FSC'S LAW & ECONOMICS INSIGHTS

Issue 13-3 Fisher, Sheehan & Colton, Public Finance and General Economics May/June 2013

IN THIS ISSUE

NOTE TO READERS

ON-LINE DELIVERY

This document presents the bi-monthly electronic newsletter of Fisher, Sheehan & Colton: *FSC's Law and Economics Insights*. Previous issues of the newsletter can be obtained at FSC's World Wide Web site:

http://www.fsconline.com (click on "News")

Fisher, Sheehan & Colton
Public Finance and General Economics
34 Warwick Road, Belmont, MA 02478
(voice) 617-484-0597 *** (fax) 617-484-0594
(e-mail) roger@fsconline.com

Significant Privacy Issues Arise from Public Utility Frequent Collection of Customer Social Security Numbers

In response to the growing use of Social Security Numbers (SSNs) in enabling the crime of identity theft, Fisher, Sheehan and Colton (FSC) recently urged the Minnesota Public Utilities Commission (PUC) to take steps to control the collection and dissemination of customer SSNs. In comments filed with the Commission on behalf of the Minnesota Legal Services Advocacy Project (LSAP), FSC said that the PUC should join the growing consensus that institutions (such as public utilities) that have collected SSNs in the past refrain from, or be prohibited from, collecting such SSNs in the future, and that Minnesota utilities be directed to seek out alternatives to the collection and use of SSNs.[1]

[1] According to the FTC: "Concerns about over-use of SSNs and their role in identity theft have increased in recent years. In a recent consumer survey, 66 percent of the respondents stated that companies should stop using SSNs to identify customers and 64 percent perceived that they were more vulnerable to identity theft when a business had their SSN." FTC (November 2007). "Staff Summary of Comments and Information Received Regarding the Private Sector's Use of Social Security Numbers," at 2.

SSNs and Identity Theft

According to FSC, the use of SSNs by private entities is one of the leading causes of identity theft. SSNs, along with a person's date of birth and name, are the three most sought-after pieces of personal information sought by identity thieves. Indeed, according to the 2007 report of the Presidential Task Force on Identity Theft, a person's SSN is the ***single*** most important piece of personally identifiable information available to identity thieves. Unlike names and addresses, which can change over a person's lifetime, it is "virtually impossible" for a person to change his/her SSN.[2]

SSNs are the key to help create false identities. A person's SSN is viewed as a "breeder document" by identity thieves. With a Social Security Number, an identity thief can create other false documents supporting a false identity, including a driver's license, retail credit account, credit card account, bank account, and similar papers. Indeed, given the lack of a standard protocol for truncating SSNs, even truncated SSNs are not helpful in preventing identity theft. While some businesses truncate the first five digits of an SSN, other businesses truncate the last four. Not only can SSNs thus be reformulated with information from multiple sources, those multiple sources need not be illicitly gained. Public documents such as tax liens, driving histories, voter registrations, bankruptcies, and the like, are all publicly-available information which might be used to match all or part of an SSN obtained from a utility record with a specific individual.

Limiting Use of SSNs

The clear direction today is to reduce, and eliminate where possible, the unnecessary collection of SSNs, FSC told the Minnesota Commission. In 2007, the federal Office of Management and Budget (OMB) issued a memo requiring federal agencies to examine their use of SSNs in systems and programs in order to identify and eliminate instances in which collection or use of SSNs is unnecessary. OMB required agencies to explore alternatives to their use of SSNs.

Like OMB's guidance to federal agencies, the Federal Trade Commission (FTC) has urged a reduction in the use of SSNs in the private sector. FTC testified to Congress that there was a need to eliminate the unnecessary use of SSNs. The FTC cited the observation of the Presidential Task Force on Identity Theft that it is not clear whether the use of SSNs by the private sector was a necessity, or a result of "convenience and habit."[3] The President's Task Force stated quite simply in its 2007 report that: "More must be done to eliminate unnecessary uses of SSNs."

[2] Unlike a lost key, the social security number cannot be changed merely because it has been lost or stolen. "Identity Theft and Your Social Security Number," Social Security Administration, Pub. No. 05-10064, Oct. 2007, at 6, available at http://www.ssa.gov/pubs/10064.pdf. There must be evidence that (1) someone is in fact wrongfully using the number, ***and*** (2) that the individual to whom the number belongs is being disadvantaged by the wrongful use.

[3] President's Identity Theft Task Force (2007). Combating Identity Theft: A Strategic Plan, at 24.

