Comments to Selected Portions of the Department of Commerce's Internet Policy Task Force Report, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*
Docket No. 101214614–0614–01

by

Robert Sprague, Associate Professor
University of Wyoming College of Business
Department of Management & Marketing
1000 E. University Ave., Dept. 3275
Laramie, WY 82071
(307) 766-5670
spraguer@uwyo.edu
http://www.uwyo.edu/mgtmkt/directory/faculty-pages/sprague.html

Introduction

In its December 2010 report, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" (hereinafter "IPTF Report"), the Department of Commerce's Internet Policy Task Force expresses a number of pertinent themes. First and foremost, consumer trust—the expectation that personal information that is collected will be used consistently with clearly stated purposes and protected from misuse—is fundamental to commercial activities on the Internet (IPTF Report, p. 15). Yet, many of the key actors in Internet commerce (online advertisers, cloud computing services, location-based services, and social networks) operate without specific statutory obligations to protect personal data (IPTF Report, p. 12). This last statement is quite literally true, as Congress has failed to enact any meaningful data protection legislation and the forty-six states that have enacted data breach notification laws address only the security of data and the conduct of service providers once a data breach has occurred.[1] These state statutes do not address what information can be collected, nor how it can be used or shared.

The current privacy policy framework has created an environment in which "creative re-sue of existing information" has led to innovations; and if the information is collected under sufficiently broad statements in a privacy policy, the legal risk—in contrast to the privacy risks—from this re-use may be minimal (IPTF Report, p. 38). While businesses generally

[1] *See* Nat'l Conf. of St. Legis., *State Security Breach Notification Laws* (Oct. 12, 2010), http://www.ncsl.org/IssuesResearch/TelecommunicationsInformationTechnology/SecurityBreachNotificationLaws/tabid/13489/Default.aspx (listing citations to individual state data breach notification laws). The majority of these statutes require data collectors to send notice of unauthorized access of unencrypted personal information to affected individuals. Penalties relate to failure to timely send adequate notice, not for failing to prevent the breach itself. *See* Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 105 (2009). Massachusetts's security breach statute, MASS. ANN. LAWS ch. 63H, §§ 1-6 (LexisNexis 2010), is the only statute that addresses data security procedures. It requires that the department of consumer affairs and business regulation adopt regulations to, in part, "insure the security and confidentiality of customer information in a manner fully consistent with industry standards…." *Id*. at § 2(a).

recognize that their sustainability depends on maintaining consumer trust (IPTF Report, p. 22), from the consumer perspective, the current system of notice-and-choice does not appear to provide adequately transparent descriptions of personal data use, which may leave consumers with doubts (or even misunderstandings) about how companies handle personal data and inhibit their exercise of informed choices (*id*.).

The Federal Trade Commission's (FTC) self-regulation approach has also created the concerns underlying the IPTF Report. FTC actions against companies for failing to enforce their own privacy policies are rare.[2] In 2000, the FTC concluded that only about one-fifth of surveyed websites that collect personal identifying information implement, at least in part, the Fair Information Practice Principles of Notice, Choice, Access, and Security;[3] resulting in the Commission concluding that legislation was necessary (in conjunction with self-regulation) to compel companies to comply with the principles.[4] Most privacy-related FTC actions are associated with data breaches. While the FTC has brought just 28 cases involving data breaches,[5] the Privacy Rights Clearinghouse reports over 2,300 known data breaches since 2005, affecting over one-half billion records.[6] Of course, the FTC's present enforcement capabilities are limited to first finding deceptive acts under § 5 of the Federal Trade Commission Act.[7]

Concepts of individual privacy formulated long before the advent of the Internet, search engines, e-commerce, online advertising, and online social networks are just as applicable in the twenty-first century:

> A central aspect of privacy is that individuals … can determine for themselves which matters they want to keep private and which they are willing—or need—to reveal.[8]
>
> Privacy is the right to live one's life in one's own way, to formulate and hold one's own beliefs, and to express thoughts and share feelings without fear of observation or publicity beyond that which one seeks or acquiesces in. … [W]hat is private varies for each person and varies from day to day and setting to setting. … [T]he very core of the concept is the right of each individual to determine for himself in each particular setting or compartment of his life how much of his many-faceted beliefs, attitudes, and behavior he chooses to disclose. … Every person lives in several different worlds, and in each his mode of response may—indeed must—be different … The right to privacy includes the

---

[2] *See, e.g., In re* Gateway Learning Co., No. 042-3047, Complaint (F.T.C. July 7, 2004) (alleging Gateway rented customers' personal information to marketers despite promises to the contrary in its privacy policy). *See also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 9 n.17 (Dec. 2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf [hereinafter "FTC 2010 Privacy Report"] (citing three consent orders involving deceptive statements in companies' privacy notices about their collection and use of consumers' data).

