Outside Counsel

Outside Counsel

Identity Protection: Can We Live Without It?
By Harry A. Valetk
New York Law Journal

Information technology revolutionized not only the way we communicate, entertain, and learn, but also the way we shop, socialize, and conduct our daily affairs. Together with the joys of instant messaging, flashing commercial banners, and waves of spam email, the Internet introduced new threats to individual privacy that are different from anything previously possible.

Using current information technology, for example, entities can generate comprehensive records of online behavior and distribute a person's most intimate secrets in ways few can imagine, much less control. To no surprise, selling individual profiles and developing marketing lists that are sorted by political affiliations, medical conditions, body weight, ethnic groups, or religious beliefs, is a booming industry that faces few legal restrictions.

However, having so much personal information meticulously collected and freely exchanged facilitates identity fraud and, in some cases, even endangers lives.

"It's actually obscene what you can find out about people on the Internet," wrote Liam Youens before killing Amy Boyer in 1999 at the Nashua, N.H. dentist's office where she worked and then killing himself.[1] Mr. Youens' online journal chronicled his obsession with Ms. Boyer and detailed the way he paid hundreds of dollars to online research services to learn Ms. Boyer's birth date, social security number, home address, and the location of the dentist's office where she worked.[2]

In April, Robert Horowitz received a telephone call from a collection agency trying to collect on several past due debts. Because he had never applied for credit with the companies described by the collection agency representative, Mr. Horowitz believed that this was just a simple misunderstanding. However, after obtaining copies of his credit report, Mr. Horowitz learned that six accounts had been fraudulently opened in his name and were now past due. Even more disturbing, after Mr. Horowitz requested copies of the phony credit applications, he found that his name was repeatedly misspelled and that his address, date of birth, and telephone number were all incorrect. In fact, the only piece of information that was accurate was his social security number. "So much credit was handed out based solely on my social security number and not on any kind of cross-references."[3]

Information predators are quick to blame governmental agencies and lax corporate practices that post sensitive individual information online for the world to see and often misuse. According to a 23-year old computer buff from Old Bridge, N.J., convicted of bank fraud, if the Securities and Exchange Commission had not posted all those names and social security numbers on its Web site, he would not have applied for car loans using 14 other individual's names.[4]

Many believe that identity theft related crimes are rising because no law prevents or even restricts anyone from buying, selling, or displaying something as sensitive as a person's social security account number (SSN).

The Social Security Administration, for one, is powerless to control how private companies use someone's SSN because there is no provision in federal law governing or limiting the use, or disclosure, of someone's SSN, except for fraudulent use.[5] Some restrictions on the use of an individual's SSN by other governmental agencies exist under the Privacy Act that make it "unlawful for any Federal, State, or local government agency to deny any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number," unless otherwise required by statute.[6]

However, private companies are free to refuse any services, credit, deny admission, or extend membership, to anyone unwilling to furnish their SSN.[7] The imminent danger by our present state of affairs is that individuals are left vulnerable to identity theft, unchecked invasions of privacy, and subject to a growing number of serious cyberspace crimes.

Last year, Congress undertook a genuine effort to address some of these popular concerns by introducing legislation that would have prohibited the sale or purchase of social security numbers and strengthened federal authority to punish identity predators. In an effort to highlight some of the important public concerns raised by this ongoing debate, this article will discuss four bills introduced by both the House and the Senate.

Legislative Actions

The first is the Social Security Number Confidentiality Act of 2000 (SSNCA) which was proposed "to prohibit the appearance of social

security account numbers on or through unopened mailings of checks or other drafts issued on public money in the Treasury."[8]

In introducing this 1999 proposal, Representative Ken Calvert, R-Calif., expressed concern that "by simply taking a quick peek in a mailbox, or in a pile of mail left in a person's car, anyone could obtain the information needed to steal someone's identity. The open display of such private and confidential information is an invitation for scam artists to rip off our senior citizens."[9] Although the SSNCA was enacted on Nov. 6, 2000, its significance was lessened by the fact that the Treasury Department already employed protective measures to avoid displaying SSNs on unopened envelopes.[10] In effect, the SSNCA was more a formality than anything substantive.

Next, the Privacy and Identity Protection Act of 2000 (PIPA) was proposed by Senator Jim Bunning, R-Ky., and Representative E. Clay Shaw, Jr., R-Fla., to protect individuals from "the sale and purchase of social security account numbers in circumstances that might facilitate unlawful conduct or that might otherwise likely result in unfair and deceptive practices."[11] Unlike the SSNCA, the PIPA tried to significantly reform the way both the public and private sector handle an individual's SSN. In three of its seven findings, for example, the PIPA acknowledged that:

(1) The inappropriate sale or purchase of social security account numbers is a significant factor in a growing range of illegal activities, including fraud, identity theft, and, in some cases, stalking and other violent crimes.

