609 - Privacy Update

Andrew J. Heaton
Associate General Counsel
Ernst & Young LLP

Nuala O'Connor-Kelly
Chief Privacy Leader & Senior Counsel
General Electric Company

Lisa J. Sotto
Partner
Hunton & Williams LLP

Faculty Biographies

Andrew Heaton

J. Andrew Heaton is a principal in the Washington, D.C. office of Ernst & Young LLP and holds the position of associate general counsel. He is Ernst & Young's lead lawyer for privacy, client confidentiality, data security, and e-commerce matters in the Americas. His duties also include serving as the principal counsel for Ernst & Young's office of ethics and compliance and overseeing the operation of the firm's ethics hotline.

Mr. Heaton is a certified information privacy professional and a member of the bars of the District of Columbia, New York, and Maryland.

Mr. Heaton graduated summa cum laude from Bradley University in Illinois. He received his law degree with honors from the University of Chicago Law School, where he was founding editor-in-chief of the University of Chicago Legal Forum, a finalist in the moot court competition, and a member of the law review.

Nuala O'Connor-Kelly
Chief Privacy Leader & Senior Counsel
General Electric Company

Lisa Sotto
Partner
Hunton & Williams LLP

HUNTON& WILLIAMS

CLIENT ALERT

April 2007

Contacts

Martin E. Abrams*
Senior Policy Advisor and
Executive Director,
Center for Information
Policy Leadership
1900 K Street, N.W.
Washington, DC 20006
(202) 778-2264
mabrams@hunton.com

Paula J. Bruening
Deputy Executive Director,
Center for Information
Policy Leadership
1900 K Street, N.W.
Washington, DC 20006
(202) 955-1803
pbruening@hunton.com

Lisa J. Sotto
Partner
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Additional Lawyers
Isabelle Chatelier
Maureen Cooney
Joanne Du
Frederick R. Eames
Francine E. Friedman
James A. Harvey
Jörg Hladjk
Elizabeth Hendrix Johnson
Stephen C. King
Christopher Kuner
Manuel E. Maisog
Elisabeth M. McCarthy
Amanda Nichols McGovern
Randall S. Parks
Aaron P. Simpson
Bridget C. Treacy
Angela Zhao

Center for Information Policy Leadership
Fred H. Cate
Orson Swindle*

*Not a lawyer

Hunton & Williams LLP

Do-Not-Mail Bills Introduced in 10 States

"Do-not-mail" legislation that would create do-not-mail registries recently has been introduced in a number of states. Modeled after the do-not-call phone registries, these bills would impose fines on marketers that mail solicitations to residents whose names are on do-not-mail lists. To date in 2007, 10 states--Arkansas, Connecticut, Hawaii, Michigan, Missouri, New Jersey, New York, Texas, Vermont and Washington--are considering this type of legislation. Do-not-mail bills had been introduced in Colorado, Maryland and Montana, but they have since been withdrawn.

Bills Vary Among States

The bills vary from state to state. In most cases, marketers who mail solicitations to individuals on do-not-mail lists would face fines. In Michigan, however, violations also can result in six months imprisonment, a fine of $500, or both. It is not clear from the language of the Michigan bill whether the $500 fine would be incurred for each separate violation.

Additional measures have been introduced in New Jersey, New York and Washington, where registries would include people with mental illnesses and certain senior citizens. Some measures would prohibit mailing credit card solicitations to those under the age of 21.

Nonprofit organizations and politicians would in all cases be exempt. There would also be an exemption for an established or pre-existing business relationship or for a contact with an existing customer. Such relationships generally are defined to exist when a customer makes a purchase or inquiry, or a business makes a follow-up contact with the customer within a prescribed period of time prior to the mailing.

Implications of State Do-Not-Mail Proposals

Proponents of the measures believe that do-not-mail laws would have the same effect as the existing do-not-call registries, giving consumers a voice in determining what marketing information they receive. Opponents of the bills contend the do-not-mail proposals raise significant legal questions. Among the arguments that have been made by the direct marketing community is a free speech argument, asserting that do-not-mail laws would impose on a commercial entity's free speech rights by limiting its communication with potential customers. Opponents say that the success of the do-not-call concept triggered the proposal of do-not-mail legislation, but that telemarketing is not comparable to direct mail because direct mail is not nearly as intrusive as phone solicitations. The U.S. Postal Service also has voiced its opposition to the bills.

We Can Help

Hunton & Williams' Privacy and Information Management team assists clients in complying with global privacy and information management requirements. We have experience in assessing privacy and information security risks and in drafting policies and procedures to comply with legal requirements and industry best practices. We also monitor privacy policy and regulatory trends within the United States and across the globe. If you have any questions about the status of the do-not-mail legislation, or would like other assistance regarding your organization's privacy and information security needs, please contact us.

HUNTON& WILLIAMS

CLIENT ALERT

August 2007

Minnesota Law Imposes Liability on Merchants for Costs of Breach

Minnesota became the first state to enact a law making retailers and other merchants liable to banks if they retain credit or debit card data beyond prescribed time limits and the retained information is compromised. Under the Minnesota law, H.F. 1758, banks could sue to recover costs they incur as a result of a merchant's card data breach. Such costs could include consumer notification and card replacement costs. H.F. 1758 amends the state's data breach notification law, which was enacted in June 2005 and took effect January 1, 2006.

Implications of the Minnesota Law

The Minnesota law restricts merchants' retention of credit and debit card transaction data. Merchants are prohibited from retaining data obtained from the magnetic stripe of a credit card and the personal identification number or access code for such a card after the completion of a credit card transaction. In the case of a debit card transaction, merchants are prohibited from storing such information for longer than 48 hours after the completion of a transaction.