[3] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 12 (May 2000), http://www.ftc.gov/reports/privacy2000/privacy2000.pdf.

[4] *Id*. at 36-37. *See also* FTC 2010 Privacy Report, *supra* note 2, at 8.

[5] *See* FED. TRADE COMM'N, Privacy Initiatives, Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html (last visited Jan. 27, 2011).

[6] Privacy Rights Clearinghouse, Chronology of Data Breaches (Jan. 27, 2011), http://www.privacyrights.org/data-breach.

[7] Act of Mar. 21, 1938, ch. 49, § 3, 52 Stat. 111, amending 15 U.S.C. § 45 (2000).

[8] ALAN F. WESTIN, PRIVACY AND FREEDOM 373 (1967).

> freedom to live in … different roles without having [one's] performance and aspirations in one context placed in another without permission.[9]
>
> As a first approximation, privacy seems to be related to secrecy, to limiting the knowledge of others about oneself. This notion must be refined. It is not true, for instance, that the less that is known about us the more privacy we have. Privacy is not simply an absence of information about us in the minds of others; rather *it is the control we have over information about ourselves*.[10]

For there to be any effective right to privacy with respect to online activities, individuals must be provided greater rights and opportunities to control the disclosure of information about themselves. While the author of this these selected comments supports comprehensive federal legislation mandating a set of Fair Information Practice Principles to better protect personal information,[11] the short time allowed to provide comments to the IPTF Report precludes a comprehensive discussion of such legislation. However, such legislation should, at a minimum, include:

- Expanding the scope of what is considered personal identifying information to be protected under an enhanced framework of Fair Information Practice Principles;
- A requirement that consumers opt-in to certain data collection and sharing rather than only being afforded an opportunity to opt-out; and
- The need for a private right of action to provide substantive consumer privacy protection.

Fair Information Practice Principles, Identifiable Data and Anonymity

Recommendation #1 within § II.A. of the IPTF Report is the adoption of a baseline commercial data privacy framework built on an expanded set of Fair Information Practice Principles (FIPPs). A brief history of the evolution and development of FIPPs is provided in Appendix A to these Comments. FIPPs, adopted by different entities over different times, reflect some similarities as well as differences. Fundamentally, they address limitations on the collection and use of data, data quality and reliability, and data security. The most significant limitation of the various FIPPs is that none of them are directly legally binding on U.S. private commercial data collectors.[12]

At the core of FIPPs is the protection of personal identifying information (PII). Fundamentally, PII is information that allows a data record to be associated with a particular person whose identity can be ascertained. Yet, just what constitutes protectable PII is unclear.

---

[9] OFFICE OF SCI. & TECH. OF THE EXEC. OFFICE OF THE PRESIDENT, PRIVACY AND BEHAVIORAL RESEARCH 8-9 (1967) (addressing behavioral research procedures).

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

[11] Without legislation, online businesses do not know the exact boundaries of what is and is not permissible when it comes to data collection. This is exemplified by the fact that within the past year, consumers have filed at least twenty-nine privacy-related class action lawsuits in the U.S. naming at least thirty-nine companies. *See* Dominique R. Shelton & Clinton J. McCord, *Consumer Privacy Litigation Alert: A Rash of Behavioral Advertising Class Actions Have Been Filed Implicating Company Websites and Mobile Applications*, WILDMAN HARROLD (Jan. 21, 2011), http://www.wildman.com/bulletin/01212011.

[12] As discussed more fully in Appendix A, companies must satisfy the Commerce Department's safe harbor provisions for transborder data flows to and from the EU.