(2) While financial institutions, health care providers, and other entities have often used social security account numbers to confirm the identity of an individual, the sale or purchase of these numbers often facilitates the commission of criminal activities, and also can result in serious invasions of individual privacy.

(3) The Federal Government requires virtually every individual in the United States to obtain and maintain a social security account number in order to pay taxes, to qualify for Social Security benefits, or to seek employment. An unintended consequence of these requirements is that social security account numbers have become tools that can be used to facilitate crime, fraud, and invasions of the privacy of the individuals to whom the numbers are assigned. Because the Federal Government created and maintains this system, and because the Federal Government does not permit persons to exempt themselves from those requirements, it is appropriate for the Government to take steps to stem the abuse of this system.[12]

To address public sector flaws, the PIPA proposed to prohibit Federal, State, or any of their political subdivisions from displaying an individual's social security account number - or any derivative of such a number - to the general public.[13] The term "display to the general public" means "the intentional placing of social security account numbers in a viewable manner on an Internet site that is available to the general public or in material made available or sold to the general public."

To reduce identity fraud opportunities in the private sector, the PIPA also proposed prohibiting the sale or purchase of a SSN and called for

regulations that would "provide reasonable assurance that social security account numbers will not be used to commit or facilitate fraud, deceptive, or crime"; and "prevent an undue risk of bodily, emotional, or financial harm to individuals." [14]

To carry out its intended purpose, the PIPA sought to create new criminal penalties for misuse of SSNs, extend civil monetary penalties, authorize judicial orders of restitution, confidential treatment of credit header information, and law enforcement authority for the Office of the Inspector General of the Social Security Administration. [15]

In his opening statement for subcommittee hearings on the PIPA, Representative Shaw recognized "identity theft [as] the fastest growing financial crime in the nation - affecting nearly 600,000 Americans annually. What was once a form of financial security has become a tool for financial ruin." [16] "Social Security numbers have become the gateway for crooked con-artists to raid your bank accounts, max out your credit cards, and literally steal your identity."[17]

In its report, the Committee on Ways and Means noted that the SSN was created in 1936 solely for the purpose of tracking workers' Social Security earnings records.[18] Today, however, the use of the SSN significantly expanded beyond its original purpose and is commonly used as a personal identifier.[19] Summarizing both arguments, the Committee noted that some believe that the expanded use of the SSN benefits the public by improving access to financial and credit services in a timely manner.[20] On the other hand, the pervasive use of SSNs makes them a primary target for fraud and misuse.[21] Citing SSA statistics, the Committee found that "identity theft" increased from 26,531 cases in fiscal year 1998 to 62,000 in fiscal year 1999.[22] Additionally, privacy concerns are continuously raised as companies increasingly share and sell personal information without the customer's knowledge or consent.[23]

An almost identical piece of legislation, the Social Security Number Protection Act of 2000 (SSNPA) was sponsored by Senator Dianne Feinstein, D- Calif., and Representative Edward Markey, D-Mass., "to strengthen the authority of the Federal Government to protect individuals from certain acts and practices in the sale and purchase of social security account numbers and for other purposes."[24] Making the same findings as the PIPA, the SSNPA also restricted governmental entities from publicly displaying SSNs and prohibited private companies from buying and selling SSN in a manner that violates regulations promulgated by the Federal Trade Commission. [25] Unfortunately, the SSNPA was referred to the Subcommittee on Telecommunications, Trade, and Consumer Protection on June 8th and never heard from again.[26]

Taking a more direct approach, the Social Security Number Privacy Act of 2000 (SSN Privacy Act) was sponsored by Senator Richard Shelby and focused only on prohibiting financial institutions from buying and selling SSNs. More specifically, the SSNPA tried "to amend the Gramm-Leach-Bliley Act, to prohibit the sale and purchase of the social security number of an individual by financial institutions and to include social security numbers in the definition of nonpublic personal information."[27]

Under the SSN Privacy Act, federal regulations would have been enacted "no broader than necessary to provide reasonable assurances that social security numbers and social security account numbers will not be used to commit or facilitate fraud, deception, or crime; and to prevent an undue risk of bodily, emotional, or financial harm to an individual."[28]

However, given the fact that regulations implementing the Gramm-Leach-Bliley Act already refer to social security numbers as "non-public personal information," legislation here may have been superfluous.[29] In any event, the SSN Privacy Act shared the same fate as its legislative counterparts when it was permanently referred to the Committee on Banking, Housing, and Urban Affairs on July 14, 2000.[30]

Conclusion

Politics and legal maneuvers aside, significant danger and concern exists about this growing epidemic for Congress to enact prophylactic legislation. Although information technology clearly improves our daily lives by personalizing services and empowering consumers with access to vast amounts of information, the high-tech economic prospects for the future will never materialize so long as a person's entire identity remains uniquely vulnerable to theft by the simple acquisition of a nine digit government account number. As it now stands, identity fraud victims are expected to undertake the time-consuming bureaucratic task of contacting every credit bureau and proving that they are not in fact dead beats. In practice, this means consumers must proceed with extreme caution before sharing any sensitive information about themselves with anyone.

