Previous article Next article

GDPR's First 150 Days Impact on the U.S.

Author:
Mike Meikle

November 1, 2018 / 5:31 pm

Weighing the impact of GDPR and how the historic legislation has shaped privacy protection measures in the U.S., so far.

Apple CEO Tim Cook publicly entered the data privacy fray earlier this month, praising the European Union's General Data Protection Regulation (GDPR). At the International Conference of Data Protection and Privacy Commissioners Conference (ICDPPC), Cook advocated for GDPR rules to have a far-reaching impact on privacy beyond the European Union and even here in the United States.

"In many jurisdictions, regulators are asking tough questions. It is time for the rest of the world, including my home country, to follow your lead," he said.

In the lead up to the passage of GDPR, Facebook, Google and Microsoft publicly expressed similar pro-privacy positions; and with good reason. U.S. companies doing business in Europe can't hide from GDPR rules and could face enormous fines for non-compliance – up to 4 percent of global annual turnover. Privacy advocates hoped that would encourage U.S. firms to tighten their own domestic privacy rules beyond the inconsistent and sometimes weak state and federal data privacy laws.

It makes sense to implement privacy rules globally, rather than to adopt a patchwork of privacy rules for each country, critics had also argued. Initially, that seemed to be the case. In May, Microsoft said its GDPR protections would be extended to all its customers, not just those in EU countries.

So, roughly 150 days after the passage of one of the most significant data privacy laws ever, how has it impacted U.S. companies' privacy efforts? The reality is, not so much.

"There is a general lack of agreement about what exactly GDPR compliance is," said Graham Dufault, senior director for public policy, at ACT | The App Association. "In the U.S., chief corporate counsels are unsure if their newly rewritten privacy policies are GDPR-compliant."

GDPR Gridlock

The lack of clarity around GDPR compliance has been compared to the Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996. HIPAA data privacy and security guidelines are broad and do not specify solutions that must be in place to secure data. GDPR suffers similarly; with open-ended language and definitions regarding how companies have to comply with the law that leaves GDPR open to interpretation.

"GDPR includes a strong data security requirement and designates cybersecurity activity as a legitimate use of personal information. However, GDPR also has challenges because its standards

are not always clear enough for businesses to act with certainty," said Harley Geiger, director of public policy, Rapid7.

For example, GDPR states the companies must provide a "reasonable" level of protection for personal data. However, there isn't a clear definition of what constitutes "reasonable" protection. This provides both GDPR enforcement bodies (called Data Protection Authorities) and companies significant leeway on how they approach and enforce compliance.

With the lack of detail, firms can approach the GDPR-compliance efforts from a myriad of directions. This confusion over what is and isn't compliant is further exacerbated by a failure on the part of tech companies to protect data responsibly even after GDPR rules were enforceable, post May 25.

In an experiment conducted by the European University Institute (EUI), researchers ran the privacy policies of the largest multinationals through an artificial intelligence program called "Claudette". Included was Apple, Amazon, Microsoft, Facebook and other tech firms. The program was specifically tuned to check for GDPR privacy-policy compliance.

The results, published in July of 2018, showed that of the 14 GDPR policies tested, all failed to be compliant. This was due, in part, to company policies being unclear how user information was stored and accessed by third parties and to policies that "...are formulated using vague and unclear language, which makes it very hard for consumers to understand the actual content of the policy and how their data is used in practice."

In July, both Google and Facebook commented on the EUI study, stating they are continually updating their privacy policies to be in line with GDPR requirements.

GDPR Impact: US Private Sector

This GDPR-compliance ambiguity is fostering a lack of urgency in U.S. companies. From small business to large firms, companies are finding it hard enough to adhere to their current security posture and U.S. regulatory requirements. The exceptions are firms who have historically had robust risk and compliance practices (Fortune 50), or companies whose operations are data-centric and handle EU citizen data. In general, companies have weighed the cost of compliance with the potential for realizing a fine, and have so far taken a wait-and-see approach.

