Data Protection Day 2022: To Protect Privacy, Remember Security

January 27, 2022

Drew Bagley

- Endpoint & Cloud Security

Today's privacy and security conversations often happen in silos, but key privacy principles from decades ago remind us that they are intertwined, especially in the face of today's risks.

January 28, 2022, marks 15 years since the first Data Protection Day was proclaimed in Europe and 13 years since Data Privacy Day was first recognized by the United States. Since then, dozens more countries recognize the day, including Canada and Israel. However, decades before these modern commemorations, key principles were introduced that remain just as relevant now, when data breaches pose some of the greatest threats to privacy.

In the 1970s, the U.S. Federal Trade Commission (FTC) established the Fair Information Practice Principles (FIPPs), and in the 1980s, the Organization for Economic Cooperation and Development (OECD) published its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Both made clear that those holding personal data must implement appropriate security

measures to protect such information against risks to loss, access, destruction, modification or disclosure. Decades later, these principles have been enshrined in laws around the globe.

In the face of today's cyber risks and modern data protection laws, remembering these fundamental concepts is important. Security and privacy compliance are as intertwined as ever in the European Union's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), Japan's Act on Protection of Personal Information (APPI), and privacy laws around the globe. Nonetheless, privacy and security dialogues are often siloed from one another. This means that it is not always obvious that many of the concerns, and even objectives, of a Chief Privacy Officer are actually shared by a Chief Information Security Officer.

When these disciplines operate in a vacuum, prescriptive privacy and security requirements can impede the overarching goal of data protection. This can take the form of selecting antiquated on-premises technologies and designing geo-restricted terms in pursuit of perceived privacy requirements or flawed perimeter security approaches. However, modern legal standards actually require protecting data with safeguards appropriate to the risk, which is dependent upon embracing the latest technologies and processes.

Take GDPR, for example. In complying with sometimes ambiguous interpretations of the European Court of Justice (CJEU) Schrems II cross-border data flow assessments, it is important not to lose sight of GDPR's oft-enforced Article 5 and Article 32 security requirements. In fact, in its "State of the Art" guidelines, the European Union Cybersecurity Agency (ENISA) calls out technologies generally dependent upon cloud-native designs, like extended detection and response (XDR), and threat hunting techniques traditionally dependent upon global data flows. The reason for this is clear. As highlighted in CrowdStrike's 2021 Global Threat Report, the definition of risk is ever-evolving in the face of innovative adversaries, novel techniques and the work-from-anywhere transformation exacerbated by COVID-19, during which millions of workers retreated to hastily equipped home offices, creating a feeding frenzy for cyber predators spurred on by the windfall of easy access to sensitive data and networks.

The need to not only be thoughtful about "privacy by design" but also "security by design" is more challenging today as data may be collected via UI and cached locally, transmitted to a database, and accessed by a cloud-based application. Consequently, the entire data lifecycle must be considered, from SecDevOps in building software, following best practices on identity and Zero Trust when granting access to data, and ultimately securing the workload, whether it is on a traditional endpoint or in the cloud. Consistent with Ann Cavoukian's Principle of *Full Functionality – Positive Sum Not Zero Sum*, privacy and security should not be treated as tradeoffs where the path of least resistance is taken. Organizations responsible for data must protect the entire attack surface.

As we recognize Data Protection Day, it is important to reflect on what holistic data protection entails, and how critical cybersecurity is, not only to compliance but to protecting privacy. For policy makers and regulated organizations alike, it is critical to focus on the big picture goal of incentivizing the adoption of the best way to protect data rather than arbitrary geo-restrictions not respected by cyber adversaries. The FIPPS and OECD guidelines mentioned above may have been developed in an era with simpler threat vectors, but implementing "appropriate" security remains critical to protecting privacy today. It is with these challenges and big picture objectives in mind that CrowdStrike seeks to provide customers with the contextual information needed to implement the robust technologies in pursuit of data protection compliance.