Northwestern Journal of Technology and Intellectual Property

Volume 11 | Issue 5 Article 3

2013

Consumer Information Privacy and the Problem(s) of Third-Party Disclosures

Clark D. Asay
Penn State University School of Law

Recommended Citation
Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 Nw. J. Tech. & Intell. Prop. 321 (2013).
http://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/3

This Article is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by an authorized administrator of Northwestern University School of Law Scholarly Commons.

NORTHWESTERN
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Consumer Information Privacy and the Problem(s) of Third-Party Disclosures

Clark D. Asay

April 2013 VOL. 11, NO. 5

© 2013 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property

Copyright 2013 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 5 (April 2013)

Consumer Information Privacy and the Problem(s) of Third-Party Disclosures

By Clark D. Asay*

U.S. consumers have little actual control over how companies collect, use, and disclose their personal information. This Article identifies two specific instances of this lack of control under U.S. law related to third-party disclosures, what I call the Incognito and Onward Transfer Problems. It then identifies the types of privacy harms that result and examines the advantages and possible drawbacks of a model law aimed at addressing these specific problems. The model law is based on a system of consumer notice and choice, the predominant method used in the U.S. to provide consumers with control over their information. Up until this point, however, this method of providing control has largely failed, and this Article seeks to address some of its failures. This Article argues that while notice and choice may be useful in addressing some information privacy problems (such as the two identified in this Article), it is not appropriate for all information privacy problems. No one-size-fits-all approach is adequate. Instead, each information privacy problem must be isolated and treated in its proper context.

I. INTRODUCTION 322
II. THE CURRENT U.S. PRIVACY REGIME 325
  A. Federal Sectoral Laws 325
  B. The FTC 327
  C. State Law 328
    1. Statutory Law 328
    2. Common Law 329
  D. Self-Regulation 331
  E. The U.S. Department of Commerce Safe Harbor 332
III. SO WHAT'S THE HARM? 333
  A. Addressing Privacy Harm Skepticism 333
  B. Defining the Harm 335
  C. A (Not-So) Hypothetical John Doe 337
IV. THE PROPOSAL 340
  A. Definitions 340

* Visiting Assistant Professor, Shughart Scholar, Penn State University School of Law. Many thanks to Erica Goldberg and Jacob Kreutzer for helpful guidance on this Article. I express particular gratitude to my former colleague, Raghu Seshadri, for inspiring much of my initial interest in information privacy, helpful discussions about information privacy in general, and specifically helping articulate the Onward Transfer Problem at a conference we both attended at Stanford in early 2010. And of course, much love to Ashli, Harris, and Teddy.

1. Personally Identifiable Information 341
2. Disclosure to Third Parties 342
B. The Mechanics 343
1. Notice 344
2. Choice 349
3. Private Right of Action 351
4. Relationship to Other Laws 352
V. AN ANALYSIS 352
A. The Costs 353
B. The Constitution 354
C. The Alternatives 355
VI. CONCLUSION 356

I. INTRODUCTION

¶1 Over forty years ago, Charles Fried, in a now classic law review article, defined privacy as the right to "control . . . information about ourselves."[1] Others have proposed alternative ways of understanding privacy,[2] but Fried's popular conception largely underlies the information privacy regime in the U.S. today.[3] This piecemeal regime—based on "Fair Information Practice Principles"[4]—consists of a mix of federal sectoral law, state law, FTC enforcement, and industry self-regulation aimed at providing consumers with notice and choice about how companies collect, use, and disclose their information. In essence, notice and choice constitute consumers' opportunity to control their information and thereby protect their privacy.[5]

¶2 Many commentators have noted the deficiencies of notice and choice in providing consumers with such control.[6] Almost no one seems to read privacy notices, for

[1] Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968).

[2] *See, e.g.*, Louis Brandeis & Samuel Warren, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (viewing privacy as the right to be let alone); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421 (1980) (viewing privacy as a form of limited access to the self); JULIE C. INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992) (conceptualizing privacy in terms of "intimacy"); Julie Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (identifying the purpose of privacy as providing individuals with autonomy for self-development purposes, which, in Cohen's estimation, is crucial to a properly functioning civil society); Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) (conceptualizing privacy in terms of "family resemblances" rather than trying to identify one common denominator for all forms of privacy).

[3] *See, e.g.*, Jerry Kang et al., *Self-Surveillance Privacy*, 97 IOWA L. REV. 809, 820, n. 30 (2012) (noting that the control conception of privacy has long been the standard in the legal and policy literature); Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CAL. L. REV. 1765, 1766-68 (2010) [hereinafter *Limits of Individual Choice*] (noting that the privacy-as-information-control approach is prevalent throughout the world, especially in the U.S.).

[4] *See* FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last visited Aug. 3, 2012).

[5] *Limits of Individual Choice*, *supra* note 3, at 1767-68.

[6] *See generally id*. at 1771-77 (arguing that privacy notices are typically inaccessible, fail to motivate consumers to action, do not provide consumers with a real choice, provide consumers with inadequate privacy protection, help perpetuate a false dichotomy between personally identifiable information and non-personally identifiable information, impose significant transaction costs on consumers, impose wasteful

instance.[7] Chief Justice John Roberts now famously indicated that he does not read the boilerplate with which every consumer is daily confronted.[8] Judge Richard Posner similarly admitted to not reading boilerplate legalese in his mortgage documents.[9] Others contend that even if consumers did read privacy notices, they would not understand them because they are written in a manner inaccessible to consumers.[10] And yet others have focused on the choice mechanism and criticized, for instance, opt-out choices as too easily manipulated by companies to serve their own purposes[11] and opt-in mechanisms as too costly to businesses while failing to provide consumers with offsetting benefits.[12] Because of these and other issues, some have largely ruled out notice and choice as an effective means to protect consumers' privacy.[13] Consumers appear to agree.[14]

¶3 Despite these criticisms, this Article argues that notice and choice can and should play a significant role—even if not the only role—in providing consumers with control over their information privacy. And, as this Article will argue, this conception of privacy as information control remains relevant in understanding and addressing certain privacy problems and harms. That notice and choice should play a significant role, but not the only role, suggests something important: a one-size-fits-all approach to information privacy problems, based on Fair Information Practice Principles, has proven and will remain unviable. Notice and choice may work for some information privacy problems, but not for others. Information privacy problems, therefore, must be isolated and addressed separately.

---

costs on businesses, fail to protect consumers against government access to sensitive personal information, and potentially undermine important industries, such as the credit reporting system); Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE 'INFORMATION ECONOMY' 343-44 (Jane K. Winn ed., 2006) [hereinafter *Failure of Fair Information*], *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1156972 (noting that notices are typically meaningless because consumers typically do not read them or choose to ignore them, they are written in overly technical language, they present no meaningful opportunity for individual choice, and they potentially interfere with important activities to society, such as credit reporting and national security).

[7] FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE iii, 19-20 (2010), *available at* http:// www.ftc.gov/os/2010/12/101201privacyreport.pdf (noting that consumers typically do not read privacy notices because they are long and incomprehensible).

[8] Mike Masnick, *Supreme Court Chief Justice Admits He Doesn't Read Online EULAs or Other 'Fine Print,'* TECHDIRT.COM, (Oct. 22, 2010, 9:48 AM), http://www.techdirt.com/articles/20101021/02145811519/supreme-court-chief-justice-admits-he-doesn-t-read-online-eulas-or-other-fine-print.shtml.

[9] *Id.*

[10] Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 107-12 (2001).

[11] Jeff Sovern, *Opting In Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999) [hereinafter *Opting In Opting Out*].

[12] Michael E. Staten & Fred H. Cate, *The Impact of Opt-In Privacy Rules on Retail Markets: A Case Study of MBNA*, 52 DUKE L.J. 745 (2003).

[13] *See Limits of Individual Choice*, *supra* note 3, at 1801-03 (arguing that in most settings, notice and choice are "neither the best tool for protecting our privacy nor an appropriate goal of our privacy laws"); James P. Nehf, *The FTC's Proposed Framework for Privacy Protection Online: A Move Toward Substantive Controls or Just More Notice and Choice?*, 31 WM. MITCHELL L. REV. 1727, 1745 (2011) (arguing that even an enhanced notice and choice regime will prove "wholly ineffectual" due to inherent defects in the notice and choice approach); *Failure of Fair Information*, *supra* note 6, at 344-45 (arguing that notice and choice, without substantive data processing restrictions, will continue to be ineffective in protecting privacy).

[14] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* 21 (2009), *available at* http://ssrn.com/abstract=1478214 (indicating that 67% of consumers feel that they have lost all control over how companies collect and use their personal information).

¶4 This Article isolates two such problems related to third-party disclosures. Under the current piecemeal regime, even in the typical best-case scenario, consumers have no real control over third-party disclosures. To illustrate: companies generally provide consumers with some notice and choice regarding third-party disclosure of their personal information, typically as part of a blanket opt-in/opt-out approach. But such notice and choice is defective because consumers receive little to no information about who specifically will receive their information and how they will use it (what I call the "Incognito Problem"). Furthermore, once consumers' information is the hands of such third parties, U.S. law provides consumers with even fewer protections (what I call the "Onward Transfer Problem").

¶5 Indeed, even if consumers read and perfectly understood all applicable privacy notices, and even if they exercised their opt-in and opt-out rights in every instance, in most cases they would still lack effective control over their information because of the Incognito and Onward Transfer Problems. While control over information may entail many things, at a basic level it must include determining with whom your information is shared and for what purposes. As a result of this lack of control, consumers experience distinct subjective and objective privacy harms.

¶6 To address these problems and the resulting privacy harms, this Article explores the possible benefits and potential drawbacks of federal legislation that would require companies to provide consumers with notice and choice regarding the specific third party recipients of their information and their intended uses. It does so by constructing and examining one possible model law. This examination is particularly relevant at a time when Congress continues to consider information privacy legislation that, some complain, simply enshrines the status quo.[15]

¶7 This Article proceeds as follows: Part I examines the current U.S. approach to the issue of third-party disclosure and highlights the problem that, even in the typical best-case scenario, consumers remain uninformed about who specifically will have access to their information and how they will use it. This scenario, which plays out because of the Incognito and Onward Transfer Problems, effectively undermines consumer control over their information. Part II examines the nature of the resulting privacy harms and offers reasons for why we might be skeptical of privacy harm skepticism. Part III then explores a system of notice and choice aimed at addressing the Incognito and Onward Transfer Problems, the privacy harms that result from them, and common critiques of notice and choice as an effective regulatory means. Part IV concludes by analyzing the proposal's

[15] *See, e.g.*, Danny Weitzner, *We Can't Wait: Obama Administration Calls for A Consumer Privacy Bill of Rights for the Digital Age*, THE WHITE HOUSE BLOG (Feb. 23, 2012, 4:00 PM), http://www.whitehouse.gov/blog/2012/02/23/we-can-t-wait-obama-administration-calls-consumer-privacy-bill-rights-digital-age (discussing a recently released Obama administration blueprint for a consumer privacy "Bill of Rights"); Tim Conneally, *Two New Internet Privacy Bills Enter Congress: How They Differ*, BETANEWS (Apr. 14, 2011), http://betanews.com/2011/04/14/two-new-internet-privacy-bills-enter-congress-how-they-differ/ (discussing the basics of two privacy bills that are currently under consideration). Several groups have criticized the McCain-Kerry bill in particular for simply enshrining current industry practices, as well as failing to provide consumers with a legal right of action against companies that fail to protect their privacy. *See, e.g.*, *Consumer Groups Welcome Bipartisan Privacy Effort, but Warn Kerry-McCain Bill Insufficient to Protect Consumers' Online Privacy*, CENTER FOR DIGITAL DEMOCRACY (Apr. 18, 2011), http://www.democraticmedia.org/consumer-groups-welcome-bipartisan-privacy-effort-warn-kerry-mccain-bill-insufficient-protect-consum.

advantages and potential drawbacks, as well as positing some lessons learned from this study for addressing other information privacy problems.

II. THE CURRENT U.S. PRIVACY REGIME

¶8 The most significant pieces of the U.S. regime governing consumer information privacy and third-party disclosures are set forth below.

A. Federal Sectoral Laws

¶9 Unlike the Europe Union (E.U.) and other parts of the world that have adopted comprehensive privacy legislation, the U.S. has adopted several federal sectoral laws that target specific industries and types of personal information.[16] Consequently, if a company does not fall within that specific industry, or if the type of personal information that the law covers is not involved, the sectoral law does not apply to either the entity or the information.

¶10 For instance, the Health Insurance Portability and Accountability Act (HIPAA) only applies to "covered entities"—health plans, health care providers, health care clearinghouses and, in some cases, business associates of the same—that have access to a person's protected health information.[17] The Fair Credit and Reporting Act (FCRA) covers consumer reporting agencies that compile or use "consumer reports."[18] The Gramm-Leach-Bliley Act (GLBA) limits itself to "financial institutions"—entities significantly involved in financial activities as defined under the Act—that handle non-public financial information.[19] The Children's Online Privacy Protection Act (COPPA) covers operators of commercial websites and online services directed to children under the age of thirteen, or such entities that knowingly collect personal information of children under the age of thirteen.[20] And the Video Privacy Protection Act (VPPA) applies to "video tape service providers"[21] that rent, sell, or deliver "prerecorded video cassette tapes or similar audio visual materials."[22]

---

[16] This Article does not address the question of whether comprehensive privacy law in the U.S. would be appropriate. For opposing viewpoints on this general question, compare Jill L. Joerling, *Data Breach Notification Laws: An Argument for a Comprehensive Federal Law to Protect Consumer Data*, 32 WASH. U. J.L. & POL'Y 467 (2010) (advocating for comprehensive privacy regulation), with Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 903 (2009) (advocating against comprehensive privacy regulation).

