Cybersecurity Law Report
An Acuris company

cslawreport.com

November 4, 2020

BREACH NOTIFICATION

Comparing U.S. and E.U. Approaches to Incident Response and Breach Notification

By Vincent Pitaro, *Cybersecurity Law Report*

The E.U. breach notification scheme is more fragmented than it appears, while the U.S. regime may be more cohesive even without a national law, panelists at a recent seminar at the Incident Response Forum Europe 2020 said.

Kimberly Peretti, a partner at Alston & Bird, moderated the program, which featured Dean Forbes, counsel at Sidley, Amelia M. Gerlicher, a partner at Perkins Coie, James Lloyd, a partner at Orrick, and Robert Maddox, an associate at Debevoise. They compared the U.S. and E.U. approaches to incident response, breach notification, the attorney-client privilege and dealing with regulators.

See "A Practical Look at the GDPR's Data Breach Notification Provision" (Jan. 17, 2018).

Despite GDPR, E.U. Legal Framework Remains Fragmented

A common misperception is that the E.U. legal framework is much more homogeneous than it actually is, Maddox noted. This is partly because, at least on paper, the GDPR harmonizes the threshold for breachnotification obligations. On closer examination, however, the regime is somewhat fragmented.

The expectations of the member states' data protection authorities (DPAs) as to when notification is required differ significantly, Maddox explained. For example, the threshold used by Spain's DPA is actually much higher than that of the U.K. DPA. In addition, it is necessary to look beyond the GDPR. "There is a bit of an alphabet soup" of frameworks that might apply in Europe outside of that regime, he said. For example, the payment services directive has a different notification period from the GDPR. Therefore, it is necessary to check sector-specific regulations, determine which regimes apply and identify the relevant regulators. A company could be subject to multiple regulators.

There is a "real patchwork quilt of different rules and regulations," with GDPR being "one of the worst offenders," Lloyd concurred. The E.U. member state regulators approach enforcement differently. Some are more literal, others more practical. Companies must be concerned not only with privacy regulators, but also with others, especially financial regulators.

See "Not Just the GDPR: Privacy Laws in Belarus, Russia, Switzerland, Turkey and Ukraine" (Dec. 18, 2019) and "Examining the Other European Privacy Laws" (Dec. 11, 2019).

Despite Fragmentation, U.S. Privacy Laws Have a Common Framework

The U.S. regime is also often referred to as a patchwork, Peretti observed. The U.S. is indeed fragmented, according to Gerlicher. There are laws in all 50 states, as well as sector-specific federal regulations, and many local bodies are now also adopting their own reporting rules. Moreover, individual states differ on whether companies must also report to a federal regulator. Nevertheless, just as there are multiple approaches to enforcement of the GDPR, a single federal law in the U.S. might not provide the desired consistency, because each state might deal with it differently.

The FTC, FCC, Department of Health and Human Services and state AGs all might be involved in enforcing U.S. privacy rules, Forbes observed. U.S. state laws sometimes help to fill gaps between federal sector-specific regulations. There is some overlap not only in legal standards, but also in industry standards and voluntary codes and guidance. Often, the standards are not fully defined by the relevant agencies.

At the same time, "the vast majority of these laws are built on the same framework," Gerlicher continued. They apply to unauthorized access to, or acquisition of, a defined type of personal information. This can be more straightforward than in the E.U. Moreover, once a breach reaches a certain size, many of the state-to-state differences fall away.

See "What to Expect From the CPRA – California's New Proposed Privacy Law" (Sep. 30, 2020); "Implications of Nevada's New Privacy Law" (Jul. 10, 2019); and "Managing Data Privacy Across Multiple Jurisdictions" (Nov. 8, 2017).

Common Breach Notification Questions to Ask in the U.S.

In the event of a nationwide breach in the U.S., a company will have to notify virtually all 50 states, Peretti noted. In contrast, in the event of an E.U.-wide breach, a company is generally required to notify only its lead supervisory regulator, which is usually the regulator in its home-state jurisdiction, Maddox said. Notifying the lead regulator satisfies the notification requirement for the entire E.U. However, this concept does not apply in all situations. For example, if a company's search engine delisting program falls outside the scope of the GDPR, and the company suffers a data breach, it might have to notify every E.U. state regulator.