The law further provides that, if a merchant retains such data in violation of the law and there is a breach, banks may sue to recover from the merchant the "cost of reasonable actions undertaken" to respond to the breach. Financial institutions may seek the costs of canceling and reissuing credit cards, closing and reopening accounts affected by the breach, stop payment actions, unauthorized transaction reimbursements and notification to affected individuals. Financial institutions are also entitled to recover costs for damages paid to cardholders injured by a security breach if the entity suffering the breach has violated the law.

The data retention provisions of the law take effect August 1, 2007. The provision allowing banks to file suit to recover breach costs will take effect August 1, 2008 and will apply to breaches occurring on or after that date. Critics of the law, including the National Retail Federation, believe the law is unnecessary and will significantly increase the costs of doing business for the many retailers that will be impacted by the law.

Similar Legislation Pending in Other States

Massachusetts, California, Illinois and New Jersey have introduced similar legislation that would make merchants liable for breach costs.

- The Massachusetts bill (H.R. 213) provides that the merchant commercial entity would be liable to a bank for the costs of the bank's reasonable actions on behalf of its customers due to a security breach including, but not limited to, the cost of card replacement. While this bill is still pending, it was not incorporated into data security legislation that recently was cleared by the legislature and is awaiting signature.
- In California, A.B. 779 would amend the existing California data breach notification law to make merchants, other businesses and government agencies liable to others, including banks, for reasonable costs associated with providing notification as a result of a data breach. Reasonable costs would include, but not be limited to, the cost of card replacement as a result of a breach.
- The Illinois bill (S.B. 1675) would make a "data collector" under Illinois' security breach notification law liable to a financial institution for the costs or damages incurred relating to unauthorized access to credit card or debit card account data.
- In New Jersey, A. 4413 would make retailers liable to banks for costs they incurred to protect credit and debit card customers as a result of a data breach incident.

We Can Help

Hunton & Williams' Privacy and Information Management team assists clients in complying with global and domestic privacy and information security requirements. We have experience assessing privacy and information security risks and drafting policies and procedures to comply with legal requirements and industry best practices. We also monitor privacy policy and regulatory trends within the United States and across the globe. If you have any questions about the revised Minnesota breach law or its progeny, or would like other assistance regarding your organization's privacy and information security needs, please contact us.

Contacts

Lisa J. Sotto
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Paula J. Bruening
1900 K Street, NW
Washington, DC 20006
(202) 955-1803
pbruening@hunton.com

Additional Lawyers
Isabelle Chatelier
Maureen Cooney
James A. Harvey
Jörg Hladjk
Elizabeth Hendrix Johnson
Christopher Kuner
Manuel E. Maisog
Elisabeth M. McCarthy
Randall S. Parks
Aaron P. Simpson
Bridget C. Treacy
John W. Woods, Jr.
Angela Zhao

Center for Information Policy Leadership
Martin E. Abrams*
Fred H. Cate
Orson Swindle*

*Not a lawyer

FOR METRO AREA IN-HOUSE COUNSEL

ALM

GC New York

JULY 17, 2006

Sounding the Alert On Data Breaches

Panoply of state laws on individual notification puts companies in a difficult position.

ART BY ISTOCKPHOTO

BY LISA J. SOTTO AND AARON P. SIMPSON

DURING THE PAST YEAR, news headlines announced a steady stream of information security breaches. During this time, roughly 170 breach incidents have been subject to public scrutiny; countless other incidents have gone unreported. It is estimated that more than 81 million individuals have been impacted by the publicized security breaches alone, including 26.5 million individuals whose personal information was contained on a laptop computer lost by an employee of the Department of Veterans Affairs in late May. While security breach incidents certainly occurred prior to 2005, a little-known California law passed in 2002 brought about the sudden surge in news coverage of such incidents.

This law, known as the California Computer Security Breach Notification Act (SB 1386), requires businesses to notify California residents whose personal information has been the subject of a security breach.

Lisa J. Sotto, *a partner in the New York office of Hunton & Williams, heads the firm's privacy and information management practice. She also serves as vice chairperson of the U.S. Department of Homeland Security's Data Privacy and Integrity Advisory Committee.* **Aaron P. Simpson** *is an associate in Hunton & Williams' New York office.*

Not to be outdone, 29 other states have jumped on the California bandwagon and passed breach notification laws of their own after witnessing the broad impact of the California law. With no federal law imminent, businesses that suffer security breaches are finding themselves in the unenviable position of having to comply with 30 state laws that require notification to affected individuals. Making matters more complex, many of these 30 state laws differ substantially, upping the ante on the need for a thorough understanding of the legal landscape in this ever-evolving area.

California and Other States

Under California's SB 1386, businesses are required to notify individuals if personal information about them maintained in computerized form was, or is reasonably believed to have been, acquired by an unauthorized person. "Personal information" means an individual's name in combination with a (i) Social Security number, (ii) driver's license or state identification card number, or (iii) account, credit or debit card number in combination with any required security code. The law provides a safe harbor for encrypted personal information such that notification is not required in the event of unauthorized acquisition.

If notification is required, businesses may satisfy the law's requirement by providing (i) written notice, (ii) electronic notice under limited circumstances, or (iii) substitute notice (consisting of e-mail notice, conspicuous posting on the business' Web site, and notification to major statewide media) if notifying customers will cost more than $250,000 or if more than 500,000 customers are impacted.

