INFORMATION SECURITY BREACHES

Looking Back & Thinking Ahead

Fred H. Cate

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

The Centre for Information Policy Leadership develops initiatives that encourage responsible information governance in today's digital society. The Centre is a member-driven organization that operates within the Privacy and Information Management practice at Hunton & Williams LLP. Through collaboration with industry leaders, consumer organizations and government representatives, the Center provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal needs and interests in today's global information age.

Fred H. Cate is a Distinguished Professor, C. Ben Dutton Professor of Law, and director of the Center for Applied Cybersecurity Research at Indiana University. A senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams LLP, he is a member of Microsoft's Trustworthy Computing Academic Advisory Board and of the National Academy of Sciences Committee on Information for Terrorism Prevention.

The views expressed herein are those of the author alone and should not be attributed to any other person or organization.

www.informationpolicycentre.com

Executive Summary

Concern over information security breaches has led to the recent publication of "guidance" concerning security breaches by data protection commissioners in the United Kingdom, Canada, New Zealand, and, most recently, Australia. A key focus of all of these documents is the notice that institutions must provide to individuals whose data are involved in information security breaches.

At the same time, the European Union has already begun the process of considering a draft directive governing electronic communications services that contains provisions governing security breaches, including a security breach notification requirement. National and multinational data protection officials have called for expanding the notice provisions to apply to information security breaches in other economic sectors.

All of these documents build on—in some cases explicitly—the experience of the United States. Beginning with California in 2002, 43 states and the District of Columbia have adopted legislation requiring that institutions suffering breaches of personal information must notify the individuals whose data are involved.

The recent proposals from the United Kingdom, Canada, New Zealand, and Australia reflect many of the practical lessons from the broad and diverse U.S. experience about the advantages and limits of notices. Some aspects of these proposals, however, as well as the pending EU directive and the responses of European data protection commissioners, suggest that important insights from the U.S. experience are being overlooked. They thus risk repeating mistakes made by their U.S. counterparts. Those include:

1. **Defining "security breach" so broadly that it makes the term, and the notices it prompts, less meaningful**. The recent government guides define "security breaches" to include the loss or theft of devices (e.g., laptops or external drives) and storage media (e.g., disks or USB drives) that happen to contain personal data, even in the absence of any evidence that the data have been accessed. Breaches are also defined to include misdirected or undelivered faxes, emails, and parcels, or other errors involving responsible parties who have no interest in accessing or misusing the data.

2. **Focusing too much on notices to address security breaches**. Notices are always a second-best tool because they only *respond* to breaches, not *prevent* them. Moreover, they shift the burden from the responsible parties to the innocent data subject. The preoccupation with notices is even more problematic when they are required when there is no risk to individuals or nothing individuals can do to guard against that risk.

3. **Justifying notices as a response to identity fraud**. Identity fraud is declining, despite information security breaches, and recent studies suggest that breaches play little role in facilitating fraud. The U.S. Government Accountability Office reported in summer 2007 that in only one of the 24 largest breaches publicly reported in the United States between January 2000 and June 2005 was there evidence of true identity theft. In 2008, researchers at Carnegie Mellon University, using data from the U.S. Federal Trade Commission, found "no statistically significant effect that [breach notice] laws reduce identity theft."

4. **Ignoring the limits of notices and the negative consequences of their inappropriate use**. Notices seem inadequate to the task of empowering consumers to protect themselves since notices are widely ignored and rarely acted on even if received. The requirement for notices in situations in which they are not realistically likely to prevent or mitigate harm threatens to exacerbate the existing tendency of recipients to ignore those notices. Similarly, the inappropriate use of notices is likely to misfocus the public and industry on security breaches, and divert scarce resources away from dealing with more pressing security threats. This is especially true of notice requirements that punish industry through public exposure for inevitable and often harmless security breaches. Put simply, if we think real risks are posed by security breaches, the notice response is too timid. If not, the notice response is too great.

5. **Applying a twentieth-century response to a twenty-first-century problem**. Breach notices—like privacy notices—were designed for a world in which data processing was infrequent, highly centralized, and clearly structured. Today, the collection and use of personal data are ubiquitous. And demand for personal data from business, the government, and other organizations is escalating. In this data-intensive, complex, and global world, wide-scale reliance on breach notices and privacy notices is increasingly outdated. If individuals must be notified every time personal data or the media on which they are stored cannot be accounted for, the public and the environment will succumb under the deluge of notices and individuals will rapidly learn to ignore them completely. Notices are too slow, too cumbersome, and too poorly timed to provide meaningful protection for information security, and requiring them as a broad response to security threats promises to inundate individuals with notices that they are ill-equipped and unlikely to act on. The proliferation of digital data, global commerce and data flows, and serious security threats challenges the old ways of thinking. Linking privacy and security protection to notices is ill-suited as a broad response to the realities of the global flows of digital information or of the sustained threats to that information in the twenty-first century.

Introduction

In recent months, concern over information security breaches has led data protection commissioners in the United Kingdom,[1] Canada,[2] New Zealand[3] and, most recently, Australia[4] to publish "guidance" concerning security breaches. While currently non-binding, these frameworks originate from regulators who exercise considerable authority over data-handling practices, and they are likely to serve as roadmaps for future legislation. In fact, the governments of Canada and the United Kingdom have already begun the process of introducing laws modeled on their prior advice. A key focus of all these documents is notice that institutions must provide to individuals whose data are involved in information security breaches.

The European Union has gone further to begin considering a draft directive governing electronic communications services that contains rigorous provisions governing security breaches, including a security breach notification requirement.[5] National and multinational data protection officials have called for expanding the notice provisions to apply to information security breaches in other economic sectors.[6]

All these documents build on—in some cases explicitly—the experience of the United States. Beginning with California in 2002, 43 states and the District of Columbia have adopted security breach legislation.[7] In addition, in 2005 U.S. federal regulators issued final interagency guidance for federally regulated financial institutions and their duty to disclose breaches.[8] These laws all have in common the requirement that institutions suffering breaches of personal information must notify the individuals whose data are involved. Beyond this core point, the U.S. laws differ as to whom they apply, how they define personal information (only a few states include medical and biometric information), what triggers notification (ranging from unauthorized access to data to reasonable possibility of harmful use of data), whether encrypting the data will exempt them from notification requirements, who must be notified (some require notification of specified state authorities), the timing of notification, the content of the notification, and the penalties for noncompliance (with many providing for statutory damages between $500 and $1,000 per person whose data is compromised, and some providing for trebling of damages for willful noncompliance).

The recent proposals from the United Kingdom, Canada, New Zealand, and Australia reflect many of the practical lessons from the broad and diverse U.S. experience about the advantages and limits of notices. Some aspects of these proposals, however, as well as the pending EU directive and the responses of European data protection commissioners, suggest that some important insights from the U.S. experience are being overlooked. They thus risk repeating mistakes made by their U.S. counterparts. The risk, as the U.S. experience suggests, is that poorly targeted breach notice requirements misfocus the resources available to enhance information security, diminish the

effectiveness of notices by inundating individuals with inappropriate notices, and contribute to industry practices and public policies that fail to address the most important security risks today or those most likely to pose the greatest threat tomorrow.

This white paper highlights five key sets of lessons from the U.S. and other nations' experiences with breach notices in light of recent initiatives to expand use of breach notices around the world.

1. Understanding Security Breaches

Information security is important; security breaches may or may not be, depending on what is included within the term "security breach." Most breach laws define "security breach" to include unauthorized access to defined categories of personal information (in the United States, usually information used to create or access financial accounts). The Australian consultation paper, for example, defines a breach as occurring when "personal information is exposed to unauthorized access, use, disclosure or modification."[9]

There are two problems with this definition. The first is that personal information is stored on devices (e.g., laptops or external drives) and storage media (e.g., disks or USB drives) that are often lost or stolen. U.S. regulators have tended to treat such data as having been "accessed," even in the absence of any evidence that they have been. The second problem is that personal data are routinely "disclosed" through misdirected faxes, emails, and parcels, or other errors involving responsible parties who have no interest in accessing or misusing the data. Again, U.S. regulators tend to treat these everyday events as involving unauthorized access to those data. Given that European data protection laws generally define personal data more broadly than their U.S. counterparts, especially in the business setting, an even wider range of misdirected communications might be expected to be regarded as security "breaches." By not addressing whether personal data have actually been accessed, and, if so, by whom and in what context, the broad definition of "security breach" lumps together deliberate theft of data with the theft or loss of equipment or media containing data, or the accidental receipt of personal data.

