THE PRIVACY–INNOVATION CONUNDRUM

by
Tal Z. Zarsky[*]

The age of Big Data is upon us. The analysis of personal data is generating greater opportunities for privacy breaches as well as innovative progress. Governments worldwide are striving to establish a proper response to the ongoing practices of personal-data collection, analysis, and usage. This regulatory discourse immediately leads to a discussion of the relation between privacy rules and the broad and complex concept of innovation. Privacy laws could either enable or impede the flow of personal data. Availability and access to such data can either enhance or undermine innovation.

The overarching debate on the relation between privacy and innovation is constantly heating, especially in the political and policy world. In addition, the link between privacy and innovation raises a variety of complicated analytical questions, hence calls for a nuanced academic and theoretical discussion. This Article introduces the first attempt to compressively map out and evaluate the various ways in which the relationship between privacy and innovation could be articulated.

In Part II, the Article launches the discussion by providing foundational working definitions of the concepts of privacy and innovation. Thereafter, it maps out five possible links between privacy and innovation. This Part concludes that among the different arguments, the "privacy-versus-innovation" theme is of greatest interest and relevance to the current academic and policy discourse. Part III scrutinizes this latter theme closely. At first blush the "privacy-versus-innovation" argument seems absurd or intentionally manipulative. Yet a deeper examination

---

[*] Professor, University of Haifa, Faculty of Law; LL.M., J.S.D. Columbia Law School; Fellow, Information Society Project Yale Law School. I thank the participants of the University of Pennsylvania Law School–Bar Ilan University "Understanding Entrepreneurship" Symposium, the IBM-Haifa "Information Privacy" Seminar, Yale Law School's "Innovation Law Beyond IP Conference" and the "Privacy Legal Scholars Conference" panels devoted to this Paper as well as those of the "Law and Economics of Innovation" Workshop at ETH Zurich and The University of Zurich, the "Law and Technology" Workshop at Tel Aviv University and the "Private Law Workshop" at the Hebrew University in Jerusalem, Norberto Andrade, Stefan Bechtold, Michael Birnhack, Bryan Choi, Julie Cohen, Bruno Frey, Raphael Gellert, Andreas Heinemann, Dennis Hirsch, Joris van Hoboken, Chris Hoofnagle, Alan Miller, Michal Shur-Ofry, Frank Pasquale, Karl-Nikolaus Peifer, Daniel Weitzner, and Assaf Yaakov for their suggestions and comments. This project also benefited from conversation with Yochai Benkler, Geoffrey Delcroix, Claudia Diaz, Mireille Hildebrandt, Margot Kaminski, Daniel Le Métayer and Deirdre Mulligan, and from the research assistance of Talya Ponchek.

shows that it might rely on the argument that peripheral privacy rights are potentially uncertain or overbroad.

Part IV strives briefly and cautiously to move the "privacy-versus-innovation" argument, and the cross-Atlantic policy debate it involves, to the empirical realm. Here the Article confronts the possible linkage between lenient privacy laws in the United States and the success of U.S. firms in the internet/ICT environment, as opposed to strict privacy and relative failure in Europe. This Part strives to properly frame the meaning of this linkage in the underlying privacy–innovation discussion.

In addition, Part IV carefully examines the policy implications of recognizing a causal relationship, as opposed to mere linkage, between privacy and innovation in the United States and the EU. One course of action would be to change the existing EU data-protection scheme and to assure the persistence of lenient privacy laws in the United States. However, other theories and policy steps, which account for the way laws shape technologies in a global setting, might recommend the adoption of a global, strict privacy regime. The Article concludes by alluding to the most recent trends and transactions in global ICT markets, which might indicate a new direction for privacy, innovation, and the interaction between them.

I. INTRODUCTION: ANALYZING PRIVACY VERSUS INNOVATION—WHY, WHY NOW, AND HOW?

The age of Big Data is upon us. The analysis of personal data is generating greater opportunities for privacy breaches as well as innovative progress. We might be entering the golden age of innovation in data analysis and the dark age of information privacy. Governments worldwide are striving to establish a proper response to the ongoing practices of personal data collection, analysis, and usage.[1] This regulatory discourse immediately leads to a discussion of the relation between privacy rules and the broad and complex concept of innovation.[2] This should be no surprise, as innovation-related interests are omnipresent in a variety of policy and legal debates.[3] In the technology-related realm, where information-privacy policy plays an important role, innovation is often considered when intellectual property policy is being formulated.[4] Indeed, in

[1] *See infra* notes 10–17.

[2] Anupam Chander, *How Law Made Silicon Valley*, 63 EMORY L.J. 639, 641–42, 667 (2014) (discussing the various reasons for the success of information and communication technology ("ICT") firms in California and their relative failure elsewhere, while touching upon the role of privacy law and policy in this outcome).

[3] There are many discussions of innovation policy in other fields of law, such as immigration and employment. For a recent discussion of the latter, see generally ORLY LOBEL, TALENT WANTS TO BE FREE (2013). *See also* Chander, *supra* note 2, at 641 (citing Ronald J. Gilson, *The Legal Infrastructure of High Technology Industrial Districts: Silicon Valley, Route 128, and Covenants Not to Compete*, 74 N.Y.U. L. REV. 575, 578 (1999)). For a recent discussion in the context of law and economics, see generally ROBERT COOTER WITH AARON EDLIN, THE FALCON'S GYRE: LEGAL FOUNDATIONS OF ECONOMIC INNOVATION AND GROWTH (2014), *available at* http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1000&context=books.

[4] Stanford Law School has even devoted a clinic to this issue. *See Juelsgaard Intellectual Property and Innovation Clinic*, STANFORD L. SCH. (2014), http://www.law.stanford.edu/organizations/clinics/juelsgaard-intellectual-property-and-innovation-clinic. For a discussion in the context of copyright (arguing limited effect of copyright law on innovation), see Peter S. Menell, *Indirect Copyright Liability and Technological Innovation*, 32 COLUM. J.L. & ARTS 375, 376–79 (2009). For the

some contexts, such as patent law, the impact of policy and legal decisions on innovation is central to regulatory debates, and rightly so.[5]

Innovation-based considerations are often also cited by policymakers and academics when contemplating decisions destined to impact infrastructures that enable the transfer of data and information. These could be physical, such as fiber, or virtual, namely software.[6] A natural extension of these realms of discussion is the examination of the relation between innovation and policy decisions governing data protection and information privacy. Framed differently, privacy and data protection laws are a legal infrastructure that impacts the transfer of a certain form of rich, yet possibly harmful, data: personal information.

Privacy laws could either enable or impede the flow of personal information to various parties in the information society. Availability and access to such data, currently collected in enormous quantities, can enhance innovation. Access to such information allows knowledge generation, and the development of technologies for analyzing the data as well as business models to utilize the derived information. These advances lead to social benefits and the enhancement of social welfare.[7] On the

opposite view, see Michael A. Carrier, *Copyright and Innovation: The Untold Story*, 2012 WIS. L. REV. 891, 936–58. Yet, see the discussion below regarding the important differences between IP and privacy policy when addressing innovation-related interests. *Infra* notes 128–29 and accompanying text.

[5] For a recent reference to this point in the popular press, see Patrick Hall, *Patent Law Broken, Abused to Stifle Innovation*, WIRED (July 26, 2013), http://www.wired.com/insights/2013/07/patent-law-broken-abused-to-stifle-innovation. For some selected academic references, see Gaia Bernstein, *In the Shadow of Innovation*, 31 CARDOZO L. REV. 2257, 2260 (2010), Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 CALIF. L. REV. 1, 4–6 (2001), Michael A. Heller & Rebecca S. Eisenberg, Review, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCIENCE 698, 698–99 (1998), Robert P. Merges, *The Trouble with Trolls: Innovation, Rent-Seeking, and Patent Law Reform*, 24 BERKELEY TECH. L.J. 1583, 1584–86 (2009), and Philip J. Weiser, *The Internet, Innovation, and Intellectual Property Policy*, 103 COLUM. L. REV. 534 (2003). For policy papers on this matter, see FED. TRADE COMM'N, TO PROMOTE INNOVATION: THE PROPER BALANCE OF COMPETITION AND PATENT LAW AND POLICY (Oct. 2003), *available at* http://www.ftc.gov/sites/default/files/documents/reports/promote-innovation-proper-balance-competition-and-patent-law-and-policy/innovationrpt.pdf, and *R&D, Innovation and Patents*, WIPO, http://www.wipo.int/patent-law/en/developments/research.html.

[6] For a recent discussion, see Christopher S. Yoo, *Protocol Layering and Internet Policy*, 161 U. PA. L. REV. 1707, 1714 (2013). For a critical view of such discussions, see Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1919 (2013). Cohen sees these steps as mostly moves to ease regulation. *Id.*; *see also* Bernstein, *supra* note 5, at 2269.

[7] See generally Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239 (2013) for a discussion of the benefits of "Big Data" analysis, spanning from healthcare, to mobile, to smart grids and retail. Much of the information discussed is personal in nature. For a specific example, see Avi Goldfarb & Catherine Tucker, *Privacy and Innovation* 4–11 (Nat'l Bureau of Econ. Research, Working Paper No. 17124, 2011), *available at* http://www.nber.org/papers/w17124.pdf (discussing the use of personal information to improve various aspects of life, such as neonatal care).

other hand, personal information flows might undermine innovation, as the prospect of such flows might chill various innovation forms. Beyond these basic points, laws governing personal information flow also impact innovation by changing the overall business and social environment.

In contrast to other realms of law, where academics blazed the trail and policymakers followed, in the specific context here discussed, the dynamic is reversed. In the United States, innovation considerations are central to the privacy based policy discussion,[8] but the academic discussion is lacking.[9] Regulators often note risks to innovation when contemplating privacy related regulation. For instance, the Department of Commerce issued a "Notice of Inquiry" addressing this exact issue. The comments received, together with the Department's own conclusions, were presented in an important Green Paper, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[10] Innovation-based considerations are also prominently discussed in a report issued in 2012 by the Federal Trade Commission[11] and in reports issued by the White House in 2012[12] and 2014[13]—the three most central documents addressing privacy considerations authored by the U.S. government.

The overarching debate on the relation between privacy and innova-

[8] While considering innovation concerns for various regulatory frameworks might seem natural and intuitive, it is, in effect, a recent trend. Merely 30 years ago, Richard Stewart noted, in the context of environmental law, that "[w]ith limited exceptions, Congress and administrators have not been much concerned with market innovation in designing and implementing regulatory programs." Richard B. Stewart, *Regulation, Innovation, and Administrative Law: A Conceptual Framework*, 69 CALIF. L. REV. 1256, 1288 (1981).

[9] A notable exception is Julie Cohen's illuminating book chapter. Julie E. Cohen, *The Surveillance–Innovation Complex: The Irony of the Participatory Turn*, *in* THE PARTICIPATORY CONDITION (Darin Barney et al. eds.) (forthcoming 2015) (manuscript at 1), *available at* http://ssrn.com/abstract=2466708. Other scholars address various facets of the innovation–privacy linkage, as discussed below.

[10] DEP'T OF COMMERCE INTERNET POLICY TASK FORCE, COMMERCIAL DATA PRIVACY AND INNOVATION IN THE INTERNET ECONOMY: A DYNAMIC POLICY FRAMEWORK (Dec. 16, 2010), *available at* http://www.ntia.doc.gov/files/ntia/publications/iptf_privacy_greenpaper_12162010.pdf [hereinafter GREEN PAPER].

[11] References to innovation appear on pages 9, 13, 26, 27, 36, and 38 of the FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (Mar. 2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC REPORT].

[12] "Innovation" is even noted in the document's title. The WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (Feb. 2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter WHITE HOUSE REPORT].

[13] EXEC. OFFICE OF THE PRESIDENT, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 20 (May 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf ("The Internet's complexity, global reach, and constant evolution require timely, scalable, and innovation-enabling policies.").

tion is constantly heating. It is fair to assume that much of the attention devoted to innovation in the discussion of privacy policy results from lobbyists pushing this point in various contexts. One dominant context pertains to debates on the enactment of the EU Data Protection Regulation Proposal.[14] As EU officials ponder the intricacies of these new provisions in Brussels, U.S.-based interest groups (as well as the U.S. government itself) try to influence the process, and call for a more lenient approach.[15] Among the various issues set forth, innovation-based concerns are prominently cited.[16] Needless to say, these foreign-based interventions are often criticized by EU authorities, NGOs, and privacy actors.[17] It is yet to be seen how this issue will ultimately unfold, but innovation-based concerns will surely impact the final decisions made by EU legislators, one way or another. Similarly, the "innovation" argument will affect the outcome of U.S.-based regulatory debates. In all these contexts, the voice of academia is warranted and crucial.

Beyond the political and policy realm, however, the link between privacy and innovation raises a variety of complicated analytical questions, hence calls for a nuanced academic and theoretical discussion. The terms "innovation" and "privacy," and their relation, are invoked in a variety of contexts.[18] In academic analyses thus far, when innovation and privacy were examined in concert, the discussion that followed was somewhat limited and even confusing. The issues were approached from a variety of perspectives that implicitly rested on different understandings and definitions of key foundational notions. Clearly, when stakes are high and terms are flexible, their meaning and the outcomes of the analysis can be easily misunderstood and manipulated. In response to these concerns, this Article is the first attempt to comprehensively map out and

[14] *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)*, COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Personal Data Regulation Proposal*].

[15] *See* Jennifer Baker, *EU Data Protection Proposals Taken Word for Word from US Lobbyists*, CIO (Feb. 12, 2013), http://www.cio.co.uk/news/strategy/eu-data-protection-proposals-taken-word-for-word-from-us-lobbyists; *see also, e.g.*, DIGITALEUROPE, DIGITALEUROPE COMMENTS ON THE RISK-BASED APPROACH 6–10 (Aug. 28, 2013), *available at* http://www.digitaleurope.org/DocumentDownload.aspx?Command=Core_Download&EntryId=601.

[16] *See, e.g.*, William E. Kennard, U.S. Ambassador to the EU, Remarks at Forum Europe's 3rd Annual European Data Protection and Privacy Conference (Dec. 4, 2012), *available at* http://useu.usmission.gov/kennard_120412.html. The ambassador refers several times to the threat to innovation set by strict privacy laws. Note that the U.S.-based firms are not alone in this process. For a similar position taken by UK-based firms, see MARK LLOYD, CBI, DATA PROTECTION IN THE EU: THE CASE FOR A RE-THINK 1–2 (Feb. 2012), *available at* http://www.cbi.org.uk/media/1356711/cbi_response__data_protection_in_the_eu__feb_2012_.pdf. *See also* Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1, 62 (2012).

[17] April Dembosky & James Fontanella-Khan, *US Tech Groups Criticised for EU Lobbying*, FIN. TIMES (Feb. 4, 2013).

[18] *See infra* Part II.

evaluate the various ways in which the relation between "privacy" and "innovation" may be articulated. In addition, this study strives to derive important insights from the innovation–privacy nexus: both policy implications regarding the next steps in privacy regulation and unique theoretical lessons on the deeper meaning of information privacy in the digital age.

In Part II, the Article launches the discussion by providing foundational working definitions of the concepts of privacy and innovation. Thereafter, it maps out five possible links between the notions of privacy and innovation. It does so while weaving together discussions presented in the privacy-related literature and concepts arising from the innovation-based discourse. This Part concludes that, among the different arguments, the "privacy-versus-innovation" theme is of greatest interest and relevance to the current academic and policy discourse—the notion that at some point greater privacy protection inhibits innovation. Arguments holding that privacy promotes innovation should generally be set aside.

Given the popularity and intuitive appeal of the "privacy-versus-innovation" argument for some, and its objectionable nature for others, Part III scrutinizes it closely. At first blush the argument seems absurd or intentionally manipulative. Yet a deeper examination shows that it might rely on the notion that peripheral privacy rights are potentially uncertain or overbroad, and in specific instances have merit. The Article articulates the boundaries of each of these justifications, and the policy implications they might have. Parts II and III, while conveying only one theoretical theme, strive to make two different points for two distinct audiences. For the U.S.-based reader, the Article calls for examining the "privacy-versus-innovation" analytical move with caution, as at times it might merely be a manipulation to further relax privacy regulation. On the other hand, for the EU-based audience, which seems quick (perhaps too quick) to reject the "privacy-versus-innovation" policy argument,[19] the Article strives to demonstrate that, in some instances, this notion should be considered as presenting feasible arguments to limit the extent of data protection laws. This is true even in a regime that considers privacy as a fundamental right which calls for sufficient and significant precaution.

Part IV strives briefly and cautiously to move the "privacy-versus-innovation" argument, and the cross-Atlantic policy debate it involves, to the empirical realm. Here the Article confronts the possible correlation between lenient privacy laws in the United States and the success of U.S. firms in the internet/information and communication technology environment, as opposed to strict privacy and relative failure in Europe. It further notes that the failure of web-related ICT innovation in Europe is harmful not only to the EU economy but to the EU citizens' privacy as

[19] For a recent attempt to bridge the divide between these two different perspectives, see Paul M. Schwartz & Daniel J. Solove, *Reconciling Personal Information in the United States and European Union*, 102 CALIF. L. REV. 877 (2014).

well. It is fair to assume that when privacy-related cross-Atlantic policy debates unfold, this uncomfortable comparison and the possible causation it might indicate lurks in the background. Obviously, this provocative premise and empirical anecdote must be followed up by additional theoretical and empirical work. This Part merely strives to spark a discussion on this matter by drawing out the phenomenon noted and properly framing it in the underlying privacy–innovation discussion. In addition, when noting the possible causal connection between privacy and innovation, the analysis addresses accepted alternative reasons adduced to explain the disparity between the United States and the EU regarding ICT innovation, as well as counter arguments that dismiss them. It also points to interesting test cases of ICT success followed by failure in Europe which might clarify the role of privacy regulation in this context.