In the initial months following the effective date of SB 1386 on July 1, 2003, companies that suffered security breaches complied by providing notice to impacted individuals in California. If the breach impacted people outside of California, many companies chose not to notify these non-California residents, reasoning that the legal notification obligation was limited to residents of California. While this approach is correct from a strict legal perspective, companies that took this approach suffered significant reputational harm in the media firestorm that ensued following discovery of the breach. This media frenzy resulted in the passage of state security breach notification laws in a handful of other states in which state legislators feared businesses would continue to suffer breaches and not notify their state residents. This handful, which did not begin passing breach notification laws until 2005, quickly became 30 states by the beginning of 2006.

> *It is imperative that businesses fully understand, and prepare to address, each of the 30 state laws governing breach notification.*

The panoply of security breach notification laws at the state level has made compliance challenging for companies that have suffered national breaches in the past year. While the state laws are similar in many ways, they differ in four crucial ways, all of which bear on a company's notification obligations. First, the laws address different media. While most states follow California's approach and regulate breaches that involve "computerized" data, others (like North Carolina and Wisconsin) require notification if there has been unauthorized access to and acquisition of personal information in any form, whether computerized, paper or otherwise.

A second area of conflict arises in how states define "personal information." A significant percentage of states follow California's approach and define personal information to include name plus Social Security number, driver's license or state identification card number, or financial account number. Other states, however, use a more expansive definition of personal information. For example, personal information includes medical information in Arkansas, date of birth and mother's maiden name in North Dakota, and DNA profile in Wisconsin.

A third key difference among the state laws turns on whether the law contains a harm threshold that triggers notification. In California, no such harm threshold exists—all California residents whose personal information has been acquired, or is reasonably believed to have been acquired, must be notified. That is not true in several states, where notification is required only if there is a reasonable likelihood that information acquired by an unauthorized person will result in harm. In addition, the state laws have different requirements about who should be notified by businesses that suffer security breaches. In California, businesses are required to notify only those individuals affected by the breach. In other states, state regulators and consumer reporting agencies must be notified. For example, in New York and North Carolina, businesses that suffer security breaches must notify the Attorney General's office, while in New Jersey the state police must be notified.

These substantive differences highlight the need for businesses that suffer a breach to understand all 30 state laws. This understanding is particularly important in light of the reputational risk associated with notifying only in those states that require notification. Given this reputational risk, a business' decision to notify all individuals impacted by a breach (a number that often reaches into the hundreds of thousands and sometimes millions) can turn on a faraway state's notification requirement. Thus, from both a compliance perspective and a bottom line perspective, it is imperative that businesses fully understand, and

GC New York
New York Law Journal

July 17, 2006

prepare to address, each of the 30 state laws governing breach notification.

How to Respond

The first, and most critical, step any company that learns of a possible security breach must take is to determine whether personal information is reasonably believed to have been acquired or accessed by an unauthorized person. In making this determination, companies should look to several indicators, including whether the information (i) is in the physical possession or control of an unauthorized person (e.g., a stolen computer), (ii) has been downloaded or copied, or (iii) was used by an unauthorized person, such as having fraudulent accounts opened or reported instances of identity theft. Making this determination is often easier said than done. Depending on the complexity of the circumstances, determining whether a breach has even occurred could require working with a forensic investigator, at significant expense, to recreate activity on the database.

Once there is a reasonable belief that a security breach has occurred, the next step involves going to law enforcement (if necessary) and taking any internal measures necessary to restore the integrity of the affected system. As part of the report to law enforcement, companies should explain that they intend to provide notice of the breach to affected individuals in the most expedient time possible and without unreasonable delay. In certain situations, law enforcement authorities will ask companies to delay notification so as not to impede their investigation. Most of the state breach notification laws provide a safe harbor for these circumstances, but companies in this situation should make sure to ask law enforcement when it would be appropriate to send the notification and to be prepared to send the notices as soon as reasonably practicable after getting the go-ahead from law enforcement.

Once given the go-ahead to notify, companies should provide written notice to affected individuals in the most expedient time possible. In some states, such as Florida and Ohio, there is a time limit of 45 days after discovering the breach or receiving the go-ahead from law enforcement. Depending on the sensitivity of the circumstances, drafting breach notices can be an arduous task that requires significant assistance from counsel and public relations resources. At the very least, a breach notice should include (i) a general description of what happened, (ii) the nature of the personal information involved, (iii) a description of the steps taken by the company to protect personal information from further unauthorized acquisition or access, (iv) a description of how the company will assist affected individuals (e.g., by providing credit monitoring for the affected individuals), (v) information on how individuals can protect themselves from identity theft, including contact information for the three credit reporting agencies, and (vi) contact information for the Federal Trade Commission.

In addition to affected individuals, companies that suffer security breaches may be required to notify other stakeholders, including state and federal regulators, credit reporting agencies and credit card issuers. New York, New Jersey, North Carolina and Maine all require some form of notification to state regulators, typically the state Attorney General's office. New Jersey is unique in that it requires companies that suffer a security breach to notify the state police, and this notification must take place prior to notifying affected individuals.

The notification to state regulators should provide information as to (i) the nature and circumstances of the breach, (ii) the timing, content and distribution of the notices, and (iii) the approximate number of affected individuals. Because the credit reporting agencies will likely be inundated with calls from individuals affected by the breach who wish to sign up for credit monitoring or obtain a credit report, it is also a good idea, and a legal requirement in several states, to notify the credit bureaus. In Minnesota, this notification is required to occur within 48 hours of notifying affected individuals. Finally, if the breach involves personal information associated with a credit card, the company is likely contractually required to notify affected credit card issuers.