Many of the largest "breaches" reported to date turn out not to involve access to data at all. For example, the May 2005 theft from a Department of Veterans Affairs' employee's home of the laptop containing Social Security numbers and birthdates for 26.5 million veterans and active-duty military personnel constitutes the largest public sector data breach in the United States. It triggered months of press attention, led to the notification of all 26.5 million individuals and the firing or disciplining of numerous employees, and it cost the government millions of dollars. But when the laptop was recovered two months later, the FBI reported that the data had never been accessed. The thieves had stolen the laptop for the laptop, not for the data it contained.[10]

Similarly, that same month a box containing four back-up tapes of data about millions of CitiFinancial customers disappeared while being shipped via United Parcel Service. At the time, the loss of the box was heralded by the press as the United States' largest private-sector security breach, and CitiFinancial provided notice and credit monitoring services to every individual with data on one of the four missing tapes. The tapes have never been recovered. There has been no higher than normal incident of identity theft involving the individuals whose data was on the tapes. In fact, there is no evidence that any of the data on them was every accessed by anyone. Rather, the box containing them is just another of the thousands of packages lost each year while in transit. Because the tapes contained personal data, the loss of the box in which they were being shipped constitutes a "breach" under U.S. law. The misdelivery of mail, faxes, and email similarly have been regarded as breaches, even in the absence of evidence that the personal data they contain was accessed by anyone.

Most of the more recent breach guides highlight the breadth of the definition. For example, the U.K. Information Commissioner's Office notes that a breach can result from "loss or theft of data or equipment on which data is stored," "equipment failure," "human error," or even "unforeseen circumstances such as a fire or flood."[11] Such a sweeping scope necessarily means that the guidance or rules that follow will apply not only when information has been accessed without authorization, but also in circumstances in which the data merely *could* have been accessed, even if there is no evidence that they have been, and experience and professional judgment suggests that they have not been. This breadth poses real challenges for regulators about how to write and enforce rules for mere potentialities, as opposed to actual occurrences. As discussed in greater detail below, it also poses challenges for businesses and other institutions holding personal data.

The recent guides from the United Kingdom, Canada, New Zealand, and Australia demonstrate sensitivity to the challenges posed by such a broad definition of data breach by recognizing that notification is not appropriate in response to all breaches. In the words of the U.K. guidance, "informing people about a breach is not an end in itself."[12] Instead, each of the guides provides factors that should be considered when determining whether notification is appropriate.

Several of the guides include language suggesting that in situations in which data are lost, are stored on equipment that is lost or stolen, or are sent to a responsible but unauthorized party by accident—where there is no evidence that the data themselves have been accessed—notification might be inappropriate. The New Zealand information paper suggests that where "an address database may in error be sent out of a company to a trusted mail house used by the company" and "the error may be quickly discovered and the database be retrieved safely," there may be "little point in notification."[13] The Australia consultation paper stresses that notification is necessary only when "an information security breach creates a real risk of serious harm to the individual."[14] The Canadian guide suggests that one factor to be considered when determining whether to notify is whether the disclosure was to an "unknown party or to a party suspected of being involved in criminal activity."[15]

This qualitative analysis of the risk of harm to the individual stands in stark and welcome contrast to most U.S. laws, which typically require notification on a strict liability basis. Unfortunately, it also contrasts with the approach recommended by data protection officials in the European Union, which follows the U.S. model in requiring "mandatory notification." The European Data Protection Supervisor issued an opinion on the pending ePrivacy directive in which he recommended that "the ePrivacy Directive and particularly Article 4 [concerning security breaches] should not contain any exception to the obligation to notify."[16] This is even broader than the U.S. approach, which generally provides an exception for notification if data are encrypted.

2. The Role of Notices

Breach notices are justified on several grounds. The most common is to "enable individuals to take steps to protect themselves from any harmful effects" of the breach, most commonly thought to be identity or financial fraud.[17] Other justifications include to increase "accountability" of organizations that suffer breaches, raise "awareness among the public,"[18] and "allow the appropriate regulatory bodies to perform their functions, provide advice and deal with complaints."[19] As a practical matter, only the first justification, which is discussed in greater detail below, should require notification directly to the individuals whose data were involved in the breach. The others may require more public disclosure or notice to applicable regulators.

The United Kingdom, Canadian, New Zealand, and Australian documents all note the importance of having a "clear purpose" for notification and only using notice when it serves that purpose.[20] Even when notices have a clear purpose, however, it is important to recognize how limited their role may be in the overall context of data security. For example, notice is always a *response* to an event after it has occurred, rather than the *prevention* of that event. Moreover, where sensitive personal information is involved, notice is almost always an inadequate response. Not even the best notice can restore confidentiality to data that have been disclosed, and while some personal data may be capable of being changed (e.g., credit card numbers or account numbers), most are not.

Notice is also problematic because it shifts—or gives the appearance of shifting—the burden from the organization possessing the data to the individuals whose data were breached. This is especially problematic if the breach does not pose a reasonable risk of harm to the individual or if there is nothing that the individual can do to mitigate that harm.

The United Kingdom, Canadian, New Zealand, and Australian documents demonstrate an acute awareness of the limited role and function of notices. The Australian consultation paper, for example, places notices within a broader context of the need to keep personal information secure and the tools (in some cases, legally required) for doing so. The paper addresses "risk assessment, policy development, staff training, technology, monitor[ing] and review[ing], standards, and privacy impact

assessments and audits," before ever getting to information security breaches.[21] The New Zealand information paper notes that the best way to prevent breaches is to have a "well thought out and effectively implemented information security plan for all personal information held."[22]

This broader context is very important because it not only highlights the importance of prevention, as well as response, but also helps focus attention on the existence of many possible tools that address not only security breaches but other potential threats. For example, credit card fraud existed long before security breaches. Fortunately, efforts to detect and block fraudulent charges and illicit access to accounts are highly successful. The financial services industry, for example, intercepts and blocks most fraudulent credit card charges. Moreover, research suggests that only a small percentage of breached credit card numbers are ever involved in subsequent attempts at fraudulent use. Visa estimates that fraudulent use is attempted with only 2 percent of compromised credit card numbers, and the company blocks most of those attempts.[23] Other evidence collected in a July 2005 study by Thomas Leonard and Paul Rubin suggests that the percentage of fraudulent use may be lower.[24]

The guides also all treat notices as only one of four components of a response to a data breach: (1) "containment and recovery"; (2) "assessment of ongoing risk"; (3) "notification of breach"; and (4) "evaluation and response."[25] And even then they limit notices to when notification serves a "clear purpose"[26] and is "necessary in order to avoid or mitigate harm to an individual."[27]

This approach differs significantly from that followed in most U.S. states, which have adopted breach notification laws as standalone measures, divorced from any broader security context and unconnected to any obligations to attempt to prevent security breaches. Moreover, most state laws require notification even when there is no risk to the individual or nothing the individual can do to mitigate that risk.

The other common response to security breaches in the United States—adopted by 47 states and the District of Columbia—is credit "freeze" laws.[28] These laws permit individuals to restrict access to their credit reports, thereby hopefully diminishing the ability of those who possess breached personal information to use it to commit identity fraud. Ironically, credit freeze laws are another example of an incomplete response to breaches: they don't address the fraudulent use of credit card, debit card, or account numbers, or other harms resulting from breaches that don't involve access to a credit report; they shift the burden of acting to individuals; and they operate without regard to risk of harm.

3. The Relationship of Security Breaches to Identity Fraud

The most common justification for breach notices is the need to protect personal information from use in identity fraud. Identity fraud involves one person impersonating another for the purpose of obtaining a benefit, for example, opening a credit account or taking out a loan, writing a check, filing a claim, or otherwise attempting to enrich oneself by claiming to be someone else. Given the breadth of offenses the term includes, identity fraud (or "identity theft" as it is often called) is a common and frightening crime, and one that advocates of breach notice laws appear to believe is facilitated by security breaches. Breach notices are thus seen as an important tool for notifying people whose data have been involved in a breach to be especially vigilant for signs of identity fraud.

State and federal interest in identity fraud and security breaches in the United States over the past decade has led to the creation of data about both and about their interrelationship. Two observations from this research are particularly pertinent.

First, all of the government, industry, and academic studies of identity fraud in the United States show that the crimes grouped under that name are actually *declining*. According to a household telephone survey conducted by Synovate on behalf of the U.S. Federal Trade Commission in 2003 and 2006, and four times beginning in 2005 by Javelin Strategy & Research, the frequency of identity fraud has fallen every year in both real numbers and as a percentage of the U.S. population from a high of 10.1 million predicted victims in 2003 (4.7 percent) to 8.1 million (3.6 percent) in 2008.[29] Moreover, this survey lumps together two distinct forms of identify fraud: "account takeover" (where the perpetrator makes fraudulent use of an existing account, most commonly through a credit or debit card transaction) and what researchers label "true identity theft" (where the perpetrator uses personal information about another individual to open a new account in the victim's name). Account takeover is comparatively easy to detect, and under U.S. law, consumers are generally insulated from financial liability for credit and debit card fraud.[30] Although the numbers vary from year to year, account takeover accounts for between two-third and three-fourths of identity fraud incidents; true identity theft is far less common.