Next, Part IV carefully examines the policy implications of recognizing a causal linkage, as opposed to mere correlation, between privacy and innovation in the United States and the EU. Obviously, and as advocated by the interest groups, one course of action would be to change the existing EU data-protection scheme and to assure the persistence of lenient privacy laws in the United States. However, other theories and policy steps, which account for the way laws shape technologies in a global setting, might recommend the adoption of a global, strict privacy regime, one that would lead to diverse innovations. After further consideration, this final recommendation is rejected, noting that the risk of stalling internet-related innovations is too great, especially given the huge social benefits to free speech, democracy, and freedom.

The Article concludes by alluding to the most recent trends and transactions in global ICT markets. For instance, the rise of WhatsApp and Snapchat might indicate a new direction for privacy, innovation, and the interaction between them.

While the relation of innovation to privacy has been discussed for some time, a thorough discussion of the privacy–innovation nexus is of great importance at this specific juncture—the age of "Big Data." As noted, this technological realm is generating vast innovation with a variety of business models popping up almost daily. Such innovation is often enabled by extensive data collection, powered by data mining, and potentially generating substantial privacy problems and vulnerabilities. Both innovation and privacy issues are exacerbated in this novel setting. Furthermore, a fully developed privacy–innovation discussion is urgently called for, given current pressing regulatory trends. A new wave of privacy regulation and other government-related decisions is upon us. Lawmakers in the EU, Asia,[20] and perhaps even in the United States (on the Fed-

[20] In 2012, additional countries have applied to join the pan-Asian schemes, as endorsed by the Asia Pacific Economic Cooperation ("APEC") forum. *The Cross Border Privacy Rules System: Promoting Consumer Privacy and Economic Growth Across the APEC Region*, APEC (Sept. 5, 2013), http://www.apec.org/Press/Features/2013/0903_cbpr.aspx.

eral and state levels) will be taking privacy-related action while striking a balance among interests.[21] Given looming regulation, it is crucial to fully understand the impact these decisions are destined to have on innovation.

Before proceeding, a final caveat is due. While the discussion below addresses the notion of "innovation," it does not do justice to the current rich academic literature devoted to this issue.[22] Such scholarship examines, among other things, whether innovation is firm- or user-centric (with much evidence indicating the latter), dynamic or static,[23] and if it thrives in closed or open environments.[24] Scholars distinguish different kinds of innovations: those performed in great leaps or in small steps, those produced by incumbents or by startups, and those that are embedded in new products or that modify existing ones.[25] These distinctions are only briefly noted and discussed throughout the analysis. This drawback is undoubtedly substantial, yet it is the price that must be paid for achieving the important objective of a foundational—and therefore relatively short—text to address the crucial link between privacy and innovation. The fundamental innovation-based literature must of course make its way into future discussions regarding the privacy–innovation nexus.

II. INNOVATION AND, OR VERSUS, PRIVACY—UNDERSTANDING THE LINKAGE

A. Privacy and Innovation: Basic Definitions

The link between innovation and privacy can be articulated in several ways. Yet before proceeding to address the relationship between them, here are a few words on the basic notions of "privacy" and "innovation." "Privacy" is narrowly defined here to address issues of information privacy, and mostly pertains to the rights individuals have (or should have) to their personal information that is potentially collected, analyzed, passed

[21] For a very recent indication that the White House is intending to take action regarding this matter, see John Podesta, *Big Data and the Future of Privacy*, WHITE HOUSE BLOG (Jan. 23, 2014), http://www.whitehouse.gov/blog/2014/01/23/big-data-and-future-privacy.

[22] For a mapping of the various disciplines addressing "innovation," see S. Gopalakrishnan & F. Damanpour, *A Review of Innovation Research in Economics, Sociology and Technology Management*, 25 OMEGA INT. J. MGMT. SCI. 15, 15–19 (1997). For a comprehensive discussion of the analytical elements this topic involves, see Org. for Econ. Co-Operation & Dev. ("OECD"), *Oslo Manual: Guidelines for Collecting and Interpreting Innovation Data* (3d ed. 2005) [hereinafter *Oslo Manual*].

[23] *See* Gina Neff & David Stark, *Permanently Beta: Responsive Organization in the Internet Era*, *in* SOCIETY ONLINE: THE INTERNET IN CONTEXT 173 (Phillip N. Howard & Steve Jones eds., 2004).

[24] *See generally* ERIC VON HIPPEL, DEMOCRATIZING INNOVATION 77–106 (2005); ERIC VON HIPPEL, THE SOURCES OF INNOVATION (1988).

[25] *See* Gopalakrishnan & Damanpour, *supra* note 22, at 18.

on, and eventually used by others.[26] To further narrow our debate on digital-media-related issues, the discussion specifically addresses digital data stored in datasets, as opposed to issues involving photos (which of course are now digital as well, yet will not be further examined) or analog recordings. Furthermore, the examples discussed mostly pertain to data collected in an internet environment.

In addition, given that parts of the analysis include a comparative element, the discussion will focus on several privacy norms which are implemented and interpreted differently on either side of the Atlantic. Accordingly, the Article focuses on regulations implementing rules of Fair Information Practice Principles ("FIPPs")—a broadly discussed framework,[27] which is implemented to a great extent in the EU[28] and to a lesser degree in the United States (although many have called for changing this outcome).[29] Within these rules, the Article focuses on two key elements:

[26] This definition excludes discussions of "decisional privacy" which are beyond the context of this Article. This Article also does not distinguish between concerns arising from the actual collection, analysis, or usage of the information. For these distinctions, see generally Tal Z. Zarsky, Desperately Seeking Solutions: *Using Implementation-Based Solutions for the Troubles of Information Privacy in the Age of Data Mining and the Internet Society*, 56 ME. L. REV. 13 (2004), DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008), and Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

[27] For a recent discussion of the formulation of Fair Information Practice Principles, see ROBERT GELLMAN, FAIR INFORMATION PRACTICES: A BASIC HISTORY (Aug. 2014), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf. FIPPs' most basic structure was broadly introduced in the Organisation for Economic Co-operation and Development Guidelines. Org. for Econ. Co-operation & Dev., *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Sept. 1980) [hereinafter *OECD 1980 Guidelines*], *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.
Note that the OECD has recently introduced updated amended guidelines that adhere to a similar framework. *See* Org. for Econ. Co-operation & Dev., *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* 14 (July 2013), *available at* http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. For basic and early discussions of FIPPs in U.S. information-privacy scholarship, see Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 498 (1995). *See also* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy in Europe: Initial Data on Governance Choices and Corporate Practices*, 81 GEO. WASH. L. REV. 1529, 1539–51 (2013).

[28] In the EU, FIPPs were broadly integrated into the EU Data Protection Directive and thereafter an abundance of member-state laws. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 32 (EC) [hereinafter EU Data Protection Directive]. This directive is currently under review, yet the new regulation which would be adopted will surely reflect FIPPs as well.

[29] In the governmental sphere (federal), see the Privacy Act of 1974 § 3, 5 U.S.C. § 552a (2012); in the commercial sphere, see Cable Communications Policy Act of 1984 § 631, 47 U.S.C. § 551 (2012). For a discussion of this issue, see Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STAN. TECH. L. REV. 1, ¶¶ 39–43, *available at* http://journals.law.stanford.edu/

"notice and choice" and "secondary use/purpose specification/use limitation." The former refers to the informed consent data subjects must provide prior to the collection and use of their data. The latter pertains to the requirement that those collecting information specify the purpose of subsequent use and refrain from uses that are incompatible with the purpose the data subject consented to.[30]

As noted, these FIPPs are regulated sporadically (and to some extent, voluntarily) in the United States,[31] and more comprehensively in the EU as part of the Data Protection Directive (which was implemented in all member states and might soon be followed by the EU Data Protection Regulation).[32] The theoretical justification behind these FIPPs could be articulated while relying upon different analytical elements. These will vary among the underlying legal systems and their privacy-related values. In the EU, the justification for these two privacy principles derives from the notion of the control that individuals should have over information pertaining to them.[33] It also derives from the data subjects' basic human rights.[34] In the United States, the justification for the protection of these rights is premised on the harm (a key concept in U.S. privacy policy)[35] individuals will experience when information is used and passed on against their will.

Generally speaking, privacy norms could be legislated and regulated to several degrees of detail. The law could detail specific parameters which the industry must meet to achieve an acceptable privacy level. Regardless of the discussion below, such a regulatory response is ill-advised in the contexts here addressed. The relevant technological settings are highly dynamic and ever changing. Today's specific regulation will most likely become obsolete tomorrow. Therefore, privacy norms will most likely be enacted into law using broad language and general concepts. These will allow industry, courts, and regulators to adapt after the fact to

stanford-technology-law-review/online/fair-information-practices-and-architecture-privacy-what-larry-doesnt-get. *See also* Bamberger & Mulligan, *supra* note 27, at 1542–43.

[30] *OECD 1980 Guidelines*, *supra* note 27, at para. 10; EU Data Protection Directive, *supra* note 28, at 34.

[31] FTC REPORT, *supra* note 11, at 11 (discussing the adoption of FIPPs).

[32] *See Personal Data Regulation Proposal*, *supra* note 14.

[33] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). For a critique of this theory, see Paul M. Schwartz, *Beyond Lessig's* Code *for Internet Privacy: Cyberspace Filters, Privacy Control and Fair Information Practices*, 2000 WIS. L. REV. 743, 746–62.

[34] Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 10. For a discussion of these rights in light of previous human rights treaties, see Lee A. Bygrave, *Data Protection Pursuant to the Right to Privacy in Human Rights Treaties*, 6 INT'L J.L. & INFO. TECH. 247, 255, 264 (1998). *See also* Bradford, *supra* note 16, at 22–23.

[35] *See, e.g.*, Schwartz & Solove, *supra* note 19, at 880–81 ("EU law views privacy as a fundamental right, while U.S. law considers it one interest that is balanced against others. . . . [T]he general approach is to allow personal data processing unless it causes a legal harm or is otherwise restricted by law.").

the changing environment. Yet such broad and abstract regulation generates concerns as to its impact on innovation, as explained below.[36]

Defining "innovation" for this discussion presents a greater challenge. Let us briefly examine this concept, with regard to its definition, salient forms, and measurement. Innovation can be intuitively understood as referring to new or improved processes or services.[37] It should be distinguished from merely an invention on the one hand and diffusion of innovation on the other.[38] Innovation is deemed to exert a substantial effect, yet the nature of such an effect may be understood in very different ways. Intuitively, it is understood to promote progress and therefore welfare.[39] Yet innovation often might not achieve this objective. To clarify, I refer to a helpful taxonomy borrowed from studies on the interaction between regulation and innovation in the context of environmental law.

Discussing the definition of innovation in environmental regulatory debates, Richard Stewart distinguished "market innovation" from "social innovation."[40] Market innovations are developments that allow firms to offer new and improved products that appeal to consumers.[41] Such innovations create benefits to the firms, which they can capture while selling or utilizing such products and services. Yet these benefits need not go further and be shared with the public at large.

At first blush, the definition here provided might defy common sense and basic economic theory; innovation and thus growth enhances welfare even when its benefits are confined to specific sectors or groups of players, given measures of redistribution. Yet the innovation scenario noted here is indeed possible when the firms' market innovations generate negative externalities, which decrease the welfare of others while enhancing their own. In this context, it is interesting to note that according to one commentator, "innovation" was initially used as a negative term.[42]

On the other hand, "social innovations" are practices which offer social benefits that firms cannot necessarily capture, but are shared (via positive externalities, redistribution, or other measures) with users and

---

[36] *Infra* Part III.B.

[37] *Oslo Manual*, *supra* note 22, at 46 (defining innovation as "implementation of a new or significantly improved product (good or service), or process, a new marketing method, or a new organisational method in[ ]business practices, workplace organisation or external relations."). For another discussion of the meaning of this term, see EVERETT M. ROGERS, DIFFUSION OF INNOVATIONS 14 (4th ed. 1995).

[38] Bernstein, *supra* note 5, at 2259 n.6.

[39] Gaia Bernstein, *When New Technologies Are Still New: Windows of Opportunity for Privacy Protection*, 51 VILL. L. REV. 921, 927–28 (2006). *See also* COOTER, *supra* note 3, at 1.16–1.17.

[40] Stewart, *supra* note 8, at 1277–79.

[41] *Id.* at 1279.

[42] *See* Jill Lepore, *The Disruption Machine: What the Gospel of Innovation Gets Wrong*, NEW YORKER (June 23, 2014), http://www.newyorker.com/magazine/2014/06/23/the-disruption-machine (noting the use of this concept in the context of the French Revolution).

customers.[43] When discussing this category, Richard Stewart mainly refers to technologies that offer cleaner air.[44] However, this category could apply to actors in the IT–privacy context as well. Indeed, technologies provide social innovation when they meet the public's privacy expectations and information-usage norms, or provide society with other benefits.

Although the term "innovation" is often used in the policy (and at times even academic) setting when addressing privacy regulation, it is unclear which form of innovation—"social" or merely "market innovation"—is discussed or advocated in every instance.[45] One might cautiously note that at times the line between these forms of innovation is purposely blurred. This is unfortunate, as privacy laws noted in innovation-based discussions at times promote either market or social innovations. They might decrease innovation on the market level by limiting the profits of a specific firm, but enhance social welfare by protecting general interests (as well as vice versa). Clearly, policymakers should have limited sympathy for mere market innovation that does not have an overall positive impact on social welfare. Yet, as Stewart explains, in the environmental context, and as technological advances have shown, market innovation might lead to social innovation at a later time.[46] For instance, innovations might start out by merely advancing firms, but over time increase overall social welfare, and thus enhance the consumers' utility as well, by enabling lower prices or a higher quality of life. The following analysis therefore distinguishes these two forms of innovation, integrates both concepts into the discussion, and explains how they might be impacted by various legal settings and regulatory strategies.

Beyond the noted distinction, which focuses on aggregated welfare and efficiency, another possible distinction might be premised on fairness.[47] Here, one must note that innovation might indeed increase overall welfare, yet such an increase will not be distributed fairly and equally among the firms (and their shareholders, officers, and other employees), customers, and third parties. They might benefit one social segment (the rich or sophisticated) but not another. In other contexts, these ethical issues could be resolved by secondary distributions, for example, through the taxation system. However, there is no guarantee that these practices will indeed follow or prove successful in the privacy context. This is yet another subtlety that is lost when referring to "innovation" as a general term, rather than distinguishing between the fair and unfair outcomes of innovations.

Another important innovation-related distinction addresses *four sali-*

[43] Stewart, *supra* note 8, at 1279.

[44] *Id.*

[45] *See* Gopalakrishnan & Damanpour, *supra* note 22, at 19 (noting that economists discussing innovation tend to address this notion on a "high level of aggregation" as opposed to other fields, which focus on particular firms).

[46] Stewart, *supra* note 8, at 1279.

[47] I thank Dennis Hirsch for this observation.

ent forms of innovation firms engage in: (1) product innovations (new goods and improvements), (2) process innovations, (3) organizational innovations, and (4) marketing innovations.[48] The discussion below focuses on forms one and four. Different arguments addressing the privacy–innovation relationship pertain to different forms of innovation. Refraining from distinguishing between them generates confusion and perhaps even leads to wrongly applying arguments from one context to the (irrelevant) other.[49]

Once innovation is defined, the difficult notion of measuring innovation follows. An entire science has risen to this challenge with several parameters introduced and methodologies set forth. Popular methods examine the number of registered patents[50] or patent forward citations.[51] Another notes the extent of R&D investment.[52] This Article's analysis focuses on innovation (and its measurement) in the ICT sector.[53] Overall, while in most cases the discussion below does not delve into the various ways to measure innovation, it is premised on the understanding that innovation is not an abstract notion but a measureable element, even though the form of measurement is contestable. Furthermore, it examines which claim regarding a privacy–innovation relation will enable measurement.

With these basic concepts regarding privacy and innovation in mind, let us now critically examine five ways in which privacy and innovation (both market and social) might interact, while confining our discussion

[48] *See Oslo Manual*, *supra* note 22, at 17. Note that Robert Cooter recently stated that "[i]nnovations use new ideas to produce goods cheaper or to make better goods." COOTER, *supra* note 3, at 1.6. Yet this definition does not encapsulate all four dimensions noted in the text. *Id.*

[49] For a discussion of a similar form of analytical confusion which follows from the discussion of innovation among individuals from different disciplines, see Gopalakrishnan & Damanpour, *supra* note 22.

[50] *Oslo Manual*, *supra* note 22, at 22, 128. For a critique of the ability to use this factor, see MARIANA MAZZUCATO, THE ENTREPRENEURIAL STATE 42–45 (2011), *available at* http://oro.open.ac.uk/30159/1/Entrepreneurial_State_-_web.pdf.

[51] This method was introduced in the seminal work of Professor Manuel Trajtenberg. *See* Manuel Trajtenberg, *A Penny for Your Quotes: Patent Citations and the Value of Innovations*, 21 RAND J. ECON. 172, 172 (1990). However, this factor is not without difficulties. *See, e.g.*, Juan Alcácer & Michelle Gittelman, *Patent Citations as a Measure of Knowledge Flows: The Influence of Examiner Citations*, 88 REV. ECON. & STAT. 774, 778–79 (2006); Adam B. Jaffe et al., *Geographic Localization of Knowledge Spillovers as Evidenced by Patent Citations*, 108 Q.J. ECON. 577, 580–85 (1993).

