# Succeeding at the Intersection of Security and Privacy

## Background

For years, data compromises have seemingly followed a power law curve, with high frequency/low magnitude security events coupled with some less frequent but increasingly high magnitude events. As the magnitude of these data compromises continued to exceed previous records and reach into the billions of records compromised, pundits and experts alike declared each passing year the year of the breach. And with each record-breaking breach, the focus remained on the technical, security issues with much less attention paid to privacy.

However, 2018 was an inflection point wherein the razor-sharp focus on security began to blur with a growing emphasis on privacy as the impact of unauthorized data access shook both the private sector as well as the public conscience. A confluence of three factors helped instigate these changes. First, the steady pace of cyber attacks continued, with both intellectual property (IP) as well as personally identifiable information (PII) compromised. Too frequently measured in the millions of data records breached, these cyber attacks are impactful, but alone were not significant enough to shift opinions thanks to breach fatigue and the growing feeling of helplessness when it comes to data protection.

Instead, two other events—in conjunction with the steady deluge of data compromises—provide the additional necessary conditions for today's growing social movement in favor of greater security and privacy. The Cambridge Analytica data sharing scandal brought to light the extent of some corporate data collection efforts as well as how little consumer visibility exists when it comes to where their data is shared or sold. In addition, the European Union's General Data Protection Regulation (GDPR) came into effect in May 2018 and is the most prominent example of the global rise of regulatory frameworks focused on data protection. Under GDPR, organizations holding data on European Union (EU) citizens are required to comply, regardless of whether they are located within an EU member state.

Together, these events continue to reverberate and elevate the focus on unauthorized data access. Whether from malicious compromise, nebulous data sharing, or compliance mechanisms, this focus on unauthorized data access reflects the growing nexus of security and privacy. In turn, organizations that focus on this intersection and data-level protections are much better equipped to navigate today's modern data landscape, including the regulatory and attacker dynamics. Before describing the benefits of such a strategy focused on the nexus of security and privacy, it is important to first explore this growing convergence of security and privacy and the underlying forces behind the privacy and security awakening.

## Traditional Approaches to Security and Privacy

Traditionally, the security and privacy communities and concepts have remained separate. The security industry tends to focus on the technical implementation of protecting data, while the privacy community focuses on the legal and ethical considerations behind the storage, access, protection, and sharing of data. In many areas, this separation of the two is relevant and appropriate. For instance, privacy expertise remains essential for greater transparency in terms of service documentation and ensuring consumers better understand the repercussions of their decisions. In January 2019, the French data authority, CNIL, issued the largest fine under the new GDPR "opting in" component. Under this facet of GDPR, Google was hit with a $57 million fine for forced consent and the lack of transparency about the processing of people's data and how they use it. Refining and defining the boundaries of opting in rests largely on privacy expertise.

In contrast, the denial of service attacks that interrupted electrical grid operations in March 2019 reflects a security incident. In this case, the energy company serving parts of California, Wyoming, and Utah was flooded with internet traffic. While this did not halt service, it did disrupt operations. According to intelligence officials, Russia and China have the ability to disrupt critical infrastructure in a similar manner, while North Korea and Iran are attempting to develop these capabilities. These kinds of attacks largely require security expertise and defenses.

The key differentiator in each of these scenarios is the outcome, not the actors involved. While it is important to acknowledge the areas where security and privacy remain distinct, they increasingly intersect, resulting in unauthorized data access compromises which impact both security and privacy. This is especially relevant given that most people focus on the outcome as opposed to distinguishing between security and privacy. According to a recent Forrester survey, many businesses don't understand the difference between the two. The growing societal swell further reflects a broader focus on data protection. This nexus of security and privacy has since become the epicenter of the public awakening in favor of renewed privacy and security.

The momentum of popular opinion may prove to be the spark that ignites the policy, legal, and technological innovation required to counter the full range of unauthorized data access. By taking an effects-based view of security and privacy, organizations can better implement a strategy that optimizes data protection against the full range of scenarios that lead to unauthorized data access. As previously noted, both corporations and individuals view these incidents as unauthorized data access as opposed to security or privacy events. However, these compromises can occur through a variety of means, which are explored in the following section.

## The Growing Challenge of Unauthorized Data Access

The intersection of security and privacy only continues to grow as new forms of unauthorized data access emerge. This section addresses the three most prominent forms of unauthorized data access, illustrating how operating at the nexus of security and privacy can improve data protection against a broad range of scenarios.

## Cyber Attacks

When the Office of Personnel Management (OPM) breach was revealed in 2015, many never believed PII would be the target of a nation-state attack. Since then, these kinds of privacy breaches through security compromises are all too frequent. The Marriott data breach exposed almost 400 million guest records, including unencrypted passport numbers. The Yahoo breach compromised three billion records, including names, birth dates, and phone numbers. The Sony hack is best known for the security implications and wiper malware that destroyed three-quarters of their computers, but it also was an enormous privacy compromise of Sony employees and partners.