"We've seen this in the past with Sarbanes Oxley or HIPAA," says Loretta Mahon Smith, President, and CEO, DAMA International. "Until there is accountability for corporate officers, companies will lag behind in GDPR compliance." Sarbanes-Oxley holds corporate officers individually responsible for the accuracy and completeness of corporate financial reports. GDPR opens the door for personal criminal liability for corporate board members, but this penalty has yet to be exercised.

GDPR has raised the profile of cybersecurity and data privacy within the C-suite. CIOs and CISOs have used the threat of GDPR non-compliance to accelerate the procurement of technical risk controls. It has also provided more appetite for funding risk-management initiatives and privacy policy reviews. As in the past with HIPAA or Sarbanes-Oxley, there will be multiple spikes in C-Suite interest that will coincide with GDPR enforcement hitting U.S. companies.

To that end, it appears GDPR's impact on compliance spending far exceeds actual new privacy protection among U.S. companies, so far. Fortune 500 firms have spent over $8 billion in their compliance efforts in the run-up to May 25, 2018, according to an estimate by the International Association of Privacy Professionals and Ernst & Young.

Making matters worse, said ACT's Dufault, is "GDPR initiatives have also been accused of adding mud to the water by diverting resources that would be better spent on more direct security solutions."

GDPR Impact: US Public Sector

At the U.S. state government level, some politicians view GDPR as a wake-up call to take aggressive action to protect consumer data privacy. For example, California was influenced by GDPR when Governor Jerry Brown proposed and passed the California Consumer Privacy Act (CCPA).

Both CCPA and GDPR share very similar frameworks. CCPA gives California residents certain rights on how their personal data can be stored, accessed, sold and deleted. Each is on par with GDPR rules.

However, there are a few differences, the most significant being that GDPR requires users to opt-in for personal data collection, while the CCPA offers CA residents an opt-out mechanism for having their data collected. In other words, the CCPA allows websites to initially collect your information when users sign up, while the GDPR requires a user's consent explicitly before gathering any information.

The CCPA is scheduled to go into effect on January 1, 2020.

Eleven other states are following suit with newly passed data protection and breach notification laws for 2018, energized by GDPR and CCPA. In July of 2018, Senator Mark Warner released a position paper on the subject. The document contained statements that the "U.S. could adopt rules mirroring GDPR, with key features like data portability, the right to be forgotten, 72-hour data breach notification, first-party consent, and other major data protections."

GDPR Impact: EU

In Europe, where GDPR became law as of May 25, there have been enormous compliance efforts, followed by a bevy of lawsuits that could potentially cost companies such as Google and Facebook billions of euros. The jury is still out whether GDPR has made the type of big changes to user privacy its most enthusiastic supporters promised. It has raised security awareness but right now Data Protection Authorities are overwhelmed with complaints, and there is significant confusion around the law.

In this sense, GDPR can be again compared to HIPAA. Some argue HIPAA has hurt many people since doctors are now reluctant to share any patient data with other healthcare providers.

As of October, only a few companies are facing GDPR fines. The Canadian data analytics company AggregateIQ, which has been tied to the Cambridge Analytica scandal, is the first. The UK Information Commissioner's Office (ICO) issued a GDPR notice in September, saying that the company had 30 days to comply, appeal or potentially face a fine of up to 20 million euros.

Also facing GDPR fines is Barreiro Hospital in Portugal. The Portuguese Data Protection Authority found the hospital granted inappropriate access to patient records. The hospital is currently appealing a 400,000 euro fine.

GDPR: Next 150 Days

So what does the next 150 days hold for GDPR? We will continue to see European Union GDPR enforcers overwhelmed with EU citizens lodging complaints and requests. In the case of AggregateIQ and others, fines will officially be levied after appeals and remediation are exhausted.