In the U.S., the trigger for reporting a data breach is generally the unauthorized access or acquisition of personal information, Peretti explained. In contrast, in the E.U., reporting turns on whether there is a risk to individual rights and freedoms arising out of a breach.

In the U.S., in the event of a breach, to preserve privilege, a company might retain outside counsel which, in turn, would retain a forensic investigator, Gerlicher said. Investigators typically focus on "technical unauthorized access." Once a company confirms that there was unauthorized access, it is hard to rely on a "risk" standard.

Regulators in both the E.U. and the U.S. generally have "no real patience for an opinion about what a criminal is about to do with your information," she remarked. The type of information involved is also significant. For example, credit card information is usually held

on a separate system. If it can be determined that type of information was not involved in the breach, it can make the scope of the investigation narrower.

Not every breach in the U.S. will trigger a notice requirement, Peretti noted. Under state breach notification laws, a number of threshold questions must be answered, Forbes said:

- Is an entity covered under the relevant regime?
- Is the information covered by the regime?
- How is a breach defined?
- What event triggers disclosure?
- Is there a duty to conduct a risk of harm analysis?
- Does the regime apply to paper records?
- Are there any exemptions?
- What method of notice is required?
- What should the notice contain?
- When must the notice be given?

Forbes noted that if, after answering these questions, a company decides that a forensics expert is needed, the expert can help determine when an attack started and stopped, and whether:

- the affected data contained the types of information covered by a notification law;
- there was infiltration;
- any data was removed; and
- if so, what data was removed.

That information could help narrow the scope of any requisite notice. There are many points in the investigation process where a company may determine that a notification is not required, including finding an available exemption or determining that there was no unauthorized acquisition, Peretti added.

E.U. and U.S. Approaches Converging

Because U.S. companies face the threat of class actions and other litigation, Lloyd observed, they tend to approach investigations more carefully and thoroughly than many European companies traditionally have. However, the GDPR regime and the rise of collective action lawsuits are changing how European companies react. They are beginning to think more about litigation risk and preserving privilege. It is also important to consider which regulator is involved. For example, the Luxembourg regulator is "very conservative," while the U.K. Information Commissioner's Office is more "pragmatic," Lloyd said.

The approach to deciding whether, where and when to notify of a breach is similar in the U.S. and the E.U., Lloyd continued. The U.S. and E.U. approaches are indeed converging, Maddox concurred. The GDPR allows room for a somewhat more "aggressive" legal analysis. Some E.U. regulators are "rather unhelpful in a breach scenario." For example, after a company made a breach notification and was in the process of investigating and remediating, the regulator began asking about data transfer agreements and compliance documents, which was a big distraction while the company was working to minimize harm to individuals, Maddox recounted.

The decision whether to notify under the GDPR turns on the likelihood of risk to individuals' rights and freedoms, which is an extremely broad concept, Maddox explained. A company has some leeway to consider the facts and circumstances. If, for example, there is a theft of Social Security numbers, a company could investigate what happened to

them. If they were accessed in a ransomware attack and the attacker provided proof of deletion, the company might not have to notify.

In contrast, in the U.S., the theft would likely trigger notification duties under state data breach laws. Even in the U.S., lawyers who work closely with forensic investigators and "really dig into the forensic facts" are finding that there can be some flexibility as to whether notification is required, Peretti added.

See "Establishing a Foundation for Breach-Notification Compliance in a Sea of Privacy Laws" (Jan. 29, 2020).

Evolving Role of Counsel in the E.U.

In Europe, lawyers traditionally have played a more limited role in incident response than in the U.S., Maddox said. First, although there are many more privacy specialists in Europe than in the U.S., there are fewer incident response specialists. Second, companies do not feel that they have the same potential legal exposure as they would in the U.S. Third, because it is much harder to obtain work product protection in the E.U., especially for in-house counsel, companies are less likely to get counsel involved for purposes of protecting privilege. This has been changing in the past few years, as more companies take a U.S.-style approach.

In the E.U., companies are often reluctant to get a lawyer involved from the outset, Lloyd said. A call to a lawyer might be the last call a company makes in the E.U., whereas in the U.S. it might be the first. This, too, is changing, but slowly. Data is global and breaches are rarely limited to one jurisdiction. Therefore, getting legal guidance is becoming more and more important. Companies typically involve counsel sooner in global breaches than in local ones, he noted.