In its initial development of a Code of Fair Information Practices (see Appendix A), the Department of Health, Education and Welfare (HEW) emphasized *identifiable* data records:

> An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it. Any recording, disclosure, and use of identifiable personal information not governed by such procedures must be proscribed as an unfair information practice unless such recording, disclosure or use is specifically authorized by law.[13]

Despite a focus on protecting "personal information," the FTC does not formally define the term. It has described personal information as including bank and credit card account numbers, income, Social Security number (SSN), name, address, and phone numbers.[14] While the Department of Homeland Security FIPPs reproduced in the IPTF Report (see Appendix A to these comments; IPTF Report, pp. 26-27) emphasize protection of PII, the FIPPs themselves, nor their underlying Privacy Policy Guidance Memorandum, define PII. However, the Privacy Policy Guidance Memorandum notes that § 222 of the Homeland Security Act calls on the Chief Privacy Officer to assure that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974.[15] The Privacy Act defines a "record" as including "any item, collection, or grouping of information about an individual that is maintained by an agency, … that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual…."[16]

---

[13] DEP'T HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, Safeguards for Privacy (July 1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/c3.htm (emphasis omitted). The central theme of the HEW report was to analyze the use of the Social Security number (SSN) as a standard universal identifier. The report recommended "against the adoption of any nationwide, standard, personal identification format, with or without the SSN, that would enhance the likelihood of arbitrary or uncontrolled linkage of records about people…." *Id*., The Social Security Number as a Standard Universal Identifier, *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/c7.htm (emphasis omitted).

[14] *See, e.g.*, FED. TRADE COMM'N, PRIVACY: TIPS FOR PROTECTING YOUR PERSONAL INFORMATION (Aug. 2008), http://www.ftc.gov/bcp/edu/pubs/consumer/alerts/alt106.shtm; FED. TRADE COMM'N, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, http://www2.ftc.gov/bcp/edu/pubs/business/idtheft/bus69.pdf (last visited Jan. 18, 2011).

[15] Dep't of Homeland Security, Privacy Policy Guidance Memorandum (Dec. 29, 2008), at 3, *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf (citing 6 U.S.C. § 142(a)(2) (2007)).

[16] 5 U.S.C. § 552a(a)(4) (2010). *See* Frederick Lah, *Are IP Addresses "Personally Identifiable Information"?*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 681, 706-07 (2008) (providing selected Federal statutory definitions of "personal information"); Joshua J. McIntyre, *The Number Is Me: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV., at *11 (Aug. 15, 2010) (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621102 (noting there is no single definition of PII under federal law).

The historical development of FIPPs by U.S. federal agencies demonstrates a bias toward limiting the scope of PII to an individual's name, combined with an account number, credit or debit card number, SSN, driver's license number, or date of birth, etc.[17]

Baseline commercial data privacy principles, such as comprehensive FIPPs, should incorporate an expanded concept of PII.

Many commentators in the legal and computer disciplines have lately embraced the realization that PII is represented by more than a name combined with a limited collection of other data. In 2000, Latanya Sweeney's research revealed that 87% of the U.S. population could be uniquely identified through a combination of only three data points: 5-digit ZIP code, gender, and date of birth.[18] In his article discussing "de-anonymization," Paul Ohm notes that data not traditionally considered PII can still be used to identify individuals by combining supposedly anonymized data with outside information.[19]

There is precedent for a more expansive concept of PII. The FTC recently embraced a more expansive definition of "personal information" in its 2008 Consent Order resulting from the notorious TJX data breach:[20]

> "Personal information" shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name, that reveals an individual's email address; (d) a telephone number; (e) a Social Security number; (f) credit or debit card information, including card number, expiration date, and data stored on the magnetic strip of a credit or debit card; (g) checking account information,

---

[17] *See* McIntyre, *supra* note 16, at *11-12 (describing various definitions of PII from different federal privacy laws).

[18] Latanya Sweeney, *Uniqueness of Simple Demographics in the U.S. Population* (Laboratory for Int'l Data Privacy, Working Paper LIDAP-WP4, 2000) (cited in Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1705 n.4 (2010)). Sweeney also reported that 53% of the U.S. population are likely to be uniquely identified by only place, gender, and date of birth (where place is the city, town, or municipality in which the person resides). *Id*. In a later, similar study, Philippe Golle, while agreeing with Sweeney's results, found that disclosing one's gender, ZIP code and full date of birth allows for unique identification of 63% of the U.S. population. Philippe Golle, *Revisiting the Uniqueness of Simple Demographics in the U.S. Population*, 5 ACM WORKSHOP ON PRIVACY IN THE ELEC. SOC'Y 77 (2006).