Planning Is Key

Given the panoply of state breach notification laws and their varying requirements, it is only a matter of time before Congress passes a federal security breach notification law. There are currently more than a dozen security breach notification bills that have been introduced in Congress. Most commentators agree that a law will not be passed by the end of this fall's congressional session. From a business perspective, the most important feature of any federal breach notification law is that it pre-empt state law. Because data often flows beyond state boundaries, a federal law that preempts state breach notification laws would ensure that affected residents of every state are notified of a data breach while at the same time easing the ability of companies to provide such notification by allowing them to adhere to a single standard.

Until a federal law is passed, companies that suffer security breaches across state lines find themselves in the difficult position of analyzing the law in 30 or more states to understand their compliance obligations. Given the reputational risks associated with security breaches, in addition to legal compliance exposure, it is imperative that companies not only understand these issues, but also have a plan in place to manage the notification process in the event they suffer a security breach.

HUNTON& WILLIAMS

CLIENT ALERT

November 2006

Contacts

Martin E. Abrams*
Senior Policy Advisor and Executive Director,
Center for Information Policy Leadership
1900 K Street, N.W.
Washington, DC 20006
(202) 778-2264
mabrams@hunton.com

Lisa J. Sotto
Partner
200 Park Avenue
New York, NY 10166
(212) 309-1223
lsotto@hunton.com

Elizabeth Hendrix Johnson
One Bank of America Plaza
Suite 1400
421 Fayetteville Street
Raleigh, NC 27601
(919) 899-3073
ehjohnson@hunton.com

Additional Lawyers
Isabelle Chatelier
Maureen Cooney
Frederick R. Eames
James A. Harvey
Jörg Hladjk
Stephen C. King
Christopher Kuner
Manuel E. Maisog
Elisabeth M. McCarthy
Amanda Nichols McGovern
Randall S. Parks
Kathy Robb
Ashley B. Rowe
Aaron P. Simpson
Angela Zhao

Center for Information Policy Leadership
Fred H. Cate
Orson Swindle*

*Not a lawyer

Hunton & Williams LLP

New Law Requires Agencies to Develop Model GLBA Privacy Notice

President Bush recently signed into law the Financial Services Regulatory Relief Act of 2006. Section 728 of the new law requires federal financial services agencies to jointly develop a model form privacy notice that provides the disclosures required by section 503 of the Gramm-Leach-Bliley Act (GLBA). Section 728 also provides a safe harbor; financial services institutions that elect to use the model form will be deemed in compliance with GLBA notice requirements.

Section 728 provides that the model form must:

- be comprehensible to consumers, with a clear format and design;
- provide for clear and conspicuous disclosures;
- enable consumers to easily identify the sharing practices of a financial institution and compare privacy practices among financial institutions; and
- be succinct with an easily-readable type font.

The agencies are required to publish the model form in the Federal Register for comment within 180 days of the statute's enactment, i.e., on or before April 11, 2006.

Prototype Notice

Federal financial services regulators have been field-testing a prototype notice and other types of simplified notices, and are well into the second phase of their two-part research project. The prototype notice and summary of phase one research were published on February 28, 2006. Simplified privacy notices were pioneered and advanced by policy leaders at Hunton & Williams' Center for Information Policy Leadership, as discussed in Ten Steps to Develop a Multilayered Privacy Notice.

The prototype notice is three pages long, providing a "Key Frame" intended to give consumers context to increase comprehension, a "Secondary Frame" providing answers to frequently asked questions and definitions, and an opt-out form that provides several mechanisms by which consumers can opt out of certain types of disclosures. The prototype notice also includes a "Disclosure Table" listing seven types of information-sharing practices in which financial services institutions may engage. The institution issuing the notice must indicate which sharing practices it employs and whether the consumer may opt out of each practice. The prototype notice is unique among previously tested notices in its provision of this Disclosure Table, which allows consumers to easily compare sharing practices.

Insurance Notices

The Financial Services Regulatory Relief Act of 2006 does not address insurance industry compliance with GLBA, which is regulated by the states. Thus, the impact of the proposed model notice on the insurance sector is uncertain.

Future Outlook

U.S. financial services companies generate hundreds of millions of privacy notices each year. Simplified notices in the financial services sector may well have an impact on consumer expectations outside the financial services sector. Data protection agencies in Europe, New Zealand, Australia and Canada already encourage the use of simplified notices such as those discussed in Ten Steps to Develop a Multilayered Privacy Notice.

We Can Help

Hunton & Williams' Privacy and Information Management team assists clients in evaluating compliance with evolving privacy and information security standards. We frequently help clients develop privacy notices, including GLBA-compliant notices and website privacy statements. If you would like assistance in developing a privacy notice, please contact us. For additional information about the Center for Information Policy Leadership at Hunton & Williams, please contact Marty Abrams.

New York Law Journal
INVESTIGATIONS & COMPUTER FORENSICS
Tuesday, May 29, 2007
ALM

Data Breach!

Correct Response Crucial

BY LISA J. SOTTO, JOHN W. WOODS JR. AND JOHN J. DELIONADO

THE THREAT TO CORPORATE networks, and the information contained on those networks, has never been greater. While 15, or even five, years ago the compromise of computer data would likely have been the work of a lone hacker or disgruntled insider, there are increasing signs that these events are often the work of complex criminal organizations. The need for sophisticated professionals knowledgeable in the legal issues surrounding these events has increased.

Most individuals familiar with these events understand that a breach involving the compromise of personal data will trigger state laws requiring notification to affected individuals. For lawyers, however, these events pose a myriad of additional competing and important legal issues. Of critical importance is how a company handles a compromise event. The actions it takes in the first days after learning of an event can have a profound

ART BY NEWSCOM

Lisa J. Sotto *is a partner in the New York office of Hunton & Williams,* **John W. Woods, Jr.** *is a partner in the firm's Washington, D.C. and Richmond, Va. offices, and* **John J. Delionado** *is an associate in the firm's Miami office.*

The threat to corporate networks, and the information they contain, has never been greater.

effect, including the possibility of litigation, government scrutiny, negative public attention and the erosion of the organization's customer base.

