



# [Cyber] Space Invaders

Data privacy events are increasing but case law gives little guidance on how companies should respond.

by John F. Mullen, Meredith Schnur and Chris Dilenno

**W**hen an entity suffers a data security event, it faces the daunting task of determining what happened, whether the event is over and

how to respond. The answers may involve developing a potentially costly mandatory legal response in a short period of time. Complex technical and legal analyses are undertaken, often including legal judgment calls.

One would think that, with the rising number of data-breach events, entities whose data is compromised would be able to learn from those companies that were victimized before them. Yet, after nearly 10 years of data-breach-notification law evolution, there remains a notable lack of judicial opinions interpreting fundamental statutory questions faced every time a data event occurs.

Some data events are not reported (and arguably need not be). Those that are, do not routinely lead to litigation. If litigation ensues, the

## Key Points

- ▶ **The Situation:** Current data breach law is a jumble of state statutes and federal rules but few court decisions.
- ▶ **The Back Story:** As breaches occur, companies must understand their obligations clearly.
- ▶ **The Upshot:** Cyber insurance to cover damages and legal costs from data infringement is a must-have for businesses.

*Contributors:*  
*John F. Mullen*  
*is a partner*  
*and chair of*  
*the Complex*  
*Liability*



Mullen



Schnur

*Practice Group*  
*at Nelson Levine de*  
*Luca & Horst; Meredith*  
*Schnur is senior vice*  
*president, Wells Fargo*  
*Insurance Services;*  
*and Chris Dilenno is*  
*an associate in NLdH's Complex*  
*Liability Practice Group. They*  
*may be reached at jmullen@*  
*nldhlaw.com.*



Dilenno

matters are frequently settled. Without a case law record, the underlying legal analysis and interpretation remains inaccessible to outsiders and untested by the courts, forcing data breach victims to reinvent the wheel and revisit uncertain risks each time a data event occurs.

Before an entity decides to notify, it must ask whether its event is legally a breach. For instance, the

Health Information Technology for Economic and Clinical Health Act amendment to the Health Insurance Portability and Accountability Act defines “breach” as “the acquisition, access, use, or disclosure of protected health information... which compromises the security or privacy of the protected health information.”

Each breach notification law has its own nuances. The Hitech Act only applies to health care (HIPAA-covered entities and business associates) but its definition provides a good starting point to discuss the variables of defining a breach.

### Narrower Meaning

Some state statutes narrow the definition of “breach,” defining it as “acquisition and use” of personal information. This may remove questions surrounding the definition of “access” as “disclosure” to particular fact patterns, but other hypothetical situations can raise the question of what “acquisition” of data really means.

Further, if acquisition can be shown but “use” cannot, can notification be legally avoided where statutes require “acquisition and use?” After all, use can happen years later. These legal uncertainties are magnified by the fact that each breach event is unique and full of its own factual uncertainties.

Should the factual analysis determine with some level of certainty that acquisition and use occurred, the question then becomes whether protected personal information was compromised. State notification statutes define personal information as first and last name, or first initial and last name, in combination with a Social Security number, or driver’s license number or state-issued identification card number, or financial account number or credit or debit card number in combination with any required security code, access code or password that would permit access to the individual’s financial account.

According to this definition, a first and last name with a credit card number plus expiration date may not be personal information because it may not include any required code, access code or password. On the other hand, it is certainly possible that a name, credit card number plus expiration date could be used to perpetrate fraud. After all, when is the last time you were asked for a password, access

## Data Breach Compliance

### Regulations:

46 state statutes.  
Various industry-specific federal laws.  
International laws.

### What They Require:

Entities that suffer a data breach must notify individuals that their personal information may have been exposed to unauthorized individuals.

### Compliance Costs to Businesses:

Legal services, expert computer forensics, mass mailings, acute customer support, credit protection offerings, legal communications with state and federal regulators and public relations management.

### Other Results of Compliance:

Loss of goodwill, company value and sales.

or security code when you provided your credit card number and expiration date?

Part of the interpretation problem is that people use the word breach in multiple contexts. If a computer system is accessed without authorization, instinctively it’s called a breach. Investigators come in to investigate the breach. Legal experts are retained to see if the breach requires notification or response. However, significant fact-gathering and legal analysis are required before anyone can conclude that a breach as defined in these statutes actually occurred, despite the computer system intrusion.

This leads to questions regarding the timing of the potentially required notifications. Most notification laws require notice be provided “in the most expedient manner possible” or “within a reasonable time” after discovery of the breach. To promote prompt notification, some statutes require that notice be provided no later than 45 or 60 days after discovery of the event. However, how is the discovery of the event defined?

