?

European policymakers typically resist the discussion of privacy harms, arguing that privacy is a fundamental human right and should therefore be protected without harm analysis.[229] This approach is unsatisfactory. Fundamental human rights are not absolute and are frequently balanced against conflicting rights (e.g., freedom of speech) or legitimate interests[230] (e.g., national security,[231] law enforcement,[232] economic efficiency or public

---

[225] Diaz, Tene & Gürses, *supra* note 154; Hon & Millard, *supra* note 211, at 26–28.

[226] Brave attempts have been made: HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 1–4 (2010); WESTIN, *supra* note 157, at 42; Ruth Gavison, *Privacy and the Limits of the Law*, 89 YALE L.J. 421, 422–24 (1980); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 422–23 (1960); Solove, *supra* note 119, at 562–64; Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214–20 (1890).

[227] *See, e.g.*, Low v. LinkedIn Corp., No. 11-CV-01468-LHK, 2011 WL 5509848, at *6 (N.D. Cal. Nov. 11, 2011); *In re* iPhone Application Litig., No. 11-MD-02250-LHK, 2011 WL 4403963, at *15 (N.D. Cal. Sept. 20, 2011); *In re* JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 330 (E.D.N.Y. 2005). *But see* Krottner v. Starbucks Corp., 628 F.3d 1139, 1141–42 (9th Cir. 2010) (holding that "increased risk of future identity theft" and "generalized anxiety and stress" constitute injuries sufficient to support standing to sue).

[228] *General Data Protection Regulation*, *supra* note 76, at 92–94.

[229] *See id.* at 2.

[230] *See* Directive 95/46/EC, *supra* note 3, at 7.

[231] *See, e.g.*, Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1871 (2006).

health[233]). Fundamental rights are moderated through application of the principle of proportionality. Risk of harm analysis is thus required not in order to *recognize* a right to privacy, but rather to delineate its limits vis-à-vis other compelling policy considerations.[234] Privacy is an important legal right and value, but not one that trumps every other social consideration.

Few commentators have attempted to address the privacy harm conundrum. Dan Solove's *A Taxonomy of Privacy* defines privacy through a classification of harms, consisting of categories such as aggregation, identification, secondary use, exclusion, breach of confidentiality, disclosure, exposure, and blackmail.[235] Ryan Calo distinguishes between subjective privacy harms, which he refers to as a perception of unwanted observation (also known in colloquial English as a feeling of "creepiness"); and objective privacy harms, which include unanticipated or coerced use of an individual's information against that individual.[236] Security breach legislation in the United States is premised on an assumption of harm caused by unauthorized access to one's name in conjunction with a credit card number, social security number, or financial account information.[237]

Analysis of harm is particularly important given privacy's proximity to tort law, which tailors compensation and damages to harm. Courts tend to disfavor intangible, non-pecuniary damages, which are difficult to assess and may be perceived as non-tort penalties. Consequently, in a recent decision, the Supreme Court of the United States held that the "actual damages" standard under the Privacy Act of 1974 was not clear enough to allow damages for mental and emotional distress.[238] The Court decided that a pilot whose HIV-positive status was improperly shared between government agencies could not collect damages for emotional distress.[239] Dissenting, Justice Sotomayor stated: "After today, no matter how debilitating and substantial the resulting mental anguish, an individual harmed by a federal agency's intentional or willful violation of the Privacy Act will be left without a remedy unless he or she is able to prove pecuniary harm."[240]

---

[232] *See, e.g.*, Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2012).

[233] *See* Jules Polonetsky & Omer Tene, *Privacy and Big Data: Making Ends Meet*, 66 STAN. L. REV. ONLINE 25, 25 (2013), http://www.stanfordlawreview.org/sites/default/files/online/topics/PolonetskyTene.pdf.

[234] *Id*.

[235] Solove, *supra* note 119, at 490–91.

[236] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1142–43 (2011).

[237] *See* Paul M. Schwartz & Edward J. Janger, *Notification of Data Security Breaches*, 105 MICH. L. REV. 913, 934 (2007).

[238] Fed. Aviation Admin. v. Cooper, 132 S. Ct. 1441, 1456 (2012). Specifically, the Court held that the term "actual damages" was too ambiguous to be used to waive sovereign immunity in a case involving mental or emotional distress. *Id.*

[239] *See id.*

[240] *Id.* at 1463 (Sotomayor, J., dissenting).

A harms-based approach to privacy need not be limited to tangible harms. A better understanding of the effect of data analysis on fairness, discrimination, and narrowcasting can expand the scope of privacy harms that are subject to legal protection. Cynthia Dwork and Deirdre Mulligan refer to fairness concerns heavily weighted by issues of discrimination, including price discrimination based on location (redlining) or on knowledge of a consumer's state of mind.[241] In a big data reality, the processing of personal data increasingly affects fairness, equality, and other values that are no less important than—even if theoretically distinct from—core privacy interests.[242] This means that the debate over privacy has become conflated with broader social values, bringing to the forefront questions about the use of information to categorize and draw distinctions between individuals. Even where such distinctions do not implicate legally suspect categories, such as race, gender, or age, they may well remain normatively suspect, such as where an employer screens out job candidates based on good looks[243] or a retailer assigns shoppers a "pregnancy score."[244]

To justify civil and criminal enforcement efforts and ward off arguments concerning lack of clarity and focus, the information privacy framework needs to construct a clearer model for harm.

V. CONCLUSION

The dawning of the second wave of global information privacy laws coincides with seismic shifts in the business and technological landscape. Personal data have become a valuable asset class, an indispensible means of production driving business models such as big data, mobile communications, social networking, and cloud computing. Yet the frameworks emerging from the review processes launched by the OECD, EU, and United States remain firmly rooted in principles and laws dating back to the age of punch cards and mainframe computers. Specifically, the reform processes fail to address challenges to the definition of personal data and science of de-identification; continue to rely on individuals' consent to legitimize processes far removed from individuals' knowledge and comprehension; condition scientific advances and big data societal gains on individuals' fickle choices; frame data collection and use as a linear process despite the explosion of user-generated content and

---

241 Cynthia Dwork & Deirdre K. Mulligan, *It's Not Privacy, and It's Not Fair*, 66 STAN. L. REV. ONLINE 35, 36–38 (2013), http://www.stanfordlawreview.org/sites/default/files/online/topics/DworkMullliganSLR.pdf; Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 12 J. ON TELECOMM. & HIGH TECH. L. (forthcoming 2013); *see also* Dana Mattioli, *On Orbitz, Mac Users Steered to Pricier Hotels*, WALL ST. J., Aug. 23, 2012, http://online.wsj.com/article/SB10001424052702304458604577488822667325882.html.

242 Tene & Polonetsky, *supra* note 241.

243 *See, e.g.*, *Attractiveness Discrimination: Hiring Hotties*, ECONOMIST, July 21, 2012, http://www.economist.com/node/21559357.

244 Duhigg, *supra* note 119.

introduction of a broad array of parties into any data transaction; insist on framing data flows in a geographical context while disregarding the effervescent nature and rapid movement of data across borders; and lack a coherent model for privacy harms, which would allow policymakers to tailor appropriate responses.