Companies must recognize that a data breach requires actions that go well beyond simple compliance with state breach notification laws. Some of the issues about which a business may need legal advice are:

(1) conducting an investigation into the event;

(2) notifying auditors and the securities regulators;

(3) notifying law enforcement authorities;

(4) notifying contracting parties (such as payment card issuers);

(5) notifying regulatory agencies with oversight authority or consumer regulatory bodies; and

(6) notifying the public.

Investigating the Event

Given the issues that can arise, understanding the factual contours of the event are critically important. Most importantly, companies must recognize that upon discovery of an issue, the event should not be handled like just another problem for the Information Technology (IT) department.

Ignoring the threat is not an option, but it may be equally dangerous to engage the problem with inadequate resources. The most important step is for a company to retain a qualified network security consultant to conduct an investigation overseen by legal counsel. The structure of the engagement of outside experts in these events is critical, and these experts must be focused on conducting the investigation in a way that will best assist the company.

Many businesses have sophisticated counsel who are well versed in the litigation process and may have the ability to direct consultants and determine the source of the compromise. A word of caution, however.

Corporate counsel generally engage in a variety of functions within a company and often make or assist in its business decisions. This dual role of corporate counsel may serve to unravel what might have been a privileged internal investigation. Engaging and obtaining the advice of litigation counsel will best serve a company in such a situation since it provides to it the best chance to preserve available privileges. Legal privileges are hard to come by, and easy to lose.

Privilege extends to communications between a company and outside legal counsel. Courts also protect as "work product" any material prepared by a party or its attorneys or other representatives in anticipation of litigation.[1] Where an internal investigation is undertaken and experts are used, *United States v. Kovel*[2] provides the benchmark standard and must be considered by counsel. Courts have routinely applied the *Kovel* test to third party consultants ranging from accountants to patent consultants.[3] Where privilege has been properly protected, the work-product doctrine will extend to materials prepared for counsel by the consultants.[4]

A company must keep in mind that whatever is determined in the investigation, even where privilege is successfully protected, privilege "only protects disclosure of communications; [not] underlying facts[.]"[5] What will be protected by privilege in the event it is preserved are the judgments, strategy and recommendations by counsel and counsel's agent, the expert consultants.

Devoting proper attention to a breach event is a company's best chance to limit or, in some instances, avoid entirely any damage to itself. Taking all reasonably possible steps to preserve the privilege is fundamental when dealing with a breach, regardless of whether there was a compromise of personal information. How forensic experts are retained to go about the task at hand and who directs them can mean the difference between creating a valuable privileged engagement that can benefit a company versus a road map to would-be litigants and government regulators that documents a company's darkest hour.

After taking all prudent steps to best preserve privilege, the internal investigation must focus first on the nature of the compromise and how it occurred. Given that the response must begin immediately to determine the source and scope of the compromise, it is often necessary, or at least expedient, to have the outside consultant obtain information from a trusted internal IT professional within the company. As with any highly confidential and significant event, it is prudent to keep the circle of people circumscribed.

Inform Senior Management

The compromise of personal data has become a boardroom event.

The scope of the breach and the effect that it can have on a company may be an event that affects the corporate public profile and possibly its stock price in the event the company is publicly traded. Since a data compromise can have such a wide-ranging and significant impact, company management must be kept abreast of the information developed during the investigation, and particularly any significant revelations.

What the decision-makers in the organization must be informed of immediately is the security posture of the network and whether there has been compliance with relevant industry standards. In addition, a company needs to review whether it has followed its own information security policies and procedures.

Where an event is significant enough that the business' independent auditors must be informed, the auditors will undoubtedly seek answers to many hard questions. Auditors will focus on the findings resulting from the investigation as well as the methodology used in evaluating the event. They will also scrutinize the quality of the investigation and what it revealed.

For a publicly traded company, the decision-makers will need to evaluate whether a disclosure is warranted. Trusted securities counsel is essential to this process and should be engaged from the outset of the investigation to assist in making this critical determination.

Involving Law Enforcement

A compromise event is very often the work of criminals and not simply the result of negligence. Federal law enforcement has become increasing sophisticated and has developed the tools to identify and arrest those who commit criminal acts against a victim company.

The U.S. Secret Service has had great success with the Electronic Crimes Task Force that has been developed and flourished in many of the Service's large field offices and headquarters in Washington, D.C. This task force allies itself with state and local law enforcement as well to ensure that the best resources are brought to bear. Similarly, the Federal Bureau of Investigation has grown its crack Computer Analysis and Response Team and has had significant success combating computer crime.

Along with the Secret Service and the FBI, the U.S. Department of Justice (DOJ) now has a group of experienced and knowledgeable prosecutors to combat computer crime. At DOJ headquarters, there is now a group of trial attorneys in the Computer Crimes and Intellectual Property Section devoted to investigating and prosecuting computer crimes throughout the country. Further, many of the large U.S. Attorney's offices have sophisticated Assistant U.S. Attorneys designated as computer and telecommunications coordinators experienced in investigating and litigating complex computer crimes.

The Computer Fraud and Abuse Act (CFAA) is the primary federal criminal statute that addresses computer crimes.[6] Potential criminal liability attaches when someone intentionally accesses a computer without authorization, typically known as an outside hack, or when someone exceeds authorized access.

