Guest

EU gets serious on privacy, but too many companies ignore the risk

Seth Batey, Fivetran

November 26, 2022 9:10 AM

Image Credit: Photo by Mikhail Nilov

If you ask most tech workers the difference between security and privacy, they probably won't be able to tell you the difference — unless their main job is working on one of those teams. Given how much of our life is now online, this is a problem that can lead to corporate liability and multimillion-dollar fines, especially from European regulators. With this increased focus, what's the difference between security and privacy, and how should employees think about these issues?

To start, let's look at Twitter's announcement this summer that a hacker had been in its system for more than six months, and was offering to sell user data from 5.4 million accounts. (In 2020 a Florida teen was also charged with taking over accounts). Hackers breaching Twitter's system pose a security problem. But since these hackers may have had access to millions or billions of records, that's also a privacy problem.

This summer, Meta was fined $403 million by Ireland's GDPR (General Data Protection Regulation) authority. Last year, European regulators fined Amazon $888 million. This is a big problem for major platforms, but it can hit almost any company today: California recently fined Sepora $1.2 million for violating the CCPA (California Consumer Privacy Act).

If we want to reduce the impact of fines and breaches, we need software companies to focus on privacy as much as security, and make sure their employees know the difference. If you go to the doctor, your doctor knows exactly what HIPAA regulations allow them to disclose. Any trucker on the road knows exactly how many hours they can drive based on DoT Hours of Service regulations. But if you ask tech workers what they can and can't do under CCPA, most may not even recognize the acronym.

Privacy is about creating trust in your organization. It's about how you handle personal information, and making sure that you're treating this data responsibly and in line with what consumers would expect you to do.

TL;DR on GDPR

GDPR guidelines call for data to be stored in a manner that ensures users can request that their information be corrected, deleted as part of the "right to be forgotten," or accessed so the user

knows what data the company has collected on the user, along with various other privacy rights requests. But when data is stored in multiple disconnected databases, it's much more challenging to stay compliant, as requests require multiple steps and coordination across databases.

Rules also focus on where data is stored, aiming to regulate the flow of data between the U.S. and European countries. Facebook is fighting this policy, but swears "Meta is absolutely not threatening to leave Europe." To prepare for these new regulations, companies need to ensure they have a comprehensive record of data processing activities and a data inventory to demonstrate compliance with regulators.

Ten pillars for privacy awareness

Conducting ongoing training at your company is very important for all employees accessing personal identifiable information (PII). Given the pace of announcements about new fines and updated policies, you may need to update your staff frequently.

At Fivetran, I conduct training across the company, at least every 12 months, but additional reinforcement for legal requirements is a year-round job. Awareness includes teaching the foundational aspects of privacy, rather than a long list of legal requirements, and explaining how those principles apply to each team and team member. I have a checklist of focus areas. Here's what people need to know.

- Accountability: Senior leadership needs to identify a single person ultimately accountable for an organization's privacy compliance. Many companies will designate a Data Privacy Officer, but regardless, the goal is to have someone focused and responsible for GDPR (and other regulatory) compliance.

- Identifying Purposes: Companies need to identify in their privacy notice how they will use customer data, but must also consider consumer expectations. Most people would expect video footage from a store's security camera to be accessed only if there's a break-in. But if the camera is feeding a live stream to the company's homepage, that could surprise customers and lead to privacy concerns.

- Consent: Proper consent is an essential requirement. But don't forget that data subjects have the right to withdraw consent as well, and your data systems need to support this capability.

- Limiting Collection: As tempting as it is to gather as much data as possible, the more you collect, the bigger your risk. Focus on tracking and gathering data you can actually use in your business, based on the purposes you've identified.

- Limiting Use, Disclosure and Retention: Privacy laws require companies to limit access to data to identified purposes and prevent disclosure to non-authorized personnel. But too many companies still allow general employees to access personal data. When a hacker gets into a system using a compromised account, you can minimize the extent of the damage they can do by limiting internal access to those who need it. Also, don't retain data longer than you need to, considering local retention laws and justified business purposes, and think through how you'd respond if you ever got a legal notice.

- Accuracy: Ensuring customer data is accurate is a legal requirement and a business priority for success. Accuracy is also a priority when integrating data from multiple sources, so make sure you can verify the reliability of your processes and the data.

- Safeguards: Ensure you have proper governance and safeguards for access to data, both from a privacy and a security perspective. Think of this using the "CIA triad," from IT security programs that will maintain confidentiality, integrity and availability of the consumer data you've collected.

- Openness: If your company has a unique way of using customer data, don't bury those policies in the Terms of Service agreement; someone will notice eventually. Meta agreed to pay users $37.5 million because the company was geotracking users by their IP addresses after consumers turned off location tracking on their phone. Be transparent about your data practices, and make information available in policies that use clear, concise, plain-English wording.

- Individual Access: On request, data subjects must be told the existence, use and disclosures of their personal information, and be able to access and challenge the accuracy of that information. Organizations should be prepared to handle these types of privacy rights requests.

- Challenging Compliance: Ultimately, anyone covered by GDPR and CCPA has the right to challenge a company's compliance with these regulations. If a company is challenged, it can be required to show compliance with applicable privacy requirements, including relevant policies and procedures. Working with your privacy team to role-play how you would respond to such a request will help expose any gaps in your data privacy program before regulators start looking.

With the importance of data to modern businesses, ensuring that employees are familiar with privacy law will put your company in a much better position in case of an incident. Thinking about how data is captured and stored will help minimize risks. Privacy is your company's promise to consumers that you're a trustworthy partner, and have their interests in mind. To build awareness around privacy, use the checklist above to ensure data processing teams know their data privacy responsibilities just as well as a doctor knows HIPAA requirements.

Seth Batey is senior privacy counsel with Fivetran.

DataDecisionMakers

Welcome to the VentureBeat community!

DataDecisionMakers is where experts, including the technical people doing data work, can share data-related insights and innovation.

If you want to read about cutting-edge ideas and up-to-date information, best practices, and the future of data and data tech, join us at DataDecisionMakers.

You might even consider contributing an article of your own!

Read More From DataDecisionMakers