[17] U.S. DEP'T OF HEALTH & HUMAN SERVICES, *Understanding HIPPA Privacy: For Covered Entities*, http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html (last visited Jan. 9, 2013).

[18] Subject to certain exceptions, "consumer reports" are defined as "any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (A) credit or insurance to be used primarily for personal, family, or household purposes; (B) employment purposes; or (C) any other purpose authorized under section 1681b . . . ." 15 U.S.C. § 1681a.

[19] FED. TRADE COMM'N, *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, (Jul. 2002), http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus53.shtm.

[20] FED. TRADE COMM'N, *Frequently Asked Questions About the Children's Online Privacy Protection Rule*, http://www.ftc.gov/privacy/coppafaqs.shtm (last revised Oct. 7, 2008).

[21] There is some disagreement among courts regarding who constitutes a "video tape service provider" under VPPA. *Compare* Dirkes v. Borough of Runnemede, 936 F. Supp. 236 (D.N.J. 1996) (ruling that the VPPA may apply to other parties in addition to video tape service providers, such as law enforcement

¶11 All of these industry-specific laws require covered entities to provide forms of notice and choice to affected consumers before disclosing those consumers' covered information to third parties.[23] COPPA, for instance, requires affected entities to post an online privacy policy depicting how they collect, use, and disclose personal information, and to give the parents of children a choice as to whether an affected entity may disclose the child's personal information to third parties.[24] GLBA similarly requires affected entities to provide consumers with notice about an affected entity's collection, use and disclosure practices, as well as an opt-out of some sharing of personal financial information with non-affiliated third parties.[25] HIPAA requires covered entities to use protected health information only for purposes of treatment, payment, or operations; otherwise, the covered entity must obtain specific opt-in authorization that details the information to be disclosed, the purposes of disclosure, and the entity to which disclosure will be made.[26] Under HIPAA, consumers have a right to receive an accounting of the third-party disclosures of their personal information.[27] Under FCRA, users of consumer reports must give the subjects of such consumer reports notice and the opportunity to review the information in them when and if such user takes an adverse action based on that information.[28] FCRA also provides a private right of action.[29] Finally, VPPA includes a general ban on disclosing personally identifiable rental information unless the consumer consents specifically in writing.[30] However, video tape service providers may disclose to third parties "genre preferences" along with the names and addresses of the consumers, so long as the consumer was provided an opt-out mechanism.[31]

¶12 In terms of consumer control over their information privacy, several problems arise with this sectoral approach. Perhaps most obviously, the laws only cover certain types of information and entities, thus leaving many other types of personal information and business entities unaccountable, including much of consumers' online activity. Furthermore, while the laws do require some amount of notice and choice before the covered entities may disclose the information to third parties, with the exception of HIPAA and VPPA in certain limited circumstances, this notice and choice comes in the form of a blanket opt-in/opt-out approach. The consumer does not actually know specifically who will receive their information and how such third parties will use it and further disclose it, thereby leaving the consumer with little to no control over their information. These laws thus suffer from the Incognito and Onward Transfer Problems.

officers), *with* Daniel v. Cantell, 375 F.3d 377 (6th Cir. 2004) (ruling that the VPPA only applies to video tape service providers).

[22] DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 840 (4th ed. 2011).

[23] This Article obviously cannot and does not list every federal statute that regulates consumer privacy in some manner or another, but instead focuses on some of the more well-known ones. For a more comprehensive list of federal statutes that implicate privacy, *see id.* at 37-39.

[24] *Frequently Asked Questions About the Children's Online Privacy Protection Rule*, *supra* note 20.

[25] *In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act*, *supra* note 19.

[26] *Understanding HIPPA Privacy: For Covered Entities*, *supra* note 17.

[27] *Id.*

[28] FED. TRADE COMM'N, NOTICE TO USERS OF CONSUMER REPORTS: OBLIGATIONS OF USERS UNDER FCRA (2009), http://www.ftc.gov/os/2004/11/041119factaapph.pdf.

[29] *Id.*

[30] ELECTRONIC PRIVACY INFO. CENTER, *Video Privacy Protection Act*, http://www.epic.org/privacy/vppa/ (last visited July 6, 2012).

[31] *Id.*

Lastly, with the exception of FCRA, none of these statutes include a private right of action. Consequently, consumers must rely on either the FTC or state attorney generals to protect their interests under the laws.

B. The FTC

¶13 In addition to helping enforce these sectoral laws, the FTC regulates privacy issues on the basis of Section 5 of the FTC Act.[32] Under this Act, the FTC investigates and brings actions against companies that engage in "unfair" or "deceptive" trade practices.[33] "Unfair trade practices" are defined as commercial conduct that (i) causes (or is likely to cause) substantial injury to consumers (ii) that consumers cannot reasonably avoid themselves, and (iii) without offsetting benefits to consumers or competition.[34] "Deceptive trade practices" are defined as commercial conduct that includes false or misleading claims, or claims that omit material facts.[35] With respect to deceptive trade practices, consumer injury does not need to occur; the mere fact that a company has engaged in such deceptive practices is actionable.[36]

¶14 What constitutes a deceptive or unfair trade practice has evolved, depending on what business practices the FTC has deemed problematic at any given time.[37] The FTC has brought actions against companies for reasons ranging from companies' failure to implement sufficient security measures given the sensitivity of the information collected, to companies stating certain privacy practices in their privacy notices while not actually following them.[38] Furthermore, the FTC has recently brought actions against companies for failure to adequately disclose their information-handling practices in cases where such handling involves sensitive information.[39]

¶15 However, such FTC enforcement fails to address the Incognito and Onward Transfer Problems. As of yet, the FTC has failed to require notice and choice similar to what is called for in HIPAA—identification of specific third parties and their intended uses—and has instead relied on the industry standard opt-in/opt-out regime that in reality provides consumers with little useful information. In fact, other than a few limited cases,[40] the FTC has not even made clear that notice and choice are required in the first place. Instead, typically its actions have focused on a company's failure to abide by its stated privacy practices, whatever those may be.[41] Consequently, the FTC's role in

---

[32] *See generally* FED. RESERVE, CONSUMER COMPLIANCE HANDBOOK (June 2008), *available at* http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

[33] *Id.* at 1.

[34] PETER SWIRE & SOL BERMANN, INFORMATION PRIVACY 70 (2007).

[35] *Id*.

[36] *Id.*

[37] For a general assessment of the FTC as a privacy enforcer, see Steven Hetcher, *The FTC as Internet Privacy Norm Entrepreneur*, 53 VAND. L. REV. 2041 (2000).

[38] *See generally* FED. TRADE COMM'N, *Legal Resources* (2013), http://business.ftc.gov/legal-resources/8/35 (last visited Jan. 14, 2013).

[39] *See* FED. TRADE COMM'N, *FTC Settles with Company that Failed to Tell Parents That Children's Information Would be Disclosed to Marketers*, Nov. 30, 2010, http://www.ftc.gov/opa/2010/11/echometrix.shtm; FED. TRADE COMM'N, *Sears Settles FTC Charges Regarding Tracking Software*, June 4, 2009, http://www.ftc.gov/opa/2009/06/sears.shtm.

[40] *Id.*

[41] *See, e.g.*, FED. TRADE COMM'N, *Gateway Learning Settles FTC Privacy Charges*, (July 7, 2004), http://www.ftc.gov/opa/2004/07/gateway.shtm (bringing an action against and settling with Gateway

protecting information privacy has similarly left consumers with no real control over third-party disclosures.

C. State Law

1. Statutory Law

¶16 State statutory law also provides little reason for comfort from an information privacy perspective. California's "Shine the Light Law," for instance, theoretically gives consumers greater control over their information by requiring covered companies to disclose their information-sharing practices to consumers, and, upon request, to provide consumers with a list of companies with which they have shared the consumer's information for marketing purposes.[42]

¶17 However, such laws are not widespread; at the time of this writing, California is the only state to have adopted such a law.[43] Furthermore, even under the California law, if companies provide the consumer with an opt-out or opt-in option, then such companies are exempt from the law and need not disclose to consumers the third parties with which the company shared or may share their information.[44] Lastly, even if the consumer somehow obtained access to the list of companies with which the initial company shared its information, the law does not provide any recourse to the consumer—consumers have no right to require the third party to stop using or disgorge their information. Consequently, even under California law, which many acknowledge as having some of the strongest consumer privacy protections in the U.S.,[45] consumers typically remain subject to the Incognito and Onward Transfer Problems.[46]

¶18 Most states do not even go so far as to require that companies develop privacy policies, let alone requiring useful notice and choice. California does require online companies to post a privacy policy indicating their information and disclosures practices.[47] Utah has adopted laws requiring certain companies to disclose to consumers

---

Learning for its failure to abide by its stated privacy practices).

[42] PRIVACY RIGHTS CLEARINGHOUSE, *California's "Shine the Light" Law Goes into Effect Jan. 1, 2005*, (Dec. 29, 2004), http://www.privacyrights.org/ar/SB27Release.htm.

[43] PRIVACY RIGHTS CLEARINGHOUSE, *Fact Sheet 4(a): California's "Shine the Light" Law*, (July 2005), http://www.privacyrights.org/fs/fs4a-shinelight.htm#10.

[44] *See California's "Shine the Light" Law Goes into Effect Jan. 1, 2005*, *supra* note 42.

[45] *See, e.g.*, Martyn Williams, *California to Get Tough on Behalf of Online Privacy*, PCWORLD (Jul. 19, 2012), http://www.pcworld.com/businesscenter/article/259534/california_to_get_tough_on_behalf_of_online_privacy.html (summarizing a new privacy enforcement initiative of California Attorney General Kamala D. Harris and noting that California has some of the strictest privacy regulations in the U.S. and has often acted as a bellwether state for privacy regulation); *see also* SOLOVE & SCHWARTZ, *supra* note 22, at 871 (indicating it is "probably safe to generalize that California has the strongest privacy law in the United States").

[46] This is because most companies provide some form of opt-in or opt-out in order to avoid having to disclose to consumers the third parties with which they have shared consumers' information. However, as discussed throughout, blanket opt-in/opt-out choices do not eliminate the Incognito and Onward Transfer Problems, but instead perpetuate them.

[47] *See* Cal. Bus. & Prof. Code § 22575(a). Interestingly, it remains unclear whether the California law covers mobile applications and their providers, through which companies collect vast amounts of sensitive information. The California Attorney General, Kamala D. Harris, has publicly stated that she believes they are covered and intends to enforce the law against mobile application providers that fail to post privacy policies. To that end, the State of California and six of the largest technology companies in the world—

what types of information they may disclose to third parties.[48] Connecticut also requires a privacy policy to be posted in the event that an entity collects social security numbers.[49] However, none of these state statutes require notice and choice about the specific third parties to be included in the privacy policies.[50] Under state privacy statutes, then, consumers remain subject to the Incognito and Onward Transfer Problems.[51]

¶19 All states also have some form of a deceptive trade practices act.[52] These laws are similar to the FTC Act in scope, and state courts have typically followed the FTC's lead in interpreting what constitutes a deceptive or unfair trade practice.[53] Some states have been more generous to consumers under their acts,[54] and so, theoretically at least, state deceptive trade practices acts could help address the Incognito and Onward Transfer Problems. However, up until now states have failed to interpret their statutes to address these issues, and nothing suggests this will change anytime soon.

2. Common Law

¶20 Another possible solution to the Incognito and Onward Transfer Problems is state common law. Almost all states recognize certain privacy torts at common law.[55] Generally, these include: (1) intrusion upon seclusion or solitude, or into private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false light in the public eye; and (4) appropriation of one's name or likeness.[56] Some have advanced these as the best means to protect consumer information privacy. One organization claims these torts are sufficient, and any proposed administrative regulations would simply burden companies with no real privacy benefits to consumers.[57] Some have advanced the tort of appropriation in particular as the best hope for protecting consumer information privacy in the modern world of data mining, in part because other means of protecting consumers are not, in their view, feasible to implement.[58]

Amazon.com, Inc., Apple, Inc., Google, Inc., Hewlett-Packard Company, Microsoft Corporation, and Research In Motion Limited—recently drafted a non-binding Joint Statement of Principles aimed at promoting privacy best practices among mobile application developers. *See Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications*, OFFICE OF THE ATT'Y GEN. (Feb. 22. 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

[48] *See* NAT'L CONF. OF STATE LEGISLATURES, *Selected State Laws Related to Internet Privacy*, http://www.ncsl.org/default.aspx?tabid=13463#isp (last updated Feb. 7, 2012).

[49] *Id.*

[50] *Id.*

[51] This section obviously does not cover all state statutes that implicate consumer privacy. For instance, both Minnesota and Nevada have laws requiring Internet service providers to keep private certain information about their consumers, unless the consumer gives the ISP permission to disclose the information. *See Selected State Laws Related to Internet Privacy*, *supra* note 48. However, these laws only cover ISPs, and other state statutes are similarly or otherwise limited in their application.

[52] *See* SOLOVE & SCHWARTZ, *supra* note 22, at 831.

[53] *Id.*

[54] Jeff Sovern, *Protecting Privacy with Deceptive Trade Practices Legislation*, 69 FORDHAM L. REV. 1305, 1352-53, 1357 (2001).

[55] *See The Privacy Torts: How U.S. State Law Quietly Leads the Way in Privacy Protection*, PRIVACILLA.ORG (July 2002), http://www.privacilla.org/releases/Torts_Report.html.

[56] *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (systematically spelling out for the first time the four general categories of privacy torts).

[57] *The Privacy Torts*, *supra* note 55.

