December, 2017

This Month's Top Issues

Technology companies rely on customers who entrust them with vast amounts of their private data — a role that thrusts those companies into the center of debates around individual protections, law enforcement access, and culpability in breaches. The stories this month all touch on aspects of these issues. What follows is a roundup and analysis of key data privacy and security issues making headlines, and what cybersecurity professionals should know.

FISA Reauthorization Heats Up Surveillance Debate

As the December 31 deadline nears for the Foreign Intelligence Surveillance Act (FISA) Section 702 reauthorization, lawmakers are considering three competing bills – each with a different approach to renewal. The Act governs when and how the U.S. can spy on digital communications of foreign nationals, and has drawn criticism for being overly broad and incidentally including the data of Americans in searches. However, the intelligence community credits the Act as instrumental in preventing terror attacks.

The bills illustrate diverging opinions among lawmakers, the intelligence community, privacy advocates, and the tech world. "The question is… particularly in the post-Snowden, post-WikiLeaks era, what is the appropriate set of safeguards and meaningful privacy protection to ensure that everybody gets a fair shake while law enforcement and national intelligence entities are able to access the information they need," said John Verdi, vice president of policy at the Future of Privacy Forum in Washington, D.C.

The intelligence community backs a so-called "clean reauthorization," such as Arkansas Sen. Tom Cotton's bill to renew FISA as-is with no sunset provision, though Democrats have argued a sunset is necessary to maintain oversight. Senate Intel Committee Chairman Richard Burr's bill would extend reauthorization for eight years instead of six, and require the Foreign Intelligence Surveillance Court to weigh in if inquiries return data on Americans.

Tech leaders seek further reform. In a joint letter, 31 companies, including Google and Facebook, urged Virginia Rep. Robert W. Goodlatte, chairman of the House Judiciary Committee, to increase judicial oversight and provide greater transparency in the law. Some of those urged changes were incorporated into Goodlatte's USA Liberty Act, which was approved by the House Judiciary Committee on November 8 and aims to ensure Section 702 "accords with principles of privacy and due process."

If U.S.-based companies are perceived to be subject to intelligence agency searches that expose customer data, then that carries a "real reputational risk," said Verdi, who noted that U.S. surveillance law safeguards also matter to non-U.S. businesses wherever their data is subject to U.S. jurisdiction.

"The fact that this law is up for renewal really invigorates and renews the debate about what an appropriate level of foreign surveillance is."

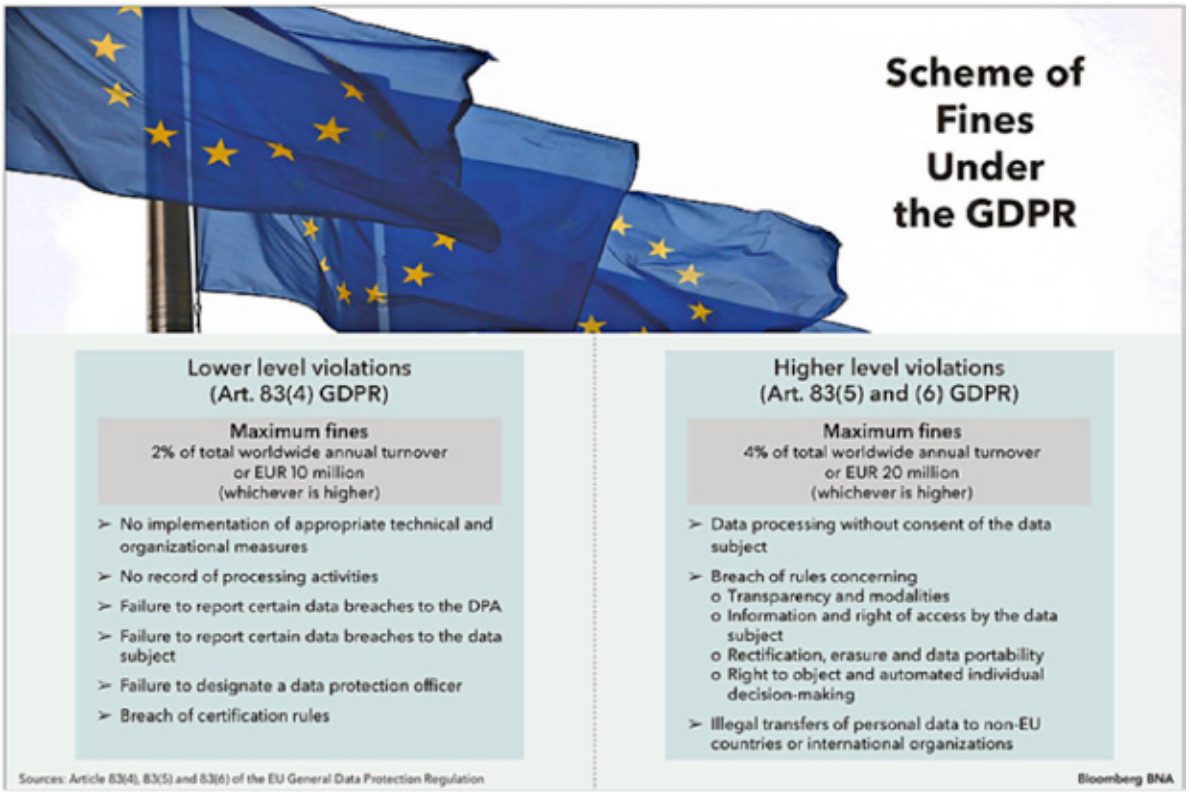
The Takeaway: With a leader yet to emerge from competing reauthorization bills, the scope of any eventual FISA reform remains unclear. If U.S.-based tech companies get their way, greater oversight and transparency measures will attempt to mitigate reputational risks posed under the surveillance law.