It may take weeks after a computer system intrusion or a laptop goes missing to determine what personal information was ever involved. Discovery of a computer system intrusion is not discovery of a legal conclusion, namely the existence of a breach.

So the question is: Does the race to provide notice “in the most expedient manner possible” start when a) the intrusion or other loss of data occurs; b) when it is initially discovered; or c) when the entity concludes that a legal breach occurred?

The Hitech Act treats a breach as discovered as of the first day on which such a breach is known to the breached entity, or would have been known by the entity exercising reasonable diligence. Is it reasonable diligence to check all local hard drives accessible to burglars proven to have accessed a computer system during a break-in? What if there are 1,000 workstations, making analysis of all non-network activity a costly, multiweek exercise?

### Jurisdictional Questions

There are many breach notification statutes and terminologies that remain untested by the courts. Each state’s statute applies to entities that possess the protected personal information of its residents. This leads to jurisdictional questions. Can Pennsylvania enforce its notification law against a small shop owner in New Mexico, a state with no notification law? What if the

## Regulatory/Law

New Mexico shop owner has made no attempt to do business in Pennsylvania? Just because the Pennsylvania resident used his credit card to buy a \$5 souvenir while on vacation in Albuquerque, does the Pennsylvania law really apply?

The statutes place different legal duties on service providers and business associates who do not, themselves, own the data. These requirements add areas of uncertainty regarding time lines and discovery dates. Some statutes allow for a risk-of-harm analysis, meaning even though there was a breach of personal information, notification is unnecessary if the risk of harm is arguably low enough. How this type of analysis ought to be applied, like so many other issues, is yet to be tested and defined.

### A Little Light

There are rules and guidance issued by various federal agencies that shed some light on some federal statutory provisions. These can be helpful, but some are from previous administrations with different priorities. In any case, they are not applicable to the 46 state laws, do not address all the issues, and like many statutory provisions they remain, in most instances, untested by the courts.

Data privacy events occur every day. They cause significant first-party breach expenses and raise the specter of massive third-party defense and indemnity exposure.

This year has seen two huge events at Sony and Epsilon. Soon enough, one of these data events is going to reach a jury and lead to a verdict based on identity theft, fear of identity theft, expenses incurred, or lost time.

Faced with this kind of risk, the breached entity will want to avoid the problem and define the data loss event as not a breach. This, however, is getting more difficult to do without legal rationalizations that themselves create risk.

Data security awareness, education and breach-response preparation are critical in addressing the uncertainty of complying with breach notification laws.

The more aware and better prepared an organization is in the event of a breach, the better its chances of mitigating the costs involved and avoiding permanent harm to its bottom line.

If an organization decides to transfer some of its breach risk to an insurance product—and most should—in order to protect its balance sheet, adequate protection is available.

**After nearly 10 years of data-breach-notification law evolution, there remains a notable lack of judicial opinions interpreting fundamental statutory questions faced every time a data event occurs.**

Risk managers or other insurance buyers will weigh the cost benefit of purchasing the insurance product just as they do with any other risk transfer mechanism.

Relatively new insurance products typically offered as Network Security and Privacy Liability insurance policies, also called cyber policies, have been introduced during the past decade.

In the United States alone, more than 20 carriers offer this type of risk-transfer product.

### Cyber Cover

The main purpose of these policies is to provide insurance coverage for an organization if or when it incurs first- and/or third-party

response and defense expenses, and/or damages should an event or breach occur.

Although case law related to “standing” has proven to be favorable to defendants in the current environment (albeit less favorable each year), the costs associated with notification response, regulatory investigation or private rights of action are very high.

Regardless of whether state notification laws apply, any organization that suffers a data event will incur potentially significant out-of-pocket expenses.

A cyber policy will provide the organization with a sublimit of coverage for what are considered crisis-management expenses in the event of a data event. These include out-of-pocket expenses for legal, forensics, notification, credit monitoring, public relations and call-center costs.

Most insurance buyers look at this sublimit as the reason to actually purchase the policy.

In the event of a breach or suspected breach, the policy will mostly pay for itself since actual expenses will be incurred regardless of severity.

These policies may have various other benefits, including first-party business income and data asset-loss reimbursement.

As consumers continue to give out medical information and Social Security numbers and use credit cards, the number of breaches will continue to mount.

More predictable answers to the questions surrounding data breach notification laws will eventually exist. But for now, the best hedges against the risks of uncertainty are: data security awareness/education; breach response preparation; and appropriate insurance.

Given the difficulty in entirely preventing such data events, the uncertainty of many of the legal issues and the costs involved, all three hedges are advised. **BR**