TOPICS COVERED
// Regulation & Risk

CYBER ENFORCEMENT PICKS UP...

...And New Risks Emerge

Written by Evan Norris

You know your company's data is a valuable asset and that you have to protect it. But how well do you know what your company actually does with its data and where it stores it? And how well do you know how data-protection regulators around the world would view your company—and the adequacy of your internal controls (and your vendors' internal controls)—if you're hit with a data breach?

As global enforcement arising from cross-border data breaches starts to accelerate, companies that fall victim to a cyberattack are now facing the prospect of multiple, uncoordinated investigations across a number of continents. Assessing your company's exposure to these emerging risks starts with understanding the big picture.

What does the cyber enforcement picture look like globally?

Accelerating, but uneven. In the U.S., the pace of enforcement following data breaches is picking up, but the tracking of enforcement actions remains difficult because there is no comprehensive domestic legal framework similar to the General Data Protection Regulation (GDPR) in the EU, which went into effect in May. We recently saw the first enforcement action under the GDPR by the U.K.'s data protection regulator, brought against a non-EU company for using data "in a way that the [U.K.] data subjects were not aware of, for purposes which they would not have expected, and without a lawful basis" for that usage. Elsewhere in the world, while some countries appear to be watching to see how the GDPR's regulatory and enforcement mechanisms play out in practice, others have already passed—or are debating—their own strict data protection laws modeled on the GDPR.

What are the key federal laws and enforcement agencies in the U.S.?

There are a number of different federal cybersecurity laws enforced by different regulators with at times overlapping jurisdiction. Which federal laws apply to a company often depends on the industry in which the company operates. For instance, PayPal recently settled with the Federal Trade Commission (FTC) under both the Gramm Leach Bliley Act, which regulates financial institutions, and the FTC Act. One of the most active federal agencies is the Securities and Exchange Commission (SEC), which frequently issues pronouncements stressing the importance of timely disclosure of cybersecurity risks and incidents, and recently established a Cyber Unit that has already brought over a dozen enforcement actions.

What's happening at the state level?

State laws vary widely, and 50 state attorneys general are in charge of enforcement. Companies tend to default to the strictest standard—for instance, if a company handles data of residents of New York and Washington State, it may have to make notification of a data breach "without unreasonable delay" (as required under New York law) even though it benefits from a 45-day window under Washington law. In the area of enforcement, Uber recently entered into a nationwide multistate settlement of $148 million—the biggest data breach settlement to-date—to resolve allegations that it concealed a 2016 data breach that affected tens of millions of U.S. data subjects and violated state data breach notification laws. Looking ahead, all eyes will be on California as the Consumer Privacy Act, the state's strict new data protection regime, comes into effect in January 2020.

What does the enforcement picture look like in the EU?

Accelerating. The GDPR is a comprehensive data privacy and protection regime sweeping in its scope and jurisdictional reach. It extends to "any information concerning an identified or identifiable natural person" and applies to "controllers" and "processors" of such data that maintain an "establishment" in the EU, offer goods or services to individuals in the EU or monitor the behavior of individuals in the EU (e.g., by using website cookies). The GDPR vests the EU members' 28 data-protection regulators with the authority to impose enormous fines: up to 2% of a company's worldwide turnover for late notification of a data breach, and up to 4% for violations such as the breach of key data processing principles and transferring personal data outside of the EU without a valid ground. Since May 2018, when the GDPR went into effect, the U.K.'s data protection agency alone has brought enforcement actions against Equifax, Facebook and a Canadian data analytics company for failing to protect and in some cases actively misusing personal information of U.K. data subjects. While two of these three actions related to breaches that occurred prior to the GDPR's effective date, notably, those saw the imposition of the maximum fine allowed under the pre-GDPR legislation for the first time. The trend is clear, and more enforcement actions are coming under the GDPR.

Does the GDPR apply to non-EU companies that have no physical presence in Europe?

Yes. In certain cases, the GDPR has extraterritorial effect.

The GDPR applies to companies established wholly outside of the EU that conduct business in the EU, either by offering goods or services or by processing data of EU data subjects. For example, the GDPR would likely apply to an online company established outside the EU that specifically targets individuals in the EU that access its website. Companies are anxiously awaiting further guidance from the European Data Protection Board, which has recently been published for public comment, to understand how the new regulation will apply in practice. In the meantime, non-EU companies will continue to watch closely the developments in the first enforcement action brought in September by the U.K.'s data protection watchdog against the Canadian data analytics firm. Non-EU companies will also continue to watch closely the U.K. after its planned exit from the EU next year to see whether the U.K. negotiates a separate status with the EU for purposes of GDPR regulation and enforcement or whether it becomes like the U.S. and any other non-EU member state.

What's happening in countries outside of the U.S. and EU?

A lot. Brazil recently passed a new Data Protection Law that is based on GDPR and applies to Brazilian and non-Brazilian companies that collect or process data in Brazil, or process data for the purpose of targeting consumers in Brazil. As companies await how the new law is enforced in Brazil, companies should also closely monitor developments in the world's other major economies as new laws are being proposed with regularity. India's draft Data Protection Bill, to take one recent example, has been hotly debated since it was introduced, and it will be important to see what is finally enacted.

Can we expect increased coordination among various enforcement authorities at home and abroad?

UUnclear. Recent enforcement actions suggest reason for optimism within the U.S. but also the prospect of a future with limited coordination with foreign enforcement agencies and a potential for "piling on" of data breach-related enforcement actions. For instance, over the past couple of years U.S. states have entered into a number of joint settlements, including one in which the FTC also participated. By contrast, unlike in the cross-border corruption sphere where international coordination has become common and the U.S. Department of Justice has indeed recently pledged to avoid "piling on," we have yet to see a coordinated enforcement action following a cross-border data breach. Experience suggests that governments still handle those investigations separately, and the early evidence points to the potential for piecemeal resolutions of global data breaches to become commonplace.

Companies outside the EU that are subject to the GDPR's extraterritorial reach will face additional challenges in obtaining a coordinated resolution. Unlike companies that are established in one of the EU member states, they do not benefit from the GDPR's coordinated enforcement mechanism under the "one-stop shop" principle and so need to deal separately with local supervisory authorities in each EU country in which they are active. Such companies will need to actively push regulators in EU member states to coordinate their separate enforcement actions.

What is the main lesson here?

The main lesson is that as companies continue to calibrate their existing enterprise-wide risk management systems and update them to the specific risks they face, they should now consider the potential that they will face multiple enforcement actions following a cross-border data breach. Data breaches will happen even to those whose networks are best prepared against an attack, and so every company should consider whether its critical response plan needs a section on making timely breach notifications and responding to demands for information from regulators not just at home but abroad as well.

Author Biography

Evan Norris *is counsel in the Investigations Group at Cravath in New York. He advises U.S. and multinational companies, boards and senior executives on government and internal investigations, regulatory compliance and related civil litigation, with a focus on cross-border, multi-jurisdictional investigations. Before joining Cravath in 2017, Evan served for ten years as a federal prosecutor in the Eastern District of New York, where as chief of the cybercrime unit he conducted and supervised investigations and prosecutions of cyber matters ranging from international data breaches to industrial espionage and corporate insider attacks. He was also the lead prosecutor of the FIFA case, one of the most far-reaching cross-border corruption cases ever brought by the Department of Justice.*

Evan thanks Alma Mozetič, an associate at Cravath who assisted with the preparation of this article.

This article first appeared in the Fall 2018 issue of *Ethisphere Magazine*.