In investigating crimes, law enforcement has the power and ability to go beyond the limitations of an internal investigation. Investigative techniques can include grand jury subpoenas, search warrants, Pen Registers (surveillance devices), Electronic Communications and Privacy Act warrants (which are essentially search warrants aimed at a user's account with an Internet service provider), and even Title III wire interceptions. Generally, any hope of catching the individual or group responsible for criminal conduct against a company depends on allowing law enforcement the time and ability to use the techniques available to it.

The state breach notification laws actually encourage companies to notify law enforcement by allowing a cooperating company to delay public notification in order to allow law enforcement to conduct a confidential investigation (assuming law enforcement agrees that a delay in notification would assist in its investigation). At least one state, New Jersey, has made notification to law enforcement a condition precedent to notifying affected individuals.

Notifying Contracting Parties

A company must evaluate whether it has contractual obligations to notify significant business partners of the compromise event.

Where payment cards are involved, the terms of the contract often require consultation with the card issuers in the event of a security breach. Where such obligation exists, the notification should be accomplished as soon as possible. Typically, a company will reveal the relevant facts discovered through its investigation, but not the privileged opinions of counsel or the experts.

Depending on the contract, the notice may need to take the form of a formal incident report filed with the card company. Further, card companies may require an independent audit by a data security firm conducted on their behalf and funded by the company that experienced the breach.

Contacting Regulators

Any company that is within a regulated industry will need to consult counsel about whether the entity regulating it must be informed.

There are strict guidelines, for instance, where a federally insured financial institution is involved since there is oversight by Federal Depository Insurance Company, the Office of the Comptroller of Currency, or the Federal Reserve. Compromise events, however, draw regulatory scrutiny even where a company is not federally regulated.

The Federal Trade Commission (FTC) has enforcement authority in the privacy arena pursuant to Section 5 of the FTC Act,[7] which prohibits unfair or deceptive trade practices. The FTC has demonstrated its commitment to investigate data breach events as it recently established a new division of Privacy and Identity Protection. The FTC looks to whether a company has failed to take appropriate action to protect personal information of individuals and, thus, constitutes an unfair or deceptive trade practice.

The FTC has focused its enforcement actions pursuant to Section 5 on security breaches. Notifying the FTC of the event and framing the circumstances can greatly assist a company in avoiding an enforcement action, rather than taking a more passive approach whereby the FTC may learn of the event through information in the public realm that may be rife with inaccuracies and hearsay.

Letting the Public Know

California was the first state to pass a law requiring organizations to notify affected citizens where their personal information was compromised.

As these compromise events came to light with some frequency in 2005 and garnered significant attention from the media and lawmakers, approximately 35 other states, plus New York City, Washington, D.C. and Puerto Rico, have enacted similar notification laws. At the state level, the duty to notify individuals affected by a breach generally arises when there is a reasonable belief that computerized sensitive personal information has been acquired or accessed by an unauthorized person in an accessible form.

State laws typically define "personal information" to include an individual's first name or first initial and last name, combined with one of the following: (a) a Social Security number; (b) a driver's license or state identification card number; or (c) a financial account, credit or debit card number, along with a required password or access code.

Where notification is required, it generally must be done in the most expedient time possible and without unreasonable delay. Companies are generally given time to investigate the event and, as discussed above, may be able to delay notification where they have notified law enforcement. In several states, however, including Florida, Ohio and Wisconsin, notification is required within 45 days of the date the incident was discovered.

Conclusion

Companies that are afflicted with a data breach cannot give such an event short shrift. As these events have become more widespread, public and government scrutiny over a company's handling of a breach event have increased. It is essential that victim companies take all prudent steps to prevent becoming further victimized in the legal courts or the courts of public opinion.

A company so afflicted must prepare to address the problem in a well-organized and meticulous manner, led by a team of sophisticated professionals able to recognize the myriad issues confronting the company. Recognizing that such a situation is front page news and not a back room event is the first step toward surviving the crisis and getting back to (successful) business as usual.

1. See generally *Hickman v. Taylor*, 329 U.S. 495 (1947).
2. *United States v. Kovel*, 296 F.2d 918 (2d Cir. 1961).
3. See, e.g., *In re Grand Jury Proceedings Under Seal*, 947 F. 2d 1188 (4th Cir. 1991) (finding privilege applied to communication with accountant where communication was "made for the purpose of facilitating the rendition of legal services covered by the privilege").
4. See *United States v. Nobles*, 422 U.S. 225, 239 (1975).
5. *Upjohn Co. v. United States*, 449 U.S. 383, 395 (1981).
6. 18 U.S.C. §1030.
7. 15 U.S.C. §45.

THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

HUNTON & WILLIAMS LLP
1900 K STREET, N.W.
WASHINGTON, D.C. 20006-1109

TEL 202 • 955 • 1500
FAX 202 • 778 • 2201

FRED H. CATE
DIRECT DIAL: 202-419-2019
EMAIL: fcate@hunton.com

September 5, 2007

Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex K)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: SSNs in the Private Sector—Comment Project No. P075414

Dear Mr. Clark:

Thank you for the opportunity to respond to the July 30, 2007, request of the Federal Trade Commission (FTC) for public input on private-sector uses of Social Security numbers (SSNs). I am a Distinguished Professor at the Indiana University School of Law-Bloomington, director of Indiana University's Center for Applied Cybersecurity Research, and a Senior Policy Advisor in the Center for Information Policy Leadership at Hunton & Williams (the Center).

These comments are submitted in my capacity as a Senior Policy Advisor in the Center. The Center was founded in 2001 to develop innovative, pragmatic approaches to privacy and information security issues from a business-process perspective while respecting the privacy interests of individuals. These comments have benefitted from the Center's extensive work on identity verification and authentication and the input of Center members, but they do not necessarily reflect the views of the Center or its members.