Each of these has been linked to China, Russia, and North Korea, respectively, and each has resulted in enormous privacy violations for the victims. Similarly, the Iranian cyber espionage group Advanced Persistent Threat 39 is currently targeting the telecommunications and travel industries for PII, while the Iranian group Cobalt Gypsy has exploited social media to target corporate executives across a range of industries demonstrating another means of compromising both privacy and security. The tactics and techniques of these four countries continues to diffuse to smaller nation-states who also target both PII and IP. For example, the Vietnamese advanced persistent threat group, OceanLotus, targets both the private and public sectors mainly for cyber espionage that includes transcripts of private conversations of national leaders.

Of course, non-state actors have a similar track record with significant amounts of unauthorized data access leading to both security and privacy compromises. Criminal groups and cyber mercenaries target PII for a wide range of objectives, including financial theft and corporate espionage. From tax refund fraud to selling identity on the dark web to credential harvesting, each of these security breaches can be lucrative for criminals and is directly a privacy compromise. The Lebanese group Dark Caracal launched a global campaign targeting Android devices, stealing hundreds of gigabytes of data, including sensitive data. The private sector is also increasingly adopting these same tactics. Whether it is competitors hacking each other for IP or trade secrets, or vendors who sell hacking as a service, these facets of the private sector should be included in any threat model when it comes to preventing unauthorized data access.

## Third-Party Data Sharing & Access

Cambridge Analytica's data gathering and sharing awoke public conscience to the vast market of monetized data. Cambridge Analytica reflects the lack of transparency in exactly how accurately consumer data is shared and sold. It also is indicative of how third-party data exposure through partnerships, supply-chains, and internet infrastructure remains a growing threat to security and privacy.

For instance, T-Mobile was significantly impacted when the consumer credit reporting company, Experian, suffered a data breach. This breach exposed a range of T-Mobile customers' personal data, including social security numbers and dates of birth. Similarly, in April 2019, data from a range of Fortune 500 companies was exposed when internet infrastructure provider, Citycomp, was hacked. Some of the files were initially posted online while the attacker demanded ransom before threatening to dump the remaining data.

Unauthorized data sharing also can occur through intentional monetization of personal data without consent. In January 2019, an investigative report revealed that major telecommunications companies were selling consumer geo-location data. This data was sold to bounty hunters, on the dark web and to other companies who then resold the data to organizations across a range of industries. While some of this reselling did violate corporate privacy policies, it nevertheless persisted and resulted in a class-action lawsuit.

## Misconfigured Databases & Servers

Many of the largest data breaches have actually been due to human error in unknowingly exposing data online, demonstrating the impact of privacy compromises following insufficient security measures. For the most part, these data compromises occur due to misconfigured cloud servers or exposed databases. In fact, two billion records were leaked online when a database of an email verification platform used by marketers was accidentally exposed. The records included credit scores, birth dates, and physical addresses.

Misconfigured cloud servers, platforms, or accounts similarly are frequent culprits for significant data breaches. In March 2019, security researchers found sensitive corporate data online due to misconfigured Box storage accounts. The leak exposed everything from passport photos to social security numbers and financial data. A few years earlier, a researcher found an exposed AWS bucket with data labeled as classified as well as software from a cloud-based component of the Distributed Common Ground System - Army (DCGS-A). A Department of Defense contractor had left the storage bucket publicly accessible due to misconfigured permissions. In each of these instances, the misconfiguration could have been avoided with the proper permissions applied, as well as through data-centric protections encrypting data in the cloud or on-premise databases.

## The Regulatory Landscape at the Intersection of Security and Privacy

The persistence of unauthorized data access continues gives additional fuel to the privacy movement, which in turn prompts a steady drumbeat of legislation aimed at data protection. While many aspects of existing privacy legislation focus solely on privacy - such as opting-in and Right of Access requests - core portions of data protection legislation focuses on unauthorized data access and therefore address core security and privacy concerns.

## Security Safeguards

The GDPR is often referred to as Europe's privacy law, but it is much more than that, impacting the data of European Union citizens wherever it resides. It focuses on data protection writ large, with core components operating at this intersection of security and privacy. For example, Article 32 of the GDPR addresses the security of processing data, noting "the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk." Relevant measures listed include encryption and pseudonymisation, ensuring the CIA of data (i.e., confidentiality, integrity and availability), restoring personal data in light of an incident in a timely manner, and implementing a security assessment process.

While some general guidelines are offered, it is not entirely clear how to evaluate what security processes are required in conjunction with risk. Fortunately, a few cases have emerged that at least begin to offer some guidelines. Last November, a German firm was fined €20,000 for failing to encrypt their data, which resulted in 330,000 credentials being posted online.

More recently, the Italian data protection authority issued its first GDPR fine, which similarly focused on inadequate security measures. In this case, a platform that ran websites associated with an Italian political party experienced a data breach and was fined €50,000 for implementing inadequate security measures. The Italian data protection authority pointed to complicated and time-consuming vulnerability patching processes, weak passwords, weak encryption on the storage of passwords, and weak auditing measures that inhibited the recording of access and operations employed on the database. Shared accounts and large access privileges received significant scrutiny, especially in conjunction with the inability to audit access.