Companies often see lawyers as slowing down their efforts to find out what went wrong and remediate, Lloyd added. They do not understand that specialized lawyers can help to guide and run investigations. Experienced attorneys will be able to step back and allow a company to function and to resolve things as quickly as possible.

See "There Really Isn't a Quarterback: Uber and Equifax Executives Share Insights on Incident Response Best Practices and the Lawyer's Role" (Jun. 12, 2019).

Attorney-Client Privilege

Attorney-client privilege is meant to protect communications made for the purpose of seeking or providing legal advice, Gerlicher said. It does not cover investigations done for business purposes. The work product doctrine protects work done by attorneys in anticipation of litigation. It can be hard to determine whether communications related to cybersecurity issues are made solely for business purposes, for legal purposes, or both.

U.S.

In the U.S., the expectation is that companies will be conducting at least some investigations under privilege and retaining forensic firms under privilege, Peretti said. A recent opinion and order in the multi-district litigation against Capital One has sparked a great deal of discussion on this topic, Gerlicher said.

In that case, a report prepared after a data breach by the company's regular information

security/incident response vendor was denied work product protection, even though the report had been commissioned by the company's outside counsel. The vendor "did what it was hired to do for business purposes, which was respond to the breach," she explained. The court determined that the report was not prepared in contemplation of litigation. Moreover, there was no way for it to qualify for attorney-client privilege, as it had already been disseminated to auditors, regulators and other third parties.

See "After Capital One Ruling, How Will Companies Protect Forensic Reports?" (Jun. 10, 2020).

E.U.

In the E.U., it is wise to assume that a forensics report is likely to end up in the hands of a regulator at some point, Lloyd noted. It is very difficult to claim that an investigation that simply records facts should be protected by the E.U. equivalent of the work product doctrine. In the U.K., litigation privilege arises when there is a significant risk that litigation will arise. Litigation risk may include regulatory investigations, but the issue is by no means settled.

E.U. countries take different approaches to privilege. For example, the U.K. DPA, upon a claim of privilege, has been amenable to receiving excerpts from reports and an explanation of what happened, Lloyd said. In contrast, Ireland's data protection commissioner recently stated that the DPA expects full investigation reports to be turned over in the first instance, Peretti noted. Some regulators insist on receiving a full forensic report, Maddox concurred. They do not agree that the recording of facts by outside vendors is a matter of privilege, even if the vendors are helping a company's lawyers.

In practice, lawyers still have an important role in incident response, even when materials are not going to be privileged, Maddox continued. For example, lawyers can offer a "legal filter" and assist forensics firms in presenting information in a way that will reduce litigation risk, even if their report will not be privileged.

See "Preserving Privilege in Audits and Internal Investigations" (Jun. 3, 2020); "Increased Post-Breach Discovery Turns Spotlight on Privilege" (Mar. 20, 2019); and "Foreign Attorneys Share Insight on Data Privacy and Privilege in Multinational Investigations" (May 25, 2016).

Contending With Regulators

U.S. regulators and AGs talk to each other, Forbes emphasized If a company decides that it is only required to notify in one state, but another state regulator finds out and takes a different position, the company may face an even deeper inquiry from the other state's regulator. In multinational and multistate matters, it is important to consider how to navigate the different regulators that will be involved.

For example, in a multistate matter, it may be possible to collaborate with state regulators so that the company can produce the same information to each state. Nevertheless, companies must be attuned to the specific requirements of each regulator.

Often, in the U.S., companies must notify regulators with which they do not have any established relationship, Peretti added. This is very different from how a regulated entity like

a bank operates. It is also different from the notification regimes in the E.U.

In the E.U., there is a tendency for privacy lawyers to "bend over to help the regulator," and not push back on overbroad requests, Lloyd said. This could also hamper incident response. Litigators, in contrast, may be more inclined only to give the regulator the minimum needed to satisfy a request. If an attorney "opens the kimono" and invites in the regulator, the regulator will inevitably find things. Consequently, although it is important for a company to maintain a good relationship with its regulator, it is equally important for it to get advice, understand its obligations and put appropriate boundaries on that relationship.

See "Regulators Speak Candidly About Cybersecurity Trends, Priorities and Coordination" (Apr. 27, 2016).