These comments will address the critical roles that SSNs play in aiding in the identification of individuals and helping to ensure that data about an individual is accurately associated with that individual, and the challenges to accomplishing these vital tasks. Rather than attempt to restrict the availability of SSNs, the government should focus its efforts on addressing three issues that threaten the use of SSNs for these important purposes:

1. The inappropriate use of the SSN as a default password or as a stand-alone evidence of identity;
2. The use of the SSN by criminals to impersonate others and commit fraud; and

3. The difficulty the government faces in ensuring that its system for issuing, maintaining, and canceling SSNs is efficient and accurate.

These comments conclude by recommending that the policy discussion should focus not on the SSN, but on how best to meet the needs of identifying individuals, verifying identities, and accurately linking data to individuals.[1]

The Role of SSNs as Unique Identifiers

As FTC Chair Deborah Platt Majoras testified before the Senate Commerce Committee in 2005, "Social Security numbers today are a vital instrument of interstate commerce. With 300 million American consumers, many of whom share the same name, the unique 9-digit Social Security number is a key identification tool for business."[2] Indeed, SSNs currently fill three critical roles in the private sector as identifiers of individuals. The first is aiding in the identification of individuals—helping us to differentiate among individuals with the same or similar names. The second role is assisting in verifying that the person presenting himself or herself—to apply for instant credit, seek a government benefit, or board an aircraft—is who he or she claims to be. The third is helping to ensure that data about an individual is associated with that individual and no one else.

The first role—the identification function—is clear and critical. Too many people share the same or similar names—there are more than 60,000 John Smiths and 43,000 Robert Joneses in the United States alone[3]—and, as discussed in greater detail below, addresses change too frequently and are subject to too many variations for either to serve as reliable identifiers. As a result, a distinctive number is required.

The second role—identity verification—is often misunderstood and, on occasion, still misapplied in practice. Obviously, the fact that an individual presents an SSN does not prove that he or she *is* the person that the SSN identifies. Rather, the SSN, when combined with other information, provides an efficient, reliable way of locating a credit report or other record

[1] These comments address SSNs in the private sector in connection with commerce and consumer transactions rather than the employer-employee relationship. Legal requirements concerning the use of SSNs in the employment context raise important issues that are beyond the scope of these comments.

[2] *Data Breaches and Identity Theft*, Hearing of the Committee on Commerce, Science, and Transportation, U.S. Senate, June 16, 2005 (prepared statement of the Federal Trade Commission).

[3] *Enhancing Social Security Number Privacy*, Hearing of the Social Security Subcommittee of the House Ways and Means Committee, June 15, 2004 (statement of Brian McGuinness).

containing information that can then be used to verify the identity of a person. So, for example, if I call a financial institution to perform a transaction or obtain account information, I may be asked for my SSN (and other information) to link me to the right account; information in that account can then be used to verify my identity. Or if I apply for instant credit at a retailer, the retailer may ask for my SSN as a way of locating a summary credit report about me. That credit report may list, among other things, my name, address, phone number, past addresses, and other identifying information. The retailer can then compare the information I have put on the credit application with the information contained in the credit report to determine if I am who I claim to be.

Knowing the SSN alone does not and should not be used to establish identity; it is merely an effective way of locating reliable information about an individual that then can be used to verify his or her identity. SSNs do not have check digits, they are often mistyped in records, they have been issued to more than one individual, and fraudsters intentionally link SSNs to fictional people. The SSN is not proof of anything related to identity; it is merely a link to data that can be used to verify identity.

SSNs also play an essential third role: helping to ensure that data are linked to the right individuals. SSNs help to ensure the accuracy and completeness of records. As a result, individuals can be treated fairly and subsequent users of the data have confidence in the data. When an individual applies for instant credit or an auto loan or a mortgage the lender wants to know that it is seeing an accurate and complete picture of that individual's creditworthiness and that there will be reliable, affordable ways of determining if the individual declare bankruptcy or overextends himself or herself on credit in the future. SSNs facilitate the correct linking or association of data in the databases that do this. This is critical to ensuring that the underlying data store is sufficiently accurate and reliable to support not only credit and other important decisions, but also the identity verification function described above.

The Challenge of Accurately Linking Data and People

The challenge of associating the right data with the right people is greater than might first appear. Consumer and privacy groups have highlighted the magnitude of this challenge in their complaints about alleged inaccuracies in credit reports and public records. The heart of their charges is not that the data are wrong, but that they are linked to the wrong person. This challenge is exacerbated by many factors, including:

- The frequency of common names and the fact that names are not constant, thanks in part to 2.3 million marriages and 1.1 million divorces every year.[4]

- The variety of addresses available to many people (e.g., home, office, vacation home, Post Office box), the fact that several people may share the same address, and the speed with which addresses and telephone numbers change: according to the U.S. Postal Service, approximately 17 percent of the U.S. population—about 43 million Americans—changes addresses every year; 2.6 million businesses file change-of-address forms every year.[5]

- The inconsistencies with which we record names (e.g., J. Smith, J.Q. Smith, John Q. Smith) and addresses (e.g., "123 Main," "123 Main Street," "123 Main St.," "123 S. Main Street," "123 Main Street, Apt. B").

- The spread of first telephone and then Internet technologies, the increased mobility of the population, and the development of truly national competition mean that fewer transactions are conducted face-to-face, much less with people we know.

As a result of these and other factors, the need for a unique, ubiquitous, national, constant, and authoritative identifier has become inescapable. Many activities in which we engage in both public and private sectors are impossible or impractical without it. That is why the SSN has evolved to fill this role: modern government and business activities required it to identify individuals and ensure that information about one individual is not erroneously attributed to another individual.