FISA FACT

Google reports that in the last half of 2016, the most recent period for which numbers are available, it received between 500-999 FISA requests, affecting 35,000-35,499 user accounts. This number has risen from 2009, when it received requests affecting between 5,500-6,498 user accounts for the whole year.

Privacy Fines Guidance Signals Regulator Thinking for GDPR

In October, businesses got their first look at how regulators will approach levying the possible penalties under the impending General Data Protection Regulation (GDPR), via new guidance issued by the E.U.'s Article 29. The regulation supersedes the non-binding 1995 Data Privacy Directive and mandates strict data breach notification timelines, individuals' rights to access their data, and data erasure requirements. Notably, GDPR claims jurisdiction over organizations that process E.U. residents' personal data, regardless of where the data is processed. That means many non-E.U. organizations will be subject to enforcement.



While the severity of the maximum fines is possible – 20 million euros or 4 percent of global turnover – have grabbed headlines, the non-binding guidance outlines several factors that can positively or negatively impact assessments. These include the "nature, gravity, and duration of the infringement," mitigating actions taken by the violator, the number of previous violations, and the degree of cooperation with regulators.

Courtney Bowman, a Los Angeles-based privacy and cybersecurity lawyer at the Proskauer law firm, explained that the guidance gives regulators considerable discretion to determine the level of penalty assessed and also provides a number of less severe alternatives, such as data processing bans, orders to comply, and formal warnings.

What's still unclear is how aggressive enforcement will be when the GDPR goes into effect in May 2018. It seems unlikely that the top tier of fines will be levied right off the bat, particularly, as FPF's Verdi said, the guidance includes a "repeat offender factor" that can increase fines – and it will be difficult, "if not impossible," to qualify as a repeat offender in initial enforcements.

The Takeaway: While the maximum penalties are unlikely to be handed down in initial enforcements, their potential severity should be taken seriously. The exacerbating and mitigating factors warrant close attention – and corrective action if necessary.

Conclusion

The tech community has an obvious commercial stake in protecting users' data from undue government surveillance, just as it does in protecting it from breaches and hacks. However, competing views from lawmakers and law enforcement ensure that the obligations with respect to those protections are far from a settled, or harmonious, matter.

On The Record

"The DOJ's position would put businesses in impossible conflict-of-law situations and hurt the security, jobs, and personal rights of Americans."

— Brad Smith, *president and chief legal officer, Microsoft*

About (ISC)²

(ISC)² is an international nonprofit membership association best known for its award-winning Certified Information Systems Security Professional (CISSP®) certification, with additional certification and education programs that holistically address security. Our membership, 125,000 strong internationally, is made up of sought-after cyber, information, software and infrastructure security professionals who are making a difference and helping to advance this new industry. Our vision to inspire a safe and secure cyber world reaches the general public through a commitment to social responsibility via our charitable foundation – The Center for Cyber Safety and Education™. For more information on (ISC)², visit http://www.isc2.org, follow us on Twitter or connect with us on Facebook.