[19] Ohm, *supra* note 18, at 1723, 1724. *See also* McIntyre, *supra* note 16 (arguing that Internet Protocol Addresses should be recognized as PII); Lah, *supra* note 16 (arguing same); Arvind Narayanan & Vitaly Shmatikov, *De-anonymizing Social Networks*, PROC. OF THE 2009 IEEE SYMP. ON SECURITY AND PRIVACY (2009), *available at* http://arxiv.org/PS_cache/arxiv/pdf/0903/0903.3276v1.pdf (discussing an algorithm to de-anonymize anonymous users of one social media application (Twitter) based on registration information contained in a different social media application (Flickr), with only a 12% error rate); Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets (How to Break Anonymity of the Netflix Prize Dataset)*, PROC. OF THE 2008 IEEE SYMP. ON SECURITY AND PRIVACY (2008) *available at* http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf (discussing a study using the Internet Movie Database as the source of background knowledge, successfully identifying Netflix records of known users, uncovering their apparent political preferences and other potentially sensitive information); Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, Aug. 9, 2006, at A1 (reporting that supposedly anonymous AOL search users could be identified by cross-linking with other available data).

[20] *See* Sprague & Ciocchetti, *supra* note 1, at 97-100 (describing the background and extent of the TJX data breach).

> including the ABA routing number, account number, and check number; (h) a driver's license, military, or state identification number; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; or (j) any information that is combined with any of (a) through (i) above.[21]

In addition, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (see Appendix A) define "personal data" as any information relating to an identified or identifiable individual,[22] as does EU Directive 95/46/EC.[23] The definition of "personal data" in Article 2 of EU Directive 95/46/EC states that "an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[24] In conjunction with establishing Safe Harbor Principles to provide an "adequate" level of privacy protection for transferred data, the Commerce Department defines "personal data" and "personal information" as "data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form."[25]

The EU Article 29 Data Protection Working Party recently re-evaluated the concept of personal data."[26] As noted above, the EU considers personal data as data that can directly or indirectly identify an individual. As such:

> As regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations", whether small or large in size. In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others.[27]

"In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name."[28]

---

[21] *In re* TJX Cos., File No. 072-3055, at 2 (F.T.C. Mar. 27, 2008), http://www.ftc.gov/os/caselist/0723055/080327agreement.pdf.

[22] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 18, 2011).

[23] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, Article 2 (Nov. 23, 1995), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[24] *Id*.

[25] Dep't of Comm., Safe Harbor Privacy Principles (July 21, 2000), http://www.export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 14, 2010).

[26] Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN/WP136, 13–15 (June 20, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

[27] *Id*. at 13 (emphasis in original).

[28] *Id*. at 14.

Ultimately, individual privacy is not protected when only traditional concepts of PII are used. We must protect not only data that does indentify an individual, but also data that can identify an individual.[29]

Opt-in vs. Opt-out

Section II.B. of the IPTF Report requests comments to promote substantive privacy protection through an enhanced FIPPs-based framework. As noted in the IPTF report, privacy policies are generally written in unintelligible legalese (p. 31), and are designed more to provide legal protection for the service provider than privacy protection for the consumer. In its December 2010 Privacy Report, the FTC recommends eliminating the consent requirement for service providers to collect and use consumer data for "commonly accepted practices" (e.g., product and service fulfillment, internal operations, etc.).[30] Under the FTC's examples, though, first-party marketing would be consider a commonly accepted practice; but this could include behavioral tracking on the provider's own site, as well as tracking by the provider on other sites.

The U.S. has taken an opt-out approach to data privacy protection. In other words, it is left to the consumer to affirmatively notify the data collector to *not* collect data. This places the onus on the consumer to decide, site by site, whether to take steps to stop data collection. While a site such as Facebook provides users with multiple privacy options, most sites simply inform users of their privacy policies—implying consent to those policies *in toto* by using the site. With the growing length and complexity of privacy policies,[31] it is much more practical for users to not even bother to read a site's privacy policy.[32] This requires users to trust the sites they visit. But as noted in the IPTF Report, users may not appreciate the extent to which data relating to them is tracked and used (p. 22). Indeed, users may be surprised to learn the extent of tracking that occurs.[33] To better align consumer expectations and actual information practices (IPTF Report, p. 38):

Consumers should be allowed to opt-out of first-party data collection used for commonly accepted practices for purposes of behavioral tracking, and service providers should be prohibited from collecting or using any other data unless the consumer expressly opts-in.