[58] Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer*

¶21 However, in terms of information privacy, these torts largely fail to provide consumers with much recourse at all. The torts and their standards regarding information privacy are outdated and have not been adequately adapted to take into account new technologies and their effects on information privacy. For instance, courts have been reluctant to recognize privacy torts in cases where the information collected was publicly available or where a reasonable person would not be offended by the collection in each instance, even though modern database compilation technologies can quickly render thousands of such bits of information about a person into a sensitive, comprehensive profile.[59] The Incognito and Onward Transfer Problems exacerbate this situation by making it easy for companies to share such information with third parties.

¶22 Courts have also tended to adopt a binary view of privacy—some bit of information is either public or private—when in reality information is only rarely entirely public or private in the modern age; context matters.[60] Other commentators point out that the privacy torts rely on a concept of physical space to define privacy expectations and harm.[61] As a result, courts in applying privacy torts to the digitized world have largely neglected privacy harm that does not fit neatly into the old paradigm.[62]

¶23 Another more obvious shortcoming exists: since most companies do provide consumers with some form of notice and choice, technically the torts would not apply because the consumer had "notice" and therefore had no expectation of privacy, or because the consumer had provided their "consent" to the companies' practices.[63] However, as argued throughout, this notice and consent in almost all cases is severely deficient due to the Incognito and Onward Transfer Problems. As a result of the privacy torts' general inadequacies, commentators have called for reform of the privacy torts in order to better address information privacy issues in the modern age.[64]

Data Profiling, 98 NW. U. L. REV. 63 (2003).

[59] Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1919-20 (2010).

[60] *Id.*

[61] Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 46 (2007).

[62] *Id.*

[63] *See, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995) (ruling that the plaintiffs failed to successfully allege the tort of invasion of seclusion because they voluntarily provided spending information to American Express through use of the American Express card, which American Express was then free to disclose to third parties in connection with marketing activities, despite the plaintiff's additional claim of appropriation); *see also* Shibley v. Time, Inc., 341 N.E.2d 337 (Ohio Ct. App. 1975) (reaching a similar conclusion on the tort of appropriation claim because the tort of appropriation is only available if a person's name or likeness is publicly displayed to indicate the person endorses a particular product or service. In this case, Time was selling its subscription lists to direct mail advertising businesses).

[64] *See* Abril, *supra* note 61; Richards & Solove, *supra* note 59; *see also* Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. (2011) (arguing that the traditional privacy torts, in addition to being ineffective in the modern age, in some cases also conflict with First Amendment doctrines, and suggesting other tort doctrines, such as trespass and confidentiality, as possible remedies to today's privacy issues); Lior Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007 (2010) (arguing that the privacy tort categories should be abandoned and replaced with a unitary tort for invasion of privacy); Jessica Litman, *Information Privacy/Information Property*, 52 STAN. L. REV. 1283 (2000) (proposing as a partial solution to the privacy torts' inadequacies reliance on the tort of breach of confidentiality); Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140 (2007) (advocating creation of a common law tort based on Fair Information Practices).

¶24 State contract law could also be a source of information privacy protection. Eugene Volokh has raised this possibility.[65] However, this solution is implausible for several reasons. First, unless companies voluntarily addressed the Incognito and Onward Transfer Problems in contracts with consumers,[66] then those problems would remain unaddressed. Furthermore, even if solutions to these problems were adopted as the default rules, freedom of contract would allow companies to disclaim them, which they almost undoubtedly would.[67] Lastly, damages under contract law are generally limited to economic losses flowing directly from the breach.[68] Because privacy harms are often difficult to measure in terms of direct economic losses, contract law would provide consumers with insufficient remedies for information privacy violations.

D. Self-Regulation

¶25 In addition to federal and state law, industry self-regulation is a significant part of the U.S. approach to information privacy. Because consumers have become increasingly wary of providing their personal information to companies for fear of theft, misuse, or, simply, the unknown, many companies have responded by developing and adopting privacy "best practices," joining privacy "seal" programs such as TrustE,[69] or joining privacy alliances such as the Online Privacy Alliance.[70]

¶26 In general, such best practices require companies to provide consumers with notice regarding what information the company collects, how the company will use it, and the types of third parties with which the company will share this information.[71] Furthermore, if the company wishes to disclose personal information to third parties for purposes other than for which the company collected the information, the company should provide the consumer with a choice regarding such disclosure in the form of an opt-in or opt-out.[72]

¶27 Two drawbacks to the self-regulation approach immediately become obvious, however: adequacy and enforcement. That is, given companies' self-interest in retaining flexibility with respect to the consumer information, it is doubtful that a self-regulatory approach gives companies the right set of incentives to provide consumers with adequate protection and control.[73] Furthermore, the self-regulation approach relies primarily on

---

[65] Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You*, 52 STAN. L. REV. 1049 (2000).

[66] One commentator notes that online companies often incorporate their privacy notices into their terms of use, and therefore the privacy notice becomes part of a contract between the consumer and company. Otherwise courts have typically not found privacy notices to be enforceable contracts. However, companies typically will construct privacy notices to favor themselves, and so the incorporation of the privacy notice into the enforceable terms of use is not generally beneficial to consumers. *See* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN ST. L. REV. 587 (2007).

[67] *See* Volokh, *supra* note 65, at 1061-62.

[68] *In re* Jetblue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299 (E.D.N.Y. 2005) (holding that a well-settled principle of contract law is that only economic damages are available for breaches of contract, and in the instant case the only damages that the plaintiff suffered were non-economic privacy harms).

[69] *See generally* TRUSTE, http://www.truste.com/ (last visited Jan. 9, 2013).

[70] *See generally* PRIVACYALLIANCE.ORG, http://www.privacyalliance.org/ (last visited Jan. 9, 2013).

[71] *See Protecting Customer Information Online*, TRUSTE, http://www.truste.com/why_TRUSTe_privacy_services/privacy_best_practices (last visited July 12, 2012).

[72] *Id.*

[73] *See* Ira Rubinstein, *Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes*, 6 I/S, J.L. & POL'Y FOR INFO. SOC'Y 356-57 (2011) (noting the many deficiencies of the self-regulation model,

companies regulating their own behavior,[74] although the FTC's enforcement activities under the FTC Act help ensure that companies at least adhere to their stated privacy practices.[75]

¶28 But even if companies do abide by these so-called "best practices," such best practices still suffer from the Incognito and Onward Transfer Problems. A best practice from the consumer's point of view—and from the perspective of privacy as information control—would include consumers receiving notice and choice regarding who specifically is receiving their information and how that company will use it, rather than merely a general notice that unidentified third parties may in the future receive and use their personal information in manners similarly unknown. As with the other pieces of the U.S. regime, self-regulation provides consumers with little real control over their personal information.[76]

E. The U.S. Department of Commerce Safe Harbor

¶29 E.U. law has also influenced U.S. consumer privacy law and, therefore, provides an additional source of information privacy regulation in the U.S. The E.U. has implemented comprehensive privacy regulation pursuant to the E.U. Data Protection Directive (95/46/EC) (the "Directive"). Under the Directive, the E.U. has deemed that U.S. law provides "inadequate" protection of consumer data, and thus forbids transfers of such data from the E.U. to the U.S. absent an exception.[77] As one such exception, the U.S. Department of Commerce, together with the European Commission, has developed a safe harbor framework.[78] Under the safe harbor framework, U.S. companies, by adhering to certain information privacy principles, can self-certify that they provide "adequate" privacy protections sufficient to permit a transfer of data under the Directive.[79]

¶30 One of the Directive's principles, "Onward Transfer", requires certifying companies to provide notice and choice before disclosing information to third parties.[80] In addition, where a certifying company wishes to transfer information to a third party acting as its agent, it must either ascertain that the third party subscribes to the same principles, is subject to the Directive, qualifies for another adequacy finding, or enter into

---

including weak enforcement and free rider issues); Michael Froomkin, *The Death of Privacy*?, 52 STAN. L. REV. 1461, 1524-27 (2000) (suggesting the self-regulation model is a chimera whose real purpose is to avoid government regulation).

[74] *Id.*

[75] *See supra* Part I.B.

[76] For a poignant recent example of why self-regulation is severely deficient, see Nicole Perlroth & Nick Bilton, *Mobile Apps Take Data Without Permission*, N.Y. TIMES TECH. BLOG (Feb. 15, 2012, 10:09 PM), http://bits.blogs.nytimes.com/2012/02/15/google-and-mobile-apps-take-data-books-without-permission/ (discussing a maelstrom of consumer outrage over an alleged industry "best practice" of mobile application companies taking sensitive address book information from smartphones without consumers' notice or consent).

[77] *U.S.-EU Safe Harbor Overview*, EXPORT.GOV, http://export.gov/safeharbor/eu/eg_main_018476.asp (last updated Apr. 26, 2012).

[78] *Id.*

[79] *Id.*

[80] *Safe Harbor Privacy Principles*, EXPORT.GOV, http://www.export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 30, 2009).

a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as the principles require.[81]

¶31 The safe harbor thus only applies to the certifying company and, with the exception of third parties acting as "agents," does not require the certifying entity to impose any controls on third parties obtaining information from them. The Onward Transfer Problem thus persists. And, even though participating companies must provide notice and choice, this notice and choice suffers from the same Incognito Problem: blanket opt-in/opt-out without identification of the specific third parties or their specific uses.

¶32 Furthermore, even if a savvy consumer was aware of a company's self-certification and became aware that such company had violated the principles, that consumer would have no recourse. They would be solely dependent on the Department of Commerce to police the company. And even if the Department of Commerce had the resources to police companies and enforce these principles in all cases, they could only do so against those companies that wished to transfer consumer data between the U.S. and the E.U. and which had self-certified. Consequently, though the safe harbor provides greater consumer information privacy protection than would likely exist without it, it still falls short in addressing the Incognito and Onward Transfer Problems.

III. SO WHAT'S THE HARM?

¶33 So far this Article has shown that in most cases U.S. consumers have little real knowledge or choice about which specific third parties may have their information and how those third parties will use and further disclose such information. These Incognito and Onward Transfer Problems effectively undermine any real consumer control over their information. Arguably, however, these Problems only need redress if consumers are suffering significant harm as a result. The next section addresses this issue.

A. Addressing Privacy Harm Skepticism

¶34 Some have downplayed the concept of privacy harm in general.[82] Richard Posner claims that "as long as people do not expect that the details of their health, love life, finances, and so forth, will be used to harm them in their interactions with other people, they are content to reveal those details to strangers . . ." because Americans have become "habituated . . . to radically diminished information privacy."[83] Others contend that whatever minimal privacy harm that may result from privacy violations is offset by the benefits of the free flow of information, including economic advantage to consumers in

[81] *Id.*

[82] *See, e.g.*, Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978) (indicating that in most cases people want privacy solely in order to be able to conceal discreditable information about themselves, rather than due to legitimate privacy harms they are suffering); Jonathan Franzen, *How to Be Alone: Essays* 42, 45-46 (2003) (indicating that Americans only care about privacy in the abstract); Juliana Gruenwald, *Lawmakers Tangle Over Consumer Harm From Lack of Privacy Rules*, NATIONALJOURNAL.COM (May 9, 2012, 5:24 PM), http://www.nationaljournal.com/tech/lawmakers-tangle-over-consumer-harm-from-lack-of-privacy-rules-20120509 (reporting on a legislative debate between Senators John Kerry and Pat Toomey in which Senator Toomey remains skeptical that consumers are experiencing privacy harm through data collection and use).

[83] Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 249-51 (2008).

the form of more relevant advertising, cheaper products, and expedited services.[84] Courts also have been reluctant to award damages for privacy harm without something more specific or "actual" than abstract claims of mental injury.[85]

¶35 Others have argued that if consumers continue to disclose their information to companies in exchange for those companies' goods and services, and fail to take advantage of technological, legal, and other solutions available to them, arguably whatever privacy harms consumers may be experiencing are offset by the perceived benefits; otherwise consumers would change their behavior.[86] Some evidence suggests consumers are willing to sell their personal information to companies quite cheaply.[87] Thus, though seemingly all available consumer surveys suggest consumers are worried about their information privacy,[88] according to this line of argument they are obviously not that worried.

¶36 However, simply because consumers may have become habituated to decreased information privacy does not mean that they do not experience privacy harms. As Posner himself notes, it is virtually impossible to participate in the modern world without disclosing vast amounts of information about oneself to third parties.[89] Thus, rather than a conscious choice by consumers, the tradeoff between decreased information privacy and the benefits of disclosure in many cases seems to be something to which consumers have simply become resigned.[90] Viewed in this light, decreased information privacy

---

[84] *See, e.g.*, Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000) (arguing that the free flow of information is not only a vital part of a democratic society, but also benefits consumers in the form of faster and better services and products); Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, 2000 STAN. TECH. L. REV. 2, 39, 46, 48 (2000) (making similar claims as Cate).

[85] M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1132, 1132 n.2 (2011); *see also* Doe v. Chao, 540 U.S. 614 (2004) (holding that in order to qualify for statutory damages for violations of the Privacy Act of 1974, plaintiffs must show more evidence of actual harm than simply conclusory allegations of distress). As discussed in *supra* Part I.C.2, this reluctance of the courts to recognize privacy harm is yet another reason to doubt the efficacy of privacy torts (at least in their current form) in helping address the issues raised in this Article.

[86] *See, e.g.*, Eric Goldman, *The Privacy Hoax*, FORBES (Oct. 14, 2002), *available at* http://www.forbes.com/forbes/2002/1014/042.html (arguing along these lines that consumers do not seem to care about their online privacy, and so privacy regulation is unnecessary).