Ironically, the need for unique identifiers is so great that data systems which for legal or other reasons do not rely on SSN, have consistently had to create other unique identifiers. Where those data systems interact with each other or with systems that require SSNs (e.g., payroll, tax, etc.), they must employ translation tables to link one unique identifier with another. This introduces inefficiencies and greater risk of errors, as well as requires creating and maintaining new datasets of potentially sensitive information.

[4] National Center for Health Statistics, *National Vital Statistics Reports*, vol. 51, no. 8, May 19, 2003, at 1, table A.

[5] United States Postal Service Department of Public Affairs and Communications, *Latest Facts Update*, June 24, 2002.

SSN Recommendations

There are, of course, problems with SSNs in our society today. Three are especially acute.

First, some institutions use SSNs inappropriately as a default password or as stand-alone evidence of identity. This is akin to using street address or telephone number as a password or proof of identity. It is inappropriate, and policymakers would do well to discourage such uses through education, regulatory oversight, and, if necessary and after an appropriate opportunity for updating or replacing legacy systems, prohibition, enforcement, and prosecution. Similarly, the government should evaluate whether its increased reliance on the SSN in employment and other settings is appropriate.

Second, criminals seek to use SSNs to impersonate others and commit frauds. This exploitation in part seeks to take advantage of the inappropriate role given SSNs by some institutions. So, for example, a business that sets default consumer online account passwords to SSN invites the fraudulent use of SSNs by criminals seeking illegal access to those accounts. Eliminating those inappropriate uses will curtail those criminals' efforts to exploit the SSN.

But other criminals seek to use SSNs even in settings where they are being appropriately used. This almost always requires combining the SSN with other data. The criminal then fraudulently presents the SSN as his or her own, for example, when applying for credit, and attempts to supply the other data (e.g., name, address, account information) from other sources that the creditor will match with the data linked to the SSN in an effort to verify identity. This is a real and growing risk, but it is not best addressed by restricting the availability or use of SSNs. In fact, restricting access to SSNs may be counterproductive, since fraud tools to detect the patterns associated with fraudulent use of SSNs often require access to SSNs.

Moreover, since other unique identifiers will just take their place, restricting access to SSNs will only have the effect of pushing the attempted fraud from one identifier to another. Rather, more effective responses are to create incentives for the more accurate matching of less readily available data, encourage the use of SSN-related data matching in connection with other identification tools, enhance penalties for the fraudulent use of SSNs and the creation of fabricated SSNs, vigorously enforce SSN fraud laws, and intensify research into other means for verifying identity.

It is striking both how obvious the need to make SSNs harder to exploit is and how little policymakers have focused on it. The Strategic Plan issued in April by the President's Identity Theft Task Force, for example, identified "making it harder to misuse consumer data" as one of

its four strategies for combating identity theft, but then offered only two specific recommendations for implementing this strategy: "hold workshops on authentication" and "develop comprehensive record on private sector use of SSNs."[6] I urge you not to fall into this same trap; making SSNs harder to misuse will not be simple, but it is an important goal and worthy of your sustained attention.

The third problem with SSNs today, especially given their importance in a wide range of settings, is ensuring that every individual has a unique SSN, that they are linked to the correct person from the start, that the government does not issue duplicate SSNs, and that the registry of deceased person's SSNs is kept up-to-date. In short, it is essential that the Social Security Administration makes certain that the system of issuing, maintaining, and canceling SSNs is efficient and accurate.

In summary, rather than attempt to restrict the availability or appropriate use of SSNs, policymakers should instead focus on how to restrict their inappropriate use. In fact, given the importance of accuracy in data matching and in linking people to data, we should be encouraging, not diminishing, the appropriate use of SSNs. The alternative is less accuracy, less efficiency, and greater risk as different users or groups of users create their own unique identifiers and then have to create translation tables to equate them.

The recent trend among policymakers to encourage the treatment of SSNs as secret information creates the misimpression among individuals and institutions that they can be used alone for identity verification, as if knowing a SSN somehow proved that you were that individual. This is unfortunate and could easily be avoided by treating SSNs as the public information they have historically been. This would focus attention on their appropriate use, and make clear, once and for all, that they are not appropriate to use as passwords or proof of identity themselves.

A Misfocused Policy Debate

The reality of the essential roles that the SSN plays as an identifier and the challenges the SSN is essential to overcoming suggest that the current debate over SSNs is misfocused. Banning private-sector uses of the SSN would solve no problems. In fact it would exacerbate current problems related to fraud and authentication. SSNs are not the issue, rather, it is the need to distinguish among individuals, verify identity, and accurately link data that should be the focus of our concern. If Congress eliminated the private-sector use of SSNs tomorrow, another unique identifier would of necessity be created. We could call it something different than SSN,

[6] The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 42 (2007).

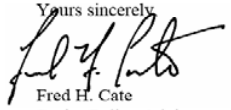
THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

but it would have to serve the same purposes and it would present the same issues. Policymakers should therefore be concerned with those underlying issues.

This may not always be the case: new data-matching technologies and algorithms are already enhancing the ability of some sophisticated organizations to match data without SSNs and research is continuing into tools for verifying identity that do not involve data matching. But for the present, SSNs are widely relied on as part of the process for verifying identity and ensuring that information is associated with the correct person. Policymakers and the public have a significant interest in ensuring that both of these tasks are carried out accurately, efficiently, and reliably. Ensuring that—whatever the means—is the critical issue on which our attention should be most focused.

The Center for Information Policy Leadership and I stand ready to assist in fostering an informed and thoughtful discussion on these issues. Again, thank you for the opportunity to submit these comments.

Yours sincerely,



Fred H. Cate
Senior Policy Advisor