The General Accounting Office agreed. According to GAO:

> Limiting the collection of personal information, among other things, serves to limit the opportunity for that information to be compromised. For example, key identifying information –such as Social Security numbers—may not be needed for many agency applications that have data bases of other personal information. Limiting the collection of personal information is also one of the fair information practices which are fundamental to the Privacy Act and to good privacy practice in general.[4]

Reason to Limit Use of SSNs

Utilities would be hard-pressed to provide legitimate reasons to collect SSNs in today's world.[5] For example, SSNs should not be needed to identify customers who seek to present themselves as someone other than who they really are. Under the Federal FACTA statute, each Minnesota utility should by now have prepared its federally-prescribed Red Flags Plan in compliance with the statute and the FTC's Red Flags Rule. Given the ***mandatory*** nature of the Red Flags Rule as applied to public utilities, the need to ***also*** collect SSNs to authenticate that a person is who he/she purports to be has become minimized.

Limiting the collection of personally identifiable information such as SSNs is particularly important when faced with companies that operate

---

[4] GAO (June 2006). "Privacy: Preventing and Responding to Improper Disclosures of Personal Information," at 11.

[5] LSAP endorses the view expressed in the North Carolina Journal of Law and Technology:

> commentators have lamented that the social security number has become a "skeleton key" for identity theft criminals. Even more troubling, the availability of the number increases in direct proportion to its use as a key. Any organization that wishes to use an individual's social security number must make at least one copy of it; this copy is frequently stored in a computer system that may be accessible by a global workforce of employees. Given that thousands of organizations collect the number and share it with affiliates, contractors, government entities and others, the number's vulnerability to loss, employee misuse, or theft by third parties quickly becomes apparent. The advent of the Internet and the proliferation of outsourcing have only magnified the speed and extent of dispersal of the social security number. Just as the weakest link will make a chain give way, the institution with the most lax security procedures or least honest employees may be the only thing standing between a thief and the contents of an individual's bank account and private records.
>
> How secure would one feel if she gave the key to her home to every government agency, health care provider, credit card company, and other business organization with whom she had a direct or indirect relationship? What would one do if a copy of this key could be located, inexpensively or even for free on the internet, by anyone with basic information who is willing to look for it? Yet this is exactly the system that has been created via the use of the social security number as a password that can provide the holder with access to an individual's financial resources, retirement accounts, private health information, and more. Worse yet, unlike locks which can be changed if a key is lost or falls into the wrong hands, the social security number is virtually unchangeable.

Darrow and Lichtenstein. "'Do You Really Need my Social Security Number?' Data Collection Practices in the Digital Age," 10 N.C. J. L. & Tech. 1, 4 – 5 (Fall 2008) (internal citations omitted).

over multiple jurisdictions, as some Minnesota utilities do. Use of SSNs in this respect is like pollution. Once the use spills over into another jurisdiction, the state of Minnesota loses control over it. The "next" state, however, may have inconsistent protections for personal information, if any. The only way to effectively control the use of customer data, therefore, is to control it at its source, to prevent it from being collected in the first instance.

No reason exists for the Minnesota PUC to lag behind in eliminating or minimizing the use of SSNs. At the state and federal level, as well as at the regulatory level for businesses other than public utilities (e.g., educational institutions, financial institutions), there is a distinct move to find alternatives to the use of SSNs to help reduce the threat of identity theft. The Commission should join in those efforts.

Utility Use of Fair Information Practices

FSC urged the Minnesota Commission to adopt the policy that Minnesota utilities should adopt Fair Information Practices (FIPs) as the basic foundation for the privacy protection of personal information. In both the public and private sectors, Fair Information Practices are not seen as a set of legal requirements, but rather as a "framework of principles."[6] FIPs have been "widely adopted as the standard benchmark for evaluating the adequacy of privacy protections."[7] Indeed, GAO has referenced FIPs as a "universal benchmark of privacy protections."[8] The FIPs "in many ways represent the international consensus