News reports about the political, marketing, and financial motives that may lead some political and industry leaders to focus so much attention on identity fraud, despite the evidence of its decline, have appeared in the Associated Press,[31] *BusinessWeek*,[32] *Money* magazine,[33] the *New York Times*,[34] *Slate* magazine,[35] and other publications.

Second, there is very little evidence of any link between security breaches and identity fraud. In the 2007 Javelin survey, of the 31 percent of self-reported identity theft victims who knew how their information was obtained, only 3 percent thought that the source was "possibly related to a security breach."[36] Even more telling is a 2006 study performed by ID Analytics, operator of the largest U.S. commercial fraud-detection network. ID Analytics analyzed approximately 500,000 accounts and identities involved in four security breaches that occurred in 2003 and 2004. Two of the

breaches involved identity-level information (e.g., names and Social Security numbers), which are typically used to commit true identity theft. Two involved account-level information (e.g., account numbers or passwords), which are more likely to lead to fraudulent use of existing accounts (i.e., account take-over).

For the two breaches involving account-level data, six and eight months, respectively, after the breaches, ID Analytics found *no increase* in the misuse rates for the affected accounts.[37] The same was true for the breach involving identity-level information (in this case full consumer name, address, phone number and Social Security numbers for almost 200,000 individuals) stored on a laptop. Six months following the theft of the laptop, ID Analytics found a "misuse rate" of 0.0 percent: none of the data had been used to open new credit card, wireless, or retail credit accounts in the names of the people affected by the breach.[38]

The other breach of identity-level information that ID Analytics studied involved the deliberate targeting of data (including name, date of birth and Social Security number for more than 100,000 individuals) by a highly sophisticated fraud ring. Two years after the breach, the misuse rate was .098 percent; ID Analytics detected an effort to open a fraudulent credit card, wireless, or retail credit account for one out of every 1,010 people whose data were involved in the breach. This is slightly lower than the average fraud rate of 1 per every 1,020 accounts that ID Analytics observed for "non-breached" data.[39]

This breach appears to be that suffered by ChoicePoint, but whether it is or not, it is consistent with ChoicePoint's experience. In early 2005 ChoicePoint reported that thieves had deliberately targeted sensitive personal data on 163,000 individuals. The company provided notice to the affected individuals and settled a Federal Trade Commission suit for allegedly failing to secure data adequately by paying a $10 million fine and establishing a $5 million restitution fund—the largest settlement in the Commission's history.[40] In June 2008, the Commission notified ChoicePoint that it had transferred the balance of the $5 million redress fund to the U.S. Treasury after finding that only 131 consumers had presented valid claims for a total of $141,753.[41] The actual fraud rate was therefore 1 per every 1,244 individuals who had data breached—less than the "ambient" fraud rate in the United States.

The U.S. Government Accountability Office reported in summer 2007 that of the 24 largest breaches publicly reported in the United States between January 2000 and June 2005, in only three was there evidence of any resulting misuse of an existing account, and in only one was there any evidence of true identity theft.[42] These data are supported by the fact that while the number of reported information security breaches in the United States, Canada, the United Kingdom, Japan and other countries has soared over the past five years—to include more than 322 million records as of August 2008—identity fraud appears to have declined by one-fifth.[43]

Identity fraud and security breaches are both certainly important issues, but there is little evidence connecting the two, especially in the case of true identity theft. As a result, data breach notice

laws are unlikely to have any effect on the prevalence of fraud, which is precisely what researchers have found. Using data from the U.S. Federal Trade Commission, researchers at Carnegie Mellon University in 2008 attempted to measure the impact of breach notification laws on identity fraud from 2002 to 2006; they found "no statistically significant effect that [such] laws reduce identity theft."[44]

Studies and surveys are backward-focused, and so may not accurately predict the future relationship between information security breaches and identity fraud. In addition, it is important to recognize that virtually all the studies on the link between breaches and identity fraud focus on the United States. While this is not surprising, given that the United States has the longest experience with security breach notices, it is important to recognize that there are fundamental differences between credit markets in the United States and those in most other parts of the world. For example, the United States has three national credit reporting bureaus, but there is no similar pan-European system in the European Union.[45] But the available data to date shows little relationship between security breaches and identity fraud.

4. The Risks of Notices

Breach notices can pose risks to their recipients and to society's interest in good information security more broadly. These risks may be divided into three broad categories: risks resulting from the realities of the notification process, risks resulting from the impact of notices on their recipients, and risks resulting from the incentives they create for industry and other entities that collect, use, or store personal data.

a. The Notice Process

We know a great deal about notices and how they work in practice from a variety of contexts, but the most immediately applicable is the arena of privacy notices. Notice is a fundamental principle of most data protection standards around the world, including the OECD's 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*,[46] the European Union's 1995 data protection directive,[47] APEC's 2004 Privacy Framework,[48] and most of the national and provincial data protection laws enacted in the past three decades.[49] This extensive experience has taught us that notices are often never received, never read, or never acted upon.

For example, in the United States, according to the U.S. Postal Service, 52 percent of unsolicited mail is never read.[50] Similar figures are reported by companies about the rates at which their emails are opened by consumers. One of the United States' largest online service providers indicated in 2002 that 58 percent of its marketing emails sent to its own customers were never opened.[51] In 1997, U S WEST (now Qwest Communications), one of the largest telecommunications

companies in the United States, tested a variety of methods for seeking consent from its customers to use information about their calling patterns (e.g., volume of calls, time and duration of calls, etc.)—to market new services to them.[52] Of all the residential customers that U S WEST attempted to contact, 55 percent never received the offer or request for consent, despite multiple attempts.[53]

Moreover, the available evidence indicates that individuals tend to ignore privacy notices even when they are made aware of them. The chief privacy officer of Excite@Home told an FTC workshop on profiling that the day after *60 Minutes* featured his company in a segment on internet privacy, only 100 out of 20 million unique visitors to its website accessed that company's privacy pages.[54] According to an independent research firm's analysis, an average of 0.3 percent of Yahoo! users read its privacy policy in 2002. Even at the height of the publicity firestorm created in March 2002 when Yahoo! changed its privacy policy to permit advertising messages by email, telephone, and mail, that figure rose only to 1 percent.[55] This is by no means limited to privacy notices. It appears to be true of most mandated disclosures, whether medical informed-consent forms, mortgage disclosure forms, or license terms on software packages and splash screens.

There is no better example of the failure of notices to alert consumers to the need for action than the Gramm-Leach-Bliley financial privacy notices. Under that U.S. law, by July 1, 2001, the tens of thousands of financial institutions to which it applies had mailed 2 billion or more notices.[56] If ever consumers would pay attention, this would appear to be the occasion: the notices came in an avalanche, the press carried a wave of stories about the notices, privacy advocates trumpeted the new law, and the information at issue—financial information—is among the most sensitive and personal to most individuals. Yet the consumer response was negligible, and a late September 2001 survey revealed that 35 percent of the 1,001 respondents could not recall even receiving a privacy notice, even though the average person had received a dozen or more.[57]

The lack of consumer attention to Gramm-Leach-Bliley notices prompted then-Federal Trade Commission Chairman Timothy Muris to comment at the end of 2001:

> The recent experience with Gramm-Leach-Bliley privacy notices should give everyone pause about whether we know enough to implement effectively broad-based legislation based on notices. Acres of trees died to produce a blizzard of barely comprehensible privacy notices. Indeed, this is a statute that only lawyers could love—until they found out it applied to them.[58]

So one of the important risks of breach notices is that because they do not reach the affected individuals or the individuals fail to read them, the notices do not result in consumers having the opportunity to take those steps that might mitigate the harm caused by the breach. Notices thus seem inadequate to the task of empowering consumers to protect themselves when a breach threatens them with harm.

b. The Impact on Individuals

A second category of risks is that associated with how individual can—and do—respond to breaches if they are made aware of the risk. Again, the experience with privacy notices is instructive. Even when privacy notices are received, the evidence suggests they usually fail to provoke any significant response—positive or negative. Ironically, in the context of privacy notices, it does not matter whether the notice is asking for a response from the consumer to permit use of personal data or to block such use; neither prompts consumers to respond.