[52] *See, e.g.*, *Oslo Manual*, *supra* note 22, at 37.

[53] It should be noted that ICT innovation generates specific interest as its measurement is utilized for two analytical purposes. The extent of ICT innovation is obviously measured to examine innovation in the ICT industry (and compared to other sectors and industries, as well as among countries). Yet ICT innovation (or lack thereof) is considered indicative of innovation in other, related sectors (such as financial sectors) whose innovation is both reflected and caused by ICT growth. Our discussion will focus on the former perspective. *See id.* at 24.

to ICT- (mostly internet- and cyber-) related contexts.[54]

B. The Privacy–Innovation Relation: Five Perspectives

The relation of privacy to innovation is often noted yet rarely fully analyzed and explained. It can be articulated in five distinct ways, which, while relying on similar terminology, refer to different contexts and vary in their analytical-construct force. Note that the analysis below focuses on the flow from privacy to innovation, rather than vice versa. Indeed, some forms of innovation enhance privacy (i.e., encryption) while others potentially undermine it (i.e., infrared cameras).[55] Yet, this aspect of the relationship between these two terms merits a separate analysis.

1. The Privacy/Trust/Innovation Linkage: Privacy Enhances Trust, Which Leads to Online and Virtual Engagement, Which Leads to Greater Market Innovation, Which Leads to Greater Social Innovation

This first privacy–innovation hypothesis is premised upon the belief that commercial conduct that respects consumer privacy (especially in the context of e-commerce and other long-distance transactions) is crucial for generating trust. In other words, when consumers understand that their personal information is compromised, or subjected to constant analysis or other privacy risks or breaches, trust will be decreased or even lost.

Trust is a crucial element, especially in the ICT context and particularly online.[56] After all, the virtual realm does not allow reliance on physical cues in interpersonal interactions—measures humans have relied on for many centuries. Trust arguably is required for the success of virtual retail markets which involve long-distance transactions. Without it, some consumers will refrain from engaging in this commercial realm, opting for the more conservative and conventional modes of commerce.[57] Limited engagement will lead to limited incentives to develop this novel online medium, hence limited innovation. Or, from a positive perspective and while referring to terminology used in the innovation discourse, trust will generate demand, which in turn will drive innovation.[58] This argument mostly concerns "product innovation"; firms will be driven to develop new forms of products (and will benefit from additional income in doing so) given the enhanced demand privacy provides.

---

[54] Several of these key themes were mapped out at a Yale Law School Information Society Project symposium. *See Privacy and Innovation Symposium*, YALE L. SCH. (2010), http://www.law.yale.edu/intellectuallife/Privacy%20Symposium.htm.

[55] I thank Bryan Choi for this observation.

[56] The meaning of the term "trust" in this context merits an article of its own, yet due to obvious space constraints, the intuitive meaning will have to suffice for this context. For a recent discussion of the notion and definition of "trust" in the online context, see Justin (Gus) Hurwitz, *Trust and Online Interaction*, 161 U. PA. L. REV. 1579, 1584 (2013).

[57] *See* FTC REPORT, *supra* note 11, at 12; GREEN PAPER, *supra* note 10, at 15.

[58] *See Oslo Manual*, *supra* note 22, at 139–40.

The conclusion derived from the analytical move set out above is that privacy laws should be set in place to promote innovation in the ICT setting. This argument has been popular with policymakers active in the privacy realm, although not all will agree on which form of laws will promote trust. In the EU, at least, they provided a reason to mandate strong privacy rules.[59] This concept is perhaps best encapsulated in a recent statement by Viviane Reding (European Commissioner for Justice, Fundamental Rights and Citizenship) in reference to the new proposed privacy rules formulated by the EU:

> The new rules . . . give EU companies an advantage in global competition. . . . [T]hey will be able to assure their customers that valuable personal data will be treated with the necessary care and diligence. Trust . . . will be a key asset for service providers and an incentive for investors . . . locating services.[60]

In the past, U.S. regulators have made similar comments as well.[61]

While those noting this dynamic do not distinguish market from social innovation, it is fair to argue they assume, or rather hope, that this dynamic will generate both. They concede that innovation that will unfold in a privacy-respecting or trust-generating environment will obviously benefit firms developing new measures and models. Yet this innovative process will supposedly enhance their users' welfare as well. Such ICT-related innovation should also be easily measured using the factors noted above, rendering the argument a plausible policy statement.

However, this argument has two central weaknesses, even setting aside the fact that it is not supported by empirical evidence tying the measurement of innovation to stricter privacy laws (the same could be said of almost all hypotheses discussed here).[62] First, one must ask whether this argument can justify mandatory privacy rules, given that firms should have sufficient incentives to promote privacy, hence their own business interests.[63] A strict libertarian might even turn this argument on

[59] *See, e.g.*, *Communication from the Commission to the Europeans Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Towards a Thriving Data-driven Economy*, at 3, COM (2014) 442 final (July 2, 2014) (noting that the European Commission will "continue to address them by enacting effective data protection and network and information security rules, supporting secure technologies and informing the public about ways to reduce privacy and security risks," and that "[a] high level of trust is essential for the data-driven economy").

[60] Viviane Reding, *The European Data Protection Framework for the Twenty-First Century*, 2 INT'L DATA PRIVACY L. 119, 129 (2012); *see also* Chander, *supra* note 2, at 693.

[61] *E.g.*, Chander, *supra* note 2, at 665 & n.113 (discussing statement made by the Department of Commerce in 1995).

[62] The Article will address empirical weaknesses. *Infra* note 79, *see* David Alan Sklansky, *Too Much Information: How Not to Think About Privacy and the Fourth Amendment*, 102 CALIF. L. REV. 1069, 1097–1100 (2014).

[63] This argument can generate several reasonable responses—some of which are addressed below. Beyond them, here one might argue that firms will have limited

its head. She will seize upon it to argue that privacy regulation is unnecessary altogether. According to this argument, firms have sufficient motivation and incentives to meet high privacy standards.[64] As there are other good reasons for privacy regulation, we will set this latter part of the argument aside.

The common response to this first critique is that firms might not be wise enough, or properly motivated, to provide sufficient protection on their own.[65] The legal literature examining behavioral economics might provide additional support. Such studies have recently noted that individuals act irrationally not only as consumers but in their capacity as firm managers as well.[66] Firms and their managers might be lured by the prospect of the short-term gains that the breach of privacy, and thus consumer trust, brings about. They will therefore ignore the long-term disadvantages the lack of privacy might entail. Or more simply, they might not know what is good for them. Even the safeguards of internal review and group thinking that corporate decision making provides might still prove unhelpful in limiting the corporate attraction to personal-data abuse.[67]

While this response might have merit, it still requires additional facts and evidence to prove that firms will act against their long-term interests in such competitive markets. Empirical work has indeed shown that individuals in their capacity as consumers neglect to properly account for

incentives to promote privacy as their users will have no knowledge as to the level of privacy protection the firm provides—an assertion that could be backed by the low levels of users reviewing privacy policies. *Global Internet User Survey 2012: How Often Do You Read the Privacy Policies of Websites or Services That You Share Personal Information With?*, INTERNET SOC'Y, http://www.internetsociety.org/apps/surveyexplorer/online-privacy-and-identity/how-often-do-you-read-the-privacy-policies-of-websites-or-services-that-you-share-personal-information-with-17 (indicating, on a global scale, that only 16% of respondents always read privacy policies of websites they shared personal information with, 31% "most of the time," 41% "sometimes" and 12% "never"). However, in response, it is important to note that users gain information as to the firm's privacy-related practices from other information flows and online sources. *See generally* Shmuel I. Becher & Tal Z. Zarsky, *E-Contract Doctrine 2.0: Standard Form Contracting in the Age of Online User Participation*, 14 MICH. TELECOMM. & TECH. L. REV. 303 (2008) (explaining that the internet enables various information flows between *ex post* and *ex ante* online users and consumers). Also, if consumers do not know of the firm's privacy transgressions, the entire argument noted here fails, as it is premised upon the individuals' discontent with the low level of privacy they receive.

[64] Some evidence to this claim might be the higher level of privacy norms adhered to by U.S. firms "in action," as opposed to "privacy on the books." This result was made apparent in a recent survey. *See generally* Bamberger & Mulligan, *supra* note 27. See also the discussion of such firms in today's market in this Article's Conclusion, below.

[65] Info. Soc'y & Media, European Comm'n, *Towards a Competitive European Internet Industry*, at 36, SMART 2009/0044 (May 2012) [hereinafter *European Internet Industry*].

[66] *See* Avishalom Tor, *Understanding Behavioral Antitrust*, 92 TEX. L. REV. 573, 632–34 (2014).

[67] *See id.* at 636.

their privacy needs.[68] Yet one cannot jump quickly to a similar conclusion for managers. In addition, while it is possible that managers conceptually err, especially given their tendency to take risks, there is an even greater probability that governments will err as well in their efforts to regulate them. Once errors in judgment are considered on the managerial level, they must be addressed across the board. Thus, the benefits of such regulation in terms of promoting trust and innovation might be quickly lost. For that reason, the argument here discussed must be approached with caution.

A second flaw in this privacy–innovation-linkage argument is that (perhaps unfortunately to those who hold privacy dear) there is very limited evidence that users consider privacy protection to be an important requirement for achieving online trust.[69] Surveys indeed indicate the public's discontent with firms lacking in privacy-promoting practices.[70] Still, in practice, the public continues to flock in even greater numbers to internet and mobile services that provide limited privacy protection. Demand for services that use individuals' personal information in unexpected ways is soaring.[71] While it is possible that innovation could be even greater if firms abided by privacy standards, this statement too has no backing.

In sum, this first statement linking privacy and innovation, although popular with policymakers, features substantial analytical flaws. Innovators need not be deterred by the lack of privacy and its impact on trust, and can probably continue innovating in this realm without fear. It ap-

[68] For a recent discussion of this point, see Daniel J. Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880–81 (2013).

[69] A somewhat dated yet still important source for this assertion is Susannah Fox, *Trust and Privacy Online*, PEWRESEARCH INTERNET PROJECT (Aug. 20, 2000), http://www.pewinternet.org/Reports/2000/Trust-and-Privacy-Online.aspx ("American Internet users overwhelmingly want the presumption of privacy when they go online. . . [, but] a great many Internet users do not know the basics of how their online activities are observed and they do not use available tools to protect themselves." And despite their concerns, "Americans continue to trust email, surf the Web for advice about intimate aspects of their lives, make friends online, and turn to Web sites for health information, for spending their money, and for material about their finances.").

[70] *See* Lee Rainie et al., *Anonymity, Privacy, and Security Online*, PEWRESEARCH INTERNET PROJECT (Sept. 5, 2013), http://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online. See also the sources noted in Katherine J. Strandburg, *Free Fall: The Online Market's Consumer Preference Disconnect*, 2013 U. CHI. LEGAL F. 95, 105–06 nn.44–47.

[71] *See* Strandburg, *supra* note 70, at 105–06 nn.44–47. See also the results of an extensive survey reported by Fred Stutzman, Ralph Gross, and Alessandro Acquisti. Fred Stutzman et al., *Silent Listeners: The Evolution of Privacy and Disclosure on Facebook*, 4 J. PRIVACY & CONFIDENTIALITY, no. 2, 2012, at 7. They draw out interesting dynamics which show rises and falls in the sharing of personal information on Facebook, which have very limited correlations with Facebook's privacy-protection practices. Actual engagement was greatly affected, though, by changes in the online interface. *See id.* at 8–9.

pears that this argument's popularity is dwindling, and losing its intuitive appeal.[72]

2. The Privacy/Creativity/Innovation Linkage: Privacy Leads to Greater Creativity (Enhancing Human Resources), Which Leads to Greater Market Innovation, Which Leads to Social Innovation

A different analytical statement of the privacy–innovation nexus focuses on privacy's linkage to the notion of *human creativity*. Enhancing privacy, the argument goes, will enhance creativity. Enhanced creativity will in turn promote innovation.[73] By contrast, the lack of privacy and the omnipresence of surveillance will substantially limit both creativity and innovation.[74] This argument was most recently set forth by Julie Cohen.[75] She states, "[c]onditions of diminished privacy . . . impair the capacity to innovate," explaining that innovation requires critical thinking and room to tinker—and both of these are inhibited by excessive surveillance.[76] Constant surveillance, or knowing that information about us is being analyzed and examined, leads individuals to engage in constant self-monitoring and conforming behavior—mindsets that are arguably destructive to the processes that promote innovation.

A quick review of the principles of innovation scholarship noted above makes for supplementing this privacy-based argument, further elucidating it, and adding three important insights. First, the argument clearly refers to "market innovation." Firms will generate better and more sophisticated products and services given their employees' enhanced creativity. However, the argument implicitly supposes that overall market innovation will lead to social innovations as well. Second, the increase in innovation will be due to the enhancement of the "human resources,"[77] a topic broadly discussed in the innovation literature. Most studies, however, focus on human-resource enhancement through higher education and the ability to share and discuss ideas.[78] The argument set out here

[72] Along these lines, it is interesting to note that in a recent set of interviews conducted with privacy professionals throughout Europe, respondents have referred to the term "trust" infrequently, and mostly in the context of actions taken in the absence of law. *See* Bamberger & Mulligan, *supra* note 27, at 1573.

[73] The linkage between creativity and innovation is far from clear. For a brief discussion and review of the literature in psychology addressing this matter, see Gopalakrishnan & Damanpour, *supra* note 22, at 16.

[74] *See* M. Ryan Calo, *The Unknown Unknowns: The Role of Innovation in Privacy*, (Yale ISP Symposium 2010–11), *available at* http://www.law.yale.edu/documents/pdf/ISP/Yale_ISP_Calo.pdf.

[75] Cohen, *supra* note 6, at 1918.

[76] *Id.*; *see also id.* at 1927 ("If privacy and serendipity are critical to innovation—by which I mean critical both to the likelihood that innovation will occur and to the substance of that innovation—there is reason to worry when privacy is squeezed to the margins and when the pathways of serendipity are disrupted and rearranged . . . .").

[77] *See Oslo Manual*, *supra* note 22, at 43.

[78] Joint Research Center Technical Reports, *Comparing Innovation Performance in*

points to a more abstract form of enhancement: a nurturing social environment. Third, this argument seemingly contends that privacy will enhance all forms of innovation, as it points to the enhancement of creativity in general. This part of the argument is therefore quite speculative and will require additional empirical research.[79] Intuitively, at least, some forms of innovation should receive a greater boost than others in a privacy-respecting environment.

This second analytical argument differs from the previous privacy–innovation-linkage point given its focus on individuals' capacity as creators and producers, rather than consumers and users.[80] In light of this different perspective, the critiques of the previous argument lose some of their edge. On the face of it, here again one can argue that firms that wish to enhance innovation will create an atmosphere that is attentive to and respectful of privacy for their employees. Yet this argument may not hold, as firms might be unable to achieve this objective on their own. In an overall environment of omnipresent surveillance, negative spillovers from the actions of both other firms and governments will undermine creativity regardless of the actions of a specific firm, while generating an ecosystem of suspicion and reduced innovation. And, of course, innovation might not flow exclusively from large corporations, but also from individuals or dispersed networks of users who are working on their own and thus vulnerable to various privacy risks.[81] For those who strive to advance innovation, the only possible response is governmental enforcement of acceptable privacy norms. In addition, the fact that people continuously flock to privacy-breaching websites need not undermine the argument that their innovative capacities are deteriorating.

Yet, a close examination of this privacy–innovation nexus leads to a second set of critiques. This argument is quite broad and abstract—perhaps excessively so. It notes a very general link between two human states but does not clarify how measures at one end will impact outputs at the other. So the practical guidance it provides regarding how privacy and other interests can be calibrated is limited, as both privacy and innovation are not absolute elements. In addition, this theory might be extremely difficult to test and prove.[82] It leads to difficult questions: Can we measure the extent surveillance in one context impacts innovation

the EU and the USA: Lessons from Three ICT Sub-Sectors, 45 Report EUR 25961 EN (2013) [hereinafter JRC REPORT]; *Oslo Manual*, *supra* note 22, at 37; Chander, *supra* note 2, at 641.

[79] In a recent article, David Sklansky noted his skepticism regarding the negative impact privacy will have on this form of innovation, stating that there is no evidence to this point, but rather to the contrary. Sklansky, *supra* note 62, at 1099–1100.

[80] Recent scholarship has addressed the role of users as innovators, thus undermining the distinction noted. *See* Eric von Hippel, *Democratizing Innovation: The Evolving Phenomenon of User Innovation*, 55 MGMT. REV. Q. 63 (2005).

[81] *Id.* I thank Julie Cohen for elucidating this point.

[82] *See* Sklansky, *supra* note 62, at 29–30.

(which as explained above[83] is a measureable element)? Will creativity rise linearly in a response to privacy, or will some other dynamics unfold? Considering these analytical difficulties, this argument is of limited utility (clearly a word those furnishing this argument will reject) in the realm of policy debates. Invoking "innovation" calls for an analytical process that needs to be somewhat measurable and feature a testable causal connection—both elements that this argument cannot muster.

3. The Privacy/Competition/Innovation Linkage: Privacy Leads to Lower Market Barriers, Which Fosters Competition, Which Leads to Greater Market Innovation, Which Leads to Social Innovation

An additional argument linking privacy and innovation has been voiced recently, this time from the perspective of antitrust and competition law. It states that today's information environment allows some firms to achieve a position of dominance given their ability to collect a vast amount of personal information.[84] With this strategy of vast data collection, the firms are able to solidify their dominance still more. They can use such information to provide their users and customers with better, personalized, services. They can also use personal information to assist advertisers effectively to cater to their users' needs. Salient examples of this dynamic are Google, Amazon, and Facebook. Google uses personal information to provide customized search results to its returning users, based on previous preferences.[85] Amazon uses personal data of browsing and purchase histories to provide a powerful recommendation system.[86] Facebook allows advertisers to provide users with ads premised on their users' detailed demographics.[87] It would be very difficult for any competitor to provide similar services on par with these dominant leaders. Therefore, the ability to collect, analyze, and utilize users' personal information generates a first-mover advantage for the dominant firms, and a barrier to entry by all the others.[88]

---

[83] *See supra* Part II.A.