[87] *Id.*

[88] *See, e.g.,* Allison Enright, *Consumers Worry About Online Privacy, but Shop Anyway*, INTERNET RETAILER (May 11, 2012, 1:30 PM), http://www.internetretailer.com/2012/05/11/consumers-worry-about-online-privacy-shop-anyway; Alex Palmer, *Report: 90% of Consumers Worry About Online Privacy*, DIRECT MARKETING NEWS (Feb. 10, 2012), http://www.dmnews.com/report-90-of-consumers-worry-about-online-privacy/article/227373/; Mary Beth Quirk, *Consumer Reports Survey Confirms That We're Worried About Online Privacy*, THE CONSUMERIST (Apr. 3, 2012, 5:00 PM), http://consumerist.com/2012/04/consumer-reports-survey-confirms-that-were-worried-about-online-privacy.html; Janet Jaiswal, *Survey Results Are In: Consumers Say Privacy is a Bigger Concern Than Security on Smartphones*, TRUSTE BLOG (Apr. 27, 2011), http://www.truste.com/blog/2011/04/27/survey-results-are-in-consumers-say-privacy-is-a-bigger-concern-than-security-on-smartphones/.

[89] *See* Posner, *supra* note 83.

[90] This sense of consumer helplessness is what Daniel J. Solove identifies as the primary privacy problem resulting from computer databases. *See* Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); *see also* Turow, *supra* note 14 (indicating that the majority of consumers feel like they have lost all control over how companies use and collect their personal information).

might be considered a negative externality that companies impose on consumers rather than internalizing it themselves.[91]

¶37 Furthermore, the failure of the average consumer to take advantage of technological and other means of protecting their information privacy is not surprising. The average consumer is not a technologist and so is typically unaware of software programs, browser settings, and other means of protecting their privacy.[92] Or even if they do know about them, generally they do not know how to use them.[93] Because consumers generally do not read privacy notices or pay much attention to them, the fact that they do not scrutinize companies' practices and proactively protect their privacy is also not surprising.[94] The Incognito and Onward Transfer Problems suggest that even if they did, they would still not have control over their information, at least with respect to third-party disclosures. These realities thus should not be read as evidence that consumers avoid significant privacy harms in the current piecemeal privacy regime, or that they do not care much about privacy in general. Seemingly all available surveys suggest otherwise.[95] More likely, these realities may simply mean that the average consumer feels helpless with respect to their information privacy and the privacy harms that they experience.[96]

B. Defining the Harm

¶38 Ryan Calo recently grouped privacy harms into two categories that are helpful in defining the nature of this harm more clearly: subjective and objective privacy harm.[97] Subjective privacy harm may result from a perception of unwanted observation or surveillance,[98] or simply from an utter feeling of helplessness or lack of control over information about oneself.[99] For example, as consumers become increasingly aware of companies creating databases of information about them (or even, simply, perceive that such may be a possibility), subjective privacy harm may result due to anxieties associated with these activities.[100] This discomfort may grow as consumers become more aware of

---

[91] *Opting In Opting Out*, *supra* note 11, at 1116.

[92] *See* DEP'T FOR CULTURE, MEDIA, & SPORT, RESEARCH INTO CONSUMER UNDERSTANDING AND MANAGEMENT OF INTERNET COOKIES AND THE POTENTIAL IMPACT OF THE EU ELECTRONIC COMMUNICATIONS FRAMEWORK 2-3 (Apr. 2011), *available at* http://www.culture.gov.uk/images/consultations/PwC_Internet_Cookies_final.pdf (U.K. study indicating that 85% of respondents were unaware of internet cookie "opt-out" solutions, and only 9% of respondents were aware of the possibility of anonymous browsing).

[93] *Id.* (indicating that the majority of survey respondents had very limited understanding of internet cookies and how they work).

[94] Jeff Sovern argues that companies often purposefully impose significant transactions costs on consumers to make it less likely that consumers will exercise whatever choices they may have. *Opting In Opting Out*, *supra* note 11. *See also* Turow, *supra* note 14 (study suggesting that most consumers mistake the existence of a privacy policy as evidence that a company cannot share the consumer's information without their consent).

[95] See *supra* note 88 for a sampling. *See also* DEP'T FOR CULTURE, *supra* note 92, at 2 (indicating that 75% of survey respondents were concerned with the abuse of personal information sent over the Internet).

[96] *See* Turow, *supra* note 14.

[97] Calo, *supra* note 85.

[98] *Id.*

[99] Solove, *supra* note 90, at 1421 (arguing that the privacy harm resulting from the collection and use of personal information as part of computer databases is best understood as a form of powerlessness without meaningful consumer participation).

[100] Calo, *supra* note 85; *see also* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 489-

companies routinely sharing their information with the government for surveillance and law enforcement purposes.[101] Such discomfort may cause the consumer to alter their behavior in meaningful ways, resulting in a form of social control that potentially inhibits freedom and personal autonomy.[102] This form of harm was one of the motivations behind the Privacy Act of 1974, which regulates the government's collection, use, and disclosure of information about its citizens.[103]

¶39 Objective privacy harm may follow when that same information is used against the consumer in an unexpected, forced manner.[104] Identity theft, wrongful disclosure of information that results in damage to a consumer's financial reputation, blackmail, or a widespread data security breach are all examples of this type of objective privacy harm.[105] Unwanted spam, junk mail, solicitations, and other undesired contacts can also be viewed as a form of this privacy harm since they often cause consumers to waste significant amounts of time and money protecting against such activities. This form of privacy harm was also one of the motivations behind the Privacy Act of 1974.[106]

¶40 The Incognito and Onward Transfer Problems play a crucial role in causing both types of harms. Indeed, as consumers become increasingly aware through media reports or otherwise about the vast amounts of information companies are gathering and sharing with others,[107] subjective privacy harm becomes more likely because consumers are completely helpless to stop the exchanges. While some consumers may not give any thought to these issues, many do, and so subjective privacy harm may result for people more worried about information privacy issues.[108] Ignorance may be bliss for some, but

---

91 (2006) (categorizing harmful privacy activities into four distinct categories that, though not categorized in this "subjective" v. "objective" dichotomy, identify many of the same harms).

[101] *See* Christopher Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595 (2004) (indicating that government has access to large amounts of personal information on consumers through commercial data brokers); *see also* The Att'y Gen.'s Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations § VI (May 30, 2002) (indicating that the FBI is permitted to obtain information for surveillance purposes "through services or resources (whether nonprofit or commercial) that compile or analyze such information; and information voluntarily provided by private entities").

[102] Solove, *supra* note 100, at 493-94; *see also* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1260 (1998) (claiming that surveillance activities lead to self-censorship). Some may counter that consumers are not experiencing significant subjective privacy harm given that they do not seem to alter their online behavior in response to privacy concerns. *But see supra* notes 89-96 and accompanying text for a discussion of this point. Furthermore, it is difficult to prove that consumers do not alter their behavior in response to privacy concerns. While many consumers continue to shop online, perhaps many more would if their privacy concerns were allayed, or even the ones that do shop would shop more. Furthermore, consumers may find shopping online at, say, Amazon.com, relatively safe, while avoiding other less well-known sites. Indeed, it seems more logical to conclude that if consumers repeatedly indicate that they are concerned with their information privacy, that they do alter their behavior in a variety of ways that, collectively, may be significant.

[103] *See* Elec. Privacy Info. Ctr., *The Privacy Act of 1974*, EPIC.ORG, http://epic.org/privacy/1974act/ (last visited July 27, 2012).

[104] *See* Calo, *supra* note 85, at 1148.

[105] *See* Calo, *supra* note 85 at 1147-52; Solove, *supra* note 100, at 532-48.

[106] *See* Elec. Privacy Info. Ctr., *supra* note 103.

[107] For a recent example of one such media report that caused panic among consumers, see Perlroth & Bilton, *supra* note 76.

[108] It may be argued that such types of people are precisely those who will diligently exercise control over their information, thereby limiting subjective privacy harm. However, because of the Incognito and Onward Transfer Problems, even when exercising whatever choices they may have, in some cases such

for others it may be the cause of anxiety that results in undesirable distortions to their behavior.

¶41 As more and more third parties have access to the consumer's information, the likelihood of objective harm occurring also increases. The more third parties that have the consumer's information, the more likely it becomes that the consumer will receive unwanted contacts or be subjected to a harmful external action. Though the current notice and choice regime may in the first instance help limit the likelihood of objective harm because consumers can prevent some disclosures if they are scrupulous,[109] once information is disclosed to third parties, those third parties have no obligation, except in limited circumstances, to provide choice regarding how they will use and further disclose the consumer's information. Aside from failing to provide consumers with this secondary layer of notice and choice, such third parties may also use insufficient data security measures.[110] Thus, once a consumer's information is beyond the first set of limited hurdles, it is impossible to determine where that information may end up. One of the destinations could very well be in the hands of persons that use it against the consumer in an objectively harmful manner. Or, it could end up with third parties that employ lax data security standards, which itself increases the likelihood of objective privacy harm.

C. A (Not-So) Hypothetical John Doe

¶42 A thought experiment helps illustrate these types of privacy harms more clearly. Assume John Doe is a 30-year old male living in Palo Alto, California, working as an engineer for a start-up company. The minute John wakes up, and until he goes to sleep, an army of information collectors takes notes of his movements, activities, and preferences. These details are combined with other sources of data previously collected about John. Some of this data collection is done with John's "consent," but even in those cases, John typically is not fully aware of the nature and extent of the collection, even in the few cases where he bothered to read through the collector's notice about its practices (if provided). Where he likes to eat, where he was throughout the day, his favorite hobbies, the types of books he reads,[111] among other intimate details about John, are collected and stored into a comprehensive profile.

---

consumers' information will still be legitimately shared with unidentified third parties. And once in those third parties' hands, the consumer's ability to control their information is mostly at an end.

[109] *But see supra* notes 89-96 and accompanying text for reasons why most consumers are not scrupulous in protecting their information privacy.

[110] It may be reasonable to believe that companies that legally receive information from consumers will put in place contracts with additional third parties with which they share their consumers' information. Even if that is true in most cases, the point remains that in such scenarios consumers have no control over their information and must rely on a third party enforcing whatever contractual standards the initial third party is able to negotiate with the additional third parties.

[111] California recently passed legislation that prohibits providers of book services from disclosing to government or private entities or persons certain personal information relating to users of book services, including information relating to the person's reading preferences, subject to certain exceptions. One of the exceptions occurs if users have given their consent to the specific disclosure for a particular purpose. *See* S.B. 602, 2011 Leg., Reg. Sess. (Ca. 2011); Elec. Frontier Found., *Reader Privacy Act of 2011* (Apr. 5, 2011), https://www.eff.org/cases/sb-602-californias-reader-privacy-act-2011. However, arguably a general opt-in/opt-out choice would satisfy this requirement. Furthermore, this law only applies to California.

¶43 The data collectors then share his profile with third parties (through sale, license, or otherwise), who similarly may combine such data with preexisting sets of information they have about John. Again, in some cases this sharing is done with John's "consent," although, again, even in cases of consent John does not know what specific third parties will receive his information, how specifically they will use it, and to which other third parties they may further disclose his information. These third parties then use the information for their own purposes and similarly pass the information along to other third parties, who are under no direct obligations to John.[112]

¶44 John is often oblivious to these information collectors and the other third parties that receive his information. However, he increasingly hears stories about them and their activities, and this mere knowledge causes him some unease. Often an information collector will approach him out of nowhere and offer him something. Sometimes someone approaches him that he recognizes, but at other times he is completely unfamiliar with the person approaching him, and he wonders how that person knows his name or anything about him. Sometimes these approaches are mere annoyances, and occasionally he is approached with something that actually interests him, but at other times the approach causes him real concern because of the nature of the party approaching him and the information they seem to possess about him. As a result, John begins to alter his behavior. He avoids some of his previously favorite haunts because he has experienced some of the more distressing encounters there. He even begins to go out and socialize less, wary of who he might encounter and what others may know about him.[113]

¶45 At some point a third party burglarizes John's home. The third party was able to case John's home and successfully burglarize it through information it had obtained about him from the information market. Later, a new website called "Consumerleaks," styled after Wikileaks, posts some embarrassing information about him that causes John to lose his job. Again, the information was obtained through the information market.

¶46 The above examples describe much of what happens in the market today.[114] Whether it be through online browsing, shopping (online or offline), social networking, photo sharing, smartphones, geolocation tracking, WiFi hotspot data collection, or offline collection, companies constantly collect information about consumers, combine it with other sources into databases, and exchange it with third parties.[115] And they often do these things with notice to consumers and the consumer's "consent." In some cases consumers can simply choose not to use third party services or buy their goods and thereby avoid disclosing information to them, but in the modern world complete

[112] *Cf.* Posner, *supra* note 83, at 247-49. The hypothetical described here mirrors the reality of modern society as Posner describes it, even though Posner remains a privacy harm skeptic.

[113] Some may argue that the analogy above fails because in the real world, these information collectors are typically simply technologies employed by third parties that lack a human face. The examples above, with their human collectors, seem much more invasive and thus potentially overstate the harm. This criticism may be relevant to subjective privacy harm. That is, if the shadowy information collectors were replaced with robots, tracked persons may feel less anxiety knowing that it is not another human being that is actively processing and using their data, at least in a personal way. However, the subjective privacy harm still exists since the level of anxiety is strongly related to the possibility of objective privacy harm, which this criticism does nothing to undermine. Consequently, both types of harm remain relevant.

[114] *See* Posner, *supra* note 83, at 248.