This was clearly demonstrated by a late 2000 test conducted by one of the United States' ten largest online service providers. The company randomly selected two groups of its registered online users and sent to both an email about a change in the company's policy regarding email notices of "special offers and events." To the first group of 94,421 users, the company wrote that they would receive those communications unless they opted out within 14 days. To the second group of 88,787 users, the company wrote that users who wished to receive notices of "special offers and events" from the company would need to opt in within 14 days. Both emails included the same links to the notification preferences section of the user profile, information on how to access that section in the future, and links to the company's user agreement and privacy policy. The response rates were virtually identical: 4.41 percent responded to the first (opt-out) email; 4.55 percent responded to the second (opt-in) email.[59] The fact that the opt-in and opt-out rates were virtually the same suggests that the figures reflect little if anything about privacy preferences, but a great deal about the difficulty of getting consumers to respond to any request.

Anecdotal evidence suggests that security breach notices are provoking precisely the same lack of reaction. Many organizations that have sent notices report that they rarely receive any response from consumers, especially as breach notices have become more common. Offers of credit monitoring or other tools to help guard against harm that might be caused by the breach are rarely taken advantage of by more than 5 percent of recipients. To the extent notices are being relied upon to inform and motivate consumer behavior, five years of experience with them in the United States suggests they are failing to do so. Thus, if harm is threatened by a security breach, notices are not working to cause consumers to take the steps available to them to protect themselves—a key goal of breach notices identified in all the consultation guides to date.

The lack of individual response may reflect a calculation that either the breach poses no reasonable risk of harm to the recipient of the notice or that there is nothing the individual can do to protect himself or herself. If that calculation is inaccurate, then it reflects a failing of the notice process: the notice has not been received or it has not been sufficiently informative or persuasive to motivate the desired behavior. But there is growing evidence, as already discussed, that the calculation often is accurate—that no real harm is threatened by the breach or that if there is harm, there is little the individual can to mitigate it—which makes the use of the notice inappropriate.

Defining the terms under which notice is appropriate, and those in which it is not, is a major focus of the United Kingdom, Canadian, New Zealand, and Australian guides. For example, the Canadian document notes that "the challenge is to determine when notices should be required … on a case-by-case basis."[60] According to the guide, "the key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an individual … tak[ing] into account the ability of individuals to take specific steps to mitigate any such harm."[61]

This is a critical and necessary inquiry if notices are to have their intended impact. And while it is consistently stressed in the United Kingdom, Canadian, New Zealand, and Australian guides, it is ignored in the United States, at least at the state level, where most states require notification irrespective of risk of harm and of whether there is anything the recipient can do to mitigate harm. Some federal policymakers in the United States, by contrast, have shown greater concern for targeting notices to those situations in which they might make a meaningful difference.

What is more surprising are the current proposals in the European Union for the expansive use of notices, even where there is no risk of harm or nothing the individual can to do guard against that harm. The current draft of the EU ePrivacy directive would require mandatory notification of both national regulatory authorities and individual customers of "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of publicly available electronic communications services."[62] Even the accidental destruction of data, where there is no risk posed of any harm whatever, would require mandatory notification. The European Data Protection Supervisor and the Article 29 Working Party of European data protection commissioners have recommended expanding this provision still further to apply to all "information society services."[63]

Requiring breach notices in situations other than those in which they are realistically likely to prevent or mitigate harm or serve some other clearly articulated valuable function threatens to exacerbate the existing tendency of recipients to ignore those notices. Like the boy in the fairy tale who cried "wolf" too many times when no wolf was present, thereby causing the villagers to ignore his cries when a wolf really did threaten their home, regulators run the risk of teaching individuals to ignore notices by using them inappropriately.

Similarly, the inappropriate use of notices seems likely to misfocus the public on security breaches, when the evidence suggests that individuals face more serious threats that there actually are practical steps they can take to guard themselves against. For example, identity fraud is often perpetrated by people the victim knows. Of the one-quarter to one-third of victims of identity fraud surveyed in the Synovate and Javelin studies who knew who had taken their personal information, more than half of the perpetrators every year was a friend, family member, neighbor, in-home worker, or co-worker.[64] In fact, according to the 42 to 54 percent of victims in those studies who knew how

their personal information was obtained, between 29 and 38 percent report each year that it was a lost or stolen wallet or purse.[65] So while regulators are requiring that consumers be notified of security breaches—the least common way to date that information used for identity fraud is obtained—those notices may be unintentionally causing individuals to ignore the practical steps that they—and only they—can take to protect themselves against far more common threats closer to home.

c. Industry Incentives

Empowering individuals to protect themselves is not the only justification for breach notification laws. Proponents also point to the incentives that notices can create for better security through public embarrassment, legal liability, and regulatory pressure. These are potentially powerful incentives, but using notices as a way of achieving them is not without risks, especially if notices are required for all breaches indiscriminately.

Most security experts recognize that some unauthorized access to data is inevitable, no matter how great the investment in securing the data. This inevitability is of course much broader when applied not only to the theft of sensitive data, but also to the theft or loss of equipment and media that contain such data. If data processors suffer the same financial and reputational penalties for negligently permitting personal data to be accessed by an unauthorized third party, as opposed to being incidentally involved in the loss or theft of some of the media on which they are stored, it is not clear that they will be motivated to invest in better security for personal data, as opposed to investing in insurance, attorneys, and public relations staff to deal with the inevitable loss. In other words, if this incentive operates irrespective of the institution's investment in good security, past security success, or the harm posed by the breach, then the incentive is not likely to prove effective in motivating the desired behavior. In fact, the U.S. experience suggests that one major incentive of breach notification laws for organizations suffering security breaches is not to report. According to one 2008 survey, only 11 percent of security breaches are actually reported.[66]

Another risk posed by notice requirements is that the incentive effect is short-lived. Considerable attention has been focused on the fact that organizations suffering security breaches paid a high price in terms of their stock price and market value. One 2003 study showed that firms victimized by an information security compromise that involved theft of credit card information suffered a stock market loss of 9.3 percent on the day the incident was announced, increasing to 14.9 percent over three days[67]—three to five times the amount found in similar studies for other classes of events."[68] But as breaches have become more common, that effect has not only diminished, but also proved short-lived. The same is true of the risk of customer defections. Customers may claim in surveys that they would consider moving to a competitor because of a breach, but as more and more of those competitors have suffered breaches themselves, the incentive to move has declined. It is ironic that the same notices that first alerted the public and the press to the problem of security breaches,

have contributed to desensitizing them to those breaches and reducing the long-term effect of those breaches.

It is also important to remember that at least in the United States, organizations already have significant incentives to avoid security breaches that contribute to identity fraud or other financial injuries because businesses already bear the lion's share—some studies estimate 90 percent—of the losses resulting from those criminal acts.[69] Notification requirements thus burden the institutional victims of security breaches with the additional costs associated with providing notice even though the likelihood of an individual recipient being harmed as a result of the breach, or taking action to reduce that likelihood in response to a notice, is very low.

Finally, as is the case with individuals, if avoiding having to send notices becomes the major focus of industry security efforts, that preoccupation is likely to divert scarce resources away from dealing with other security threats. To the extent that laws require the use of notices even when the breach threatens no harm, it seems likely that the notice requirements will result in those resources being poorly invested.

These important lessons have been lost on many U.S. policymakers, especially at the state level, who have almost universally opted for requiring notices even for breaches that threaten no harm and for a strict liability approach that applies the same penalties—in this case, primarily public embarrassment—irrespective of the measures taken by the data processor or the breadth of the term security "breach." The result is plain to see: consumers are rapidly learning to ignore breach notices; they are losing the ability to distinguish in the market between responsible organizations with good security that happen to suffer one inevitable breach and irresponsible organizations with poor security that suffer an easily preventable breach. Consumers and businesses alike are having the attention and other resources that they invest in security focused on less serious threats, at the cost of failing to address more serious threats.

To the extent notices are intended to motivate "individuals to take steps to protect themselves from any harmful effects" of the breach,[70] the U.S. experience suggests that not only do they often not work, but they impose other, unintended costs as well. To the extent breach notices are designed to increase "accountability" of organizations that suffer breaches, raise "awareness among the public,"[71] and alert "appropriate regulatory bodies,"[72] there would appear to be more effective and efficient methods: such as requiring reporting of breaches to an agency or on a breach website (New Hampshire, for example, now maintains a public website of notices of breaches affecting New Hampshire residents[73]). Better designed reporting obligations might lead to greater reporting of security breaches.

Put simply, if we think real risks are posed by security breaches, the notice response is too timid. If not, the notice response is too great.