[84] Howard A. Shelanski, *Information, Innovation, and Competition Policy for the Internet*, 161 U. PA. L. REV. 1663, 1687 (2013) (The "site's exclusive access to its large share of customer information could help maintain its market position.").

[85] Danny Sullivan, *Google Now Personalizes Everyone's Search Results*, SEARCH ENGINE LAND (Dec. 4, 2009), http://searchengineland.com/google-now-personalizes-everyones-search-results-31195.

[86] JP Mangalindan, *Amazon's Recommendation Secret*, FORTUNE (July 30, 2012), http://tech.fortune.cnn.com/2012/07/30/amazon-5.

[87] Kelly Cooper, *Digital Ads: How Facebook, Google, and Twitter Target Us*, READWRITE (Jan. 1, 2014), http://readwrite.com/2014/01/01/digital-ads-personalization-google-facebook-twitter#awesm=~owoPxW99T1neOu.

[88] European Data Protection Supervisor, *Preliminary Opinion of the European Data Protection Supervisor: Privacy and Competitiveness in the Age of Big Data: The Interplay Between Data Protection, Competition Law and Consumer Protection in the Digital Economy*, at 30–31 (Mar. 2014) [hereinafter *Preliminary Opinion of the EDPS*], *available at* https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-03-26_competitition_law_big_data_EN.pdf.

With this insight in mind, a possible novel nexus between privacy and innovation could be set forth. Privacy laws will require the mentioned firms to curb the data analyses and usage practices noted. Thus, competitors will be able to enter these markets and offer competitive services. Both incumbents and competitors will innovate as part of this competitive dynamic. Such market innovations will, it is hoped, transform into social innovations which all users will enjoy. With sufficient competition, all forms of innovation noted above might follow. In addition, the effect discussed here might be indeed measurable. Markets could be compared for privacy, innovation, and competition levels, thus examining the significance of the noted effect.

This novel and speculative argument has begun to generate some traction,[89] yet it suffers from several flaws.[90] First, in the information realm, early movers benefit from various advantages, including substantial network effects. It is unclear whether the changes noted in privacy laws will substantially undermine these advantages. Second, even with privacy laws in place, these firms will be able to generate some of these advanced services for their clients after obtaining proper consent from their users. Third, one can easily argue that lenient privacy rules are actually extremely helpful to new firms striving to enter the market (as opposed to powerful incumbents).[91] Such firms, by nature, have limited access to users. Yet their ability to purchase personal information on a secondary market might allow them to bridge this gap and enter the market. Strong privacy rules and measures, on the other hand, might render access to online users extremely difficult to any entity except those controlling the digital infrastructure.[92] In other words, thanks to enhanced privacy, these latter firms might rise to become monopolists in the online-advertising markets.[93] Given these strong countering claims, this argument overall should be set aside.

4. The Direct Privacy–Innovation Linkage: Privacy Laws Foster Market and Social Innovation (Product Innovation and Marketing Innovation), Which Leads to Privacy-Protective Platforms

Yet another interesting positive link between privacy and innovation

[89] *See, e.g.*, *id.*

[90] For a similar discussion, see Goldfarb & Tucker, *supra* note 7, at 25–27.

[91] *See* Zarsky, *supra* note 26, at 33–35; FRED H. CATE, PRIVACY IN PERSPECTIVE 14 (2001).

[92] *Preliminary Opinion of the EDPS*, *supra* note 88, at 31.

[93] J. Thomas Rosch, *The Dissent: Why One FTC Commissioner Thinks Do Not Track Is Off-Track*, ADVERTISINGAGE (Mar. 24, 2011), http://adage.com/article/guest-columnists/ftc-commissioner-thinks-track-track/149558. FTC Commissioner Roth argues that adopting "do not track" mechanisms might have an anticompetitive effect. These privacy-enhancing tools will in fact leave the online advertising market to be dominated by entities, such as browser operators. This view was recently repeated by a former FCC executive in a New York Times Editorial. Fred. B. Campbell, Jr., *The Slow Death of Do Not Track,* N.Y. TIMES, (Dec. 27, 2014), http://www.nytimes.com/2014/12/27/opinion/the-slow-death-of-do-not-track.html.

emerges from the argument that privacy-based regulation requires innovations in the field of privacy enhancement (such as encryption, data security, obfuscation, etc.). Thus, privacy laws *directly* enhance innovation by generating demand for a new form of products. While this discussion addresses market innovation, it clearly enhances social innovation as well. In this specific instance, both market and social innovation are by definition aligned, as they are designed as such by government. In terms of innovation terminology and taxonomy, here privacy enhances innovation directly by driving demand through a governmental mandate.[94] Such innovation will probably be limited to improving products, or generating new ones. Indeed, privacy rules will call for the development of some new products—commonly referred to as Privacy Enhancing Technologies, or "PETs."[95] Such innovation can also be easily and clearly measured and studied. The level of innovation from the enactment of a specific privacy-preserving law could be compared to that in the previous timeframe. Note that similar arguments were set forth in the environmental context as well, with some findings indicating innovation in specific sectors which were heavily regulated.[96]

However, viewed from a broader perspective this argument is extremely limited. To understand why, let us reframe the argument as part of the broader issue which promotes innovation that is driven by specific government policy. This issue has been addressed previously in the context of environmental regulation. In that context, Richard Stewart explains the limited prospect of enhancing social innovation through government regulation.[97] He notes the problems government faces when striving to define the state of the art and engaging in "technology forcing" for the specific technological designs it labors to promote.[98] In addition, such actions often generate inadequate incentives for firms to invest in different forms of innovation and achieve "better social perfor-

[94] For a list of projects for enhancing privacy that received federal funding, see EXEC. OFFICE OF THE PRESIDENT, *supra* note 13, at 55.

[95] For a recent discussion of the role of government in motivating the development of PETs, see Claudia Diaz et al., *Hero or Villain: The Data Controller in Privacy Law and Technologies*, 74 OHIO ST. L.J. 923 (2013). On the other hand, Michael Froomkin explains that current laws do not encourage the development of PETs. Quite to the contrary, the development of some PETs is restricted by law. *See* A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965 (2013).

[96] Press Release, Baskut Tuncak, Ctr. for Int'l Envtl. Law, *Stronger Laws for Hazardous Chemicals Spur Innovation* (Feb. 2013), *available at* http://www.ciel.org/Chem/Innovation_Chemical_Feb2013.html; *see also* Nicholas A. Ashford et al., *Using Regulation to Change the Market for Innovation*, 9 HARV. ENVTL. L. REV. 419, 463 (1985) ("The history over the last fifteen years reveals significant innovation and essential compliance with very stringent regulation.").

[97] Stewart, *supra* note 8, at 1281–83.

[98] *Id.* at 1296–1310.

mance."[99] It should be noted that Stewart does *not* assert that *all* regulation undermines innovation. Indeed, Stewart maintains that other forms of regulation, which enable various markets and trades, might indeed enhance innovation.[100] Yet the restrictive forms of privacy-enhancing regulation here discussed do not seem to fit within this latter category.

While governments are at times capable of identifying innovative realms, or even innovating themselves (especially in military contexts), it is probably a safe bet that they will utterly fail to do so in the web-related ICT context. The government's inability to get an ICT project successfully off the ground even when the political stakes of failure are extremely high was reflected in recent events involving the failed launch of the "Obamacare" website.[101] News reports indicated systematic failures by both the government and the government contractors who were asked to follow its specifications, and in that way "innovate."[102] Indeed, governments are usually ill-equipped to identify upcoming needs and technologies correctly, and lack the agility to formulate a quick and adequate response to them. Therefore, it is highly unlikely that innovation following specific government regulation (including privacy-preserving regulation) will be substantial and supersede innovations that will come to life under an alternative regulatory regime.

To be fair, and as explained above,[103] privacy law need not be understood to include specific regulatory frameworks that technological design must comply with (hence "innovate"). It might merely include broader concepts—such as "consent" or "purpose specification/use limitation"—which technologies currently do not adhere to. In these cases, government's tendency to demonstrate myopia and incompetence when introducing technological design is irrelevant. Yet, even in these cases, such laws will most likely fail to generate substantial innovation. True, they may provide limited incentives for one sort of innovation, but in the process probably inhibit a much greater form of innovation that might have arisen.[104] In other words, even though these regulations can generate measurable market innovation, the alternative policy (namely the lack of

[99] *Id.* at 1324; *see also* Bruce A. Ackerman & Richard B. Stewart, Comment, *Reforming Environmental Law*, 37 STAN. L. REV. 1333, 1336 (1985) (explaining that, in the environmental context, applying policy which called for the use of the best available technology ("BAT") does not encourage the development of new technology—and even discourages the development of it).

[100] *See* Richard Stewart, *A New Generation of Environmental Regulation?* 29 CAP. U. L. REV. 21, 94–127 (2001) (particularly p. 99). For a clearer distinction between the two forms of regulation noted, and some comparison between them and privacy-based regulation, see Dennis D. Hirsch, *Protecting the Inner Environment; What Privacy Regulation Can Learn From Environmental Law,* 41 GA. L. REV. 1, 30–40 (2006).

[101] *See* Robert Pear et al., *From the Start, Signs of Trouble at Health Portal*, N.Y. TIMES, Oct. 13, 2013, at A1.

[102] *Id.*

[103] *See supra* Part II.

[104] *See* Ackerman & Stewart, *supra* note 99, at 1336.

such regulation) will generate a greater amount of social innovation. In this alternative universe, firms will not limit their innovative energy to a specific government-defined context and will freely innovate as they choose. For that reason, this privacy–innovation nexus, when properly understood, and accounting for the noted privacy rules, should have limited force in the policy debate. This point, however, will be revisited in Part IV.C, below. Regulation, in fact, is usually associated with the limitation of innovation—a notion the Article now explores.

5. The Privacy Versus Innovation Linkage: Privacy Leads to Limited Market Innovation (Product Innovation–Marketing Innovation), Which Leads to Limited Social Innovation

While the above arguments point to the positive relation between privacy protection and innovation, they all suffer from various analytical flaws. At the same time, a very different, negative, link between privacy and innovation has emerged. Broadly speaking, this argument states that privacy regulation impedes the development of innovation. The "privacy-versus-innovation" argument is generating popularity in various policy realms in the U.S.[105] and lobbying efforts in the EU.[106] The argument itself can be understood on two levels. First, there are "general" arguments which link regulation to adverse effects on market innovation.[107] Regulation is noted for imposing technical constraints, forcing additional expenditures, as well as causing uncertainty and delay.[108] So privacy laws, being regulatory steps by nature, will therefore tax and possibly even deter innovators in this way.

This general "regulation-leads-to-impediment-to-innovation" argument is of limited force in the present privacy context. As opposed to environmental regulation, most privacy rules are broad and relatively simple—with the possible exception of HIPAA compliance rules in the medical context.[109] For instance, to meet the notice and consent re-

[105] *See supra* notes 10–13; *see also* THOMAS M. LENARD & PAUL H. RUBIN, TECH. POL'Y INST., THE BIG DATA REVOLUTION: PRIVACY CONSIDERATIONS 26 (Dec. 2013), *available at* http://www.techpolicyinstitute.org/files/lenard_rubin_thebigdatarevolutionprivacyconsiderations.pdf. *See generally* Adam Thierer, *Privacy Law's Precautionary Principle Problem*, 66 ME. L. REV. 467 (2014). A somewhat milder, yet very similar argument states that opting for self-regulation in the privacy realm enhances innovation. *See* Peter P. Swire, Information Privacy, *Trustwrap: The Importance of Legal Rules to Electronic Commerce and Internet Privacy*, 54 HASTINGS L.J. 847, 864–65 (2003).

[106] *See supra* notes 10–17; *see also* Anne Grauenhorst, *Data Protection in Europe*, http://www.dataprotectioneu.eu (discussing a position taken by 100 privacy scholars for the new regulation). The *first* point the privacy scholars choose to counter is that privacy and innovation are not necessarily conflicted, while responding to critics.

[107] *See, e.g.*, *Oslo Manual*, *supra* note 22, at 19; Stewart, *supra* note 8, at 1281–83.

[108] Stewart, *supra* note 8, at 1279. See also discussion in *supra* note 100 regarding the forms of regulation which might *not* have such an effect (but generally do not pertain to the discussion here addressed).

[109] The Health Insurance Portability and Accountability Act of 1996 (HIPAA) (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.). Regarding the difficulty of meeting HIPAA compliance levels, see Joseph Conn, *HHS Estimates*

quirements outlined above, firms might merely be required to add additional buttons and menus to their systems' interfaces, solicit consent, and provide information. This is a far cry from the expenditures discussed by Richard Stewart in the environmental context, which at times calls for applying detailed designs and implementing substantial changes.[110]

A possible exception to this assertion (and thus rendering this general anti-regulatory argument of some relevance at this juncture) pertains to business responses to "purpose-specification/use limitation" rules. Arguably, strong "purpose-specification" rules will require firms to substantially alter their internal information flows. With such regulations put in place, firms will be forced to ensure that the personal data they collect are used for the purposes specified by the user at the time of collection. For instance, to achieve this objective, the current literature discusses the possibility that ICT firms might be forced to structure elaborate Personal Data Management ("PDM") systems to enable compliance with the purpose-specification principle.[111] PDM systems will allow individuals to track and control subsequent uses of their personal data at various points around the data cycle.[112] They will also enable firms to request their users' consent at later points once new uses for their personal data become apparent.[113] Setting such a system in place and incorporating it into the firm's data operations will prove costly. However, rather than introducing such elaborate systems, firms might respond to purpose-specification rules in a far simpler manner. They might choose to refrain from using personal information beyond the initial authorization obtained. Adhering to such a business decision will indeed entail limited operational costs and is, again, rather simple.

Yet a second specific and far more powerful argument regarding the innovation–privacy linkage in this context could be made. Information-privacy laws substantially impact information flow, by regulating personal-data collection, transfer, and usage. Information flow is the fuel of the information economy. Stronger privacy protection slows and impedes the flow of personal data. If information flows are impaired or blocked, innovation will suffer as innovators are unable to use these data flows optimally to produce novel products and services. To apply a (somewhat problematic) analogy, the effect of strict or lenient privacy laws in the digital economy is similar to the effect of surplus or scarcity of expensive raw

32.8 Million Hours of Interaction Required to Comply with Privacy, Security Rules, MODERN HEALTHCARE (Sept. 4, 2013), http://www.modernhealthcare.com/article/20130904/BLOG/309049995/hhs-estimates-32-8-million-hours-of-interaction-required-to-comply and Derrick Wlodarz, *5 Big Myths Surrounding Computer Security and HIPAA Compliance*, BETANEWS, http://betanews.com/2013/09/02/5-big-myths-surrounding-computer-security-and-hipaa-compliance/.

[110] Stewart, *supra* note 8, at 1279–81.

[111] For a discussion of such a system, see Mireille Hildebrandt, *Slaves to Big Data. Or Are We?*, REVISTA DE INTERNET, DERECHO Y POLÍTICA, Oct. 2013, at 27, 34 (Spain).

[112] *Id.* at 37.

[113] *Id.* at 36.

materials on the conventional manufacturer.

This point can be easily demonstrated in relation to the two FIPPs discussed above: consent and purpose specification/use limitation. With broader "Notice and Choice" (or consent) requirements, data analyses will be limited to lesser information—the data uses that the firm has been able to secure proper consent for. Similarly, firms will be limited in their ability to carry out future analyses and uses when forced to adhere to a strong "purpose-specification" rule. Such a firm will be unable to engage in an innovative process at a later time if it has not properly specified said use to the relevant data subject.

Returning to the innovation-based discourse, the privacy-versus-innovation claim may be understood to argue that limiting privacy-enhancing regulation enables product innovation, given the firm's ability to introduce products and services which might be too costly under an alternative regulatory regime. It also allows firms to optimize their operations based on the personal data they gather.[114] Enhanced privacy also impacts the extent of marketing innovation as the legality of marketing models is directly affected by regulation.[115] This argument also pertains to a relatively measurable innovation factor, namely the extent of innovative progress that the loosening of some privacy laws brings about.

One of the central analytical challenges the analysis of this popular argument entails is ascertaining whether it pertains to the undermining of social innovation or merely that of market innovation. For obvious reasons, lobbyists and policymakers addressing this argument tend elegantly to avoid this question.[116] While the argument clearly leads to the conclusion that the pro-privacy regulatory moves noted decrease innovation created by firms, the question still remains as to whether a decline in social innovation will follow. It is indeed feasible that lenient privacy laws will promote market innovation, yet generate social (privacy- and autonomy-related) harms, and their aggregated (negative) value will eclipse the benefits generated by said firms.

On the other hand, one might argue that ICT-related innovation will lead to "social innovation" by promoting various social benefits. For instance, the technological infrastructure set in place enables a rich flow of information among citizens and advances free speech and democracy. In

---

[114] *See* Goldfarb & Tucker, *supra* note 7, at 9–10.

[115] *See* Chander, *supra* note 2, at 683 (explaining how strict privacy laws will block the use of targeted ads). Note that this example shows the fluidity of the "product" and "marketing" categories. Targeted ads could be considered marketing of another product or a service on its own.