[115] *See* Solove, *supra* note 90, at 1047-09 (highlighting the extent to which companies create information dossiers of consumers).

abstinence is virtually impossible.[116] In other cases, consumers may be able to opt-out of data sharing (or simply not opt-in). But often the notice regarding data sharing is buried so deeply within a privacy notice, and in language so vague as to be meaningless, that the consumer has very little chance to avoid this result, especially if it is a service or good that the person wants or needs urgently.[117]

¶47 A system of information collection and subsequent data exchange as described above would cause at least some people to experience unease and anxiety[118]—subjective privacy harm—which could cause them to alter their behavior and thereby undermine personal autonomy. Some, of course, argue that the anxiety caused is not significant enough to merit redress, and that the economic advantages of the free flow of information far outweigh any such harms,[119] but at least two additional responses seem warranted: (1) while it is possible that for many people the information collection and third-party disclosures will not cause significant anxiety or lead to altered behavior, it seems clear that some do experience anxiety as a result, as all available surveys suggest, and (2) it is unclear why the default rules should allow companies to cause that anxiety, whatever the level may be and even if the number of people affected is only a minority of the population.[120]

¶48 Posner and others offer economic justifications for the default rules being as they are: the benefits of the free flow of information outweigh the, in their view, unsubstantial privacy harms that consumers may experience. However, the economic argument can also go the other way: economic activity, such as online shopping, may increase if consumers felt more secure with disclosing sensitive information into the data exchange ether. Indeed, at least some studies suggest consumers place a significant economic value on privacy.[121]

¶49 Aside from the subjective privacy harm, the objective privacy harm also seems clear. The more information about John that companies collect and disburse to unidentified third parties, the more likely it becomes that the information will fall into the wrong hands and be used for reasons with which John does not agree. Instances of such

---

[116] *See* Posner, *supra* note 83, at 247-49.

[117] Several provisions from J.CREW's privacy notice illustrate this point: "When you supply your postal address, either when requesting a catalog or placing an order, you may receive catalogs by mail from us. We also occasionally make our postal list available for limited use by unaffiliated third parties . . . . We may also share your information, including, without limitation, your email address (but not your credit card information) with unaffiliated third parties that would enable them to contact you about products or services you may be interested in." *See J.Crew Privacy Policy*, J.CREW, http://www.jcrew.com/footer/privacy.jsp (last visited Sept. 13, 2011).

[118] *See* sources cited *supra* note 88.

[119] *See, e.g.*, *supra* note 84 and accompanying text.

[120] Indeed, laws against, say, armed robbery, are not wrong simply because a minority of the population is ever affected (thankfully). I am not trying to equate subjective privacy harm with armed robbery, but the point is that simply because only some will experience some harm absent regulation is not good reason to rule out the regulation, especially if the harm can be addressed without significant negative impacts.

[121] *See, e.g.*, Janice Tsai, Serge Egelman, Lorrie Cranor, & Alessandro Acquisti, *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, at 15–17 (2007), *available at* http://weis2007.econinfosec.org/papers/57.pdf (indicating that consumers were willing to pay up to 4% more on average for products and services if they were certain that their information privacy was being protected). *See also,* Turow, *supra* note 14, at 20–26 (study suggesting that consumers are concerned about information collection and distribution practices of companies, and in large part disfavor many of the standard tracking practices that companies employ today, including the "benefit" of targeted advertising).

misuses that cause significant harm such as identity theft may be far and few between, but they can and do happen, and increasingly so.[122]

IV. THE PROPOSAL

¶50 The realities of the current system are less than inspiring. Except in a few limited cases,[123] consumers remain without specific information about what third parties have their information, how such third parties will use it, and whether they might share it with additional third parties. And once those additional third parties have the consumer's information, they are almost entirely unaccountable to the consumer.[124] Eventually, consumers may become aware of who, in fact, does have their information through an array of marketing or other contacts (in a worst case scenario identity theft), but they remain in the dark about how those third parties received their information in the first place and how they may otherwise use the information. Furthermore, they have no legal means to force the third party to disgorge their information or prevent further disclosure. This scenario hardly inspires confidence.

¶51 As a possible solution to the Incognito and Onward Transfer Problems, this Article explores the possible benefits and potential drawbacks of a federal law that would require companies to provide notice and choice to consumers that describes the intended third party recipients and their uses, as well as providing consumers with a private right of action to protect their privacy interests under the law. This examination is particularly relevant as Congress continues to explore privacy legislation addressing similar issues.[125] It is hoped that this exploration will provide some guidance on these and similar information privacy issues.

A. Definitions

¶52 Before proceeding to the proposed law's requirements, a few key definitions are necessary.

---

[122] Instances of identity theft have been on the rise for years. *See, e.g.*, Bureau of Justice Statistics, *Identity Theft Reported by Households Rose 33 Percent from 2005 to 2010*, http://bjs.gov/content/pub/press/itrh0510pr.cfm (last updated Jul. 13, 2012). This is not to say that all or even a majority of instances of identity theft originate with information that consumers have provided to companies. However, at least some instances of identity theft may result from companies' data security breaches, which become more likely the more information that companies store and exchange. *See Threat Activity Trends*, SYMANTEC, http://www.symantec.com/threatreport/topic.jsp?id=threat_activity_trends&aid=data_breaches (last visited Jul. 13, 2012) (suggesting data breaches pose a significant risk of identity theft).

[123] For instance, with respect to protected health information under HIPAA, see *supra* Part I.A.

[124] Some laws may still impact such third parties depending on the third parties' activities. For instance, if the third party sends the consumer a "commercial email," the CAN-SPAM Act would apply to the company, subjecting it to several requirements under the law. *See* Fed. Trade Comm'n, *CAN-SPAM Act: A Compliance Guide for Business* (Sept. 2009), http://business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business/.

[125] *See* sources cited *supra* note 15.

1. Personally Identifiable Information

¶53 The proposed law should only apply to personally identifiable information (PII) that companies collect and propose to disclose to third parties, and not aggregate, anonymized information (non-PII). It excludes the latter for several reasons. First, it is not clear that third parties could easily use non-PII to cause consumers objective privacy harm.[126] The possibility of re-identification may suggest that non-PII should be regulated in some manner.[127] But because the risk of objective privacy harm is more remote with non-PII, arguably the manner in which non-PII is regulated should differ from how PII is regulated.[128]

¶54 Second, although disclosures of non-PII could still result in some subjective privacy harm for consumers who are simply anxious about any sort of collection and disclosure, arguably this type of harm is unavoidable and results more from the extreme sensitivities of a few than a legitimate issue needing redress. Indeed, for subjective privacy harm to be legitimate, objective privacy harm must also be a strong possibility. Since with non-PII objective harm is less likely,[129] arguably little rational subjective privacy harm exists in cases of non-PII disclosure. This discussion also helps define non-PII: information that cannot generally or easily be reverse engineered or otherwise linked back to individuals.

¶55 What constitutes PII is not a straightforward issue. For instance, the E.U. Directive defines "personal data" quite broadly, in a manner that may include information that a company would not be able to use to actually identify a person:

> '[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification

[126] Some have argued that true anonymization is impossible, so we should not treat non-PII any differently than PII. *See, e.g.,* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010). *Contra* Jane Yakowitz, *Tragedy of the Data Commons*, 25 HARV. J. L. & TECH. 1 (2011) (arguing that the risks of re-identifying previously anonymous information are much more remote than many believe, and that the examples Ohm used in his article were much more limited than his analysis suggested); *see also* Ann Cavoukian & Khaled El Emam, *Dispelling the Myths Surrounding De-Identification: Anonymization Remains a Strong Tool for Protecting Privacy* (June 2011), *available at* http://www.futureofprivacy.org/wp-content/uploads/2011/07/Dispelling%20the%20Myths%20Surrounding%20De-identification%20Anonymization%20Remains%20a%20Strong%20Tool%20for%20Protecting%20Privacy.pdf (arguing that the risks of re-identification are greatly overblown so long as companies take proper de-identification precautions).

[127] Paul Schwartz and Daniel Solove recently articulated a concept of PII 2.0, under which they propose three different categories of information, each of which they believe the government should regulate differently. Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814 (2011). Their categories are: information that refers to (1) an identified person, (2) an identifiable person, and (3) a non-identifiable person. *Id.* My proposed definition of PII would fall within their first category. Under this Article's proposal, their second category of information referring to an identifiable person would fall within my non-PII category since the risk of re-identification for such information is minimal. It is beyond the scope of this Article to address how such information should be regulated, if at all.

[128] *Id*. Solove and Schwartz do in fact argue that the two should be regulated differently. *Id.* at 1877.

[129] *See* Yakowitz, *supra* note 126.

> number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[130]

¶56 Under one interpretation of this definition, it may not even be necessary to be able to identify the person from the related information, so long as the information is related to an identifiable person in some way. For purposes of this proposal and its intent—to address privacy harm—this definition is too broad.

¶57 Other laws, such as the California Data Security Breach Act, define personal information as the name of an individual in combination with one of a number of other types of sensitive information (e.g., credit card number).[131] For purposes of this proposal, this definition is too limited. This type of definition seems primarily concerned with addressing certain forms of objective privacy harm (e.g., identity theft). However, this proposal seeks to address all forms of objective privacy harm as well as limiting subjective privacy harm, since the presence of legitimate, reasonable subjective privacy harm increases the likelihood that objective privacy harm will follow.

¶58 This proposal, therefore, takes a position in between these two extremes and defines PII similarly to how the U.S. Executive Branch has defined it:

> [I]nformation which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.[132]

¶59 This definition has the advantage of avoiding the excessive breadth of the E.U. definition, remaining consistent with how other important players in the U.S. already define PII, while achieving the definition's primary goal: to limit the law's application to that information that is linked or could readily be linked to an identifiable person.[133] As scoped, the definition thus focuses the model law on the two forms of privacy harm discussed herein.

2. Disclosure to Third Parties

¶60 Not all PII disclosures to third parties should trigger the law's application. For instance, the law should not apply to government actors seeking PII as part of an investigation. The standards of the Fourth Amendment and laws such as the Electronic

---

[130] Council Directive 95/46/EC, art. 2, 1995 O.J. (L 281) 38.

[131] James F. Brelsford, *California Raises the Bar on Data Security and Privacy*, FINDLAW (2003), *available at* http://library.findlaw.com/2003/Sep/30/133060.html.

[132] Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, for the Heads of Executive Departments and Agencies, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* 1 n. 1 (May 22, 2007), *available at* http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf; *see also* U.S. DEP'T OF COMMERCE, OFFICE OF THE CHIEF INFO. OFFICER, *Electronic Transmission of PII Policy*, (Jul. 30, 2009), *available at* http://ocio.os.doc.gov/ITPolicyandPrograms/IT_Privacy/PROD01_008240#P46_1812.

[133] *See* Schwartz & Solove, *supra* note 127, at 1829 (according with Solove and Schwartz's first category of information regulation: the tautological approach).

Communications Privacy Act would apply in those cases.[134] In the commercial context, if companies disclose PII to third parties that perform services solely on behalf of the company—and which do not use the PII for their own purposes or for purposes other than for which the information was originally collected—the law should not apply to that disclosure.[135] The law should only apply if the company disclosed the PII to the third party for a secondary use of the information: a use beyond the purposes for which the individual provided the PII.[136]

¶61 Consequently, if a consumer submitted PII to a company, and the submission was made for the purpose of disclosure to and use by specific third parties, then the law should not apply. However, if a consumer submitted PII to a company for a specific purpose, and the company disclosed that information to a third party to process it solely on its behalf (i.e., not for the third party's own use), but for a use other than the reason the consumer initially submitted the PII, then the law should apply.

¶62 This limitation is important in order to avoid interrupting the flow of information necessary to achieve the consumer's purposes in disclosing their PII in the first place. Hence, so long as the company discloses the PII in order to satisfy the consumer's wishes, the law should not apply. Once companies begin to disclose the PII for purposes other than the original purpose of disclosure, the law should apply.

¶63 This definition helps address privacy harms in several ways. First, subjective privacy harm would likely decrease since consumers would feel reassured that companies were only disclosing their PII for the consumer's purposes, and not those of the company or unrelated third parties (unless notice and choice had been provided, as discussed below). Second, objective privacy harm would likely decrease because fewer third parties would be PII recipients in this system.[137]

B. The Mechanics

¶64 The law would require the following elements: specific notice of intended third party recipients and their proposed uses prior to disclosure, choice, and a private right of action to enforce the law. Each of these elements is discussed more fully below, including addressing common criticisms of each.

---

[134] *See generally* SOLOVE & SCHWARTZ, *supra* note 22, at 247–376, for an overview of such standards.

[135] Whether the law would apply to subsidiaries and affiliates of a company is a difficult question. For instance, a consumer disclosing information to Amazon.com, Inc. may be surprised to learn that Zappos.com is a wholly owned subsidiary of Amazon.com, Inc. and therefore may not expect their information to be in the hands of Zappos.com. One approach might be to carve out affiliated companies from the law's effects, similar to the GLBA. However, doing so arguably violates the principle of no secondary uses, as well as still posing similar privacy harms. Consequently, this proposal does not advocate such an approach. Another approach might be simply to grant companies some additional leeway in how they share information with affiliated companies. This proposal does not address such possibilities, and instead relies on the "no secondary use" principle discussed *infra* note 136 and accompanying text.

[136] This limitation accords with generally accepted Fair Information Practice Principles. *See* FED. TRADE COMM'N, *supra* note 4.

[137] This may not be the result if the notice and choice, as discussed below, proved to be as deficient as provided for in the current system, or if consumers simply elected to make their information as available as in the current system. The latter result is consumers' choice (though it seems unlikely), and the former only results if the proposal has fatal flaws.

1. Notice

¶65 Currently only a few states require privacy notices by law.[138] Although most major companies do develop and post privacy notices,[139] they typically do so in order to protect themselves. That is, companies' privacy notices provide information in very general terms, and doing so technically puts consumers on notice and makes the company a "good citizen." However, as discussed throughout, this notice is severely deficient with respect to third-party disclosures. An outright notice requirement with consumers in mind is thus important in order to provide consumers with an ability to control their information and thereby limit privacy harm.[140] Consequently, the law should require each company that collects PII to present the consumer with notice of intended third party recipients of such PII and the third parties' proposed uses.

