MINNESOTA PASSES THE NATION'S FIRST INTERNET PRIVACY LAW

By Jordan M. Blanke*

* Professor of Computer Information Systems and Law, Stetson School of Business and Economics, Mercer University, Atlanta, Georgia

8/19/16

Abstract

The paper will examine the specifications and ramifications of a new Internet privacy law passed by Minnesota. The law restricts disclosures made by an Internet service provider (ISP) of information that identifies a consumer by physical or electronic address or telephone number, by a history of Internet or online sites visited by the consumer, or by information stored on any of the consumer's data storage devices. The law permits a consumer to authorize the release of personally identifiable information, but requires the ISP to inform the consumer, in a conspicuous manner, whether such authorization will be made on an opt-in or opt-out basis. The law applies to ISPs who provide services in Minnesota, and specifically expires on the effective date of federal legislation that preempts state regulation of the release of personally identifiable information by ISPs.

MINNESOTA PASSES THE NATION'S FIRST INTERNET PRIVACY LAW

Introduction

In a scene from Steven Spielberg's futuristic film "Minority Report," the main character is shown walking through a public mall area. Holographic billboards greet him every few seconds with statements like: "Welcome back John Anderton. Would you like to buy any more blue sweaters?" or "Good morning John Anderton. I see you haven't bought any new books recently."

While the film is set in the year 2054, when sophisticated iris scan technology provides instant recognition of people by machines that scan their eyeballs, we presently have the capability to identify and monitor the habits of online users. By tracking personal information like social security numbers, telephone numbers or e-mail addresses, individuals can be immediately identified. Unlimited amounts of information can be tied to those identifiers.

When someone buys an item in a store and is asked for his or her phone number at the cash register, all the information about that transaction can be permanently associated with that person. When one uses a grocery store's discount card, all of the purchases can be recorded. On the Internet, whenever someone visits a website or requests information or performs a search, that information can be saved and linked to that person.

In the brick and mortar world, one can choose not to divulge a phone number to a clerk at the cash register, or refuse to shop at stores that require the use of a special card to receive discounts. On the Internet, however, it is becoming increasingly difficult to retain much anonymity.

If someone entered a store at a shopping mall and was greeted with a voice saying, "Welcome back Mark Williamson. Would you like to buy some more extra-large underwear today?" he might think twice about returning to that store. While some people might enjoy a personal welcome with ready service, others might prefer to shop more anonymously. In the non-electronic world, one always has the choice to boycott a store by leaving.

One of the enticing characteristics of the early Web was its aura of anonymity. Even today, many people who might be hesitant to participate in a live, face-to-face environment might feel more comfortable contributing in an electronic chat room, for example, where they do not have to deal with traditional nuances of social interaction. The pervasive collection, sharing, and selling of personal information on the Internet threatens to undermine this essential feature of the medium.

The evolution of the Internet has seen the technology of data collection far surpass the laws that might protect the information collected. While an individual can refuse to disclose personal information at a store or over the telephone, it is virtually impossible to prevent the compilation of information that one may not even be aware is being collected.

While the tragedy of September 11 temporarily pushed many concerns about privacy to a back burner, efforts are again underway to improve the personal privacy protection of Internet users. Minnesota has taken an important step by passing the nation's first Internet privacy law.[1]

Minnesota's Internet Privacy Law

Scheduled to take effect on March 1, 2003, this new law will regulate the disclosure of personally identifiable information (PII) by Internet service providers (ISPs). The law is modeled after the federal Video Consumer Privacy Act[2] and state videotape rental privacy laws from New York[3] and Minnesota.[4] Those laws generally prohibit the disclosure of the video rental habits and PII of individuals who rent videotapes. Similarly, Minnesota's new law will prohibit the disclosure by ISPs of the browsing habits and PII of individuals who purchase services enabling them to gain access to the Internet.[5]

Under the law, ISPs will be prohibited from disclosing PII except when the PII is specifically required to be disclosed[6] or is specifically permitted to be disclosed.[7] An ISP may obtain the authorization of a consumer to permit disclosure using either an opt-in or opt-out scheme.[8] The law would expire on the effective date of any federal legislation that preempts state regulation of the release of PII by ISPs.[9]

Definitions

Section 1 of the new law defines an ISP as "a business or person who provides consumers authenticated access to, or presence on, the Internet."[10] Significantly, the scope of the

---

[1] Act of May 22, 2002, ch. 395, §§ 1- 11, 2002 Minn. Laws (to be codified at MINN. STAT. §§ 325M.01-325M.09). The Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501-6506 (2002), strictly regulates the collection and use of personal information obtained on the Internet, but applies only to individuals under the age of 13.