[116] See, for instance, the following article authored by an online advertising industry executive: Eric Wheeler, *How 'Do Not Track' Is Poised to Kill Online Growth*, CNET (Sept. 20, 2012), http://news.cnet.com/8301-1023_3-57516422-93/how-do-not-track-is-poised-to-kill-online-growth. In this article, the author notes the way various uses of user data enhanced innovation of various online leaders, and notes that introducing the "Do Not Track" tool is "a crippling blow to the technology industry." Yet, will this also be a "blow" to society overall?

other instances, the flow of personal information brought about by low privacy and high innovation can improve life quality and save lives. Examples of such dynamics were recently discussed by Avi Goldfarb and Catherine Tucker, who explained how the analysis of personal information can substantially improve neonatal care.[117] Recent reports indicate other examples, such as the ability to predict the spread of influenza.[118]

Clearly, establishing whether this dynamic will lead to social innovation, or merely market innovation, is crucial. Just to state the latter is insufficient in the policy realm. Advancing corporate interests cannot politically or socially justify regulatory change on its own. For that reason let us assume that this argument pertains to instances in which social welfare is promoted as well. Of course reaching this conclusion will call for first establishing the extent of the harms (if any) lenient privacy laws will cause, so that they could be entered into the broader social equation which will examine whether the innovation was welfare enhancing. But even if limiting privacy achieves "social innovation" this argument faces more challenges. Changes in privacy laws and personal-information flows might enhance utility, but may also propagate wealth inequality or facilitate other forms of unfairness. These issues must be kept in mind as well when discussing this privacy–innovation aspect.

To summarize this Part, the above discussion examined five popular arguments which addressed the relation between privacy and innovation, a tension often noted in the policy and academic realm. In the foregoing paragraphs these arguments were sharpened in light of privacy-policy terminology and integrated into the broader innovation-based discourse, while considering every argument's underlying definitions, strengths, and weaknesses. Of the arguments noted, the last one generates the greatest interest and rhetorical force.[119] Its dominance can also provide an interesting lesson on the nature of the concept of privacy—all issues which the next sections now discuss.

III. RETHINKING AND UNPACKING THE PRIVACY VERSUS INNOVATION CLAIM

A. The Absurdity of Balancing Privacy Versus Innovation

At its core, the last point noted regarding the privacy–innovation linkage argues that privacy requirements should be relaxed to promote the overall interest of innovation. This point is acceptable when "social

[117] Goldfarb & Tucker, *supra* note 7, at 8–9.

[118] Katie Moisse, *"Google Flu Trends" Found to Be Nearly on Par with CDC Surveillance Data*, SCI. AM. (May 17, 2010), http://www.scientificamerican.com/article/google-flu-trends-on-par-with-cdc-data. *But see* Declan Butler, News in Focus, *When Google Got Flu Wrong*, 494 NATURE 155 (2013).

[119] For instance, and as noted above, it is even reflected in the title of the GREEN PAPER, *supra* note 10.

innovation" follows, preferably with limited distributional (and thus, fairness) concerns. Enhanced innovation will lead to jobs, enhanced social welfare, and other important social objectives. Sometimes it might even save lives. This argument seems intuitively plausible,[120] is simple, and ultimately quite measurable (so far as it pertains to measurable parameters). Yet a closer look finds that it is often not only wrong but also offensive. This first Section explains why. The next Section strives to relieve some of the tensions the "privacy-versus-innovation" argument brings about, and explains why this policy argument might nonetheless have some analytical force in specific instances and contexts.

Yet first, let us move to reexamine the "privacy-versus-innovation" argument. The argument in question calls for limiting privacy regulation, thus protecting promotion of innovation. However, should innovation interests be considered when deciding upon the regulation of what many consider not only an important legal and even constitutional right (in Germany[121] and to some extent in the U.S. as well[122]) but also a basic human right according to several European and international documents?[123] Is it not clear that when balanced against such basic rights and freedoms, innovation considerations are secondary at best and cannot play a role in establishing the final legal outcomes?[124] After all, the objectives that innovation might promote (including the lives it might ultimately save) should often be considered as secondary, and could possibly be achieved in other ways, without violation of this important right.

To sharpen the apparent absurdity of the "privacy-versus-innovation" argument, note two possible comparisons. The online pornography and the gaming (a.k.a. gambling) industries are both known technological trailblazers. Given their unique products on the one hand and their vast

[120] For yet another example of this argument's intuitiveness, see KAMALA D. HARRIS, CAL. DEPT. OF JUSTICE, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM i (Jan. 2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf (California Attorney General stating: "While it is easy to conceive of innovation and regulation as mutually exclusive, California is proof that we can do both. We can innovate responsibly.").

[121] In Germany, the right to privacy is part of the constitutional right to personality. *See* Edward J. Eberle, *Human Dignity, Privacy, and Personality in German and American Constitutional Law*, 1997 UTAH L. REV. 963, 976, 979–80 ("Personality rights include protection of informational privacy . . . .").

[122] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 34 (4th ed. 2011) ("Although the United States Constitution does not specifically mention privacy, it has a number of provisions that protect privacy, and it has been interpreted as providing a right to privacy.").

[123] Charter of Fundamental Rights of the European Union No. 2000/C, Dec. 7, 2000, art. 7, 2000 O.J. (C 364) 1; Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. 12, U.N. Doc. A/RES/217(III), at 73 (Dec. 10, 1948); Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Nov. 4, 1950, 213 U.N.T.S. 221. *See also* sources in *supra* note 34.

[124] JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 143 (2012) (arguing that the entire notion of balancing privacy against efficiency or security is flawed). We will not address this position.

demand on the other, both industries led the way in ICT innovations related to security, payment methods, virtual realities, and other novel elements. Innovations in these areas quickly made their way to mainstream businesses and practices such as banking, finance, and even medicine (consider virtual procedures and training), thus clearly enhancing overall utility (or providing "social innovation").[125] In addition, the heavy usage of these services has other positive externalities. Their demand drives infrastructure investment as well as hardware and software development.[126] So in view of all this, would it be acceptable to argue that regulations harshly limiting the legality of and accessibility to these technological industries should be softened so to promote online innovation?

One would be hard pressed to find any policymaker seriously advocating this position. The negative aspects of both pornography consumption and gambling activity—even when carried out legally by autonomous adults—will intuitively trump any of the benefits resulting from the innovative practices noted. A policymaker or lobbyist (not to mention an academic) making the innovation-related point noted would probably be laughed out of the room. Why, therefore, does substituting "pornography" or "gaming" with "privacy" when discussing the balance vis-à-vis innovation generate a plausible argument? What is it about privacy that allows this argument to flourish, at least in the U.S. context?[127]

One simple response is that indeed this latter argument is mistaken and flawed. Individuals err in thinking that their privacy rights must be set aside to promote innovation. Of course this would not stop interest groups from manipulatively promoting this notion. While this response might be sufficient, I set it aside for the moment. Let us assume that the intuitiveness and persistence of the "privacy-versus-innovation" argument indicates that there is greater depth to it—depth that I will now fathom.

Before doing so, let us discard a red herring. In an attempt to ex-

[125] On innovation and the pornography industry, see Colette Symanowitz, Opinion, *How the Porn Industry Has Driven Internet Innovation*, FINWEEK (Dec. 4, 2013), http://finweek.com/2013/12/04/opinion-how-the-porn-industry-has-driven-internet-innovation/ (noting innovations, such as online streaming and payments, the pornography industry promoted). *See also* Steve Parker, Jr., *What We Can All Learn from the Porn Industry's Innovations in Advertising and Digital Media*, BUS. INSIDER (Apr. 13, 2011), http://www.businessinsider.com/what-we-can-all-learn-from-the-porn-industrys-innovations-in-advertising-and-digital-media-2011-4.

[126] *See* Keith C. Miller, *The Internet Gambling Genie and the Challenges States Face*, J. INTERNET L., July 2013, at 1, 1 ("The technology for offering poker and casino games online has been a shining light of development and innovation.").

[127] To be fair, a very similar argument is often set forth in the context of environmental regulations that are overreaching and thus impede upon innovation. Here, in fact, the argument pits innovation against the protection of life and health. The key to these arguments is most likely that the relevant environmental regulations are overreaching and unnecessary. Some of these arguments will be noted in the analysis of the privacy–innovation argument below. *See, e.g.*, Ashford et al., *supra* note 96, at 420 ("[H]ealth, safety, and environmental goals can be *co-optimized* with economic growth through technological innovation.").

plain the persistence of the "privacy-versus-innovation" argument, one might note that discussions regarding balancing or even detracting from rights to promote innovation are quite common elsewhere in the information environment. Indeed, innovation interests are commonly balanced, and with limited controversy, against intellectual-property ("IP") rights.[128] As noted, innovation policy discussions often argue for both expanding (to incentivize additional invention) and limiting (to allow for other, similar, forms of innovation) IP rights.[129] If the innovation-based argument is acceptable for limiting IP, should it not pertain to Data Protection ("DP") (a relevant segment of privacy) as well? Or, if authors', inventors', and creators' rights could be curbed in view of innovation interests, shouldn't data subjects suffer the same fate?

Although they are often grouped together in discussions of the digital age's challenges,[130] privacy and IP rights are very different. Privacy is premised on autonomy-based arguments, actual harms,[131] and the protection from chilling effects or the excessive force of the state.[132] These are the rights and interests to be balanced against the promotion of innovation. IP's central justifications—at least in the U.S.—point elsewhere. As Professor William Fisher explains, IP is mostly premised on utilitarian theories and considerations;[133] IP rights are therefore mostly means to achieve an end.[134] One of the central objectives IP policy rights strive to promote is the notion of progress—one closely related to that of innovation. In essence, IP rights and law are closely linked to the notion of promoting innovation. Therefore, tinkering with the core of these rights to promote innovation in other contexts is an acceptable move, and within the scope of IP rights' overall objective. Yet the same cannot be said of

[128] *See supra* notes 4–5.

[129] *See, e.g.*, Chander, *supra* note 2, at 669 (discussing various statements noting that Google could not have been created in the U.K. due to strict copyright laws).

[130] For a famous example, see LAWRENCE LESSIG, CODE VERSION 2.0 (2006). Chapter 10 discusses IP, while the subsequent Chapter 11 discusses privacy concerns.

[131] *See supra* notes 33–35 and accompanying text.

[132] For the variety of theories justifying privacy, see SOLOVE, *supra* note 26.

[133] In his survey, Fisher identifies four theoretical approaches to explain IP. The first and "most popular" is a "utilitarian guideline" which is premised on an attempt to maximize "net social welfare." William Fisher, *Theories of Intellectual Property*, *in* NEW ESSAYS IN THE LEGAL AND POLITICAL THEORY OF PROPERTY 168, 169 (Stephen R. Munzer ed., 2001). An additional, related justification is that these rights are needed to "help foster the achievement of a just and attractive culture." *Id.* at 172. Regarding this option, Fisher notes: "This approach is similar to utilitarianism in its teleological orientation, but dissimilar in its willingness to deploy visions of a desirable society richer than the conceptions of 'social welfare' deployed by utilitarians." *Id.*

[134] Justifying IP rights is also premised on other theories, such as Lockean and Hegelian principles—that these rights are given to the individuals as fruit of their labor, or that the rights are required to satisfy a basic human need. Yet these justifications are secondary in the United States's IP regime and are also of limited relevance in the commercial and industrial contexts discussed in this analysis. *See id.* at 168–72; *cf.* ROBERTA ROSENTHAL KWALL, THE SOUL OF CREATIVITY: FORGING A MORAL RIGHTS LAW FOR THE UNITED STATES xiii (2010).

privacy rights and laws. The objectives of privacy and innovation are far from identical. Therefore, IP and DP might sound the same, but they are far from being analogous in this context.

B. Privacy Versus Innovation's Outer Realm: Deeper Insights

To further establish how a balance between innovation and privacy can formulate an acceptable legal paradigm we must first define the specific context of this inquiry. The arguments to balance privacy against the prospect of innovation would not pertain to cases in which a core privacy value or law conflicts with the relevant innovation (i.e., a new or advanced product, service, or marketing technique). In such a case, those planning or implementing the innovation, most likely, must restrict it (or it be restricted by the state) due to privacy considerations. In other words, such innovations will most likely be merely "market" rather than "social" innovation, or generate fairness-based concerns. Therefore, the "privacy-versus-innovation" argument pertains to the outer realm of the information-privacy debate. These are instances where the core privacy values are not compromised, or where their applicability to relevant contexts could be questioned.

Nonetheless, it is still puzzling why privacy (as opposed to other important interests, such as anti-pornography and anti-gaming interests) is often confronted with the innovation-based argument in policy discussion, even at its outer limits. Two possible responses come to mind: (1) privacy law introduces extensive uncertainty; (2) privacy laws are unnecessarily broad. Let us examine these in turn, while mostly rejecting the former and carefully accepting the latter.

1. Innovation, Privacy, and Uncertainty

Some aspects of privacy law might be understood to generate extensive uncertainty. Generally speaking, privacy laws address complex situations and pertain to cutting-edge technologies. Predicting how such rules will be applied to future developments is quite difficult, rendering the regulatory environment uncertain. Uncertainty is often noted as a factor undermining innovation.[135] Such uncertainty might encumber the ability to innovate in all digital realms which call for virtual interactions with individuals—interactions which almost always (and even inadvertently) involve the collection, analysis, and use of personal information.

The two FIPPs noted might be used to demonstrate the uncertainty

[135] *S*ee, for example, Harri Jalonen & Annina Lehtonen, *Uncertainty in the Innovation Process* (European Conference on Innovation and Entrepreneurship, 2011), *available at* http://www.virtuproject.fi/wp-content/uploads/2011/02/ECIE2011_Jalonen_Lehtonen_VIRTU_April_2011.pdf, who note eight forms of uncertainty in the innovation process: technological uncertainty, market uncertainty, regulatory uncertainty, social and political uncertainty, acceptance and legitimacy uncertainty, managerial uncertainty, timing uncertainty, and consequence uncertainty. Further note that in some instances, and for some innovators, uncertainty can provide an advantage.

such privacy rules might generate. Let us first examine "notice" and "choice," or the requirement to secure the individual's "informed consent" prior to data collection and usage. Establishing whether an interaction with a technological interface indicates user consent to other data-related practices is a challenging task. It is quite difficult to consider this factor in advance with regard to novel technological and business models. For instance, there is sharp disagreement as to what form of consent is required prior to installing different forms of cookies on the users' computers.[136] This issue is complicated by the fact that at times the data collectors might arguably rely on implied consent deduced from website usage.[137]

Cookies have been around for decades,[138] yet still create uncertainty. The uncertainty generated by the need to meet the consent requirement becomes even more acute for developers in newer settings, such as the mobile context. Here, achieving informed consent is far more complicated, given the limited screen space.[139] In addition, it is unclear what individuals' privacy expectations are in this realm—for instance, do they understand that location-based data are constantly being collected, given that they receive location-tailored ads and information?[140] It is fair to as-

[136] Natali Helberger, *Freedom of Expression and the Dutch Cookie-Wall* 3 (Amsterdam Law Sch. Legal Studies Research Paper No. 2013-66, 2013), *available at* http://ssrn.com/abstract=2351204 ("European law has introduced a provision that requires anyone who wishes to place a cookie in a user's browser to obtain informed consent prior to the placing of a cookie. The introduction of these provisions has been accompanied by many controversies. One of these controversies concerned the question of the form in which informed consent needed to be acquired: prior to entering a website, explicit or implicit?" (footnote omitted)). *See also* Article 29 Data Protection Working Party, *Opinion 2/2010 on Online Behavioural Advertising*, at 15 (June 22, 2010), 00909/10/EN (discussing what form of consent is fitting for the installation of cookies).

[137] The FTC, for instance, believes that first-party cookies could be used to enable marketing an advertisement by the specific website for the returning user. *See* FTC REPORT, *supra* note 11, at 41. The EU, however, finds that only first-party cookies strictly necessary to provide the service are allowed without prior consent. *See* Peter Traung, Computers and Internet, *EU Law on Spyware, Web Bugs, Cookies, etc., Revisited: Article 5 of the Directive on Privacy and Electronic Communications*, 31 BUS. L. REV. 216, 224 (2010).

[138] The use of cookies for web browsing is dated back to 1994. *See* John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. TIMES, Sept. 4, 2001, at A1; Sandi Hardmeier, *The History of Internet Explorer*, INTERNET EXPLORER COMMUNITY (Aug. 25, 2005), https://archive.is/TBm3T.

[139] *See* Peter Swire, Ohio State Univ., *Wrap Up on Privacy and Location Based Services* (June 28, 2011), http://transition.fcc.gov/presentations/06282011/peter-swire.pdf.

[140] For recent regulatory attempts to define privacy regulations and expectations, see FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES: BUILDING TRUST THROUGH TRANSPARENCY (Feb. 2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf. For a discussion of users' expectations, see *id.* at 3; for novel disclosure requirements for platforms, see *id.* at 15; and for disclosure requirements for application developers, see *id.* at 22.

sume that every new technological medium will add a wrinkle of complexity and thus uncertainty to this difficult issue. Therefore, applying a strict "informed-consent" rule in all instances requires innovators to make difficult predictions regarding the regulator's future response, and possibly "chill" their innovative activities—even those that might lead to the development of products and services individuals will ultimately agree to use.