In the U.S., data privacy and security concerns will continue to gain traction at the state level. Many of those efforts, like CCPA, will be modeled in part by GDPR, say experts.

"Security and privacy issues are growing in severity, undermining trust in technology and prompting real-world consequences. A patchwork of privacy and security regulations has arisen, but this offers consumers spotty protection, and the legal complexity creates barriers to compliance for businesses with limited resources. It is time for Congress to step in," said Geiger.

Meanwhile, it appears the Big Five tech firms are stepping up to the plate regarding data privacy and security in response to high-profile data breaches, consumer distrust and state government legislation.

In September, Google released its Framework for Responsible Data Protection Regulation. The framework was released ahead of the company's disclosure of a breach of 500,000 Google+ accounts that may have leaked private user data to hundreds of third-party sites. The framework

covers how the company will collect and use the personal data it collects. It also outlines how individuals can control and delete the information gathered by the information giant.

Still, in a move seen as an attempt to skirt GDPR rules, in April Facebook shifted the responsibility of managing 1.5 billion user accounts located outside the U.S., Canada and the EU from its international headquarters in Ireland to its U.S. offices.

Last month, in a thinly veiled critique of his rivals, Apple's Cook decried what he called the "data industrial complex" at the ICDPPC event. "Our own information, from the everyday to the deeply personal, is being weaponized against us with military efficiency."

However, in May Apple introduced new data and privacy tools for its European customers. The tools allowed EU Apple customers to download the data that Apple has collected about them and the devices they own. But, here in the US, Apple has only promised to broaden the availability of the tools.

Write a comment

Share this article:

Government Privacy

SUGGESTED ARTICLES

UK Slaps Facebook with $645K Fine Over Cambridge Analytica Scandal

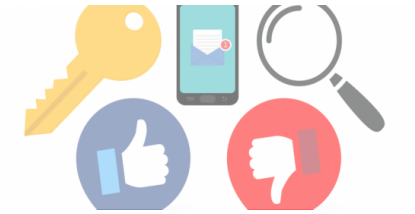
The amount is the max allowed under pre-GDPR regulation, but is barely a financial slap on the wrist for the social-media giant.

October 25, 2018 2

Calif. Law Takes Aim at Weak IoT Passwords

Concerns over data privacy and security push California to roll out the first legislation on connected devices.

October 11, 2018



Norwegian Agency Dings Facebook, Google For "Unethical" Privacy Tactics

Facebook and Google are doing anything they can to nudge users away from data privacy, a Norwegian agency alleged in a new report.

June 28, 2018

DISCUSSION

Leave A Comment

Write a reply...

Your name

Your email

Save my name, email, and website in this browser for the next time I comment.

Notify me when new comments are added.

Send Comment

I'm not a robot

reCAPTCHA
Privacy - Terms

This site uses Akismet to reduce spam. Learn how your comment data is processed.

EDITOR'S PICKS

PoC Attack Leverages Microsoft Office and YouTube to Deliver Malware

October 26, 2018

DemonBot Fans DDoS Flames with Hadoop Enslavement

October 26, 2018

UK Slaps Facebook with $645K Fine Over Cambridge Analytica Scandal

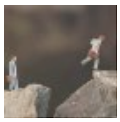
October 25, 2018

2

Debunking AI's Impact on the Cybersecurity Skills Gap

October 25, 2018

2



ThreatList: 3 Out of 4 Employees Pose a Security Risk to Businesses

October 23, 2018

Newsletter

Subscribe to *Threatpost Today*

Join thousands of people who receive the latest breaking cybersecurity news every day.

Subscribe now

Twitter

The Kraken ransomware gets its "arms" around the #Malware -as-a-service model on the Dark Web: https://t.co/kClHLrG0QA

2 days ago

Follow @threatpost

Subscribe to our newsletter, *Threatpost Today*! Get the latest breaking news delivered daily to your inbox.

Subscribe now

The First Stop For Security News