This suggestion does not completely abandon the FTC's current notice-and-choice approach, but adds a level of informed consent for data collection and use that may not be readily

[29] *See* McIntyre, *supra* note 16, at 16-17.

[30] FTC 2010 Privacy Report, *supra* note 2, at 53-54.

[31] *See, e.g.*, Kim-Phuong L. Vu et al., *How Users Read and Comprehend Privacy Policies*, HUMAN INTERFACE & MGMT. INFO.: INTERACTING IN INFO. ENV'TS, II Proceedings of the Symposium on Human Interface 802 (July 2007) (finding that, overall, survey participants showed poor comprehension of the information conveyed in privacy policies even though they were written at the participants' level of education).

[32] McDonald and Cranor estimate that if U.S. Internet users read the privacy policy of each site they visited at least once per year, it would take approximately 201 hours per year, at a national annual cost of approximately $781 billion in time lost. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 565 (2008). If consumers visit multiple sites to comparison shop, McDonald and Cranor double the estimated value of time lost. *Id*.

[33] *See, e.g.*, Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html (reporting a study that found that the nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning; a dozen sites each installed more than one hundred).

apparent to users, such as sharing data with external partners.[34] By implementing an opt-in requirement for data collection outside commonly accepted practices, a mechanism is set in place to ensure that before this data is collected and used, consumers will be informed (1) of precisely what information about them is being collected; (2) how the information is being used; and (3) in a clear and understandable fashion (necessary in order to persuade consumers to grant permission).

An opt-in approach also provides more protection than the FTC's proposed Do Not Track mechanism.[35] First, Do Not Track is another implementation of opt-out, as each consumer, at each site, must take the initiative to notify the site (and possibly third-party trackers) to not collect data. Second, without legislation, it is voluntary on the part of the websites and third-party trackers.

Private Right of Action

In § II.A. of the IPTF Report, the IPTF asks (Question 4) whether baseline commercial data privacy legislation should include a private right of action. Consumers perceive a privacy violation either when collected data are used for purposes beyond their original collection intent, or when there is an unauthorized disclosure through a data breach, meaning the data could be used for identity theft and fraud.

A private right of action is critical for substantive consumer privacy protection.

Courts have rarely upheld a private action based on use or disclosure of consumer transaction data. In 1975, when a consumer claimed that selling magazine subscription lists constituted an invasion of privacy, the court concluded that even if "personality profiles" were being created and sold, the practice was not an invasion of privacy because the "profiles are only used to determine what type of advertisement is to be sent."[36] Twenty years later, another court ruled that a credit card company's collection of spending habits, which was then sold for marketing purposes, was not an actionable invasion of privacy.[37]

More importantly, even if companies disclose collected information in violation of their privacy policies, consumers have no right of action, as exemplified in *In re JetBlue Airways Corporation Privacy Litigation*.[38] In 2002, JetBlue Airways shared passenger profile information with a data mining company that had obtained a contract from the Department of Defense with the goal of improving security in the wake of the September 11, 2001 attacks.[39] Because some of the shared information was obtained through JetBlue's website, a number of passengers sued JetBlue, claiming, *inter alia*, breach of contract—namely, that JetBlue violated the terms of its privacy policy by sharing the passengers' personal information without their consent.[40] The court dismissed the passengers' breach of contract claim because they were

[34] *See, e.g.*, Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 117 (2007) (proposing a model privacy policy that requires opt-in for "externally disconnected uses").

[35] *See* FTC 2010 Privacy Report, *supra* note 2, at 63-69.

[36] Shibley v. Time, Inc., 341 N.E.2d 337, 339-40 (Ohio Ct. App. 1975). "The right of privacy does not extend to the mailbox …." *Id*. at 339.

[37] Dwyer v. Am. Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).

[38] 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

[39] *Id*. at 304-05.

[40] *See id*. at 304.

unable "to plead or prove any actual contract damages."[41] The court ruled that "a loss of privacy… is not a damage available in a breach of contract action."[42] It is a non-economic loss that is not compensable in a contract action.[43]

Regarding victims of data breaches, while federal courts have recognized that plaintiffs have standing to sue,[44] they have generally held the threat of identity theft due to a data breach too speculative to support common law claims of negligence by the data collector.[45]

Conclusion

A mandatory comprehensive set of legislated FIPPs is necessary to adequately protect consumer privacy. Unfortunately, the brief time between the release of the IPTF Report and the deadline for comments related thereto precludes a comprehensive discussion within this document of such legislation. The selected comments within this document, though, focus on three issues that should be addressed in federal online data tracking legislation:

- An expanded scope of what is considered personal identifying information to be protected under an enhanced framework of Fair Information Practice Principles;
- A requirement that consumers opt-in to certain data collection and sharing rather than only being afforded an opportunity to opt-out; and
- A private right of action to provide redress for improper use or unauthorized disclosure of personal identifying information.