[2] 18 U.S.C. § 2710 (2002).

[3] Video Consumer Privacy Act, N.Y. GEN. BUS. LAW §§ 671-675 (2002).

[4] MINN. STAT. §§ 325I.01-325I.03 (2001).

[5] §§ 2-4.

[6] § 3.

[7] § 4.

[8] § 4 subd. 2. Most privacy policies on the Web today use an opt-out scheme, under which users implicitly give consent to have their information shared with others unless they take some affirmative step. On many websites this is accomplished by having a check box already checked at the bottom of a screen. In order *not* to have his information shared, the user must uncheck the box. Often the user is not even aware of this choice. Under an opt-in scheme, the user would have to check the box in order to have his information shared. The default is to *not* share the information. *See generally* Jordan M. Blanke, *Web Privacy Policies and Other Adventures in Never Never Land*, 18 MIDWEST L. REV. 43 (2002); Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH. L. REV. 1033 (1999); Tom Weber, *To Opt In or Opt Out: That is the Question When Mulling Privacy*, THE WALL STREET JOURNAL, October 23, 2000 at B1.

[9] § 11.

[10] § 1 subd. 3.

law does not include operators of websites. A consumer is "a person who agrees to pay a fee to an Internet service provider for access to the Internet for personal, family, or household purposes, and who does not resell access."[11] Probably the most important definition is for PII:

> "Personally identifiable information" means information that identifies:
> (1) a consumer by physical or electronic address or telephone number;
> (2) a consumer as having requested or obtained specific materials or services from an Internet service provider;
> (3) Internet or online sites visited by a consumer; or
> (4) any of the contents of a consumer's data-storage devices.[12]

Importantly, this definition includes not only traditional personal information like name, address, telephone number, and e-mail address, and standard marketing information like product inquiries, but also Internet specific information from things like "clickstream" data[13] and "cookies."[14] The inclusion of items (3) and (4) would prohibit an ISP from disclosing identifying information about a consumer's browsing activities collected from either the server side of an Internet connection or from the consumer's own computer.

There is a great deal of targeted marketing activity on the Web today related to collecting as much information as possible about the browsing and buying behavior of individual users. A good portion of this collection is done surreptitiously, or, at least, without the knowledge of the vast majority of users. Much of this is accomplished by storing information on the user's own hard drive

---

[11] § 1 subd. 2.
[12] § 1 subd. 5.
[13] Clickstream data is a trail of information that a user leaves behind while browsing on the Web. It is like a set of footprints in the sand. Whenever anyone visits a website, information is collected and saved in a log file. It typically includes things like where the user came from to visit the site (the "referral URL"), which pages the user visited, in which order they were visited, how long the user stayed on each page, and whether the user purchased anything. This information can be collected and tied to the user's PII. Many companies are building clickstream data warehouses to collect and organize this information. Using these databases, information can be compiled about the buying habits of individual users, and inferences can be made about the browsing and purchasing habits of visitors in general.
[14] A cookie is a file or information stored in a file on the user's own hard drive. It is directed to be saved there by the website visited by the user or by advertisers or marketers associated with that site. It generally contains information that will allow the website to quickly identify the user whenever he returns. This can be quite convenient. For example, if a user registers at a website, the identifying information can be saved on his hard drive so that he will not have to reenter this information each time he visits the site. Or, if a user puts an item into a Shopping Cart at a website, he will be able to retrieve that information upon his return. Data may be saved in the cookie itself, or the cookie may contain an identification number that locates the information on the website's server computer. For example, if a user searches a website to see if it has a copy of "The Princess Bride" DVD for sale, upon his next visit, he may be asked if he is interested in buying a copy of "The Princess Bride" videotape. The cookie provides instant access to the website's database, in which the user's previous query is stored. Advertisers and marketers can also use cookies to compile sophisticated databases linking PII to transactional information. Great quantities of information about users can be amassed in this manner without the user's knowledge.