5. Twentieth-Century Responses to Twenty-first-Century Information Flows and Challenges

The most significant issue raised by information security breach notification laws is that they ignore the broader context in which personal data are collected, used, and transferred today, and invoke a twentieth-century response to address the twenty-first-century reality of ubiquitous, global flows of digital data and critical security threats.

a. Ubiquitous Digital Data

Notices to individuals when personal data are potentially compromised—like privacy notices when personal data are collected, shared, or otherwise processed—were designed for a world in which data processing was infrequent, highly centralized, and clearly structured. A business might acquire a data set in a single transaction, store it on a mainframe computer, and use it only for identified purposes. Access to the data set without authorization was comparatively difficult to accomplish, easy to guard against, and capable of being identified with certainty. Notices were of questionable value in the management of data in even this antiquated environment, for many of the reasons already identified, but they were a familiar part of the dominant paradigm of fair information practice principles and imposed only modest burdens on individuals and enterprises.

Today, the collection and use of personal data are ubiquitous. As Stanford Law School professor and former dean Kathleen Sullivan has written, "[t]oday, our biographies are etched in the ones and zeros we leave behind in daily digital transactions."[74] Increasingly, everything individuals do, every step they take, every transaction they enter into is memorialized in digital data, and those data are routinely collected and stored by, and shared with, multiple third parties:

- What individuals buy and the other transactions in which they engage—30 billion checks, 26 billion debit card transactions, 22 billion credit card transactions annually.[75]

- What individuals communicate with family, friends, and colleagues in more than 30 billion emails a day.[76] The United States alone accounts for about 1.6 billion text messages a day.[77] These are all captured digitally, together with voicemail and Voice Over IP conversations, by someone other than, or in addition to, the sender.

- Location information. There are 2.7 billion mobile phones worldwide,[78] which 95 percent of users say they keep within three feet of themselves at all times.[79] Mobile phones thus constitute the world's largest sensor network. Through GPS and triangulation, these phones

generate increasingly precise information about the location, speed, and direction of movement of the user. Many cars contain navigational systems that include a GPS receiver. Laptops, PDAs, and cell phones that connect to WiFi necessarily provide information concerning the user's location. Electronic toll payment systems provide a stream of location data to anyone with an appropriate reader.

- What individuals watch, listen to, and read through digital satellite and cable, iTunes, Amazon, and hundreds of other entertainment service providers and vendors.

- What individuals are doing in the office, in public, and increasingly even at home with video and audio surveillance, key-cards, security systems, keystroke monitoring, stored email and voicemail, and remote access to networked files.

- What individuals are interested in, looking for, or concerned about. Internet users generate a reported 113 billion searches a year worldwide, doubling every two years.[80] The *New York Times* calculated that Yahoo!, Google, Microsoft, AOL, and MySpace record at least 336 billion transmission events per month, not counting their ad networks. Yahoo! alone collects data on each user an average of 811 times per month from its own sites, or 2,520 times per month if its partner sites on which Yahoo! provides ads are included.[81] Marc Rotenberg, executive director of the Electronic Privacy Information Center, has commented, "[w]e're recording preferences, hopes, worries and fears."[82]

- Data on individuals and their families, friends, and co-workers through social networking (MySpace and Facebook get a reported 100 billion page views per month[83]), blogs, photo and video sharing (e.g., YouTube, Flickr), peer-to-peer file-sharing, virtual worlds, and even remote storage of documents and financial information—what is often called "cloud computing."

Individuals increasingly live their lives awash in what the London *Daily Mail* has called a "bottomless ocean of information."[84]

At the same time, demand for personal data from business, the government, and other organizations is escalating. Access to personal data facilitates increasingly targeted products, services, and advertising. It makes possible greater user convenience, efficiency, and recognition. Personal information is regarded as increasingly essential to security and accountability.

In the face of this escalating demand for personal information, and for the technologies, products, and services that both rely on and provide an ever-increasing supply of personal data, the collection, storage, and sharing of those data are increasingly routine and even automatic. In many settings, data subjects have no choice because of government requirements or because the service or product cannot be provided without the data.

The vast majority of these data are held by third parties, while they may be invisible or inaccessible to individuals (e.g., individuals may not know where they are by looking at their cell phones, but the cellular service providers do). In fact they are often processed by numerous third parties. Consider a credit card or debit card transaction, which involves data passing through the hands of the merchant or bank at which the card is presented, the payment network, the card issuer, the clearing bank, all of the intervening communications providers (including ISPs or telephone companies for remote transactions), and companies that provide services to all of these entities.

And these data today are digital, which makes them easier and far less expensive to collect, store, share, search, and interconnect. Thus, even innocuous data or non-personally identifiable data, when combined with dozens of other data elements, may become very revealing.

In this data-intensive, complex, and, as discussed in greater detail below, global world, breach notices—like privacy notices—are increasingly outdated. If individuals must be notified every time personal data are collected or used, the public and the environment will succumb under the deluge of those notices. Alternatively, notices will become so broad and generic, that they will offer no protection. In either case, they will be uniformly ignored by individuals. This is especially true for breach notices. Notices are too slow, too cumbersome, and too poorly timed to provide meaningful protection for information security, and requiring them as a broad response to security threats promises to inundate individuals with notices that they are ill-equipped and unlikely to act on. The U.S. experience with notices indicates that this is already the case.

b. Global Data Flows

The mounting interest in mandatory security breach notices must also be evaluated in light of the increasingly global nature of commerce and information flows. The internet connects more than 200 countries. It makes data not only interconnected, but increasingly interoperable. As a result, it has become the backbone for some of our most important networks—for example, ATM transactions and air traffic control data. The internet is used every day by individuals and enterprises alike, and has facilitated dramatic growth in multinational commerce and in outsourcing, which takes advantage of reliable, affordable information technologies to provide a wide range of services—from back-office processing to customer call centers. National security and other shared concerns have also spurred greater sharing of data across borders.

The value of notices is further decreased when they involve unaccounted-for data in other countries that the individual recipient is even less-equipped to understand, evaluate, or take action concerning. Moreover, the wide variety of notice regimes being used or considered by different nations—or in the United States, by different states—highlights the incongruity between national (or provincial) requirements and global data flows. As European Data Protection Supervisor Peter Hustinx

noted in 2007, "[t]he economy depends *more and more* on global networks. … In general, the physical place of a processing operation is less relevant."[85]

The proliferation of digital data and the expansion of global commerce and data flows challenge the old ways of thinking about privacy. Linking privacy and security protection to notice is increasingly unworkable. As United Kingdom Information Commissioner Richard Thomas stressed in July 2008:

> We want to generate new thinking. European data protection law is increasingly seen as out-of-date, bureaucratic and excessively prescriptive. It is showing its age and is failing to meet new challenges to privacy, such as the transfer of personal details across international borders and the huge growth in personal information online. It is high time the law is reviewed and updated for the modern world.[86]

The need for new thinking exists not only in Europe, but also in the United States and other nations, and it applies not only to data protection law, but to information security as well.

c. Information Security Threats

The need for innovative thinking about how to protect data is especially acute in the face of a rapidly expanding array of critical information security threats—threats that are growing in frequency, variety, sophistication, and maliciousness. According to security software firm Symantec, technological attacks are "no longer carried out by hackers and script kiddies; it's gangs of criminals who are well funded and well organized."[87] A number of recent frauds reflect key similarities—e.g., common addresses, phone numbers, targets, and strategies—that cause law enforcement officials to believe they are orchestrated by well-organized and financed perpetrators.

These sophisticated fraud rings are highly specialized and operate across national borders. During the summer of 2008, U.S. authorities indicted 11 people from five countries for stealing 40 million debit and credit card numbers from at least nine major retail corporations. According to the U.S. Attorney General, the thieves "used sophisticated computer hacking techniques, breaching security systems and installing programs that gathered enormous quantities of personal financial data," which they then exploited through a variety of fraud networks.[88]

The variety and complexity of technological tools used by information thieves are astounding: rootkits that take control of individual systems; botnets that connect compromised machines to work in tandem stealing data or attacking servers; wireless communication interception and diversion; domain name server attacks that divert unwitting users to fraudulent websites and steal online information; and dozens of other measures.

Spyware is a broad and particularly vexing category of malicious software. Downloaded along with innocent programs or attached to email, spyware collects sensitive personal information, directly from users' computers. Billions of dollars are spent each year on anti-spyware software and updates. Microsoft reported that 50 percent of Windows XP operating system crashes were due to spyware. Dell and McAfee report that spyware accounts for 10–12 percent of all tech support calls.[89] Spyware has now expanded into crimeware, terrorware, vandalware, and ransomware—all of which acutely threaten both individual and institutional information.