Thank you for considering these comments.

[41] *Id*. at 326.
[42] *Id*.
[43] *See id*. at 327.
[44] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 634 (7th Cir. 2007) (holding that the injury-in-fact requirement under Article III can be satisfied by a threat of future harm); Krottner v. Starbucks Corp., Nos. 09-35823, 09-35824, 2010 U.S. App. LEXIS 25427, at *9-10 (9th Cir. Dec. 14, 2010) (holding plaintiffs met the injury-in-fact requirement for standing under Article III by alleging a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data).
[45] *See, e.g.*, *Pisciotta*, 499 F.3d at 639 ("Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."); Krottner v. Starbucks Corp., Nos. 09-35823, 09-35824, 2010 U.S. App. LEXIS 26795, *3 (9th Cir. Dec. 14, 2010) (unpublished opinion) (holding plaintiffs had not established a cognizable injury for purposes of their state-law negligence claim) (applying Washington state law).

Appendix A

Fair Information Practice Principles

Fair Information Practice Principles' (FIPPs) origins are traced to a 1973 report from the office of the Secretary of Health, Education and Welfare.[1] The report assessed the impact of computer-based record keeping on private and public matters and recommended safeguards against its potentially adverse effects.[2] The report recommended the enactment of a Federal "Code of Fair Information Practice" for all automated personal data systems, based on five basic principles that would be given legal effect as "safeguard requirements" for automated personal data systems:

- There must be no personal data record keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[3]

The Privacy Act of 1974,[4] enacted with the recognition that the increasing use of computers and sophisticated information technology has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information by Federal agencies, codified certain Fair Information Practices. The Privacy Act grants individuals access to and review of records about themselves to ensure accuracy, with an opportunity to amend information stored and collected by federal agencies.[5] And while the Privacy Act constrains federal agencies to maintain in their records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency,[6] it also permits agencies to disclose information for a routine use,[7] compatible with the

[1] DEP'T HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS (July 1973), *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.

[2] *Id*., Summary and Recommendations, *available at* http://aspe.hhs.gov/DATACNCL/1973privacy/Summary.htm. The report was particularly concerned with the "drift" toward the Social Security number becoming an all-purpose personal identifier. *Id*.

[3] *Id*.

[4] Pub. L. No. 93-579, § 2, 88 Stat. 1896 (1974) (codified as amended at 5 U.S.C. §552a (2010)).

[5] 5 U.S.C. § 552a(d).

[6] *Id*. at § 552a(e)(1).

[7] *Id*. at § 552a(b)(3).

purpose for which it was collected.[8] Paul Schwartz and Daniel Solove argue this "routine use" exception is a significant loophole when it comes to protecting individual privacy.[9]

In 1980, recognizing that conflicting individual-nation data privacy laws could hamper trans-national data flows, the Organization for Economic Development (OECD) adopted a set of Fair Information Practices Guidelines to harmonize privacy legislation, which address:

- Collection Limitation: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject;
- Data Quality: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date;
- Purpose Specification: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose;
- Use Limitation: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the Purpose Specification, except a) with the consent of the data subject, or b) by the authority of law;
- Security Safeguards: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data;
- Openness: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller;
- Individual Participation: An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him, b) to have communicated to him, data relating to him within a reasonable time at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him, c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial, and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended; and
- Accountability: A data controller should be accountable for complying with measures which give effect to the principles stated above.[10]

---

[8] *Id*. at § 552a(a)(7).

[9] Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 586-87 (1995); Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1167-68 (2002).