This emphasis on appropriate security measures is not unique to the GDPR. The California Consumer Privacy Act (CCPA) includes a similar measure, as does HIPAA. The Gramm-Leach-Bliley Act (GLBA) which addresses the financial industry, also has a similar Safeguards Rule which is currently under review by the FTC to provide greater detail specifying what those security measures entail. For instance, the recommendations include encryption for data at rest and in motion as well as access controls. Many of the growing list of bills currently introduced at state capitols also emphasize reasonable security, including New York's recently proposed legislation.

## Data Breach Notification Requirements

Existing privacy laws such as the GDPR and CCPA include data breach notification requirements, both with a 72 hour window to notify officials after discovering the breach. Absent a federal privacy law, in the United States there are currently 54 different data breach notification laws, including laws in Guam, Puerto Rico, U.S.Virgin Islands, and Washington, DC.. Last year, Alabama and South Dakota became the final two states to enact data breach notification laws.

The requirements for each of these laws differ state to state and at times contradict one another. In general, these laws are focused on security breaches, but based on existing privacy legislation, a U.S. federal privacy law could streamline this patchwork for consistency within the United States. As corporations increasingly become responsible for quick notification of a breach, these breach notification requirements function directly at the intersection of security and privacy.

## Succeeding at the Nexus of Security and Privacy

As these examples demonstrate, security violations are increasingly privacy violations as well. At the same time, the notion that security and privacy hinder innovation has been used to rationalize a deprioritization of both security and privacy. Even worse, there is a growing sense of defeatism as "assume breach" has become the default motto of the security industry, while public opinion increasingly believes all privacy is lost thanks to the endless drip of data breaches.

This must change. There is too much at risk, and too many opportunities ahead. By focusing on the intersection of privacy and security, organizations can gain a competitive advantage and garner new insights and innovations through data sharing while advancing both security and privacy. In fact, information sharing fosters efficiencies and reduces risks across both the public and private sectors, but traditionally has been challenging with data increasingly locked down and stovepiped.

In addition to limiting unauthorized data access, a holistic focus on the intersection of security and privacy provides many additional benefits. Compliance to data protection laws could spark revenue streams by encouraging greater efficiency and awareness across the entire life cycle of data. Compliance also promotes security safeguards to help protect IP and therefore safeguard innovation. Whether insider threats or external attacks, with security safeguards mandated by regulations, organizations can better protect both their IP and PII. Finally, with privacy concerns on the rise, consumers also increasingly favor compliant organizations and sales may be delayed or terminated if an organization is not compliant.

Privacy compliant organizations are also better prepared to respond to data breaches and experience fewer data breaches. In a recent survey, Cisco found that GDPR-compliant companies experience fewer data breaches. When compliant companies are breached, fewer records are lost, the costs are less, and system downtime drops by a third. Compliance is a win-win for both security and privacy.

At Virtru, we operate at the nexus of security and privacy to ensure our customers can reap the benefits of protecting against unauthorized data access while fostering data sharing and collaboration. Data protection strategies often tend to focus on locking down data, which comes at a significant cost; organizations fail to reap the benefits of collaboration and data sharing. Modern data protection requires protecting against unauthorized data access (regardless of how it occurs) while simultaneously securely sharing and collaborating internally and externally to achieve mission objectives. Data-centric security that persists with the data, including access controls and policy management, can help organizations achieve both. From law enforcement to catching software vulnerabilities to maritime safety, information sharing is essential for business success. Individuals similarly reap the benefits of a secure data sharing revolution, as Estonia demonstrates with cross border e-prescriptions and a relatively long history of secure data exchanges such as its X-Road middleware.

The intersection of security and privacy will only grow in importance thanks to the full range of unauthorized data access and leaks. The reality of the threat landscape that demands secure data is too often in conflict with the business reality of needing to share essential information for business success and innovation. This becomes even more complicated as privacy legislation provides additional guardrails and constraints.

What if you could easily secure data, control access privileges, evolve them over time including revocation, and do this at a granular level all within your current workflow? Virtru can help you achieve data-centric security, all while enabling an ecosystem that ensures secure data sharing and collaboration. From the beginning, Virtru's mission has been to protect privacy by securing data and to help organizations securely share data to best connect the dots and achieve mission success. By focusing on data-centric protections at the intersection of security and privacy, organizations gain greater control over the security and privacy of their data.

**To learn how Virtru can help your organization operate at the nexus of security and privacy, contact us at: virtru.com/contact-us**

## About Virtru

At Virtru, we understand that data is an organization's most valuable asset and sharing it is critical for business success. But sharing data creates significant risk. We believe no one should have to choose between protecting data and sharing it. We help more than 5,000 organizations, large and small, across almost every industry, protect data wherever it's created or shared so they can collaborate with confidence. Virtru provides the power to get the job done.

virtru

For more information, visit **virtru.com/contact-us**
or email **federal@virtru.com** or **partners@virtru.com**