¶66 Notice, despite being a popular means of regulation,[141] has many detractors.[142] Some of the most common criticisms include: information overload, time constraints in actually reading the notices, cognitive limitations in understanding them, and, even when taking the time to read and understand them—which most consumers do not—an inability to take action that would change the end result.[143]

¶67 Others have argued that notice is inherently defective in the information privacy context because consumers lack the ability, based on these notices, to make accurate choices that reflect their privacy preferences given certain behavioral and decision-

---

[138] *See supra* Part I.C.i.

[139] In the increasingly important world of mobile software applications, however, many companies do not provide privacy notices or choice, and it is unclear even in states that require online companies to post privacy policies, such as California, whether mobile application companies are required to. *See, e.g.*, sources cited *supra* notes 47, 76.

[140] Consumers sometimes mistake the existence of privacy notices as an indication that the company will adhere to certain privacy principles. For instance, in a recent study in California, "Californians who shop online believe that privacy policies prohibit third-party information sharing. A majority of Californians believes that privacy policies create the right to require a website to delete personal information upon request, a general right to sue for damages, a right to be informed of security breaches, a right to assistance if identity theft occurs, and a right to access and correct data." Chris Jay Hoofnagle & Jennifer King, *Research Report: What Californians Understand About Privacy Online* 2 (Sept. 3, 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1262130. In reality, often the exact opposite is the case, e.g., a privacy policy gives the company an accepted basis for disclosing consumer information to third parties.

[141] *See, e.g.*, RICHARD H. THALER & CASS R. SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 188-93 (2008); Paula J. Dalley, *The Use and Misuse of Disclosure as a Regulatory System*, 34 FLA. ST. U. L. REV. 1089, 1090-92 (2007).

[142] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1029-30 (2012) (hereinafter *Against Notice Skepticism*).

[143] *Id.; see also infra* notes 6-14 and accompanying text; FED. TRADE COMM'N, PRELIMINARY FTC STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE at iii (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (noting that the notice and choice model, as currently implemented, "has led to long, incomprehensible privacy policies that consumers do not read, let alone understand"); Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. POL'Y FOR INFO. SOC'Y 543, 544 (Sept. 26, 2008), *available at* http://www.scribd.com/doc/7550344/Cost-of-Reading-Privacy-Policies (noting that studies demonstrate that "privacy policies are hard to read, read infrequently, and do not support rational decision making"); *and* Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, IEEE SECURITY & PRIVACY, Jan./Feb. 2005, at 24, 24-30, *available at* http://www.dtc.umn.edu/weis2004/acquisti.pdf (concluding that consumers often lack enough information to make decisions that match their privacy preferences and, even when they do have sufficient information, are likely to make suboptimal decisions due to psychological deviations from rationality).

making limitations and inherent biases.[144] According to this line of argument, therefore, no matter how notice is implemented, consumers will typically fail to make decisions that align with their actual preferences.[145] As a result, notice and its counterpart, choice, are ruled out as possible means to preventing privacy harms; only substantive privacy controls will do.[146]

¶68 If notice is to be a part of an effective remedy for privacy harm, these criticisms must be addressed. These criticisms can be generally categorized in a series of things consumers don't do. Consumers don't (1) read the notices, (2) understand the notices, (3) have time to do either (1) or (2), (4) make choices consistent with their privacy preferences, (5) have the ability to affect privacy outcomes, and (6) care about privacy notices or privacy in general.

¶69 Arguably all of these sources of notice deficiency are addressable in some measure. For instance, while policymakers cannot force a consumer to pay attention to a privacy notice, they can make it more likely that they will do so by requiring notices to be accessible and in a format that more interests the consumer.[147] Similarly, a notice can be less time-consuming to review and easier to understand if it is simplified and presents a clear message.[148] Apathy about notice may not be completely solvable,[149] but making notices more accessible and easier to understand may eliminate at least some consumers' apathy. Furthermore, at least some apathy may stem from consumers feeling that they cannot affect the outcome. Choice, as described below, may help address this source of notice apathy.

¶70 Providing consumers with details regarding who specifically will receive their information and for what specific purposes arguably helps address many of these concerns. A list of specific third parties would be easier for consumers to understand—and more relevant—than general categories of the types of third parties with which a company may share the consumers' information. Because such a list would be easier to understand, it may also take less time to review.[150] And it seems more likely that a

---

[144] *See* Nehf, *supra* note 13, at 1734-43 (identifying many issues with the notice-and-choice regime, including lack of transparency, consumers' difficulty in valuing privacy, an inability to assess risks or make accurate choices because of competing goals, and behavioral heuristics, such as drawing false inferences, that lead to suboptimal decisions); Acquisti & Grossklags, *supra* note 143; McDonald & Cranor, *supra* note 143.

[145] *See* Acquisti & Grossklags, *supra* note 143; Nehf, *supra* note 13.

[146] *See* Nehf, *supra* note 13, at 1145*; see also Failure of Fair Information*, *supra* note 6 (advocating adoption of substantive restrictions on data processing in order to prevent specific privacy harms).

[147] For a recent study suggesting that the standardization and simplification of privacy policy forms leads to greater consumer ease of use and enjoyment, see PATRICK GAGE KELLEY ET AL., STANDARDIZING PRIVACY NOTICES: AN ONLINE STUDY OF THE NUTRITION LABEL APPROACH (Jan. 12, 2010), *available* at http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab09014.pdf.

[148] *Id.; see also* NATHANIEL GOOD ET AL., STOPPING SPYWARE AT THE GATE: A USER STUDY OF PRIVACY, NOTICE AND SPYWARE 7 (2005), *available at* http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags-spyware_study.pdf (noting that in an experiment where users were provided with shorter notices, participants generally reacted very favorably to such notices and could recall specific content from the notices).

[149] *See, e.g.*, HUMPHREY TAYLOR, MOST PEOPLE ARE "PRIVACY PRAGMATISTS" WHO, WHILE CONCERNED ABOUT PRIVACY, WILL SOMETIMES TRADE IT OFF FOR OTHER BENEFITS (Mar. 19, 2003), *available at* http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf (identifying, based on polling, a category of people who simply do not care about privacy).

[150] If the list is incredibly long, of course, it may take longer for the consumer to review than reading a

consumer would in fact review the list given how relevant the information is. If all of these hold true, then consumer apathy might also decrease, especially if the consumer is clearly able to affect the outcome, which under this proposal would be the case.

¶71 Furthermore, people in other contexts frequently make choices based on imperfect information about risks, and they are subject to similar behavioral and decision-making limitations and biases that lead to suboptimal choices.[151] But this does not mean that substantive controls should replace notice and choice in those contexts. For instance, in the food industry, many food products are unhealthy and can contribute to serious health conditions and even, ultimately, death. Even apparently healthy foods can have unknown negative consequences.[152] Consumers have some notice and understanding of these issues, but even the most skilled food scientists do not fully understand the science of food and its effects on humans. As in the consumer privacy context, then, perfect notice about the consequences of food choices is difficult if not impossible.[153] And even with what information is available, consumers still may not act rationally in making food choices. As a result, consumers frequently make choices about food based on imperfect information, behavioral tendencies, and bounded rationality that fall short of their actual health preferences.[154]

¶72 Despite this, Congress has not enacted general laws mandating a certain type of diet or prohibiting foods with little or no health benefits.[155] Nor would society likely countenance it: such laws, even if in Americans' general best interest, would violate significant values underlying U.S. society, such as personal autonomy and freedom of choice. Instead, the Food and Drug Administration (FDA) requires labeling that specifies health information about food products[156] and generally regulates food companies in

---

few sentences that describe general categories of third parties and their uses. There will always be tradeoffs. Arguably in a case where a company includes a long list that takes more time to go through, the consumer would be more willing to do so precisely because the information is relevant and actionable based on the choice principle described below.

[151] *See generally* HERBERT A. SIMON, REASON IN HUMAN AFFAIRS (Stanford University Press, 1983).

[152] *See, e.g.*, WebMD, *Not-So-Healthy 'Health Foods': Some Foods You Think are Good for You May Not be All they Seem*, WEBMD, http://www.webmd.com/food-recipes/features/not-so-healthy-health-foods (last visited Dec. 2, 2012).

[153] The reasons for imperfect notice may differ in the two contexts, of course. In the food context, imperfect notice may be the result of imperfect food science, whereas in the consumer privacy context the imperfect notice may be the result of poor implementation. Arguably, however, all possible implementations will include some imperfections simply because the solution must apply to all consumers, and different consumers have different preferences regarding how they receive notice.

[154] One might argue that the consumer food product and consumer privacy contexts differ in material ways, and thus the comparison above is flawed. For instance, in the food product context, the consumer does derive some benefit from his suboptimal choices, even if the long-term the effects are negative. One might argue that in the consumer privacy context, there is no such benefit to the consumer, only to the company, and thus substantive controls are merited in the one but not the other. But this view seems overly cynical. Consumers may benefit in the form of more relevant advertisements, cheaper products, and faster service as a result of information sharing.

[155] Federal and state legislative bodies have enacted laws regulating the types of foods schools offer to children. *See, e.g.*, Todd Zwillich, *Congress Weighs School Junk Food Laws*, WEBMD (Mar. 6, 2007), http://www.webmd.com/parenting/news/20070306/congress-weighs-school-junk-food-laws ("[T]he federal government already regulates the nutritional content of breakfasts and lunches served in public school cafeterias."); Anahad O'Connor, *Bans on School Junk Food Pay Off in California*, NY TIMES (May 8, 2012, 12:02 PM), http://well.blogs.nytimes.com/2012/05/08/bans-on-school-junk-food-pay-off-in-california/ (discussing the results of two laws passed in California aimed at curbing consumption of junk food at school).

[156] *See generally* U.S. FOOD AND DRUG ADMINISTRATION, *Food Labeling and Nutrition Overview*,

order to minimize misleading or deceptive labeling.[157] Cumulatively, such measures aim to help provide consumers with better notice about the food products' merits and demerits before making choices. They do not, of course, provide perfect information, and consumers still make suboptimal choices in many cases (and still would even with perfect information). But they do provide consumers with some aids in making food choices, when and if done well.[158]

¶73 As this Article argues, improving notice with respect to third-party disclosures can similarly help consumers address the Incognito and Onward Transfer Problems and thereby limit privacy harms. Of course, any proposed remedy need not fully solve for any of these issues, nor can it. Some consumers, no matter how the notice is implemented, will simply not care. Or, even if they do, they will choose not to read the notice, exercise their choices, or make choices that match their privacy preferences.[159] The purpose of the proposal is not to prevent privacy harms in all cases—a virtual impossibility—but to provide consumers with an enhanced means to limit such harms with respect to the Incognito and Onward Transfer Problems.

¶74 Exactly how the notice is implemented is vital. After all, if companies bury notice and choice regarding third-party disclosures in a remote corner (virtual or otherwise), surrounded by reams of additional legal language, then the proposed regime may be no better than the current one. Even so, preferably the law would only specify the substantive goal to be achieved without dictating the exact implementation in each case. Such "command-and-control" regulations have often proved counterproductive in other contexts, and allowing industry to help identify the best ways to implement the policy (while preserving the substance of the policy goal) seems like the best way forward, both in terms of costs and effectiveness.[160]

---

http://www.fda.gov/Food/LabelingNutrition/default.htm (last updated Mar. 23, 2011).

[157] For background on FDA regulatory activities with respect to food labeling and companies' misleading and deceptive labeling practices, see A. Bryan Endres & Nicholas R. Johnson, *United States Food Law Update: The FDA Food Safety Modernization Act, Obesity and Deceptive Labeling Enforcement*, 7 J. FOOD L. & POL'Y 135, 149-62 (2011). Note that the FTC also plays a role in regulating companies when it concerns food advertising, which is technically different from food labeling.

[158] Some recent reports suggest recent changes to food labeling requirements have in fact aided consumers in making healthier food choices. *See, e.g.*, David Morgan, *New York Study Says Menu Labeling Affects Behavior*, REUTERS (Oct. 26, 2009, 3:57 PM), http://www.reuters.com/article/2009/10/26/us-obesity-newyork-idUSTRE59P4O720091026 (indicating that laws requiring calories to be listed have in fact led to consumers choosing foods with fewer calories); COMMUNITY RES. & DEV. INFO. SERVICE, *Nutrition Labeling: Not as Effective as You Might Think*, (Feb. 20, 2012) http://cordis.europa.eu/fetch?CALLER=EN_NEWS&ACTION=D&SESSION=&RCN=34314 (summarizing a recent study in Europe suggesting consumers do rely on labels in making food choices, while also noting that consumers often lack motivation to thoroughly study labels due to a lack of health goals).

[159] *See Nutrition Labeling: Not as Effective as You Might Think*, *supra* note 156 (noting that one reason consumers failed to engage food labels is because they may lack health goals and, thus, may not take their health seriously).

[160] For an interesting perspective on the development of environmental regulation through the joint efforts of industry and regulators, and how such development may prove instructive to privacy regulation's development, see Dennis D. Hirsch, *Protecting the Inner Environment: What Privacy Regulation Can Learn From Environmental Law*, 41 G. L. REV. 1 (2006); *see also* Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L. J. 1409, 1445 (2011) (arguing that prescriptive regulation and self-regulation are not mutually exclusive, and that co-regulatory alternatives may be especially viable in the privacy realm).

¶75 One simple mechanism for providing notice would be for companies to provide a list of intended third-party recipients, followed by a short description of the intended use for each. It may even be preferable to have the third-party disclosure list separate from notice of other privacy practices so as to facilitate access and understanding. Ideally the list would be just that: a list, with at most a short blurb from the company permitted making its pitch for why consumers should let the company share their PII.