[6] The National Research Council / National Academy of Sciences, describes FIPs as follows: "Fair information practices are standards of practice required to ensure that entities that collect and use personal information provide adequate privacy protection for that information. These practices include notice to and awareness of individuals with personal information that such information is being collected, providing individuals with choices about how their personal information may be used, enabling individuals to review the data collected about them in a timely and inexpensive way and to contest that data's accuracy and completeness, taking steps to ensure that the personal information of individuals is accurate and secure, and providing individuals with mechanisms for redress if these principles are violated. Fair information practices were first articulated in a comprehensive manner in the U.S. Department of Health, Education, and Welfare's 1973 report *Records, Computers and the Rights of Citizens*.23 This report was the first to introduce the Code of Fair Information Practices, which has proven influential in subsequent years in shaping the information practices of numerous private and governmental institutions and is still well accepted as the gold standard for privacy protection. From their origin in 1973, fair information practices "became the dominant U.S. approach to information privacy protection for the next three decades." The five principles not only became the common thread running through various bits of sectoral regulation developed in the United States, but they also were reproduced, with significant extension, in the guidelines developed by the Organisation for Economic Co-operation and Development." National Research Council (2008). Engaging Privacy and Information Technology in a Digital Age, at 48, 50 (National Academies Press).

[7] See, e.g., GAO (June 8, 2006), "Privacy: Preventing and Responding to Improper Disclosures of Personal Information," at 5.

[8] GAO (April 2006). "Personal Information: Agency and Reseller Adherence to Key Privacy Principles," at 6, 65.

on what constitutes honest and trustworthy treatment of personal information."[9] A summary of the Fair Information Practice principles is set forth in tabular form immediately below:

Fair Information Principle	Description
Collection limitation	The collection of personal information should be limited, should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.
Data quality	Personal information should be relevant to the purpose for which it is collected, and should be accurate, complete, and current as needed for that purpose.
Purpose specification	The purposes for the collection of personal information should be disclosed before collection and upon any change to that purpose, and its use should be limited to those purposes and compatible purposes.
Use limitation	Personal information should not be disclosed or otherwise used for other than a specified purpose without consent of the individual or legal authority.
Security safeguards	Personal information should be protected with reasonable security safeguards against risks such as loss or unauthorized access, destruction, use, modification, or disclosure.
Openness	The public should be informed about privacy policies and practices, and individuals should have ready means of learning about the use of personal information.
Individual participation	Individuals should have the following rights: to know about the collection of personal information, to access that information, to request correction, and to challenge the denial of those rights.
Accountability	Individuals controlling the collection or use of personal information should be accountable for taking steps to ensure the implementation of these principles.

[9] Id., at 66.

It is not merely GAO that recognizes FIPs as the "universal benchmark" or "international consensus" on what represents the proper treatment of personal information. FIPS were endorsed by the U.S. Department of Commerce in 1981.[10] The Office of Management and Budget (OMB), as early as 1998, issued a memorandum to all federal agencies saying that it "shall be the policy of the Executive Branch" that "personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974."[11] In 2004, the Chief Information Officers (CIO) Council issued the Security and Privacy Profile for the Federal Enterprise Architecture that links privacy protection with a set of acceptable privacy principles corresponding to the Fair Information Practices.[12] The Securities and Exchange Commission (SEC), the National Archive and Records Administration (NARA), the U.S. General Services Administration (GSA), have all, to one degree or another, endorsed and adopted Fair Information Practices.

According to the National Research Council, "the principles of fair information practices are as relevant today—perhaps more so—for the protection of personal information as they were when they were first formulated."[13]

[10] National Institute of Standards and Technology (April 2010). "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)," at Section 2.3 (PII and Fair Information Practices).
[11] OMB (May 14, 1998). "Memorandum for the Heads of Executive Departments and Agencies: Privacy and Personal Information in Federal Records."
[12] NIST Guide, supra, at Section 2.3.
[13] National Research Council, supra, at 337.

In addition to the Fair Information Practices presented above, FSC told the PUC that it should take notice of, and incorporate, the lessons of extended inquiry into privacy protections principles. The U.S. Department of Energy (DOE), in its 2010 report "Data Access and Privacy Issues Related to Smart Grid Technologies," included an extensive discussion of Fair Information Practices.[14]

Conclusion

For more information on the privacy issues presented by public utility collection of customer SSNs, as well as for a copy of FSC's privacy comments filed with the Minnesota PUC, please write:

roger [at] fsconline.com

Fisher, Sheehan and Colton, Public Finance and General Economics (FSC) provides economic, financial and regulatory consulting. The areas in which *FSC* has worked include energy law and economics, fair housing, affordable housing development, local planning and zoning, energy efficiency planning, community economic development, poverty and telecommunications policy, regulatory economics, and public welfare policy.

[14] U.S. Department of Energy (October 5, 2010). "Data Access and Privacy Issues Related To Smart Grid Technologies."