The Social Security Administration, Federal Trade Commission, and New York State Attorney General's Office publish contact information, toll-free telephone numbers, and general suggestions on their web sites to help consumers protect themselves against identity theft.[31] Among them, the agencies warn that before revealing any personally identifiable information, consumers should ask how that information will be used and whether it will be shared with others.

Also, consumers should pay attention to billing cycles, guard their mail from theft, and provide their SSN only when absolutely necessary. A few private companies, like Privista, offer identity protection monitoring services online that warn consumers when signs of fraud appear on their credit reports.

However, in our booming information technology era, the fallacy underlying these measures is that they presume consumers actually can control the personal information already given to banks, credit card companies, landlords, employers, and online services, and put most of the burden on them to guard against fraud.

To close, consider the challenge as perceived by an expert. Qualified by twenty years of law enforcement experience, Florida Law Enforcement Special Agent Robert Ivey testified before the Subcommittee on Social Security of the House Committee on Ways and Means that "identity assumption and takeover is becoming the most serious non-violent crime challenge that America faces."[32]

FootNotes: [1]

"Killer Kept Web Pages On Victim," (visited Jan. 13, 2001) . [2]

Id. [3]

Protecting Privacy and Preventing Misuse of the Social Security Number, 2000: Hearings on H.R. 4857 Before the Subcommittee on Social Security of the House Committee on Ways and Means, 106th Cong. (2000) (statement of Robert Horowitz, Business Owner, Boca Raton, Florida). [4]

"The Web's Dark Side," U.S. News & World Report, Aug. 28, 2000, at 36. [5]

42 U.S.C. §408(a)(6)-(8) (making it a felony to use or disclose a social security number for fraudulent purposes); see also, Internet False Identification Prevention Act of 2000, Pub.L. No. 106-578, 114 Stat 3075 (strengthening the enforcement of Federal statutes relating to false identification); Identity Theft and Assumption Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat 3007 (making it unlawful for someone to "knowingly tranfer or use, without lawful authortiy, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or is a felony under State or local law"). [6]

5 U.S.C. §552a note (Disclosure of Social Security Number); see also Privacy Act, Section 7 (a)(1). [7]

Social Security Administration, Program Operations System Manual, GN 03325.001 (2000). [8]

Social Security Number Confidentiality Act of 2000, Pub. L. No.106-433 (2000). [9]

Introducing the Social Security Number Confidentiality Act of 1999 - Hon. Ken Calvert, (Extensions of Remarks - Nov. 5, 1999) (visited on January 13, 2001) ; see also . [10]

Treasury Financial Manual, Vol. 1, Part 4, §5035.35(c) (visited on January 13, 2001) . [11]

H.R. 4857, S. 2876, 106th Cong. §2 (2000). [12]

Id. [13]

Id., at §101(b)(1)(V). [14]

Id., at §102(b), (c). [15]

See generally id., at §§103-07. [16]

Protecting Privacy and Preventing Misuse of the Social Security Number, 2000: Hearings on H.R. 4857 Before the Subcommittee on

Social Security of the House Committee on Ways and Means, 106th Cong. (2000) (statement of Representative E. Clay Shaw, Jr., Chairman, Subcommittee on Social Security). [17]

Id. [18]

Protecting Privacy and Preventing Misuse of the Social Security Number, 2000: Hearings on H.R. 4857 Before the Subcommittee on Social Security of the House Committee on Ways and Means, 106th Cong. (2000). [19]

Id. [20]

Id. [21]

Id. [22]

Id. [23]

Id. [24]

H.R. 4611, S. 2699, 106th Cong. (2000). [25]

Id. [26]

Bill Summary and Status for the 106th Congress, (visited on January 13, 2001) ; see also . [27]

S. 2871, 106th Cong. (2000). [28]

Id., at §2(e)(2). [29]

See 15 U.S.C. §6809(4)(A); 16 C.F.R. Pt. 313, App. A; 12 C.F.R. Pts. 40, 216, 332, 573, App. A; 17 C.F.R. Pt. 248, App A. [30]

Bill Summary and Status for the 106th Congress, (visited on January 13, 2001) (31) See ; ; (last visited on January 17, 2001). [31]

[32]

Protecting Privacy and Preventing Misuse of the Social Security Number, 2000: Hearings on H.R. 4857 Before the Subcommittee on Social Security of the House Committee on Ways and Means, 106th Cong. (2000) (statement of Robert W. Ivey, Special Agent, Florida Department of Law Enforcement).

Date Received: *February 06, 2001*