¶76 With respect to the short descriptions following the identified third parties, the FTC could play a role in developing a list of typical uses that companies select from in building their lists. Ideally the FTC would work in conjunction with industry in order to develop the most relevant descriptions. This would have the benefit of harmonizing language among companies so that disparate practices do not lead to consumer confusion. Including industry in the discussion would also help ensure that the regulation is as relevant as possible, thereby minimizing compliance costs.

¶77 In terms of timing, the company should present the list to the consumer before the company begins sharing the consumer's PII with third parties. However, companies might choose a number of different methods of providing the notice—for instance, through e-mail, click-through, text message, or traditional mail—so long as the company actually presents the notice to the consumer. Merely posting the notice somewhere (online or offline) should not be sufficient.[161] If a company wants to add additional third parties to the list after it gives the initial notice, the law should require it to provide the consumer with additional notice and choice before doing so.[162]

¶78 Note that the law should also cover companies that initially received the PII from other companies rather than directly from the consumer. That is, if a company received the PII legally from another third party, but then desired to further disclose it to another third party, it would need to provide the consumer with notice and choice before doing so.[163] This would address the Onward Transfer Problem.

¶79 One complication naturally arises with this additional required notice: if the company has no means by which to contact the person—the PII the company received does not include contact information or such information is out-of-date, for instance—then the company has no means by which to provide the notice.[164] However, rather than

[161] Some consumers may find the proposed notice an annoyance that in certain cases slows a transaction depending on how a company presents the list. For instance, in an offline collection scenario, if a company chose to present the list to a hurried consumer at checkout, this may prove cumbersome. Indeed, one only need contemplate each customer in a grocery store line going through such a list before checkout to feel repulsed by the idea. However, companies would likely adopt more palatable methods of adhering to the law's requirements, for instance, by following up an in-store visit with an email communication or text message, since doing so would be in their best interests.

[162] The prospect of consumers constantly being bombarded with e-mails and other messages from companies asking permission to disclose their information to additional third parties may lessen the appeal of such a law. However, the net effect of the law could be that consumers actually receive far fewer messages from companies if they have declined companies' requests to share their information in the first place. Furthermore, if a consumer is averse to ever sharing their information with third parties, the law could require that companies simply provide consumers with a choice that declines permissions to share their information in perpetuity.

[163] The Driver's Privacy Protection Act, which prohibits state departments of motor vehicles from disclosing driver records to third parties without affirmative consent of the driver, addresses the Onward Transfer Problem in the same manner, i.e., by requiring driver consent to further disseminations of their personal information. *See* Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721(c) (2006).

[164] One unintended consequence of the law might be that companies end up collecting more PII than they otherwise would, precisely in order to be able to provide consumers with the required notice. For

have the default favor industry, this proposal contends that the default should instead favor consumers by allowing them to limit possible privacy harms resulting from the Incognito and Onward Transfer Problems.

2. Choice

¶80 Choice is notice's natural counterpart and is, consequently, subject to many of the same criticisms.[165] But choice also has independent detractors. For instance, some argue that additional regulation around obtaining consumer consent would lead to additional business costs for only marginal benefits at best.[166] In some cases, seeking consent may raise the cost of goods and services as well as limit consumer choice due to companies' inability to obtain such consent.[167] In other cases such costs may undermine certain business models and make offering goods and services that consumers want unviable.[168] For instance, much of the freely accessible online world relies on advertising revenues, which choice and limitations on information sharing may negatively impact.[169] Such regulations may also overly burden small, innovative companies and therefore raise barriers to entry.[170]

¶81 These considerations are mitigated by several factors. Some consumer information that companies rely on is non-PII, and non-PII is excluded from the proposed framework. One may also reasonably question the business cost claims underlying such arguments. Some studies suggest, for instance, that business studies of privacy costs are biased and incomplete.[171] Many of these costs assume that new ways of marketing to consumers

---

instance, under the law's definition of PII, a static IP address would be covered, but that, along with data about the consumer's web surfing habits, would not allow the company to easily contact the consumer through traditional means. So a company placing cookies on a computer may also seek to collect an e-mail address or other contact information. However, the actual consequence of this requirement might be that a company wanting to place cookies on a consumer's computer would notify the consumer of the use of cookies (many websites already do this), followed by the notice with the third-party list. Such issues are exactly why it would be vital to include the industry in addressing how best to implement the notice requirement, while preserving the substance of the goal.

[165] I will not rehash those criticisms and my counters to them here, but instead refer the reader to Part II.B.1.

[166] *Failure of Fair Information, supra* note 6, at 364-65 (detailing costs that companies incur in seeking consumer consent to the company's data handling practices); and Staten & Cate, *supra* note 12 (arguing that requiring companies to provide consumers with an opt-in choice, which is a less invasive approach than what this Article proposes, would likely undermine certain business models by imposing huge costs on such companies).

[167] *See Financial Privacy and Consumer Protection: Hearing Before the S. Comm. on Banking, Hous., & Urban Affairs*, 107th Cong. 10 (statement of Fred H. Cate, Professor of Law, Indiana University School of Law) (quoting Bill Pryor, *Protecting Privacy: Some First Principles*, Remarks at the American Council of Life Insurers Privacy Symposium, July 11, 2000, Washington, DC, at 4).

[168] *Id*.

[169] Rubinstein, *supra* note 73, at 413 (stating that privacy legislation may have negative economic impacts on "the online advertising revenues that currently subsidize free online content and services," and that advocates of privacy regulation must recognize "that a drop in these revenues [may] result in higher costs for consumers").

[170] Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates* 11 (AEI-Brookings Joint Ctr. for Regulatory Studies Working Paper 99-3, 1999).

[171] Robert Gellman, *Privacy, Consumers, and Costs: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, ELECTRONIC PRIVACY INFO. CENTER (Mar. 2002), http://epic.org/reports/dmfprivacy.html.

will not materialize or succeed; only old business models will do.[172] In reality, the lack of information privacy itself may cost companies significant amounts of money since many consumers choose not to use online services based on privacy concerns.[173] Furthermore, the frequent justification of "consumer benefit" is overstated; in many cases, such as junk mail and repeated solicitations, it is almost certainly a consumer detriment instead.[174]

¶82 Several of the arguments above are also based on some amount of privacy harm skepticism. However, as this Article has argued, distinct privacy harms can and do result from the current system of notice. Simply because consumers continue to participate in the commercial should not be read as evidence that they avoid privacy harm or that they are indifferent to it.[175]

¶83 Choice—real choice—with respect to third-party disclosures also provides a useful barometer by which to measure consumer attitudes about privacy harm. If a majority of consumers exercise their choice against disclosure to third parties, it suggests that we should be skeptical of privacy harm skepticism. It might be argued that providing that choice inherently suggests to the mind of consumers privacy harm, and thus biases their choice in favor of prohibiting disclosure. However, it is unclear why this would inherently be so. It is certainly possible, and even likely, as argued throughout this Article and suggested by seemingly all relevant consumer surveys, that consumers are worried about privacy harms. Furthermore, if it were the case that notice and choice somehow biased the consumer's choice in a manner that failed to provide any real benefits, the remedy would be to improve the notice and choice, if possible, rather than eliminating notice and choice altogether.

¶84 Consumers should thus have a choice as to whether the company may disclose their PII to specific third parties. Companies could allow consumers to consent to part of the third-party list (e.g., by allowing the consumer to specifically indicate which third parties are permitted and which are not) or present it as an all-or-nothing proposition; leaving this issue to the company's discretion would seem most advisable. This Article recommends an opt-in mechanism in order to avoid incentivizing companies to make it difficult for consumers to opt-out.[176] Consumers should also be able to revoke consent, though that revocation should not apply retroactively.

¶85 If companies wish to disclose a consumer's PII to additional third parties not listed in the initial notice, then, as mentioned with respect to notice, the company should be required to provide the consumer with additional notice and choice regarding whether the company may disclose the consumer's PII to such third parties. The company should be required to provide the consumer with a reasonable means by which to respond to the notice (e.g., real-time, e-mail, regular mail, or telephone).

¶86 As with notice, often companies may not have contact information for the persons whose consent they wish to obtain. Or, if they do, it may be out-of-date, or the person

---

[172] *Id.*

[173] *Id.*

[174] *Id.* (indicating, for instance, that consumers spend more than $400 million dollars per year for privacy-protecting services for telephones).

[175] *See supra* Part II.

[176] *See* Ted Janger & Paul M. Schwartz, *The Gramm-Leach Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230-32, 1241 (2002) (arguing against opt-out because such a default "creates incentives for privacy notices that lead to inaction by the consumer").

may not respond. However, this proposal contends that, in order to provide consumers with some ability to limit privacy harms, this should remain the company's issue rather than becoming the consumer's problem.

3. Private Right of Action

¶87 Under the current U.S. privacy regime, in most cases consumers have no means by which to enforce privacy statutes or hold companies accountable that fail to live up to any best practices to which they purport to adhere.[177] Instead, in most cases consumers must rely on the limited resources of the FTC and state attorney generals to keep companies honest. Or, they must simply rely on companies' own goodwill.[178]

¶88 To address this deficit, a model law should include a consumer private right of action. Statutory damages for grossly negligent or willful violations might also be included, at levels significant enough to make companies wary of failing to comply.[179] If a company illegally obtained someone's PII and did not use it in a manner that would be immediately obvious to the consumer (e.g., direct marketing), then a consumer's ability to enforce the law against such entity would obviously be limited. However, because the consumer could enforce the law against any entity that did ultimately contact a consumer, companies anywhere along the chain of information distribution would be wary of accepting consumer PII if a company along that chain could not demonstrate to the other party that it had legally obtained the consumer's PII. In addition to the consumer's private right of action, the FTC and state attorneys general would have the ability to enforce the law.

¶89 Some have argued against a private right of action in privacy statutes, contending that plaintiff attorneys tend to abuse such laws by bringing class action suits for technical violations.[180] Typically the attorneys receive a significant amount in the form of attorney's fees, while class members end up receiving little compensation.[181]

---

[177] One exception may be if the company makes certain promises in its privacy policy, that privacy policy is deemed to be part of a contract with the consumer. If the company subsequently breaches that contract, the consumer may be able to successfully bring a breach of contract claim. However, damages would be limited to contract remedies—economic damages directly resulting from the breach —without any statutory relief. *See supra* Part I.C.2 for additional discussion of this issue.

[178] Another exception is FCRA, which provides a private right of action. *See supra* Part I.A.

[179] Whether to include statutory damages, and determining the standard by which they should be triggered (i.e., negligence, willfulness, proof of actual damages, or something else), needs careful consideration. For instance, in *Doe v. Chao*, 540 U.S. 614 (2004), the majority opinion held that the text of the Privacy Act of 1974 precludes statutory damages unless the plaintiffs can show actual damages. As the dissent pointed out, showing actual damages for privacy violations is often difficult. So if proving actual damages is required in order to obtain statutory relief, the private right of action under the Privacy Act of 1974 may be toothless. Similarly, in *Andrews v. Veterans Administration*, 838 F.2d 418 (10th Cir. 1988), the court held that, although a federal agency was negligent in disclosing certain information about nurses to third parties, the nurses were not entitled to damages since the standard for obtaining damages was "intentional" or "willful" disclosure. Hence, ironically the Privacy Act of 1974 protects negligent or even grossly negligent disclosure of private information.

[180] Ronald L. Plesser & Stuart P. Ingis, *Limiting Private Rights of Action In Privacy Legislation*, CTR, FOR DEMOCRACY AND TECH. (Jul. 23, 2007), http://old.cdt.org/privacy/ccp/privaterightofaction1.shtml; *see also* Eric Goldman, *The Irony of Privacy Class Action Litigation*, 10 J. TELECOMM. & H. TECH. L. (2012) (arguing against allowing class action lawsuits as enforcement mechanisms in privacy statutes).

[181] SOLOVE & SCHWARTZ, *supra* note 22, at 890-91.

¶90 Underlying these arguments, of course, is some amount of privacy harm skepticism. This Article has shown, however, that the Incognito and Onward Transfer Problems cause both subjective and objective privacy harms. Furthermore, class action abuse is a problem with class action suits in general, not specifically to suits involving privacy harm claims. While reform in that domain may be warranted, that fact alone should not eliminate the possibility of a private right of action under a federal privacy statute. As some have suggested, it may be advisable to simply prohibit class action suits as part of privacy statutes.[182] But providing for a private right of action in the first place creates strong incentives for companies to take the regulation seriously.[183] Given that the law's requirements are clear and specific, complying with the law should also be within every company's grasp.

4. Relationship to Other Laws

¶91 The proposed law should only affect Federal sectoral laws to the extent that its provisions impose more rigorous standards on companies. Other aspects of such laws, such as the Safeguards Rule of GLBA and the Security Rule of HIPAA, should remain unaffected. The proposed law should also not preempt state law, so states could choose to impose stricter requirements and continue to experiment with different forms of possibly more effective regulation.[184]

V. AN ANALYSIS

¶92 Ultimately whether to adopt the some such solution to the Incognito and Onward Transfer Problems is a normative question. As Professor Larry Lessig has argued in the online context, the architecture of the Internet is largely what we decide it to be.[185] Similarly, with information privacy, we must choose if and to what extent we want to preserve information privacy based on what we value.[186]

¶93 The current U.S. piecemeal regime to information privacy favors commercial values above all others.[187] And some believe this focus on commercial interests is as it should be. As many commentators have argued, this commercialization of information

[182] *See generally* Goldman, *supra* note 180; *see also Doe*, 540 U.S. at 636 (Ginsburg, Stevens, & Breyer, JJ., dissenting) (arguing that courts can simply deny class certification if worried about runaway costs).