[10] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (last visited Jan. 18, 2011). In 1999, the OECD recommended applying its Guidelines to the Internet and electronic commerce. *See* A Global Action Plan for Electronic Commerce 20-21 (Oct. 1999, 2d ed.), http://www.oecd.org/dataoecd/12/22/2091896.pdf;

In 1995, the European Parliament and the Council of the European Union (EU) adopted its Directive 95/46/EC for the protection and free movement of personal data.[11] The principal goal of the data protection Directive was to harmonize privacy protection laws within the EU. Fundamental principles within the Directive include:

- Data Quality (Article 6): Personal data must be processed fairly and lawfully, collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes, and be accurate and, where necessary, kept up to date;
- Legitimacy (Article 7): Personal data may be processed only if the data subject has unambiguously given his consent, or processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- Information to Be Given to the Data Subject (Articles 10 & 11): Data subjects must be informed of the identity of the data controller, the purposes of the processing for which the data are intended, the recipients or categories of recipients of the data, whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, and the existence of the right of access to and the right to rectify the data concerning the data subject, regardless of whether the data is collected directly from the data subject;
- Right of Access (Article 12): Every data subject has the right to obtain from the data controller confirmation as to whether or not data relating to the subject are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed;
- Security (Article 17): The data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access;
- Remedies (Article 22): EU Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed by the national law applicable to the processing in question; and
- Liability (Article 23): EU Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.

Article 25 of the Directive also requires that transfers of personal data take place only to non-EU countries (such as the United States) that provide an "adequate" level of privacy protection. The Department of Commerce has established a certification program that establishes criteria for U.S.-based companies to meet the EU's "adequate" level of privacy

---

Jonathan P. Cody, Comment, *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation*?, 48 CATH. U. L. REV. 1183, 1206-07 (1999).

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050 (Nov. 23, 1995), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

protection standards.[12] The Department of Commerce has established "Safe Harbor Privacy Principles" that U.S.-based companies must adopt for *transferred* data:[13]

- Notice: An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure;
- Choice: An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (a) to be disclosed to a third party or (b) to be used for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual;
- Onward Transfer: To disclose information to a third party, organizations must apply the Notice and Choice Principles;
- Security: Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction;
- Data Integrity: Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used;
- Access: Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated; and
- Enforcement: Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed.[14]

Just prior to the Department of Commerce adopting its Safe Harbor Principles in 2000, the Federal Trade Commission (FTC) adopted its own FIPPs in 1998.[15] One of the FTC's central approaches to protecting online privacy is to encourage effective self-regulation.[16] To that end, the FTC adopted five FIPPs:

- Notice/Awareness: Consumers should be given notice of an entity's information practices before any personal information is collected from them, including identification of the entity collecting the data, identification of the uses to which the data will be put, identification of any potential recipients of the data, the nature of the

[12] *See* Dep't of Comm., U.S. – European Union Safe Harbor, http://www.export.gov/safeharbor/eu/index.asp (last visited Jan. 18, 2011).

[13] The Department of Commerce does not otherwise require the adoption of these principles. *See* Dep't of Comm., Safe Harbor Privacy Principles (July 21, 2000), http://www.export.gov/safeharbor/eu/eg_main_018475.asp (last updated Jan. 14, 2010).

[14] *Id*.

[15] FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS (June 1998), http://www.ftc.gov/reports/privacy3/toc.shtm.

[16] *Id*., II. History and Overview, http://www.ftc.gov/reports/privacy3/history.htm#History%20and%20Overview.

data collected and the means by which it is collected if not obvious, whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information, and the steps taken by the data collector to ensure the confidentiality, integrity and quality of the data;

- Choice/Consent: Consumers are given options as to how any personal information collected from them may be used, particularly for secondary uses of information (i.e., uses beyond those necessary to complete the contemplated transaction);
- Access/Participation: Individuals are to be given the ability both to access data about him or herself and to contest that data's accuracy and completeness;
- Integrity/Security: Collectors must take reasonable steps to ensure data are accurate and secure; and
- Enforcement/Redress: Among the alternative enforcement approaches are industry self-regulation, legislation that would create private remedies for consumers, and/or regulatory schemes enforceable through civil and criminal sanctions.[17]

Finally, in the IPTF Report, the Department of Homeland Security's 2008 FIPPs are reproduced, presumably as an example of enhanced FIPPs:

- Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII);
- Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate access, correction, and redress regarding use of PII;
- Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used;
- Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s);
- Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected;
- Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete;

[17] Fair Information Practice Principles, http://www.ftc.gov/reports/privacy3/fairinfo.shtm#Fair%20Information%20Practice%20Principles. Currently, self-regulation is the only enforcement/redress option directly available to consumers, though the FTC can bring a deceptive trade practice action against a company for failing to adhere to its privacy policy, should it provide one.

- Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure; and
- Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.