Many of the most rapidly growing and most successful attacks today involve social engineering—devious means of persuading individuals to part with their own data. This is often the case with spyware, which individuals are induced to download with promises of free software or pornography or breaking news stories. "Phishing" is another prominent way in which unsuspecting users are deceived—in this case, through an email message purporting to come from a friend, colleague, or respectable business or other organization—into providing personal data to a fraudulent website that impersonates a legitimate one. Phishing attacks are growing rapidly in both frequency and effectiveness. "Spear phishing," which relies on contextual information to target fraudulent messages based on characteristics of specific internet users, is proving even more effective. In one Indiana University study, the percentage of recipients of a phishing message persuaded to provide their account name and password increased from 16 percent to 72 percent when the researchers made it appear that the fraudulent message originated from a Facebook friend.[90]

Seven in ten U.S. internet users say they have been fooled by phishing messages, and a 2007 survey showed that the same percentage of Australians engaged in online behavior that put them "at risk" of falling victim to phishing.[91] According to Gartner, "phishing attacks in the United States soared in 2007 as $3.2 billion was lost to these attacks."[92] As evidence of the increasing specialization and mass availability of malicious software, consider that 42 percent of phishing websites observed in the first half of 2007 originated from just three phishing toolkits.[93]

New technologies bring with them new attacks. Cell phones, which often store extensive personal data and contain links to email accounts and servers that house even more, have been the most recent battlefield. The move toward greater handset compatibility increases the vulnerability. As the SANS Institute reported in 2008, "[a] truly open mobile platform will usher in completely unforeseen security nightmares."[94]

Unlike earlier viruses and worms, which were designed largely to highlight their youthful creators' prowess, these attacks are used to steal data, deny service, and extort payments from affected institutions. According to the SANS Institute, cybercriminals used technological attacks to extort "hundreds of millions of dollars from multiple critical infrastructure companies" in 2006 and 2007.[95] In January 2008, the U.S. Central Intelligence Agency issued a rare public warning that attackers had

broken into the computer networks of utility companies and then made demands, in at least one case causing a power outage affecting "multiple cities."[96]

The magnitude of cyber-threats has grown even further to include online terrorism and military-like attacks against both government and private sector systems and data. U.S. government agencies reported 12,986 cyber security incidents to the U.S. Homeland Security Department in 2007, triple the number from two years earlier.[97] In 2005, the last year for which complete data are available, the Pentagon reported more than 79,000 attempted intrusions into its computer networks, about 13,300 of which were successful.[98] In response, the U.S. Department of Defense has created a new Cyber Warfare Command. German and British government officials report similar attacks, many believed to have originated with a Chinese army unit, against their official and industry networks.[99]

Russian fundamentalists crippled the Baltic state of Estonia by launching attacks against government, banking, and communications networks, and the Russian incursion into Georgia was preceded by cyber assaults on critical public and private networks.[100] "Cyber-warfare is not becoming the threat of the future, it already is," said Estonian Defense Minister Jack Aaviksoo.[101] In April 2008, *BusinessWeek* warned in a special report that phishing has become the "New E-Spionage Threat."[102] Email messages are being sent to U.S. defense contractors and other major corporations that secretly install key logging software on the users' computers to "suck sensitive data" from corporate networks and report it back to a Chinese website.

The cost of cyber attacks in the United States alone was estimated in a 2007 congressional report to be $400 million a year, not counting the invasion of individuals' privacy.[103]

In the face of such aggressive, escalating, sophisticated, and costly information security attacks, breach notices seem a paltry response. With data being stolen on such a massive scale and seven out of ten individuals reporting that they are unintentionally supplying their own personal data to thieves, requiring a notice every time an institution suffers a breach, especially if the "breach" is a lost laptop or backup data, is ludicrous. The shortcomings of breach notices—in particular, their failure to prevent, rather than merely provide notice of, attacks—are intensified, and the true cost of their potential for distracting individuals and institutions from the steps they can take to thwart far more serious attacks is starkly illuminated. Perhaps most importantly, the range and severity of information security threats powerfully illustrate the urgency of the need for new and imaginative approaches to information security. While breach notices may be a familiar tool, they are ill-suited as a broad response to the realities of the global flows of digital information or of the sustained threats to that information in the twenty-first century.

Conclusion

The recent guides to breach notices from the United Kingdom, Canada, New Zealand, and Australia in many ways reflect the limits of notices and the challenges of protecting privacy and security. They provide frameworks under which notice to specific individuals would be only a small part of a broader approach to information security, and even then used only when a breach threatens actual harm to individuals and there is something those individuals can do to mitigate that harm. Those documents also recognize the risks of "over notifying."[104]

The EU and U.S. approaches to breach notices seem less sensitive to the limited role that breach notices can play or to the risks of requiring them inappropriately. Those risks are numerous. The EU and U.S. approaches rely on a tool that in most situations contributes little to the security of personal information; that requires individuals to take steps that they are unlikely to take and that may be unavailable to them in any event; that responds to breaches rather than prevents them; and that is of diminishing utility over time. By defining breaches too broadly, they require notices even when no data have been compromised and no harm is threatened, and create perverse incentives for institutions to invest in preventing breaches, and managing customer relations and public relations spin when that impossible goal is not obtained, rather than focusing scare resources on greater security threats. They diminish the value of notices when they might otherwise be appropriate.

But the greatest risk of the focus on security breach notices, magnified in the EU and U.S. approaches, is that it applies a twentieth-century tool to twenty-first-century issues, when what is desperately needed is far more forward-looking, imaginative thinking about how to protect security and privacy from far more serious dangers in a world of ubiquitous data and global information flows.

Notes

1 Information Commissioner's Office [of the United Kingdom], Guidance on Data Security Breach Management (Mar. 27, 2008) [United Kingdom Guidance], http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/guidance_on_data_security_breach_management.pdf.

2 Office of the Privacy Commissioner of Canada, Key Steps for Organizations in Responding to Privacy Breaches (Aug. 28, 2007) [Canadian Key Steps Guide], http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp.

3 Privacy Commissioner [of New Zealand], Key Steps for Agencies in Responding to Privacy Breaches and Privacy Breach Checklist (n.d.) [New Zealand Key Steps Checklist], http://www.privacy.org.nz/assets/Files/Privacy-Breach-Guidelines/Privacy-breach-guidance.DOC; Office of the Privacy Commissioner [of New Zealand], Information Paper to accompany Privacy Breach Guidance Material (n.d.) [New Zealand Information Paper], http://www.privacy.org.nz/assets/Files/Privacy-Breach-Guidelines/Information-paper-to-accompany-the-privacy-breach-guidance.doc.

4 Australian Government, Office of the Privacy Commissioner, Consultation Paper: Draft Voluntary Information Security Breach Notification Guide (Apr. 2008) [Australian Consultation Paper], http://www.privacy.gov.au/publications/breach_0408.pdf.

5 Commission of the European Communities, Proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation (COM(2007) 698 final (Nov. 11, 2007) [Commission Proposal], http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/COMdocs/2007/COM2007_698_EN.pdf.

6 See, e.g., European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Apr. 10, 2008) [European Data Protection Supervisor Opinion], http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2008/08-04-10_e-privacy_EN.pdf; Article 29 Data Protection Working Party, Opinion on the review of the Directive 2002/58/EC on privacy and electronic communications (May 15, 2008) [Working Party Opinion], http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp150_en.pdf.

7 Alaska, 2008 H.B. 65; Arizona, Ariz. Rev. Stat. § 44-7501; Arkansas, Ark. Code § 4-110-101 et seq.; California, Cal. Civ. Code § 1798.82; Colorado, Colo. Rev. Stat. § 6-1-716; Connecticut, Conn. Gen Stat. 36a-701(b); Delaware, Del. Code tit. 6, § 12B-101 et seq.; Florida, Fla. Stat. § 817.5681; Georgia, Ga. Code §§ 10-1-910, -911; Hawaii, Haw. Rev. Stat. § 487N-2; Idaho, Idaho