[183] *See* Joshua D.W. Collins, *Toothless HIPAA: Searching for a Private Right of Action to Remedy Privacy Rule Violations*, 60 VAND. L. REV. 199, 202-03 (2007) (arguing that HIPAA and its privacy protections are "toothless" absent a private right of action); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L.J. 877, 878 (2003) (arguing that the lack of a private right of action in many privacy statutes leaves a significant enforcement gap); A. Michael Froomkin, *Government Data Breaches*, 24 BERKELEY TECH. L.J. 1019, 1033-34 (2009) (noting that the Privacy Act of 1974, which applies to the government, includes a private right of action, thereby providing the law with "some teeth").

[184] The U.S. Supreme Court ruled in *Reno v. Condon* that Congress can regulate PII under the Commerce Clause of the U.S. Constitution. 528 U.S. 141 (2000). Although Congress could preempt state laws on the basis of this decision, this Article argues that allowing states to experiment in privacy regulation may lead to improvements from which Congress could learn.

[185] LAWRENCE LESSIG, CODE: VERSION 2.0, 32-37 (Basic Books, 2006), *available at* http://codev2.cc/download+remix/Lessig-Codev2.pdf.

[186] *Id.* at 33-34.

[187] *Id.* at 203-22 (describing generally how consumer privacy on the Internet has been sacrificed in favor of commercial interests).

provides significant benefits to consumers.[188] Impeding this commercialization through regulation would, therefore, harm companies and consumers alike.[189]

¶94 But, as this Article has argued, the commercialization of information also harms consumers.[190] And it is unclear that this need be so. Indeed, it may be that consumers will happily trade their information privacy for improved access to products and services. But they have never had a real choice.[191] This Article's proposal aims at improving that choice by addressing the Incognito and Onward Transfer Problems. Doing so, in turn, allows consumers to answer the normative question with respect to their information privacy and third-party disclosures.

A. The Costs

¶95 The proposed law would certainly impose some compliance costs on companies.[192] In some cases companies may need to rework their information technology systems in order to manage consumer information in accordance with the law. In other cases companies may need to spend significant time and costs determining what third parties have access to their consumer information. Arguably, however, forcing companies to manage consumer information more responsibly is a positive result. Furthermore, a co-regulatory approach that involves both industry and government in developing the solution would help minimize such compliance costs.[193] In general, precise laws that give clear notice to industry of what is expected keep compliance costs at a minimum,[194] and the model law would do just that.

¶96 Arguably the more serious costs would result if companies were unable to operate, offer goods and services at reasonable prices, or reach customers with their products and services because of the law. A fettered online world subject to frequent tolls, for instance, may be one bad outcome of such a law. But if certain business models really do depend on unfettered exchanges of PII, consumers can always allow companies to share their PII if they value commercial interests over their privacy interests. If they do not, then arguably the law reaches the right result. Indeed, arguing that the law harms consumers often assumes needs on the part of consumers that may not exist.[195]

¶97 These counterpoints assume, of course, that consumers understand the role their PII plays in helping fund the commercial world. They may, for instance, naively prohibit

---

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

[189] Staten & Cate, *supra* note 12.

[190] *See supra* Part II.

[191] LESSIG, *supra* note 185, at 228 ("The real challenge for privacy . . . is how to enable a meaningful choice in the digital age.").

[192] *See* Peter P. Swire, *Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information*, in PRIVACY AND SELF-REGULATION IN THE INFORMATION AGE (U.S. Dep't of Commerce ed., 1997), *available at* http://www.ntia.doc.gov/reports/privacy/selfreg1.htm; Rubinstein, *supra* note 73, at 413 (stating that privacy legislation may have negative economic impacts on "the online advertising revenues that currently subsidize free online content and services," and that advocates of privacy regulation must recognize "that a drop in these revenues [may] result in higher costs for consumers"). *But see supra* Part III.B.3 (arguing that the costs of compliance may be overstated).

[193] *See supra* Part III.B.1 and note 160.

[194] Swire, *supra* note 192.

[195] For instance, in one survey 66% of consumers did not favor the "benefit" of targeted advertising. Turow, *supra* note 14. These percentages increased to as high as 86% when consumers learned about how companies collect and use information about them.

companies from disclosing their PII to third parties, without understanding such a decision's true impact on what companies are able to offer them. But even this scenario is a positive result. In such a case, companies would have a strong incentive to better educate consumers about how they use their information and why they need it. Rather than simply attempting to do the legal bare minimum, therefore, companies would have incentives to do their utmost to give consumers clear information about their information handling practices. Companies may develop novel and more effective ways of educating consumers about information privacy as a result.

¶98 Another issue worth considering is that of free riders. If most consumers are "privacy pragmatists" and trade some amount of their information privacy for economic benefits, and these decisions, collectively, allow companies to offer cheaper goods and services, then such privacy pragmatists may be subsidizing the privacy preferences of others such as "privacy fundamentalists."[196] That is, such privacy fundamentalists can have their cake (control their information) and eat it, too (access to cheaper and improved products and services). We might view that result as unfair to privacy pragmatists, who are also concerned about information privacy generally.

¶99 But looking at the collective result ignores the fact that privacy pragmatists, at the individual level, were willing to concede some amount of information privacy for whatever benefits the company offered them in return. And they may be receiving greater benefits based on this tradeoff than the privacy fundamentalist does in general, such as access to exclusive offers or tailored marketing. Indeed, it is unlikely that privacy pragmatists would give up their information privacy based on notions of collective good.

B. The Constitution

¶100 Aside from the economic considerations, another possible problem with the law is that it may be unconstitutional because it unduly burdens free speech. Eugene Volokh has argued that information privacy rules such as those proposed in this Article likely violate the First Amendment.[197] The U.S. Supreme Court also recently ruled in *Sorrell v. IMS Health, Inc.* that a Vermont statute violated the First Amendment's guarantee of free speech because it prohibited, absent consent, the use and dissemination of information relating to doctors' prescription practices in various marketing activities.[198]

¶101 However, in the instant case, the constitutional concerns seem manageable. In *Sorrell*, the Court struck down the law because it included content- and speaker-based restrictions without compelling justifications for such restrictions: the law exclusively targeted marketing speech, and "more than that, the statute disfavors specific speakers, namely pharmaceutical manufacturers."[199] Given such restrictions, the Court applied heightened scrutiny and found the State's justifications of maintaining medical privacy

[196] *See* Taylor, *supra* note 149 (finding, based on surveys, that most consumers can be considered "privacy pragmatists" who, while concerned about privacy, are often willing to sacrifice it for economic benefits, while also identifying a smaller group of "privacy fundamentalists" that care a great deal about their privacy and do not wish any further erosion of it).

[197] Volokh, *supra* note 65.

[198] 131 S. Ct. 2653 (2011).

[199] *Id.* at 2663.

and improving public health unconvincing.[200] With regard to the medical privacy justification, the Court noted that almost anyone other than marketers could access and use the information; a more compelling implementation, according to the Court, would have been to limit use and dissemination of the information in all cases except for a few narrowly defined ones.[201]

¶102 The proposed law is therefore distinguishable from the Vermont statute in *Sorrell*, in that the "speech"[202] regulated here does not include similar content- and speaker-based restrictions as the Vermont statute. Indeed, the proposed law is akin to a HIPAA-type regulation, which the Court referenced with approval, where use and disclosure is broadly prohibited except in certain narrowly defined cases.[203] This may seem ironic since such an outcome means broader prohibitions on speech, but the Court in *Sorrell* was primarily concerned that the Vermont statute singled out specific speakers and a specific viewpoint. The proposed law does no such thing.[204]

C. The Alternatives

¶103 Others have argued that legislation is not feasible given the industry lobby against such regulation, and have thus proposed reliance on the judiciary to develop relevant privacy torts instead.[205] While it is true that Congress has not yet enacted a privacy bill, and that industry certainly prefers a self-regulation model, Congress continues to propose new consumer privacy-related bills.[206] Therefore, exploring the ideal tenets of such a law remains pertinent. Furthermore, this proposal is not meant to rule out other possible solutions to different pieces of the information privacy conundrum.

¶104 Indeed, the proposed law would not be a total solution to problems that exist with the current piecemeal information privacy regime. Instead, this Article focuses on the Incognito and Onward Transfer Problems. This focus is merited given the significant privacy harms that can and do result on the basis of largely unregulated third-party disclosures. However, other privacy harms may also result from lax information security, online tracking (even without disclosure to third parties), among others. Similar types of

---

[200] *Id.* at 2664-70.

[201] *Id.* at 2672.

[202] Neil Richards argues that information in the context of a commercial relationship should not be considered speech within the meaning of the First Amendment. Neil Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005). However, despite his argument, courts have and likely will continue to consider such information "speech" or "commercial speech" within the meaning of the First Amendment.

[203] *See Sorrell*, 131 S. Ct 2653 at 2668.

[204] In fact, other courts addressing statutes that restricted commercial speech in a similar manner to the proposed law upheld such restrictions. *See* Trans Union Corp. v. F.T.C., 245 F.3d 809 (D.C. Cir. 2001); Trans Union LLC v. F.T.C., 295 F.3d 42 (D.C. Cir. 2002); National Cable and Telecommunications Association, 555 F.3d 996 (D.C. Cir. 2009) (upholding the FCC's response order to the court's decision in U.S. W., Inc. v. F.C.C., 182 F.3d 1224 (10th Cir. 1999)). The *U.S. West* case held that FCC's implementing rules of the Telecommunications Act of 1996 violated the First Amendment as unconstitutional restrictions on commercial speech by restricting use and dissemination of customer proprietary network information without first obtaining customer consent. In its revised 2007 order, however, the FCC largely rejected the Tenth Circuit's holdings, and the D.C. Circuit easily upheld the order. For a critical perspective on the *U.S. West* case, see Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000).

[205] *See* Ludington, *supra* note 64, at 172-73.

[206] *See supra* note 15.

notice and choice as proposed here may not be appropriate in such contexts,[207] and substantive privacy controls may be warranted in others. "Privacy by design" and "privacy enhancing technologies" ("PETs") have also received significant attention more recently as possible pieces of the puzzle.[208] Such issues are outside the scope of this Article. What seems clear is that no one-size-fits-all approach to information privacy and security is sufficient.

VI. CONCLUSION

¶105 Consumers face significant obstacles in protecting their information privacy in the modern commercial world. This Article has identified two obstacles that significantly limit consumers' ability to control their information privacy fate: the Incognito and Onward Transfer Problems. The U.S. piecemeal approach to information privacy has failed to fill these gaps, and current legislative proposals similarly leave them gaping.[209]

¶106 Do consumers care? Surveys suggest they do.[210] But it is hard to say without giving consumers a chance to decide. Consumers may very well favor commercial interests over privacy interests. Yet to claim this is already clear based on consumer behavior assumes that the current piecemeal privacy regime does an adequate job of providing consumers with the ability to control their information privacy. The Incognito and Onward Transfer Problems suggest this is clearly not the case with respect to third-party disclosures. And loosely regulated third-party disclosures are a major piece of the information privacy puzzle.

¶107 But clearly other information privacy problems exist. Discussions of consumer tracking, for instance, have dominated much information privacy discourse over the past few years.[211] Even though this Article's proposal would prevent tracking companies from sharing consumer PII dossiers with third parties absent specific consumer notice and consent, it does nothing about the tracking in the first place. And some consumers—rightfully so—may still worry about such tracking. Certainly subjective and objective privacy harms may result from such activities.

¶108 One lesson from this study is that an effective solution to consumer privacy issues requires that the different problems be isolated and addressed separately. The days of a global privacy notice giving companies license to do whatever they would like with consumer PII, so long as they follow whatever tenets they've buried in that notice, should be numbered. Fair Information Practice Principles are not, or should not be considered, information privacy gospel. For some problems, notice and choice is almost certainly not the right solution. For instance, we may simply not want companies to use lax security

---

[207] *See* Calo, *Against Notice Skepticism*, *supra* note 142 (assessing the promise of new types of "visceral" notice).

[208] *See* Center for Democracy & Technology, *The Role of Privacy by Design in Protecting Consumer Privacy* (Jan. 28, 2010), https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy (discussing privacy by design and PETs and the roles each might play in the ongoing information privacy regime).

[209] *See* Center for Digital Democracy, *supra* note 15.

[210] *See supra* note 88.

[211] *See, e.g.,* FEDERAL TRADE COMM'N, *FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers*, (Dec. 1, 2010), *available at* http://www.ftc.gov/opa/2010/12/privacyreport.shtm (summarizing a recent FTC-issued report that endorses a "Do Not Track" mechanism in browsers in order to address the issue of consumer tracking).

when collecting, storing, and disclosing sensitive PII; consumer notice and choice, no matter how implemented, would provide no clear benefits in such a case because, arguably, only one right choice exists. Instead, we might prescribe what types of security protocols companies must adopt when dealing with such PII. Notice and choice seem to work best in scenarios where only simple, straightforward messages are to be conveyed and where we think it makes sense for consumers to have a choice. Listing third party recipients as discussed herein or the calories associated with a particular food are two such examples.

¶109 For other issues, even if textual notice and choice is not the right solution, some form of "visceral" notice and choice may be.[212] As information collection, use, and dissemination grows increasingly sophisticated, the approaches to protecting information privacy must do likewise. Indeed, if the current piecemeal approach to information privacy doesn't become an anachronism, information privacy almost certainly will. Addressing information privacy should be done in a manner that befits the issue. In the case of the Incognito and Onward Transfer Problems, a textual approach of notice and choice, as proposed in this Article, shows some promise. Other pieces of the privacy puzzle almost certainly will require different solutions.

[212] *See* Calo, *Against Notice Skepticism*, *supra* note 142 (assessing the promise of new types of "visceral" notice).

Copyright 2013 by Northwestern University School of Law
Northwestern Journal of Technology and Intellectual Property
Volume 11, Number 5 (April 2013)