A similar argument could be made regarding privacy restrictions of "secondary use"/"purpose specification/use limitation." Here, privacy rules mandate that information can only be used for predetermined tasks, with several exceptions. As a quick review of both a recent Article 29 Working Party Opinion published in the EU on this matter and a recent White House report (proposing to apply such a principle in the U.S.) indicates, finding whether this principle was breached is a complicated matter.[141] It requires establishing whether future uses fall within those that are not "incompatible" with the purposes originally indicated.[142] Another difficult question arises when striving to decide whether an analysis is merely "statistical" or "anonymous" (two popular exceptions to this privacy-based restriction) and therefore permitted.[143] Again, innovators structuring novel models will struggle with these questions, which might ultimately stall them and their technological progress.

Finally, note a recent famous EU case which addresses the "right to be forgotten," and demonstrates the difficulty of operating in an uncertain legal realm. In the recent *Google Spain* decision, the European Court of Justice ordered Google (while relying on a different data protection principle than those noted above—the principle of "data quality") to remove links to online articles referring to attachment proceedings against a specific individual.[144] This was due to the time that had lapsed since the attachment proceedings, rendering such information irrelevant and even inaccurate.[145] This somewhat surprising ruling called upon Google to alter its practices and enable the removal of separate effects.[146] The decision introduced novel requirements and was premised upon the broad language the EU Data Protection Directive sets forth. It provides greater

For a different set of recommendations for the State of California, see HARRIS, *supra* note 120, at 7, 14 (discussing recommendations for application developers and recommendations for platforms, respectively).

[141] Article 29 Data Protection Working Party, *Opinion 03/2013 on Purpose Limitation*, at 3, 31 (Apr. 2, 2013), 00569/13/EN [hereinafter *Purpose Limitation Opinion*]; WHITE HOUSE REPORT, *supra* note 12, at 18–19.

[142] *Purpose Limitation Opinion*, *supra* note 141, at 21.

[143] *Id.* at 29.

[144] Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317.

[145] *Id.*

[146] *See* Mark Scott, *Google Ready to Comply with 'Right to Be Forgotten' Rules in Europe*, N.Y. TIMES (June 18, 2014), http://bits.blogs.nytimes.com/2014/06/18/google-ready-to-comply-with-right-to-be-forgotten-rules-in-europe.

evidence of the potential broad reach of EU privacy law, and possibly contributes to the uncertainty regarding an abundance of business models and innovations whose creators and investors hesitate to enter the market.

In view of these uncertainty-related challenges privacy laws bring about, it is clear how limiting the reach of such laws might arguably advance innovation. If, for instance, the "purpose-specification" rule is to be repealed (or, in the U.S., not enacted in a general context to begin with, contrary to recent recommendations[147]), uncertainty will diminish. A similar point could be made regarding every one of the FIPPs.

Yet the innovation-versus-privacy uncertainty-based argument suffers from a severe shortcoming: there are ways to limit uncertainty other than merely repealing the relevant laws. Indeed, clear rules, yet nonetheless strict and privacy protective, can limit uncertainty concerns as well. Such detailed privacy laws will reduce innovators' uncertainty by clarifying to them (and their investors) the nature of the risks and hurdles their innovations face. Other regulatory measures could be applied to limit uncertainty. Regulators can publish previous decisions (while creating a form of "common law"),[148] structure quick pre-approval mechanisms,[149] and define safe harbors which will provide the innovator with certainty—all steps taken to some extent in various settings.[150] Furthermore, assuring that competent courts and regulators are governing these matters can also limit uncertainty. These options might not only allow for innovation, but also provide regulators with flexible tools that enable coping with an ever-changing technological reality.

Those playing the "innovation card" to argue for the limitation of privacy rules do not usually call for the latter steps to enhance certainty. They rather focus on demanding additional relief from privacy regulation. Yet the "uncertainty"-based argument for limiting privacy rules is insufficient, given the alternative measures which could limit uncertainty while still protecting privacy. Indeed interest groups and lobbyists might

[147] For instance, a recent policy paper recommended that U.S. law introduce a "Consumer Privacy Bill of Rights," which includes a right to "Respect for Context" which closely resembles the notion of "purpose specification." WHITE HOUSE REPORT, *supra* note 12, at 15–17 ("Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.").

[148] Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 627–66 (2014) (discussing how the FTC assumed this role).

[149] Bamberger & Mulligan, *supra* note 27, at 1581–84, 1620, 1630 (discussing some steps taken in the EU in this direction—especially in Germany and by the French *Commission Nationale de l'Informatique et des Libertés* ("CNIL"), which set up specific groups to discuss innovation).

[150] For instance, see safe harbors existing between the U.S. and the EU with regard to U.S. companies' compliance with the EU Data Protection Directive. *See* 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, 1049–50 (2013).

retort by noting that even clear rules will generate uncertainty, especially in legal realms that concern cutting-edge contexts. Yet the same could be said of almost all legal issues arising in the digital realms—issues related to tax, tort liability, contract formation, and more. Nonetheless, regulation of all these fields persists, and with good reason. Privacy, therefore, should prove no different.

The "uncertainty" justification for the "privacy-versus-innovation" argument is therefore quite weak. Yet it could perhaps be rephrased somewhat differently: although the privacy laws exist on the books, it is unclear whether they will eventually be enforced.[151] The norms governing them might be in flux and address abstract harms. It is possible that with time, practices today considered illegitimate will gain acceptance by the public, as norms are constantly shifting in this dynamic context. While assumedly similar, this argument leads to a very different discussion. It is a subset of a different explanation for the assumed soundness of the "privacy-versus-innovation" claim, which pertains to the excessive breadth of privacy rules—an argument the next section moves to explore.

2. Innovation and Overbroad Privacy Policy

A more convincing analytical basis for the "privacy-versus-innovation" argument is that, at some points on the periphery, privacy law (in this context—FIPPs) can no longer be justified normatively by various privacy theories. So at these points innovation-based interests should supersede those of privacy as currently articulated by law. This argument would in fact claim that some of the existing and contemplated privacy rules are over-extensive. They generate regulatory false positives[152]—prohibiting practices which privacy theory cannot ultimately find problematic. In other words, there is no real conflict between innovation and privacy, but there is between innovation and privacy law, which cannot be backed up by a convincing norm.

Upholding an overbroad right is not unacceptable in many contexts, given the interest of protecting important core values. Indeed, the EU applies the "precautionary principle" when moving to protect important interests.[153] Yet here, the argument would state, over-extensive regulation has dire consequences. Many actual and future business models might be considered as generating privacy breaches by law, even though they are normatively acceptable. Thus, innovation is needlessly stalled. Overbroad laws block the development of products and processes that would generate social benefits and utility.[154]

---

[151] For a discussion of the option of uncertainty stemming from incoherent laws, see *European Internet Industry*, *supra* note 65, at 36.

[152] In a somewhat different context, see Louis Anthony Cox, Jr., Letter to the Editor, *Regulatory False Positives: True, False, or Uncertain?*, 27 RISK ANALYSIS 1083 (2007).

[153] Bradford, *supra* note 16, at 15–16.

[154] For a similar argument directly attacking the application of the "precautionary principle" in the context of privacy, see Thierer, *supra* note 105, at 471–76.

Privacy regulation provides a fertile context for this policy-lobbyist argument. The normative justifications for privacy, especially in hard cases, are extremely complex. Usually no straightforward tangible right is violated, or harm inflicted.[155] One can also plausibly argue that many of the privacy norms discussed here are in flux, possibly still up for grabs. As new technologies lead to novel privacy-related challenges, the overbreadth argument could be set forth when the potential privacy violation is not matched with a strong visceral feeling,[156] or actual harm down the road. Regulators and academics, however, must ensure that it is noted in a fair and proper context.

In some contexts, the "overbreadth" argument is with merit. Especially in the United States, the public is adopting (even embracing) services and practices which clearly violate FIPPs. In some of these cases it is fair to assume that the privacy norms on the books probably do not reflect the public's preferences.[157] The public's preferences can serve as a reasonable proxy, in many instances, for the normative stand the law must take regarding such uses of personal information.[158] While public opinion need not necessarily indicate the normative outcome, it certainly might provide clues as to theoretical limits and shortcomings. Therefore, in some such instances, blocking these forms of innovation cannot be justified, and regulatory restrictions have gone too far.[159] The rules (both actual and proposed) that are rendering these practices illegitimate block other similar innovations from coming to life—possibly by innovators who are more timid or law-abiding by nature.[160]

---

[155] *See generally* SOLOVE, *supra* note 26 (providing the complicated theoretical mix that provides analytical backing to privacy laws).

[156] A similar point was noted by Jennifer Rothman in the context of personality rights. Rothman explains that with time, changes in technology generate novel scenarios in which the existing legal doctrine is rendered hollow. Jennifer E. Rothman, Response, *E-Sports as a Prism for the Role of Evolving Technology in Intellectual Property*, 161 U. PA. L. REV. ONLINE 317, 319–25 (2013).

[157] This argument cannot apply, however, when users agreed to the usage of the service without properly understanding how their personal information would be used, or agreeing to a certain form of usage which was later exceeded by the firm.

[158] Indeed, the lack of a subjective reasonable expectation of privacy serves as an underlying rationale for finding that no privacy protection should be provided by the state. This is part of the "reasonable expectation of privacy" test. *See* SOLOVE & SCHWARTZ, *supra* note 122, at 35.

[159] In some cases, however, the public's acceptance of a practice that is seemingly privacy-violating should not be considered an acceptable shift in privacy norms, but might indeed reflect an unfortunate outcome that resulted from misjudgment or social power structures. Julie Cohen clearly articulates this point regarding exposure in social networking. *See* COHEN, *supra* note 124, at 143–46. At other times, this might be merely a case in which the law should be channeling public opinion, norms and behavior, rather than vice versa.

[160] The fact that laws in Europe are possibly enforced far more leniently in practice in comparison to how they are conveyed "on the books" does not undermine the argument noted. Business ventures forming innovative practices cannot necessarily rely on the good graces of the regulatory entity *not* to "throw the book" at

As cases in point, let us consider both "Google Street View" and many of the features that Facebook introduced, while returning to the two FIPPs of "notice and choice" and "secondary use/purpose specification/use limitation." Both these legal constructs have sufficient theoretical justifications[161] and are backed by strong public preferences when applied to core cases. For instance, individuals would not want information they provide an insurer passed on to their employer without their knowledge. Nor would they want their health-related information used for solicitations and advertisements.

Yet in other, peripheral, cases which still negate FIPPs, the privacy protection social norm—as reflected in practice—would prove different.[162] Many of the services provided by Google and Facebook are located on such a periphery. And indeed, most Americans seem to embrace Google Street View, even though it features photos of their houses (sometimes of themselves)[163] without receiving notice or providing consent at the time of collection[164] (an aggregation practice some European countries have rejected).[165] Users also flock to Facebook, which constantly applies information provided by users for one purpose (setting up a profile page, sharing photos with friends) to another (recommending

them. Therefore, innovation is compromised.

[161] *See supra* notes 31–35.

[162] FRED H. CATE & VIKTOR MAYER-SCHÖNBERGER, NOTICE AND CONSENT IN A WORLD OF BIG DATA: MICROSOFT GLOBAL PRIVACY SUMMIT SUMMARY REPORT AND OUTCOMES 2–4 (Nov. 2012), *available at* http://download.microsoft.com/download/9/8/F/98FE20D2-FAE7-43C7-B569-C363F45C8B24/Microsoft%20Global%20Privacy%20Summit%20Report.pdf (arguing that implementing notice and consent in the age of Big Data is extremely difficult and perhaps other notions of privacy should be adopted).

[163] As an example of some of the strange images available on Google Street View, see Jessica Amason, *Top 10 Moments Caught on Google Maps Street View*, URLESQUE (Feb. 5, 2009), http://www.urlesque.com/2009/02/05/top-10-moments-caught-on-google-maps-street-view.

[164] Here one might note that the public's embrace of Google Maps need not indicate acceptance of the privacy norms it reflects, as usage does not necessarily entail the concession of one's privacy. I do not find this argument persuasive, as people's low level of opting out of this service enabled its popularity. Also, it is at least plausible to argue that individuals will shy away rather than embrace an application that is disrespectful of privacy—even if it is merely so of others' privacy.

[165] In Germany, see Ian Steadman, *Google Fined by German Regulator over Street View Privacy Breach*, WIRED.CO.UK (Apr. 22, 2013), http://www.wired.co.uk/news/archive/2013-04/22/google-germany-fine. In Switzerland, see Wendy Zeldin, *Switzerland: Court Decision in Privacy Violation Case Partially Favorable to Google*, LIBR. CONGRESS (June 15, 2012), http://www.loc.gov/lawweb/servlet/lloc_news?disp3_l205403188_text, and *Judgment of the Federal Supreme Court on Google Street View: Decisions on the Processing of Personal Data*, FED. DATA PROTECTION & INFO. COMMISSIONER (Aug. 2013), http://www.edoeb.admin.ch/datenschutz/00683/00690/00694/01109/index.html?lang=en. On the other hand, in the United States, see Chloe Albanesius, *'Boring' Family Gets $1 in Google Street View Trespass Case*, PCMAG.COM (Dec. 2, 2010), http://www.pcmag.com/article2/0,2817,2373754,00.asp.

friends, generating security questions, providing tailored ads).[166] The same can be said for many of the recommendation features provided by Amazon.com, which probably violate FIPPs, yet the public seem to enjoy, and even embrace.[167] At least in some cases, even the most avid privacy advocate might concede that the public has accepted social norms, which softened the application of FIPPs in these contexts, and this should be reflected in the law.[168]

According to this argument, in view of privacy laws' systematic overbreadth, an innovation-friendly perspective would call for more lenient and limited laws. These would protect core values (health information and privileged relations), while allowing innovators to move ahead and develop novel tools, so long as they promote social innovation. Thus, a "wait-and-see" strategy is preferable to a broad precautionary approach.[169] If the innovators' actions are found to compromise important norms and privacy rights, the innovators and their ventures could be rejected after the fact, by new laws set in place.

Of course, the seasoned and skeptic policymaker will clearly note the grave risk of adopting this lenient "wait-and-see" approach. Such a strategy will allow the innovators' firms to grow in size, capital, and political influence, while carrying out actions which are ultimately deemed unacceptable. Blocking a firm after the fact is considerably harder than doing so *ex ante*. At this later point, the innovator is already a powerful political player, controlling jobs and the ability to impact the politicians' districts. Therefore, a balance achieved after the fact will compromise privacy interests and benefits the first-mover innovators. The now-successful innovators will be able to sway not only politicians in their favor but their users as well. Constant usage of these services might convince the public (or manipulate it into believing) that the privacy breaches are acceptable,[170] even though they should not be considered as such.[171]

---

[166] The fact that all these noted U.S.-based firms operate in the EU legally today does not undermine the assertions noted in the text. As the text explains, these companies' core business is in clear conflict with FIPPs. The rules were only partially enforced after the fact due to leniency, or the limited reach of jurisdiction. Yet, this was not necessarily predictable, or even a relevant factor to other firms (especially those operating in Europe) whose innovative spirit was undermined given the existence of such rules.

[167] *See* Goldfarb & Tucker, *supra* note 7, at 11; Mangalindan, *supra* note 86 (discussing Amazon.com).

[168] For a discussion of the great difficulty of applying the "purpose-specification" principle in the age of "Big Data," see Fanny Coudert et al., *Applying the Purpose Specification Principle in the Age of "Big Data": The Example of Integrated Video Surveillance Platforms in France* (ICRI Research Paper 6/2012, 2012), *available at* http://ssrn.com/abstract=2046123.

[169] This indeed was the lobbying position in the policy paper, DIGITALEUROPE, *supra* note 15, at 6–7.

[170] For a discussion of this dynamic, see Bernstein, *supra* note 39, at 922–40. In the context of personal data, see Hildebrandt, *supra* note 111, at 37.

[171] The sentence noted in the text is complex and might appear self-

A possible response which allows for the "wait-and-see"/*ex post* strategy is to ensure that those vested with the authority of regulating these relevant technological realms are independent regulators. Such regulators must be shielded from external influence and capable of making tough decisions that might even run counter to some popular opinions.[172] Achieving this objective, however, is easier said than done.

To summarize, the tension between innovation and privacy need not undermine the existence of an important human right. Rather, it might call on regulators to exercise restraint when applying privacy protection to realms in which norms might be subject to change or have only weak theoretical backing. This approach is required given the need to consider the possible implications to innovation.

Finally, at some points these two last arguments (privacy regulation is uncertain or overbroad) converge. The innovators' fear that a weak norm will nonetheless be enforced also generates uncertainty. On the other hand, in some cases the arguments lead to conflicting outcomes. Indeed, advocating a flexible, *ex post* privacy-regulatory regime for the ICT industry might allow greater innovation in instances that are today forbidden. However, such a regime will inject an additional level of uncertainty. Innovators, nonetheless, would probably prefer some uncertainty over an overall ban on specific innovative realms.

IV. PRIVACY VERSUS INNOVATION: THE EU–U.S. ICT TEST CASE

A. An Inconvenient Truth (for Some EU Readers)

Thus far the discussion on the innovation–privacy balance has been mostly theoretical; this Article has examined arguments stating various relations between these parameters, and has striven to distinguish legitimate and sound analytical arguments from manipulative political spins. Yet an analysis of the privacy–innovation linkage, especially when comparing U.S. and EU law, must also note an uncomfortable truth. In this U.S.–EU comparison, an inescapable linkage between the strength of privacy laws and the level of ICT innovation is evident. Noting this anecdote might carry an important lesson—or perhaps be just a meaningless

contradicting. It assumes that individuals have a stable set of values, and that a subsequent shift away from them reflects a normative problem. Such values, however, might be dynamic and therefore the change in public opinion would indeed reflect an acceptable change in norms and thus prove unproblematic. A full discussion of this matter is beyond the confines of this Article.