Code §§ 28-51-104 to 28-51-107; Illinois, 815 ILCS 530/1 et seq.; Indiana, Ind. Code §§ 24-4.9 et seq., 4-1-11 et seq.; Iowa, 2008 S.F. 2308; Kansas, Kan. Stat. 50-7a01, 50-7a02; Louisiana, La. Rev. Stat. § 51:3071 et seq.; Maine, Me. Rev. Stat. tit. 10 §§ 1347 et seq.; Maryland, Md. Code, Com. Law § 14-3501 et seq.; Massachusetts, 2007 H.B. 4144, Chapter 82; Michigan, Mich. Comp. Laws § 445.61 et seq.; Minnesota, Minn. Stat. §§ 325E.61, 325E.64; Montana, Mont. Code § 30-14-1701 et seq.; Nebraska, Neb. Rev. Stat. §§ 87-801, -802, -803, -804, -805, -806, -807; Nevada, Nev. Rev. Stat. 603A.010 et seq.; New Hampshire, N.H. Rev. Stat. §§ 359-C:19 et seq.; New Jersey, N.J. Stat. 56:8-163; New York, N.Y. Gen. Bus. Law § 899-aa; North Carolina, N.C. Gen. Stat § 75-65; North Dakota, N.D. Cent. Code § 51-30-01 et seq.; Ohio, Ohio Rev. Code §§ 1347.12, 1349.19, 1349.191, 1349.192; Oklahoma, Okla. Stat. § 74-3113.1; Oregon, 2007 S.B. 583, Chapter 759; Pennsylvania, 73 Pa. Stat. § 2303; Rhode Island, R.I. Gen. Laws § 11-49.2-1 et seq.; South Carolina, 2008 S.B. 453, Act 190; Tennessee, Tenn. Code § 47-18-2107; Texas, Tex. Bus. & Com. Code § 48.001 et seq.; Utah, Utah Code §§ 13-44-101, -102, -201, -202, -310; Vermont, Vt. Stat. tit. 9 § 2430 et seq.; Virginia, 2008 S.B. 307, Chapter 566; Washington, Wash. Rev. Code § 19.255.010; West Virginia, 2008 S.B. 340, Chapter 37; Wisconsin, Wis. Stat. § 895.507; Wyoming, Wyo. Stat. § 40-12-501 to -501; District of Columbia, D.C. Code § 28- 3851 et seq. For up-to-date information on state security breach laws visit the National Conference of State Legislatures website, http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm, from which this information is excerpted.

8 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part III of Supplement A to Appendix, at 12 C.F.R. Part 30 (OCC), 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (FDIC), and 12 C.F.R. Part 568 (Office of Thrift Supervision), March 29, 2005, 70 Federal Register 15,736 (Mar. 29, 2005).

9 Australian Consultation Paper, supra at 13.

10 See Fred H. Cate, "The Identity Theft Scare," *Washington Post*, Oct. 14, 2006, at A21.

11 United Kingdom Guidance, supra at 1.

12 Id. at 3.

13 New Zealand Information Paper, supra at 2.

14 Australian Consultation Paper, supra at 27.

15 Canadian Key Steps Guide, supra at 2.

16 European Data Protection Supervisor Opinion, supra at 9.

17 New Zealand Information Paper, supra at 1-2; see also Canadian Key Steps Guide, supra at 4; Australian Consultation Paper, supra at 27; United Kingdom Guidance, supra at 3.

18 Working Party Opinion, supra at 3.

19 United Kingdom Guidance, supra at 3.

20 Id.

21 Australian Consultation Paper, supra at 17.

22 New Zealand Information Paper, supra at 3.

23 Robin Sidel & Mitchell Pacelle, "Credit Card Breach Tests Banking Industry's Defenses," *Wall Street Journal*, June 21, 2005, at C1.

24 Thomas M. Leonard & Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," *Progress on Point*, 12.12, July 2005, at 8.

25 United Kingdom Guidance, supra at 1; see also Canadian Key Steps Guide, supra at 1; New Zealand Information Paper, supra at 2; Australian Consultation Paper, supra at 20.

26 United Kingdom Guidance, supra at 3.

27 Canadian Key Steps Guide, supra at 4.

28 Alaska, Alaska Stat. §45.48.100 et seq.; Arizona, Ariz. Rev. Stat. Ann. §44-1698; Arkansas, Ark. Stat. Ann. §4-112-101 et seq.; California, Cal. Civil Code §1785.11.2 et seq.; Colorado, Colo. Rev. Stat. §12-14.3-101 et seq.; Connecticut, Conn. Gen. Stat. §36a-701 et seq.; Delaware, Del. Code Ann. tit. 6, §2201 et seq.; District of Columbia, D.C. Code Ann. §28-3861 et seq.; Florida, Fla. Stat. §501.005; Georgia, Ga. Code §10-1-913 et seq.; Hawaii, Hawaii Rev. Stat. §489P-1 et seq.; Idaho, Idaho Code §28-52-101 et seq.; Illinois, Ill. Rev. Stat. ch. 815, §505/2MM; Indiana, Ind. Code §24-5-24-1 et seq.; Iowa, Iowa Code §714F.1 et seq.; Kansas, Kan. Stat. Ann. §50-701 et seq.; Kentucky, Ky. Rev. Stat. §367.363 et seq.; Louisiana, La. Rev. Stat. Ann. §9:3571.1; Maine, Me. Rev. Stat. Ann. tit. 10, §1311 et seq.; Maryland, Md. Commercial Code Ann. §1212.1 et seq.; Massachusetts, Mass. Gen. Laws. Ann. ch. 93, §50 et seq.; Minnesota, Minn. Stat. §13C.016 et seq.; Mississippi, Miss. Code Ann. §75-24-201 et seq.; Montana, Mont. Code Ann. §30-14-1726 et seq.; Nebraska, Neb. Rev. Stat. §8-2601 et seq.; Nevada, Nev. Rev. Stat. §598C.010 et seq.; New Hampshire, N.H. Rev. Stat. Ann. §359-B:22 et seq.; New Jersey, N.J. Rev. Stat. §359B:22 et seq.; New Mexico, N.M. Stat. Ann. §56-3A-1 et seq.; New York, N.Y. General Business Law §380-a et seq.; North Carolina, N.C. Gen. Stat. §75-60 et seq.; North Dakota, N.D. Cent. Code §51-33-01 et seq.; Ohio, Ohio Rev. Code Ann. §1349.52 et seq.; Oklahoma, Okla. Stat. tit. 24, §149; Oregon, Or. Rev. Stat. §646A.600 et seq.; Pennsylvania, Pa. Stat. tit. 73, §2501 et seq.; Rhode Island, R.I. Gen. Laws §6-48-1 et seq.; South Carolina, S.C. Code Ann. §37-20-110 et seq.; South Dakota, S.D. Codified Laws Ann. §54-15-1 et seq.; Tennessee, Tenn. Code §47-18-2101 et seq.; Texas, Tex. Business & Commerce Code Ann. §20.01 et seq.; Utah, Utah Code Ann. §13-42-101 et seq.; Vermont, Vt. Stat. Ann. tit. 9, §2480a et seq.; Virginia, Va. Code §59.1-444.1 et seq.; Washington, Wash. Rev. Code §19.182.170 et seq.; West Virginia, W. Va. Code §46A-6L-101 et seq.; Wisconsin, Wis. Stat. §100.54 et seq.; Wyoming, Wyo. Stat. §40-12-501 et seq. For up-to-date information on state freeze laws visit the National Conference of State Legislatures website, http://www.ncsl.org/programs/banking/SecurityFreezeLaws.htm, from which this information is excerpted.

29 Synovate, *Federal Trade Commission—Identity Theft Survey Report* (2003), http://www.ftc.gov/os/2003/09/synovatereport.pdf; Synovate, *Federal Trade Commission—Identity Theft Survey Report* (2006), http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf; Javelin Strategy & Research, *2005 Identity Fraud Survey Report*; Javelin Strategy & Research, *2006 Identity Fraud Survey Report*; Javelin Strategy & Research, *2007 Identity Fraud Survey Report*; Javelin Strategy & Research, *2008 Identity Fraud Survey Report*. The margin of error was generally +/- 4.4 to 4.6 percent at the 95 percent confidence level on the question concerning the number of identity fraud victims.

30 Congress long ago insulated consumers from liability for account takeover, by providing a $50 limit to their liability for credit and debit card fraud. The Truth in Lending Act, as implemented through Regulation Z, limits consumer liability for unauthorized transactions to $50. 15 U.S.C. § 1643(a); 12 C.F.R. § 226.12. As a practical matter, financial institutions and other card issuers universally waive even that $50.

31 "Beware the Numbers Hype About ID Theft," Associated Press, Nov. 14, 2005.

32 Dean Foust, "ID Theft: More Hype Than Harm," *BusinessWeek*, July 3, 2006.

33 Pat Regnier, "Are You Terrified About Identity Theft Yet?," *Money*, Sept. 1, 2005.

34 Eric Dash, "Stolen Lives; Protectors, Too, Gather Profits From ID Theft," *New York Times*, Dec. 12, 2006.

35 Jack Shafer, "The *Times* Hypes ID Theft," *Slate*, May 30, 2006.

36 *2007 Identity Fraud Survey Report*, supra.

37 ID Analytics, *National Data Breach Analysis* (2006).

38 Id.

39 Id.

40 Federal Trade Commission, ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress, Press Release, Jan. 26, 2006.

41 Email to the author from Tina Snow, Assistant Chief Privacy Officer, ChoicePoint, June 11, 2008.

42 U.S. Government Accountability Office, *Report to Congressional Requesters, Personal Information* (GAO-07-737) (2007).