in the form of cookies. This law includes such information within the definition of PII.[15]

Required Disclosures

Section 2 prohibits ISPs from disclosing PII except as provided in Sections 3 and 4.[16] Section 3 **requires** that PII be disclosed:

(1) pursuant to a grand jury subpoena;
(2) to an investigative or law enforcement officer as defined in section 626A.01, subdivision 7, while acting as authorized by law;
(3) pursuant to a court order in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by other means;
(4) to a court in a civil action for conversion commenced by the Internet service provider or in a civil action to enforce collection of unpaid subscription fees or purchase amounts, and then only to the extent necessary to establish the fact of the subscription delinquency or purchase agreement, and with appropriate safeguards against unauthorized disclosure;
(5) to the consumer who is the subject of the information, upon written or electronic request and upon payment of a fee not to exceed the actual cost of retrieving the information;
(6) pursuant to subpoena, including an administrative subpoena, issued under authority of a law of this state or another state or the United States; or
(7) pursuant to a warrant or court order.[17]

Most of these required disclosures pertain to civil or criminal court activities. Subsection (5) requires an ISP to disclose the PII to the consumer himself or herself, and permits a fee to be charged for this service.[18]

Permitted Disclosures

Section 4 **permits** that PII be disclosed to:

(1) any person if the disclosure is incident to the ordinary course of business of the Internet service provider;
(2) another Internet service provider for purposes of reporting or preventing violations of the published acceptable use policy or customer service agreement of the Internet service provider; except

[15] *Id*.
[16] § 2.
[17] § 3.
[18] § 3 subd. 5.

that the recipient may further disclose the personally identifiable information only as provided by this chapter;

(3) any person with the authorization of the consumer; or

(4) as provided by section 626A.27.[19]

While subsection (1) sounds very broad, the term "ordinary course of business"" is defined to mean specifically only "debt-collections activities, order fulfillment, request processing, or the transfer of ownership."[20] Subsection (3) is probably the most important, and is tied to a definition of "authorization."[21]

Authorization

Authorization may be obtained in writing or by electronic means.[22] It "must reasonably describe the types of persons to whom personally identifiable information may be disclosed and the anticipated uses of the information."[23] In order to be effective, a provision in a contract between the ISP and the consumer must state conspicuously whether such authorization is to be obtained on an opt-in or opt-out basis.[24] Specifically, the provision "must state either that the authorization will be obtained by an affirmative act of the consumer or that failure of the consumer to object after the request has been made constitutes authorization of disclosure."[25]

The original Senate version of the bill contained only the opt-in rule,[26] but was expanded to include an opt-out alternative when reconciled with the House bill.[27] The choice between requiring an opt-in or opt-out scheme is one of the biggest battlefields in the privacy arena today.

Other Provisions

Section 5 requires that an ISP "take reasonable steps to maintain the security and privacy of " a consumer's PII.[28] Section 7 provides for enforcement of the law by consumers, awarding successful claimants the greater of $500 or actual damages, plus costs and reasonable attorneys fees.[29] Class actions are specifically

---

[19] § 4.

[20] § 1 subd. 4. This definition is identical to those in the federal Video Consumer Privacy Act, 18 U.S.C. § 2710 (2002), and New York's Video Consumer Privacy Act, N.Y. GEN. BUS. LAW §§ 671-675 (2002).

[21] § 4 subd. 2.

[22] *Id*.

[23] *Id*.

[24] *Id*.

[25] *Id*.

[26] S.F. 2908, 82nd Leg. Sess. (Minn. 2002), *available at* http://www.revisor.leg.state.mn.us/cgi-bin/bldbill.pl?bill=S2908.0&session=ls82.