[172] For a discussion regarding the importance of independent Data Protection Authorities ("DPAs"), see, for example, Hunton & Williams LLP, *European Commission Seeks Germany's Compliance with ECJ Judgment on DPA Independence*, PRIVACY & SECURITY INFO. L. BLOG (Apr. 7, 2011), https://www.huntonprivacyblog.com/2011/04/articles/european-commission-seeks-germanys-compliance-with-ecj-judgment-on-dpa-independence. *See also* Out-Law.com, *EU Judge Scolds Austria: Data Sheriffs Must Be Properly Independent*, REGISTER (Oct. 19, 2012), http://www.theregister.co.uk/2012/10/19/dpa_independence_cjeu.

manipulative statement. Even if this anecdote and its possible implications are not explicitly acknowledged in policy debates, their omnipresence haunts the discussion. Rather than ignore this matter, let us now confront this "elephant in the room," striving to properly frame its significance.

Let us begin with the facts, starting with the protection that privacy law provides. The EU features an omnibus and aggressive data-protection regime that is premised on FIPPs,[173] which might even be expanded in the near future.[174] The United States does not, but instead provides a lenient and business-friendly, sector-specific regulatory framework.[175] Few will therefore argue with the assertion that the EU upholds a significantly stricter privacy regime, for the rights' core and periphery alike. As a limited caveat, note that the existing privacy laws are enforced with greater rigor in the United States.[176] Yet even accounting for this factor, EU law provides far greater protection for individuals interacting with commercial entities, especially in the context of the internet-based ICT services addressed in this Article.

Next, let us examine innovation, while focusing on the ICT sector. There are various ways to calculate, estimate, and compare innovations. Yet even merely examining market structure and dominance leads to a very clear conclusion: not only is Europe failing to establish leadership in the internet market, it is unable to produce a presence. In fact, non-experts would be hard pressed to name even *one* significant EU-based, or even EU-originated, internet firm—at least not one that can challenge the hegemony of U.S. firms such as Amazon, eBay, Twitter, Apple, and of course the two heavyweights, Google and Facebook.[177] These U.S. firms provide vast innovation at least with regard to most of the elements noted—product innovations (both novel and improved), process innova-

[173] EU Data Protection Directive, *supra* note 28.

[174] *Personal Data Regulation Proposal*, *supra* note 14, at 1–2.

[175] Schwartz & Solove, *supra* note 19.

[176] Chander, *supra* note 2, at 670. Also note the discussion of the difference between privacy on the books and on the ground in Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011). As for weaker enforcement of privacy laws in the EU, see Bamberger & Mulligan, *supra* note 27, at 1549.

[177] It is possible that things might be changing with the rise of mobile usage and the development of supporting applications. It is a British firm—King—behind the popular "Candy Crush." This firm initially had a revenue of $1.8 billion. *See* Kim-Mai Cutler, *King's Forthcoming IPO Shows That Mobile Gaming Is Staggeringly Large, But Mature*, TECHCRUNCH (Feb. 20, 2014), *available at* http://techcrunch.com/2014/02/20/king-ipo. Yet success in this realm is far less sustainable, and the value of this firm has sharply diminished. Nick Shchetko & Telis Demos, *'Candy Crush' Shows Signs of Fading*, WALL ST. J., Aug. 13, 2014, at B1. The EU might be producing internationally successful e-commerce platforms, such as bookings.com (based in the Netherlands). However, this site as well was acquired by a U.S. platform (Priceline.com). An analysis as to whether such a scenario is an indication of failure or success in Europe is beyond the confines of this discussion.

tions (as these firms constantly upgrade their systems), and of course marketing innovations (among other things in the form of constant developments in behavioral advertising and viral marketing).[178] Finally, the analysis and usage of personal information is a key element in the business models of all of the dominant ICT-U.S.-based firms mentioned—especially of the latter two.[179] This intuitive observation must of course be followed up by further empirical studies.

Before proceeding to examine the possible meaning arising from linking these two data points, two important comments must be made. First, the European lag in the ICT realm is a widely discussed phenomenon (and will be further dissected in Part IV.B, below). It is part of a broader discussion of the "European Paradox":[180] the vast disparity between Europe's scientific leadership on the one hand, and its relative innovative failure in the ICT realm on the other.[181] The use of the term "paradox" itself is highly controversial, as some commentators argue that the EU's success on the academic level should be contested as well.[182] Yet even within this broader discourse, the European lack of success in the online markets seems to stand out. Here, the gap between the United States and the EU is substantial, and seems to be constantly growing. Thus, perhaps specific factors contribute to this outcome.[183]

Secondly, the analysis is further complicated by anecdotal case studies of early innovative successes in European ICT markets. These cases might provide insights when one strives to go beyond anecdotes, comparisons, and even speculative correlations to the realm of causation and policy implications. I now quickly note the rise and fall of Minitel (France) and StudiVZ (Germany) and examine what these examples

[178] This point is not contested in the EU. *See, e.g.*, *European Internet Industry*, *supra* note 65, at xv ("Europe has only limited presence in the new and rapidly[ ]growing areas of software and IT[ ]services and the web ecosystem, at home or abroad. In particular, business models based on advertising or data mining—characteristic of many successful players in the web ecosystem—are only sparsely represented among the European players in the European Internet industry.").

[179] Strandburg, *supra* note 70, at 158.

[180] Giovanni Dosi et al., *The Relationships Between Science, Technologies and Their Industrial Exploitation: An Illustration Through the Myths and Realities of the So-Called 'European Paradox,'* 35 RES. POL'Y 1450, 1450 (2006).

[181] European Commission, *Green Paper on Innovation* 5 (Dec. 1995), *available at* http://europa.eu/documents/comm/green_papers/pdf/com95_688_en.pdf. *See also European Internet Industry*, *supra* note 65, at xxv ("Europe has traditionally struggled to convert its scientific excellence into successful market products. It lags its global rivals in business model and service innovation.").

[182] *See European Internet Industry*, *supra* note 65, at 21, 99–101.

[183] This specific and acute innovation-related problem was also noted in an EU Policy paper. *See id.* at 12 (referring to the specific realm of limited innovation as "a fast-emerging 'web ecosystem,' whose actors provide web-based applications, services and content in a close and innovative relationship with users and with traditional players").

might add to the discussion.[184]

In France, Minitel was introduced in the early 1980s as a system for connecting computers to provide electronic dialing assistance. It eventually linked 35 million telephone subscribers. With time, it also provided weather and banking data, as well as other information sources. Its main driving force, and probably most popular function, was a chat feature that enabled the operation of extensive messaging boards (many of them were of sexual nature—yet another example of unconventional innovative forces driving ICT development[185]). This project was launched through French Telecom, and was efficiently financed as part of the regular phone bill. However, as the internet grew, Minitel's popularity dwindled, until the service was terminated in 2012.[186]

In Germany, StudiVZ and its sister sites SchülerVZ and MeinVZ were very popular and successful German-language online social networks. In 2006, for instance, they featured significant size and growth, even compared with Facebook.[187] They famously turned down a generous acquisition offer by Facebook, holding out for a higher price.[188] With time, however, users began migrating to Facebook.[189] In 2012 the VZ platforms began shutting down, unable to compete with Facebook or attract active users.[190] This latter case study is merely one example of the several local online European social networks that declined in view of Facebook's rise

[184] Another firm often discussed in this context is Skype. Skype seems to be a difficult example because it is somewhat in a different field—that of communications, rather than content as the other firms noted. It also involved an interesting mix of Scandinavian entrepreneurs, Estonian programmers, and eventually a U.S. acquisition with substantial influence along the way. For a full discussion, see JRC Report, *supra* note 78, at 66–70.

[185] For a broader discussion of the driving innovative force of the pornography industry, see *supra* note 125.

[186] *See* ROGERS, *supra* note 37, at 327–30; *see also* Hugh Schofield, *Minitel: The Rise and Fall of the France-Wide Web*, BBC NEWS MAG. (June 27, 2012), http://www.bbc.co.uk/news/magazine-18610692 (explaining how Minitel was eventually cancelled due to the success of the internet).

[187] Alex Bakst, *Internet Start-Up Auf Deutsch: StudiVZ Takes on Facebook*, SPIEGEL ONLINE (Nov. 7, 2006), http://www.spiegel.de/international/internet-start-up-auf-deutsch-studivz-takes-on-facebook-a-446353.html.

[188] Bobbie Johnson, *Crushed by Facebook, StudiVZ Teeters on the Brink*, GIGAOM (June 7, 2012), http://gigaom.com/2012/06/07/studivz-nears-the-end.

[189] Justin Smith, *Facebook Settles Suit Against StudiVZ, but Germans Already Moving to Facebook Anyway*, INSIDE FACEBOOK (Sept. 10, 2009), http://www.insidefacebook.com/2009/09/10/facebook-settles-suit-against-studivz-but-germans-already-moving-to-facebook-anyway ("If StudiVZ wants to hold onto its lead for much longer, it's going to need to do some serious innovation, as users appear to be moving to Facebook in droves.").

[190] *E.g.*, Ole Reißmann, *Netzwerk-Aus, SchülerVZ schließt Ende April* (*Network Closed, SchülerVZ Closes the End of April*), SPIEGEL ONLINE (Germany) (Apr. 9, 2013), http://www.spiegel.de/netzwelt/web/netzwerk-aus-schuelervz-schliesst-ende-april-a-893253.html.

to dominance.[191] At the end of the day, Facebook apparently provided a superior product in technology and interface to all its European competitors.[192]

These two limited case studies indicate that the EU *was* able to provide innovative success stories in the online ICT realm. Yet at a specific point the innovation was insufficient. They also show that in some cases the EU firms benefited from a "first mover" advantage. They further indicate that EU-based entrepreneurs showed talent and initiative in these realms, and that the local environment did facilitate these developments—at least to some extent. With these insights in mind, I now move on to examine what lessons the comparison between the two data points (the EU and the United States) in the context of privacy and innovation might or might not provide.

B. Cautiously Learning from the EU–U.S. Test Case

I now return to the five proposed theoretical interactions noted above to find what they might teach us about the EU–U.S. comparison noted.[193] Obviously, refuting a theory is easier than upholding one. Dynamics #1 through #4 argued that enhanced privacy will promote innovation. Intuitively, the EU provided greater privacy than the United States, yet enhanced innovation did not follow. Thus, while the EU–U.S. disparity regarding the level of privacy protection *could* have established the accuracy of the hypotheses these arguments set forth, it did not. The hypotheses might still be true, given other specific reasons that led to lower innovation in the EU (even though privacy protection was enhanced).

More specifically, there is no indication that the higher level of privacy in the EU enhanced trust, or led to greater online innovation (#1). However, trust and usage of online systems might be lower in the EU for a variety of reasons, such as different social values, lower technological adaptation or interoperability problems,[194] and for these reasons innovation did not follow. In addition, trust in the United States might have been maintained through other measures, especially the aggressive actions of the Federal Trade Commission—that rose to become a U.S. "privacy regulator."[195]

There is also no proof that the higher level of privacy in the EU led

---

[191] *See, e.g.*, Chander, *supra* note 2, at 689 n.262 (discussing the fall of Skyrock (France)); JRC Report, *supra* note 78, at 73.

[192] Martin U. Müller, *Status Update: Facebook LOL as Germany's StudiVZ Loses Ground*, SPIEGEL ONLINE INT'L (May 20, 2010), http://www.spiegel.de/international/business/status-update-facebook-lol-as-germany-s-studivz-loses-ground-a-695700.html ("VZ is considered technologically outmoded. It is significantly slower than Facebook in terms of introducing additional applications . . . .").

[193] *Supra* Part II.B.

[194] *See European Internet Industry*, *supra* note 65, at 96–97.

[195] *See* Solove & Hartzog, *supra* note 148, at 590.

to greater creativity and innovation in the ICT realm there (#2).[196] However, it is possible that greater creativity did unfold, but was not channeled to the realm discussed here. Or, that other cultural, economic, and social reasons limited EU creativity. In addition, the presumably more competitive environment that privacy laws foster did not lead to greater innovation in the EU (#3). Of course, the EU technological landscape might be concentrated and unfriendly to startups for other reasons.[197] Finally, privacy laws did not lead to privacy-protective platforms in the EU which comply with these legal requirements (#4). However, such innovations did not materialize possibly because of inherent difficulties with these business models (or given more successful services available from across the Atlantic).[198]

Evidently, the most provocative discussion comes when one matches the lessons from comparing the EU–U.S. data points and suggested linkage #5. Here, at least on the face of it, the anecdote *fits* the theory.[199] The "more privacy" (especially in terms of the implementation of FIPPs) leads to "limited innovation" hypothesis is strengthened, at least prima facie, by some field data. Yet before making this statement, it is crucial to note that as with any assumption relying on merely two data points and many forms of interference, the value of such "findings" is extremely limited and speculative. Furthermore, several other well-recognized reasons exist for stalled innovation in the EU and the U.S. innovative dominance in this field that have nothing to do with privacy. In fact, a recent study addressing such "innovation gaps," written for the EU Joint Research Centre ("JRC") and titled *Comparing Innovation Performance in the EU and the USA: Lessons from Three ICT Sub-Sectors*,[200] lists several interesting arguments, but notes the local privacy regime only implicitly and in passing.[201] Another policy paper addressing this issue ignores this notion completely.[202]

Among other things, the JRC report addresses the lack of a European "start-up culture,"[203] which results from the paucity of venture-capital

---

[196] Sklansky, *supra* note 62.

[197] *See European Internet Industry*, *supra* note 65, at 111.

[198] *See* discussion in Part IV.C, *infra*.

[199] It is of course possible that the causation flows in the opposite direction, and the lower levels of innovation have led to higher levels of privacy. Yet the previous discussion (Part I) does not set forth a theory underlying such causation.

[200] JRC Report, *supra* note 78, at 3.

[201] *Id.* at 20 (when discussing the advantages from which Amazon.com benefits), 21 (noting that the privacy issue is beyond the scope of the study), 72 (discussing the difficulties EU social-networking sites face when competing with Facebook). The notion was also noted in passing in another policy report. EU Media Futures Forum, *A Report for European Commission Vice-President Neelie Kroes to Reflect on the Future of the Media Industries from a Global Perspective* 8, 17 (Sept. 2012), *available at* http://ec.europa.eu/information_society/media_taskforce/doc/pluralism/forum/report.pdf.

[202] *European Internet Industry*, *supra* note 65.

[203] A famous joke in this context states that "there is no word in French for

funding and other unavailable governmental policies.[204] It further notes deeper problematic traits in the European business attitude to risk. This is reflected in pride, which inhibits innovators from going down a road where there is a very high chance of failure, or cultural pressure to retain long-term and stable employment.[205] As opposed to Europe, the report also points out the possible positive effects of academia in the United States (unavailable in the EU), which fosters these forms of innovation, and contributes to the formulation of innovation "clusters" (as in Silicon Valley). The success of these clusters was also aided at some point by governmental contracts.[206] Finally, the report indicates that in some instances the successful U.S. firms benefited from a "first-mover" advantage, thus leading to their long-lasting dominance.[207] An additional report commissioned by the EU touches upon similar themes.[208]

It is extremely challenging to establish whether the EU's innovative weakness in the Internet ICT context resulted entirely from the factors noted in these reports, or whether the differences in privacy law contributed as well. If the former elements are to blame, it is also possible that enhanced privacy rules enacted in the EU in fact *promote* innovation and their absence would have led to even lesser innovation.[209]

The test cases (Minitel and StudiVZ)[210] briefly noted above generate at least some reasons to doubt that the "classic" arguments set forth by the JRC are those to blame for the relative innovative failure. In fact, these test cases demonstrate that some Europeans are willing to take risks, obtain sufficient education and contacts, and secure funding. Furthermore, it was the EU firms that benefited from the first-mover advantage—a factor which did not prove helpful further down the road.[211]

The popular "other" arguments explaining the EU's ICT-innovation weakness (as set forth by the JRC) allow European regulators and privacy advocates elsewhere to reject the possible causal connection between privacy and innovation, and focus on improving other factors. They might also rely upon an argument that the correlation between weak privacy rules and limited innovation might not indicate causation among these factors at all. Rather, it might be explained by a third factor distinguish-

Entrepreneur."

[204] JRC Report, *supra* note 78, at 34, 39.

[205] *Id.* at 46, 48.

[206] *Id.* at 16. This notion is also reflected in the literature addressing the "European Paradox." *See* Dosi et al., *supra* note 180.

[207] JRC Report, *supra* note 78, at 14–15.

[208] *European Internet Industry*, *supra* note 65, at app. A (focusing on problems with trained labor, raising capital, lack of tax breaks, and other regulatory responses to start ups and harmonization problems throughout the EU).

[209] I thank Assaf Yaakov for this observation.

[210] *Supra* notes 184–92 and accompanying text.

[211] Studies of innovation indeed show that at times first-movers are provided with a competitive advantage—yet in other contexts, first-movers suffer severe drawbacks at a later time. Gopalakrishnan & Damanpour, *supra* note 22, at 24.

ing the EU and U.S. legal, social, or economic systems, which impacts both the emergence of privacy laws (or the lack thereof) and the extent of ICT innovation in both the EU and the U.S.[212] Examining this final assertion as well calls for subsequent theoretical and empirical testing.

Yet, for the sake of discussion, let us speculate and merely assume that the EU–U.S., privacy–innovation correlation implies that a causal linkage between these factors exists. If this is the case, one might argue that the EU's protective privacy policy led to the disappearance of internet-related innovation, hence the loss of jobs and income.

