Comments to Selected Portions of the Federal Trade Commission's Report,
*Protecting Consumer Privacy in an Era of Rapid Change:*
*A Proposed Framework for Businesses and Policymakers*

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

This document contains comments to selected portions of, and questions arising from, the FTC's December 2010 privacy report. It is very important that the FTC re-examine its notice-and-choice and harm-based approaches to regulating online consumer privacy. This document addresses three issues the author believes can help address strategies for providing better online consumer privacy protection:

> The scope of an enhanced privacy framework should extend beyond traditional notions of personal identifying information;
>
> An opt-in approach to data collection and use should be adopted for most personal identifying information, rather than through opt-out and a Do Not Track feature; and
>
> Consumers need to be afforded a private right of action arising from unauthorized disclosure or sharing of personal identifying information.

## It Is Feasible for an Enhanced Privacy Framework to Apply to Data That Can Be "Reasonably Linked to a Specific Consumer, Computer, or Other Device"

At the core of the Fair Information Practice Principles (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. In the development of a Code of Fair Information Practices, the Department of Health, Education and Welfare 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,

* The views expressed in this document are those solely of the author.

> 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.[1]

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.[2] Despite a focus on protecting "personal information," the FTC has not formally defined the term. 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.[3] 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.[4]

---

[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, 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).

[2] *See* Joshua J. McIntyre, *The Number Is Me: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV., at *11-12 (Aug. 15, 2010) (forthcoming), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1621102 (describing various definitions of PII from different federal privacy laws).

[3] 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).

[4] Ohm, *supra* note 3, at 1723, 1724. *See also* McIntyre, *supra* note 2 (arguing that Internet Protocol Addresses should be recognized as PII); Frederick Lah, *Are IP Addresses "Personally Identifiable Information"?*, 4 I/S: J.L. & POL'Y INFO. SOC'Y 681, 706-07 (2008) (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*

There is precedent for a more expansive concept of PII. In its 2008 Consent Order resulting from the notorious TJX data breach,[5] the Commission embraced a more expansive definition of "personal information:"

> "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, 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.[6]

In addition, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data define "personal data" as any information relating to an identified or identifiable individual,[7] as does EU Directive 95/46/EC.[8] 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."[9] 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."[10]

---

*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).

[5] *See* Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 97-100 (2009) (describing the background and extent of the TJX data breach).

[6] *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.

[7] 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).

[8] 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.

[9] *Id*.

[10] 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).

The EU Article 29 Data Protection Working Party recently re-evaluated the concept of personal data."[11] 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.[12]

"In other words, the possibility of identifying an individual no longer necessarily means the ability to find out his or her name."[13]

Rather than select certain portions of collected data that must be included within an enhanced privacy framework, all collected data should be included. This allows a uniform approach to protecting PII. 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.[14]

**Do-Not-Track is Merely a New Implementation of Opt-out; Opt-out Should be Limited to Commonly Accepted Practices; All Other Data Collection Should Occur Only through Affirmative Opt-in**

In its December 2010 Privacy Report (pp. 53-54), 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.). Under the Commission'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,[15] it is much more practical for users to

[11] 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.

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

[13] *Id*. at 14.

[14] *See* McIntyre, *supra* note 2, at 16-17.

[15] *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).

not even bother to read a site's privacy policy.[16] This requires users to trust the sites they visit. But as noted in the Commission's Report (footnote 18, pp. 9-10), many consumers are troubled by the extent to which their information is collected and used. Indeed, users may be surprised to learn the extent of tracking that occurs.[17] To better align consumer expectations and actual information practices, *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 apparent to users, such as sharing data with external partners.[18] 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). H.R. 653, introduced February 11, 2011, though limited to financial institutions, provides a template for clear privacy notice requirements and express opt-in by consumers before nonpublic information can be shared with nonaffiliated entities.

An opt-in approach also provides more protection than the proposed Do Not Track mechanism. 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. This is reflected in H.R. 654, introduced February 11, 2011, which directs the FTC to "establish standards for the required use of an online opt-out mechanism to allow a consumer to effectively and easily prohibit the collection or use of any covered information." While this proposed legislation requires a Do Not Track mechanism, it leaves it to individual state attorneys general to enforce it through civil penalties.

**A Private Right of Action Is Critical for Substantive Consumer Privacy Protection**

Although not specifically addressed in the FTC's report and questions, 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.

---

[16] 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*.

[17] *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).

[18] *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").

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."[19] 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.[20]

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*.[21] 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.[22] 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.[23] The court dismissed the passengers' breach of contract claim because they were unable "to plead or prove any actual contract damages."[24] The court ruled that "a loss of privacy… is not a damage available in a breach of contract action."[25] It is a non-economic loss that is not compensable in a contract action.[26] Regarding victims of data breaches, while federal courts have recognized that plaintiffs have standing to sue,[27] 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.[28]

A private right of action, such as that proposed in H.R. 611, introduced February 11, 2011, is required to provide consumers meaningful remedies when personal information is improperly disclosed or shared.

---

[19] 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.

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

[21] 379 F. Supp. 2d 299 (E.D.N.Y. 2005).

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

[23] *See id*. at 304.

[24] *Id*. at 326.

[25] *Id*.

[26] *See id*. at 327.

[27] *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).

[28] *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).

**Conclusion**

The comments within this document address three important issues the author believes can provide a basis for strategies to better protect online consumer privacy:

The scope of an enhanced privacy framework should extend beyond traditional notions of personal identifying information;

An opt-in approach to data collection and use should be adopted for most personal identifying information, rather than through opt-out and a Do Not Track feature; and

Consumers need to be afforded a private right of action arising from unauthorized disclosure or sharing of personal identifying information.

Thank you for considering these comments.