[27] H.F. 3625, 82nd Leg. Sess. (Minn. 2002), *available at* http://www.revisor.leg.state.mn.us/cgi-bin/bldbill.pl?bill=H3625.0&session=ls82.

[28] § 5.

[29] § 7.

prohibited.[30] Also, "it is a defense that the defendant has established and implemented reasonable practices and procedures to prevent violations of this chapter."[31] This defense was not part of the original Senate bill,[32] but was added from the House bill.[33] It potentially provides a defense for any ISP who implements a reasonable privacy policy.

The law specifically expires on the effective date of federal legislation that preempts state regulation of the release of PII by ISPs.[34] Furthermore, if federal legislation were enacted that did not preempt state law, any such federal law would supercede conflicting provisions of the Minnesota law.[35]

Minnesota has taken a bold step. While the scope of the law is not great because it does not cover operators of websites, it is the first attempt at strictly regulating the release of PII by ISPs.

Potential Challenges to the Law

The Minnesota law applies to ISPs in "the provision of services to consumers in this state."[36] A potential challenge to this law might allege that it places an undue burden on interstate commerce, and is, therefore, violative of the dormant commerce clause. Because the law is rationally related to a legitimate state end and does not discriminate against out-of-state interests, chances are good that the law would survive such a challenge.[37]

Another possible challenge to the law might involve preemption. However, the statute anticipates the enactment of federal legislation that will either specifically preempt state law, or merely conflict with it. In the former case, the Minnesota law would simply expire.[38] In the latter, any conflicting provisions of state law would yield to the federal law.[39]

Federal Legislation

In April 2002, Senator Hollings and nine co-sponsors introduced one of the most comprehensive privacy bills ever presented, the Online Personal Privacy Act.[40]

---

[30] *Id.*
[31] *Id.*
[32] *Supra* note 26.
[33] *Supra* note 27.
[34] §11.
[35] § 8(2).
[36] § 9.
[37] [Discuss Calif. case and Pike, etc.]
[38] § 11.
[39] § 8(2).
[40] S. 2201, 107th Cong. (2002), *available at* http://thomas.loc.gov/cgi-bin/query/C?c107:./temp/~c107o1Q6ke. The (bi-partisan) co-sponsors of the bill are Senators Stevens, Burns, Inouye, Rockefeller, Kerry, Breaux, Cleland, Nelson (of Florida) and Carnahan. After the bill's introduction, Senator Toricellli also signed on as a co-sponsor.

The bill would preempt any state law that regulates Internet privacy to the extent that it relates to the collection, use, or disclosure of PII obtained through the Internet.[41] Its scope is much greater than and includes that of the Minnesota law, and would certainly preempt it.

Collection, Use, or Disclosure of PII

Section 101 of the bill provides that an "internet service provider, online service provider [OSP], or operator of a commercial website [OCW] on the Internet may not collect personally identifiable information from a user, or use or disclose personally identifiable information about a user, of that service or website except in accordance with the provisions of this Act."[42] Of particular significance is that the law would include *all* operators of commercial websites.[43] The Minnesota law pertains only to ISPs.[44]

Notice and Consent Requirements

Section 102 provides that an ISP, OSP or OCW "may not collect personally identifiable information from a user of that service or website online unless that provider or operator provides clear and conspicuous notice to the user in the manner required by this section for the kind of personally identifiable information to be collected."[45] This section is significant for two reasons: first, it requires "clear and conspicuous" notice; second, it restricts the mere "collection," as opposed to "disclosure," of information.[46]

---

[41] §4.

[42] §101.

[43] An "operator of a commercial website"

> (A) means any person who operates a website located on the Internet or an online service and who collects or maintains personal information from or about the users of or visitors to such website or online service, or on whose behalf such information is collected or maintained, where such website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce--
>
> > (i) among the several States or with 1 or more foreign nations;
> >
> > (ii) in any territory of the United States or in the District of Columbia, or between any such territory and--
> >
> > > (I) another such territory; or
> > >
> > > (II) any State or foreign nation; or
> >
> > (iii) between the District of Columbia and any State, territory, or foreign nation; but
>
> (B) does not include any nonprofit entity that would otherwise be exempt from coverage under section 5 of the Federal Trade Commission Act (15 U.S.C. 45).

§ 401(10).

[44] The distinction between "internet service provider" and "online service provider" is not significant as the definition section leaves the specifics to the Federal Trade Commission to create by rule to be consistent with current technology and practice. § 401(8).

[45] § 102(a).

[46] This section also sets the tone for the rest of the bill. In its 1998 Report to Congress, the Federal Trade Commission identified the "five core principles of privacy protection" and what it termed "fair information practices" as (1) notice/ awareness; (2) choice/ consent; (3) access/ participation; (4) integrity/ security; and

The term "collect" is broadly defined as

> the gathering of personally identifiable information about a user of an Internal service, online service, or commercial website by or on behalf of the provider or operator of that service or website by any means, direct or indirect, active or passive, including--
>
> (A) an online request for such information by the provider or operator, regardless of how the information is transmitted to the provider or operator;
>
> (B) the use of a chat room, message board, or other online service to gather the information; or
>
> (C) tracking or use of any identifying code linked to a user of such a service or website, including the use of cookies or other tracking technology.[47]

The notice required by section 102 shall disclose

> (1) the specific types of information that will be collected;
> (2) the methods of collecting and using the information collected; and
> (3) all disclosure practices of that provider or operator for personally identifiable information so collected, including whether it will be disclosed to third parties.[48]

Opt-in Consent

The bill adopts a bifurcated approach to consent. Sensitive personally identifiable information requires opt-in consent. An ISP, OSP, or OCW may not

> (1) collect sensitive personally identifiable information online, or
> (2) disclose or otherwise use such information collected online, from a user of that service or website,
>
> unless the provider or operator obtains that user's affirmative consent to the collection and disclosure or use of that information before, or at the time, the information is collected.[49]

"Sensitive personally identifiable information" is defined to include PII about an individual's

---

(5) enforcement/ redress). Federal Trade Commission, *Privacy Online: A Report to Congress, (1998), § III(A) Fair Information Practice Principles, available at* http://www.ftc.gov/reports/privacy3/fairinfo.htm. The bill is consistent with and includes all five elements. *See generally* Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L.J. SCI. & TECH. 57, 69-77 (2000).

[47] § 401(1).

[48] § 102(a).

[49] § 102(b).

(A) individually identifiable health information (as defined in section 164.501 of title 45, Code of Federal Regulations);
(B) race or ethnicity;
(C) political party affiliation;
(D) religious beliefs;
(E) sexual orientation;
(F) a Social Security number; or
(G) sensitive financial information.[50]

Opt-out Consent

Nonsensitive personally identifiable information requires robust notice and opt-out consent. An ISP, OSP, or OCW may not

(1) collect personally identifiable information not described in subsection (b) online, or
(2) disclose or otherwise use such information collected online, from a user of that service or website,

unless the provider or operator provides robust notice to the user, in addition to clear and conspicuous notice, and has given the user an opportunity to decline consent for such collection and use by the provider or operator before, or at the time, the information is collected.[51]

"Personally identifiable information" is defined as

individually identifiable information about an individual collected online, including--
(i) a first and last name, whether given at birth or adoption, assumed, or legally changed;
(ii) a home or other physical address including street name and name of a city or town;
(iii) an e-mail address;
(iv) a telephone number;
(v) a birth certificate number;

[50] § 401(15). "Sensitive financial information" includes
(A) the amount of income earned or losses suffered by an individual;
(B) an individual's account number or balance information for a savings, checking, money market, credit card, brokerage, or other financial services account;
(C) the access code, security password, or similar mechanism that permits access to an individual's financial services account;
(D) an individual's insurance policy information, including the existence, premium, face amount, or coverage limits of an insurance policy held by or for the benefit of an individual; or
(E) an individual's outstanding credit card, debt, or loan obligations.
§ 401(14).
[51] § 102(c).

> (vi) any other identifier for which the Commission finds there is a substantial likelihood that the identifier would permit the physical or online contacting of a specific individual; or
> (vii) information that an Internet service provider, online service provider, or operator of a commercial website collects and combines with an identifier described in clauses (i) through (vi) of this subparagraph.[52]

This last subsection is particularly significant because it would include within the definition of PII any information collected by an ISP, OSP or OCW that is combined with PII. Thus if non-PII information about an individual is collected and combined with PII, all the information is considered PII. This would arguably include most information contained in a clickstream data warehouse.

"Robust notice" is defined as "actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the Internet service provider, online service provider, or operator of a commercial website to use or disclose that information for marketing or other purposes."[53]

Exceptions

Section 104 provides for three types of exceptions to the above rules. First, section 102 does not apply to the collection, disclosure, or use of information that is necessary

> (1) to protect the security or integrity of the service or website or to ensure the safety of other people or property;
> (2) to conduct a transaction, deliver a product or service, or complete an arrangement for which the user provided the information; or
> (3) to provide other products and services integrally related to the transaction, service, product, or arrangement for which the user provided the information.[54]

Second, disclosures may be made in good faith responding to requests for information or access to information under this law or under the Children's Online Privacy Protection Act of 1998.[55]

Third, disclosures of PII generally may be made for purposes of law enforcement or pursuant to a warrant or court order,[56] or in response to a court order in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means, as long as the individual is given notice of the

[52] § 401(11).
[53] § 401(13).
[54] § 104(a).
[55] § 104(b). Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502(b)(1)(B)(iii) (2002).
[56] § 104(c)(1)(A).

court proceeding at which the order is requested and a reasonable opportunity to appear and contest the issuance of the requested order.[57]

Change in Privacy Policy

Section 103 provides that whenever an ISP, OSP or OCW makes a material change in its policy for the collection, use or disclosure of sensitive or nonsensitive PII, it must notify all users of that service or website of the change, and may not act in accordance with the changed policy until the user is afforded an opportunity to consent or withhold consent to the new policy.[58] This section is important in light of the many changes recently made by several large websites to their privacy policies.[59]

Access

Section 105 requires that an ISP, OSP or OCW provide access to PII collected from the user online, provide an opportunity for the user to suggest a correction or deletion of any such information, and make the correction or deletion.[60] The ISP, OSP or OCW may decline to make the correction or deletion if it reasonably believes that it is inaccurate or inappropriate, and it so notifies the user, and provides an opportunity for the user to refute the reasons given for declining to make the suggested correction or deletion.[61] A reasonable access fee of no more than $3 may be charged to the user.[62]

Security

Section 106 provides that an ISP, OSP or OCW must establish and maintain reasonable procedures necessary to protect the security, confidentiality and integrity of the PII it maintains.[63]

Enforcement

Sections 201 and 202 provide for enforcement of violations of the law by the Federal Trade Commission[64] as unfair or deceptive act or practices under section 18(a)(1)(B) of the Federal Trade Commission Act.[65] Section 203 provides a private right of action for users for violations regarding sensitive PII.[66] Upon a

[57] § 104(c)(1)(B).
[58] § 103(a).
[59] Changes in privacy policies at Amazon.com and eBay caused quite a stir in the online world. *See generally* Blanke, *supra* note 8.
[60] § 105(a).
[61] § 105(b).
[62] § 105(d).
[63] § 106.
[64] § 201.
[65] § 202. Federal Trade Commission Act, 15 U.S.C. 57a(a)(1)(B) (2002).
[66] § 203(a).

showing of actual harm, the user may recover the actual monetary loss, or $5000, whichever is greater.[67] Section 204 provides for a civil action by a state attorney general on behalf of the residents of that state.[68]

Conclusion

The enactment of Minnesota's Internet Privacy law is an important event. It represents the first successful legislative action to regulate privacy on the Internet. It is narrow in scope, in that it applies only to ISPs, not to operators of websites. It is likely, however, that the law will have a short life, as there are many federal bills presently under review that would preempt it. One of them, the Online Personal Privacy Act, should receive serious consideration in this next Congressional session.

[67] § 203(a)(2).
[68] § 204.