Furthermore, by a somewhat ironic twist, the lack of innovation (which possibly comes from comprehensive privacy laws in the form of FIPPs) is actually leading to *less*, rather than more, privacy protection for the EU citizen. Given the dominance of U.S. firms (possibly due to strict privacy laws), EU citizens often have their personal information stored and analyzed by foreign firms that transfer their data outside the continent. Even if we accept the questionable assertion that these U.S.-based firms complied with EU-law when carrying out such transfers, the privacy of EU citizens was apparently greatly compromised. In fact, with such data transfers, EU citizens were potentially exposed to the U.S. government. As recent revelations showed, U.S. intelligence agencies (especially the National Security Administration ("NSA")) intercepted data flows passing through the United States, and collected information on EU citizens.[213] In other words, if looser privacy laws would have facilitated greater innovation in Europe, one might argue that EU citizens might have benefited from greater protection of core privacy values, and would have had a better chance of keeping the U.S. government out of their personal affairs. A policy compromise regarding the extent of privacy precautions taken vis-à-vis European private entities might have, at the end of the day, limited the risks and harms of direct surveillance by a foreign government. It is at least fair to note that for many, the privacy interests encapsulated in the latter scenario (involving the NSA) surpass those of the former one (involving the storage and analysis of personal data by private parties).

In sum, if additional empirical studies on the EU–U.S. innovation disparity provide stronger proof of the privacy versus innovation causation thesis, several policy recommendations might follow. Such studies could be premised on addressing other comparable innovating societies, as well as examining legal changes in any one of these jurisdictions,

[212] I thank Bruno Frey for this insightful observation.

[213] These concerns were recently voiced by German Chancellor Angela Merkel. *See* Erik Kirschbaum & Julien Ponthus, *Merkel, Hollande to Discuss European Communication Network Avoiding U.S.*, REUTERS (Feb. 15, 2014), http://www.reuters.com/article/2014/02/15/us-germany-france-idUSBREA1E0IG20140215. For a discussion of the Snowden revelations in this context, see Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

which might enable a natural experiment pertaining to these matters. One such recommendation might call for easing EU privacy laws, and refraining from adapting stricter laws in the United States (as opposed to the current move to adopt the "Consumer Privacy Bill of Rights").[214] As explained in Part III.B, this argument only pertains to the periphery of privacy rights, and to laws which might refer to contexts where social norms do not call for privacy protection. In addition, it only applies to instances where social innovation and not merely market innovation unfolds, and where the innovative practices are not blatantly unfair.[215]

But these findings and analysis might lead to very different policy recommendations as well: those calling for stricter privacy laws worldwide. The Article's final section moves to confront this bold conclusion.

C. Privacy Policy Steering Innovation: Humming Refrigerators and Humming Servers

Empirical evidence and a shaky theory of causation might suggest that strict privacy laws are leading to lower levels of internet or ICT-based innovation in the EU. Yet the same factual statement could be articulated differently, especially in global and competitive markets. The alleged correlation noted could be understood as resulting from a dynamic in which the global framework of privacy laws might be *steering* innovation in various directions.[216] Thus, the lack of successful and sustainable EU-based innovation might not be the result of an information regime which is governed by strict data protection rules that inhibit innovation. Rather, the privacy-related regulatory arbitrage between the United States and the EU is steering global innovation toward the path chosen by dominant U.S. firms, where personal information is often used to advance the firms' objectives. Only U.S.-based firms that rely on U.S.-based laws can benefit from this inevitable outcome.

The effect of such steering can be articulated and examined on several levels. At first, the differences between privacy laws in the EU and the U.S. might steer relevant technically inclined EU entrepreneurs and professionals toward progress in other scientific fields, such as medicine, biology, and chemistry or other realms of ICT developments. Overall, this outcome might not be problematic. Innovations in these other fields, in

---

[214] *See* WHITE HOUSE REPORT, *supra* note 12.

[215] This point need not seem extremely far-fetched to the European reader. After all, the full title of the 1995 EU Data Protection Directive also refers to the importance of promoting information flows ("the free movement")—an objective that enhanced innovation will clearly forward. *See* EU Data Protection Directive, *supra* note 28. Moreover, another key European document prepared and supported by the Council of Europe indicates in its preamble the interest in a free flow of information. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, pmbl., Jan. 28, 1981, 1496 U.N.T.S. 65.

[216] *See* Bernstein, *supra* note 39, at 928–29 (noting that legal structures are also a form of social shaping in this context).

turn, might lead to even greater social innovation and utility than improvements to social networks and Internet content.[217] As this argument is outside the scope of this ICT-focused discussion, as well as highly speculative (although ultimately measurable), I set it aside for future testing.

Instead, let us focus on the impact this steering effect has on the products and services made available to Internet users worldwide. Before proceeding, note that the notion that social constructs (such as laws or business decisions) steer innovation is far from novel. In her essay, *How the Refrigerator Got Its Hum*, Ruth Schwartz Cowan famously explains the dynamics which led to the market dominance of the electric (humming) refrigerator. She argues that the large refrigerator manufacturers (General Electric, Westinghouse) opted for the electric option due to its tendency to break down, and thus generate additional revenue for these firms.[218] Thus, business considerations, rather than the promotion of social innovation steered the market towards the final, inefficient, "innovative" outcome.

In the Internet context, innovations are steered toward business models rich in the use of personal data by various firms. These models allow firms to reap the various benefits brought about by the analysis of personal information—especially its utilization for personalized and behavioral advertising. Yet this need not be the only outcome in this context. A stricter privacy-enhancing legal regime will possibly lead to a different set of innovations. Here, the market will be dominated by applications that allow individuals to collect their own data and negotiate its exchange with platforms. These tools might also allow individuals to select their own ads.[219]

At this time, however, such user-centric innovations do not succeed to thrive and gain market share. In a global market, innovators are steered towards the readily attainable revenues accrued from engaging in data collection and analysis. Or, in other words, the business models the U.S. firms feature. The highly mobile global marketplace allows EU-based entrepreneurs to take their innovations across the Atlantic to a legal regime that supports them. While the business models that unfolded feature market, and even social, innovation, it is quite possible that even greater and more diverse innovation would have followed had the entire business realm not been steered in one direction—that of reliance on personal-data collection and analysis.

---

[217] According to one study, the EU maintains a relatively high level of success and innovation in other ICT realms. *See European Internet Industry*, *supra* note 65, at 1.

[218] Ruth Schwartz Cowan, *How the Refrigerator Got Its Hum*, *in* THE SOCIAL SHAPING OF TECHNOLOGY: HOW THE REFRIGERATOR GOT ITS HUM 202 (Donald A. MacKenzie & Judy Wajcman eds., 1985). *See also* ROGERS, *supra* note 37, at 138–39.

[219] *See* VINCENT TOUBIANA ET AL., ADNOSTIC: PRIVACY PRESERVING TARGETED ADVERTISING 5, *available at* http://crypto.stanford.edu/adnostic/adnostic.pdf (prepared for the March 2010 Proceedings Network and Distributed System Security Symposium); Strandburg, *supra* note 70. PDMs are another variation of this general idea. *See also* Hildebrandt, *supra* note 111, at 36–37 (discussing PDMs).

Recently, Professor Katherine Strandburg made a similar point regarding the persistence of business models premised on free (or "free") content online.[220] Strandburg explains that, at least in theory, the Internet could provide a variety of platforms and business models for delivering content and services—among other things in exchange for actual money, or for personal information (which many nowadays consider "free"). This, in fact, is the case in other media. For instance, compare broadcast television, which is free to its consumer and based on advertising to the competing subscriber-based model presented, among others, by HBO.

However, in online markets, "free" content and services are king. Options which go beyond "free" are not materializing, and in any event are not proving sustainable. Firms providing users with content and services in exchange for collecting and analyzing their personal information are relying upon the easiest and most lucrative option for carrying out business online. However, this exchange, according to Strandburg, also involves cognitive errors and collective-action problems.[221] Nonetheless, the laws enabling the "free" exchange of content for personal data are steering innovation toward this "free" business model, and away from any other. Only a different form of regulation will allow other forms of innovation to globally unfold and thrive. The existing digital environment—and the "free" exchanges it entails—is not necessarily the most efficient, or the one that generates the greatest social innovation. It is merely the equilibrium point in the market governed by a specific set of laws.

Returning to the EU–U.S. privacy–innovation discussion reveals that current online innovation is shaped by various factors: the ability to engage in privacy-related arbitrage (i.e., to move innovations to lenient privacy regimes), global markets, and a mobile workforce. It is also impacted by the fluidity of privacy norms which might be reconstructed after the fact by interest holders. All these elements lead to the outcome noted above—broad global access to, and usage of, applications which are not focused on privacy protection (to say the least) and are U.S.-based.

In view of the above, only one possible regulatory solution will remedy the problematic final outcome that is unfolding: a strict *global* privacy regime along the lines applied by the EU today. This step will ensure the development of all forms of innovative measures. Such a regime will enable innovations that rely on the analysis of personal information (after proper consent is obtained and other requirements are met) as well as others that make for greater data protection.

The blueprint for achieving this global outcome already exists. It would be part of, what Anu Bradford refers to as, the "Brussels Effect."[222] The EU will maintain its strong privacy rules which rely on FIPPs. It will

[220] Strandburg, *supra* note 70.

[221] *Id.* at 96–97.

[222] Bradford, *supra* note 16, at 3.

aggressively enforce such laws against U.S. firms operating in Europe. Such firms will move to comply, while subjecting themselves to the U.S.–EU Safe Harbor Agreement, which is supervised by the Federal Trade Commission (FTC).[223] This latter regulatory framework must be reinforced to assure that the U.S. firms are indeed operating on an adequate level.[224] At the same time, the U.S. can adopt the "Consumer Privacy Bill of Rights" which will incorporate some FIPPs into U.S. law.[225] The aggregated impact of all these steps will be closing the gap between the U.S. and the EU and limiting the steering dynamic here discussed.

Opting for this position is naturally a huge gamble, and should ultimately be rejected.[226] This proposal might lead to social innovation and user-centric online-business models. Yet it might also possibly lead to the elimination of innovation in the internet realm as we know it today. Indeed, today's powerful and popular U.S. firms possibly benefited from social steering, as well as lenient legal regimes—and without such laws these firms would never have risen to dominance or even existed. Yet the proposed global change might cause the loss of all the vast social benefits the novel ICT virtual infrastructure has brought about: the ability to empower individuals, promote free speech, and even strengthen democracy.[227] These factors cannot be easily incorporated into an analysis striving to conclude whether an application is truly innovative (i.e., generates market or social innovation).[228] However, they are indeed relevant in a broader discussion as to *what form* of innovation we are interested in producing.

In other words, the risk of applying privacy rules which might undermine the enhancement of free speech and democracy is too great to take. If the whole world had been strictly subjected to the EU Data Protection Directive, we might not have had Facebook, Gmail, or Amazon, as the business models enabling them would not have passed legal muster. In other words, we do not know whether comprehensive privacy-protection rules will lead to a more diverse information economy or one with very limited innovation. Ultimately, and in light of recent political

[223] *Id.* at 24 n.110.

[224] Bradford, *supra* note 16, at 24–25. For critiques as to the weakness of this framework, and possible steps which could be taken to correct this problem, see THE FUTURE OF PRIVACY FORUM, THE US–EU SAFE HARBOR: AN ANALYSIS OF THE FRAMEWORK'S EFFECTIVENESS IN PROTECTING PERSONAL PRIVACY (Dec. 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/FPF-Safe-Harbor-Report.pdf.

[225] EXEC. OFFICE OF THE PRESIDENT, *supra* note 13, at 20.

[226] Yet an additional wrinkle is that systems that enable individuals to have greater control over their personal information generate an additional set of privacy concerns, as these systems might be hacked, or individuals might be manipulated to hand over their entire personal-data inventory. *See* Hildebrandt, *supra* note 111, at 36–37.

[227] *See* Chander, *supra* note 2, at 641–44.

[228] *See supra* Part II.B.2 (regarding the difficulty to balance privacy and the abstract notion of creativity).

changes which these technological advances facilitated, this is a gamble society cannot afford to take.[229]

V. CONCLUSION & EPILOGUE: THE NEXT INNOVATIVE STEP—WHATSAPP AND SNAPCHAT

Optimizing the privacy–innovation balance presents serious and difficult questions. It introduces delicate political challenges and generates tensions on a global scale. It calls for in-depth policy discussions, examining what form of regulations must be introduced to enhance privacy, and what forms of innovation society is striving to achieve. It also requires properly establishing the forces of political economy at play—the relative strength of lobbying by interest groups at various points—and the ability to counter these forces when considered problematic. Overall, this analytic task also sets forth intriguing issues for academic study, which I hope many will pursue in the years to come. This field opens the door to both theoretical and empirical studies, and to future cooperation among economists, legal scholars, sociologists, and others involved in the study of innovation and privacy. Finally, it calls for enhancing the discourse between academics and policymakers regarding this important issue.

The internal forces governing this matter are ever changing. The internet-related ICT markets, especially those pertaining to social media, develop at great speed, sometimes producing a "creative destruction" dynamic. It is possible that a new generation of powerful and innovative applications, which reflects a novel set of consumer preferences, is rising. This new generation of applications and services might undermine the presumption that the existing legal regime is steering technology toward privacy-reducing innovations.

In February 2014, Facebook announced it would acquire the messaging service WhatsApp for a dazzling 16 to 19 billion dollars.[230] WhatsApp (according to its blog) has accumulated 400 million active users.[231] According to a recent newspaper report, the firm strives to limit its users' privacy concerns by refusing to maintain copies of the communications it facilitates on the company's servers.[232] According to the article, the motivation for such privacy-preserving conduct is not a legal requirement. Rather, it results from co-founder Jan Koum's harsh experience with surveil-

[229] Clearly, those favoring the protection of personal information given its centrality as a human right, or those holding that a precautionary approach must be taken regarding the fear of privacy harms, will ideologically disagree with this final assertion.

[230] Brian Solomon, *Stunner: Facebook to Buy WhatsApp for $19 Billion in Cash, Stock*, FORBES (Feb. 19, 2014), http://www.forbes.com/sites/briansolomon/2014/02/19/stunner-facebook-to-buy-whatsapp-for-16-billion-in-cash-stock.

[231] *400 Million Stories*, WHATSAPP BLOG (Dec. 19, 2013), http://blog.whatsapp.com/472/400-Million-Stories.

[232] Brian X. Chen & Vindu Goel, *Founders of an Anti-Facebook Are Won Over*, N.Y. TIMES, Feb. 21, 2014, at B1.

lance under the Soviet regime.[233] The platform's success in a competitive market (even though the firm did not strive to benefit from the personal data at its fingertips) might indicate that many users share Koum's sentiment. This sentiment, in fact, might even be driving the application's astounding success.[234]

Snapchat is another popular (but not nearly as popular as WhatsApp) media platform, which has yet to be acquired, although it has turned down multibillion-dollar offers from both Google and Facebook.[235] Snapchat is explicitly in the business of promoting privacy. Messages sent are deleted after one to ten seconds (based on the users' settings) from both the sender's and recipient's devices (although, unfortunately, not from the company's servers).[236] The driving force behind this company's pro-privacy attitude is again not regulatory. Instead, it probably results from its usage as a platform for "sexting" by younger users who do not want to leave a trace of such communications.

Both of these successful platforms, like several others,[237] have grown and prospered under a lenient privacy regime. Their emergence might indicate a shift in public preferences regarding privacy, and the market's response to such change. Their success, however, might be nothing more than a result of a manipulative marketing ploy rather than actual compliance with privacy norms.[238] It is, therefore, important to track such devel-

[233] *Id.*

[234] Yet another analysis of WhatsApp's success notes that the platform provides better assurance that information would not make its way to the users' "broader social network of employers, in-laws and ex-flames." *See* Jenna Worthman, *WhatsApp Deal Bets on a Few Fewer 'Friends*,*'* N.Y. TIMES, Feb. 22, 2014, at 1.

[235] Jenna Wortham, *Rejecting Billions, Snapchat Expects a Better Offer*, N.Y. TIMES (Nov. 13, 2013), http://www.nytimes.com/2013/11/14/technology/rejecting-billions-snapchat-expects-a-better-offer.html.

[236] *Id.*; Jenna Wortham, *Off the Record in a Chat App? Don't Be Sure*, N.Y. TIMES, (May 8, 2014), http://www.nytimes.com/2014/05/09/technology/snapchat-reaches-settlement-with-federal-trade-commission.html.

[237] Wortham, *supra* note 235. The article mentions WeChat (from China) and Line (Japan). Note that none of these are European based. A later article noted additional firms that promise "more private and anonymous interactions than existing popular services," such as Whisper, Secret, Confide, and others. Wortham, *supra* note 236.

[238] Issues have arisen regarding both of these popular apps, raising the question as to the actual privacy and security these apps provide. For a discussion of a report indicating security breaches in WhatsApp, see Reed Albergotti, *WhatsApp Faces New Challenge*, WALL ST. J. (Mar. 13, 2014), http://online.wsj.com/news/articles/SB10001424052702303546204579437103717035962. Matters are even more severe regarding Snapchat. This firm agreed to settle charges by the FTC that Snapchat misrepresents the extent of privacy and confidentiality its apps provide, the ease with which the measures it takes could be circumvented, and the information it collects regarding its users. *See* Press Release, Fed. Trade Comm'n, *Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False* (May 8, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were. Note, however, that these reports do not necessarily undermine the argument that the public appetite for privacy

opments closely. In doing so we must consider whether they further illuminate or even reinforce any of the five popular analytical paradigms for articulating the relation between privacy and innovation. Perhaps they even set forth novel ways to consider the linkage between these two fundamental concepts. If this new innovative dynamic continues, these insights must be incorporated into the important policy discussion this Article chose to define.

enhancement is growing and that U.S.-based firms are moving to satisfy it (to some extent).