43 Data on information security breaches are reported at http://etiolated.org/.

44 Sasha Romanosky, Rahul Teland & Alessandro Acquisti, "Do Data Breach Disclosure Laws Reduce Identity Theft?," *Seventh Workshop on the Economics of Information Security* 3 (2008).

45 See generally Michael E. Staten & Fred H. Cate, "Accuracy in Credit Reporting," in Nicolas P. Retsinas & Eric S. Belsky, eds., *Building Assets, Building Credit* 237 (Brookings Institution Press, 2005); Margaret J. Miller, "Credit Reporting Systems Around the Globe: the State of the Art in Public Credit Registries and Private Credit Reporting Firms"; Margaret J. Miller, ed., *Credit Reporting Systems and the International Economy* 25 (MIT Press, 2003); Fred H. Cate, "Privacy, Consumer Credit, and the Regulation of Personal Information," in Thomas A. Durkin & Michael E. Staten, eds, *The Impact of Public Policy on Consumer Credit* 229 (Kluwer, 2001).

46 O.E.C.D. Doc. (C 58 final) (Oct. 1, 1980).

47 *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* (Eur. O.J. 95/L281).

48 Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, 2004/AMM/014rev1 (Nov. 2004).

49 See Fred H. Cate, "The Failure of Fair Information Practice Principles," in Jane K. Winn, ed., *Consumer Protection in the Age of the 'Information Economy'* 341 (Ashgate, 2006).

50 "Briefs," *Circulation Management*, May 1999 (referring to the U.S. Postal Service's *Household Diary Study* (1997)).

51 Declaration of Fred H. Cate, *Bank of America v. Daly City*, 279 F. Supp. 2d 1118 (N.D. Cal. 2003), at 2.

52 Ex parte letter from Kathryn Krause to Dorothy Attwood (Sep. 9, 1997), In the Matter of Implementation of the Telecommunications Act of 1996; Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information; Implementation of Non-Accounting Safeguards of Sections 271 and 272 of the Communications Act of 1934, as Amended, 63 Fed. Reg. 20,326 (1998) (FCC, second Report and Order and Further Notice of Proposed Rulemaking). U S WEST calculated that the trial had a margin of error of less than 2 percent. Brief for Petitioner and Intervenors at 16 n.37, U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999), *cert. denied* 528 U.S. 1188 (2000).

53 Brief for Petitioner and Intervenors, supra at 10-11.

54 Federal Trade Commission, Workshop on the Information Marketplace: Merging and Exchanging Consumer Data, Mar. 31, 2001 (comments of Ted Wham).

55 Saul Hansell, "Compressed Data: The Big Yahoo Privacy Storm That Wasn't," *New York Times*, May 13, 2002, at C4.

56 *Hearing on Financial Privacy and Consumer Protection*, Senate Comm. on Banking, Housing, and Urban Affairs, 107th Cong. (Sept. 19, 2002) (statements of Fred H. Cate and John Dugan).

57 Star Systems, *Financial Privacy: Beyond Title V of Gramm-Leach-Bliley,* 2002, p. 9.

58 Timothy J. Muris, *Protecting Consumers' Privacy: 2002 and Beyond*, Privacy 2001 Conference, Oct. 4, 2001.

59 Declaration of Fred H. Cate, supra at 6-7.

60 Canadian Key Steps Guide, supra at 4.

61 Id.

62 Commission Proposal, supra at 33 (proposing amended Article 4).

63 European Data Protection Supervisor Opinion, supra at 8; Working Party Opinion, supra at 3.

64 *Identity Theft Survey Report*, supra; *2005 Identity Fraud Survey Report*, supra; *2006 Identity Fraud Survey Report*, supra; *2007 Identity Fraud Survey Report*, supra.

65 *2005 Identity Fraud Survey Report*, supra; *2006 Identity Fraud Survey Report*, supra; *2007 Identity Fraud Survey Report*, supra.

66 Thomas Claburn, "Most Security Breaches Go Unreported," *InformationWeek*, Aug 1, 2008, http://www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=209901208

67 Ashish Garg, Jeffrey Curtis & Hilary Halper, "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security*, vol.11, no. 2, 74–83 (2003).

68 Lenard & Rubin, supra at 5.

69 Id.; Romanosky, Teland & Acquisti, supra at 2.

70 New Zealand Information Paper, supra at 1-2; see also Canadian Key Steps Guide 4; Australian Consultation Paper, supra at 27; United Kingdom Guidance, supra at 3.

71 Working Party Opinion, supra at 3.

72 United Kingdom Guidance, supra at 3.

73 http://doj.nh.gov/consumer/breaches.html.

74 Kathleen M. Sullivan, "Under a Watchful Eye: Incursions on Personal Privacy," *The War on Our Freedoms: Civil Liberties in an Age of Terrorism* 128, 131 (2003).

75 Jerome R. Stockfish, "You Lock Your Door, So Guard Your Card," *Tampa Tribune*, Mar. 30, 2008, at 1 (citing the 2007 Federal Reserve Payments Study).

76 "Talk Fusion Video Email Marketing Software Debuts World Wide," *EWorldWire*, Jul. 30, 2007.

77 Jack Kemp, "Take a Timeout on Unfair Cell Phone Taxes," Copley News Service, May 16, 2008.

78 Penny Crosman, "Attracting Young Investors," *Wall Street & Technology*, Jan. 1, 2008, at 16.

79 David Jones, "Google is Watching You," *Daily Mail*, Dec. 1, 2007, at 14.

80 Martin Miller, "Leap of Faith," *L.A. Times*, Mar. 2, 2008, at 36.

81 Id.

82 Louise Story, "To Aim Ads, Web is Keeping Closer Eye on What You Click," N*ew York Times*, Mar. 10, 2008, at A1.

83 "Web Analytics," *Precision Marketing*, Apr. 18, 2008, at 51.

84 David Jones, "Google is Watching You," *Daily Mail*, Dec. 1, 2007, at 14.

85 Peter Hustinx, Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (25 July 2007) (emphasis in original), http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2007/07-07-25_Dir95-46_EN.pdf.

86 [United Kingdom] Information Commissioner's Office, UK Privacy Watchdog Spearheads Debate on the Future of European Privacy Law, Press Release, July 7, 2008.

87 Heather McLean, "Six Clicks Away from a Cyber Crook," *Daily Telegraph*, Mar. 1, 2008, at 20 (quoting William Beer, from Symantec).

88 Prepared Remarks of Attorney General Michael Mukasey at an Identity Theft Press Conference, Federal News Service, Aug. 5, 2008.

89 Federal Trade Commission Staff Report, *"Monitoring Software" on Your PC: Spyware, Adware, and Other Software* 8, 12 (2005).

90 Markus Jakobsson & Steven Myers, *Phishing and Its Countermeasures* 202-03 (2007).

91 America Online & National Cyber Security Alliance, *Online Safety Study* (2005); " 'Phishing' catches Australians online," AAP Newsfeed, Oct. 4 2007.

92 Gartner, Inc., "Gartner Survey Shows Phishing Attacks Escalated in 2007," Dec. 17, 2007.

93 Stefanie Hoffman, "Storm Warning," *Varbusiness*, Jan. 28, 2008, at 32.

94 SANS Institute, Top Ten Cyber Security Menaces for 2008, http://www.sans.org/2008menaces/?utm_source=web-sans&utm_medium=text-ad&utm_content=text-link_2008menaces_homepage&utm_campaign=Top_10__Cyber_Security_Menaces_-_2008&ref=22218.

95 Andy Greenberg, "Congress Alarmed at Cyber-Vulnerability of Power Grid," *Forbes*, May 22, 2008.

96 Ellen Nakashima & Steven Mufson, "Hackers Have Attacked Foreign Utilities, CIA Analyst Says," *Washington Post*, Jan. 19, 2008, at A4.

97 Brian Grow, Keith Epstein & Chi-Chu Tschang, "The New E-Spionage Threat," *BusinessWeek*, April 21, 2008, at 32.

98 Peter Brookes, "The cyber challenge; Cyber attacks are growing in number and sophistication," *Armed Forces Journal* 10 (Mar. 2008).

99 "The New E-Spionage Threat," supra at 32.

100 John Markoff , "Before the Gunfire, Cyberattacks," *New York Times*, Aug. 13, 2008, at A1.

101 Leander Schaerlaeckens, "Terrorism 2.0," *UPI Energy*, Feb 20, 2008.

102 "The New E-Spionage Threat," supra at 32.

103 Bruce McConnell, "How to Make Security and Privacy Fit Together," *Forbes*, May 14, 2008.

104 See, e.g., United Kingdom Guidance, supra at 3-4.

THE CENTRE
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP