Four Ways Consumer Privacy Can Give Your Organization a Competitive Advantage

The General Data Protection Regulation (GDPR) was the tip of the iceberg when it comes to privacy regulations and compliance. The U.S. followed suit two years later when the first state privacy law, the California Consumer Privacy Act (CCPA), went into effect on January 1, 2020. In the absence of a federal mandate, at least 25 states have decided to step up in the wake of the CCPA, including Maryland, Nevada, Massachusetts, Rhode Island, and others.

In recent years, the regulatory landscape has undergone significant shifts and with that comes the varied demands to preempt regulations and create a low bar for compliance. However, instead of viewing privacy regulation as a headwind to business growth, privacy can be a significant competitive advantage, especially for early adopters. Organizations who developed a more sophisticated approach to tackling GDPR compliance, rather than a more blunt tactic of blocking all visitors from Europe, found themselves in a stronger position for the arrival of the CCPA and other pending U.S privacy laws.

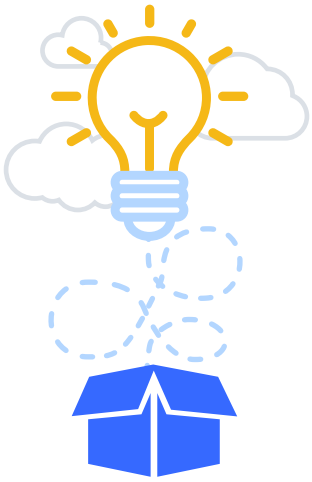
Here's how you can leverage consumer privacy to gain a business advantage against the competition.

1. Privacy can spark growth and revenue.

The most prominent argument in recent years against privacy regulation is that it will hinder innovation and limit growth. This notion is frequently reiterated during Congressional hearings and has dominated discussions leading up to both the CCPA and the GDPR. Interestingly, most evidence is anecdotal; very specific examples were offered to justify the claims while the growing list of positive business effects from privacy regulations were ignored. For instance, many GDPR-compliant organizations are seeing shorter sales cycles, a point often overlooked in privacy and compliance discussions.

Before the GDPR went into effect in 2018, many media outlets without a big European footprint chose to withdraw from the European market, which became the dominant narrative. In contrast, The New York Times depended on the European market for 15% of their global digital subscribers. They opted to drop behavioral advertising, and focused more on geographical and contextual targeting—and saw ad revenues increase. Business Insider made a similar calculation by switching to an opt-in approach to personalized ads, and also didn't see any negative effects from the move, helping them maintain a foothold in the market.

2. Privacy enhances productivity and innovation.

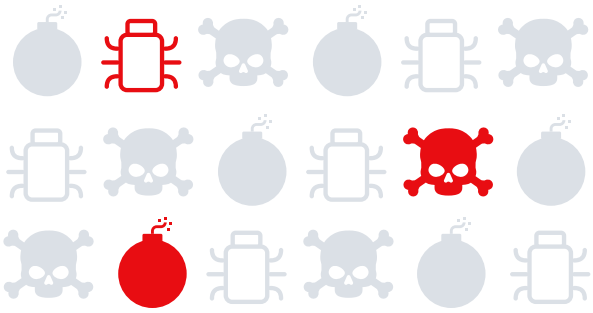


Data remains siloed within organizations. Either due to resource restrictions that inhibit optimizations to security architecture or fear of improperly exposing data, the true potential of data remains untapped for most organizations. With persistent protection and privacy controls, in conjunction with the appropriate data discovery exercise required to meet compliance, organizations can unlock the power of data while preserving privacy. Whether it is sharing relevant data across the supply chain or supporting cutting-edge research across organizations, privacy can be an enabler for innovation.

In addition, privacy can increase productivity by freeing up resources. For instance, with Data Subject Access Requests (DSARs) on the rise, organizations are struggling to keep up with these requests. But organizations that prioritize privacy have the tools and processes in place to quickly respond to these and other requests for information in a timely manner that promotes compliance and allows their employees to focus on their mission.

In short, privacy helps organizations break down data silos and begin to reap the benefits of data portability. With the proper access privileges and data inventory in place, compliant organizations can quickly and securely exchange data confidently. From financial institutions to healthcare to energy, organizations are benefitting from greater collaboration and the efficiencies that emerge through compliance with privacy regulations.

3. Privacy leads to fewer data breaches.



Privacy regulations also encourage better security practices. From inadvertent data leaks to sophisticated cyber attacks, compliance with privacy laws is a forcing function to help organizations prioritize data protection. According to a study by Cisco, companies that are GDPR-compliant experience fewer data breaches and less costly data breaches. When breaches do occur, organizations that are GDPR-compliant lose 35% fewer records than those that aren't.

With the repercussions rising for failing to notify government officials following a breach, the CCPA actually incentivizes companies to disclose breaches rather than conceal them. Given this liability, organizations that pursue data protection solutions that employees will actually use will gain the advantage and experience fewer data breaches. The GDPR, CCPA, and most likely future legislation will include a post-breach assessment as to whether organizations adhere to reasonable security procedures to preserve privacy.

With usable privacy, organizations benefit from better data protection and demonstrate sufficient steps were taken to protect data. In this way, compliant organizations are less prone to data breaches, and when a breach does occur, they can demonstrate appropriate measures were taken to protect the data.

4. Privacy helps increase customer trust, engagement, and loyalty.

Addressing privacy concerns extends beyond compliance and minimizing risk to also building more trusting customer relationships that drive consumer engagement and loyalty. A recent Deloitte survey indicates that 73% of consumers are more likely to be open to or neutral about sharing data if they are satisfied with privacy policies explaining how data is used. By simply educating consumers about how their data is used, organizations can earn their trust.

Without transparency, consumers struggle to understand what data an organization collects and how they use it. For example, according to the survey, over two-thirds of consumers believe retailers use their data for targeted marketing campaigns and 55% believe that retailers share data with third parties or sell it to outside buyers. However, retail executives indicated the top three uses of consumer data were actually for increasing efficiencies in operations (53%), improving product selection (52%), and enhancing in-store services or experiences (49%). Better transparency on data use, in accordance with privacy regulations, is essential to encouraging consumer engagement and ultimately, loyalty.

Power Your Privacy Management Initiatives with Data-Centric Protection

Organizations that take a leading-edge approach to privacy have a crucial competitive advantage in today's business landscape. Virtru helps accelerate privacy initiatives with data-centric security, including the following features, that prevent unauthorized access, wherever data is shared.

- **End-to-End Encryption:** Encrypt Gmail and Outlook messages and Google Drive files directly within the client, preventing access by Google, Microsoft, and other unauthorized parties.
- **Persistent Protection and Control:** Disable forwarding, set expiration, and revoke access immediately. Watermark files to deter data leaks. Apply persistent protection to maintain control wherever private files are shared, while giving collaborators seamless, secure access through the Secure Reader.
- **Granular Audit Trails:** View when and where private email messages, attachments, and files have been accessed during their lifecycle. Adapt controls as access requirements evolve throughout private data-sharing workflows.
- **Data Loss Prevention (DLP):** Configure DLP rules that scan emails and attachments to detect private data, then automatically enforce encryption and access controls that persist throughout collaboration workflows to ensure privacy.

To better understand how organizations can leverage these security features to enhance privacy, gain trust within the marketplace, and reap the business benefits, we look at three common industry challenges, followed by a brief overview of how a data-centric solution can address each one.

Media: Responding to DSARs

Data privacy regulations give consumers the "right to know" how their personal data is being used by an organization. In order to exercise this right, also known as "right of access," an individual can submit a data subject access request (DSAR). Take for example a media organization that uses consumer data to provide customized content recommendations. As part of the compliance requirements for both the CCPA and the GDPR, this organization must have a way to respond securely and timely to consumers who exercise their "right of access" and wish to know what personal data the organization is using and how.

Managing DSARs from consumers can quickly become a burden for organizations of all sizes. Even if your organization has already spent significant time and resources to build a secure infrastructure to store collected data, responding to a DSAR means that the data must be moved out of the encrypted data stores into something else—likely email or a custom application—to get it to the requestor. This presents a significant security and privacy challenge, as the process of fulfilling the request creates new risks for unauthorized access to the consumer's data.

Virtru's emphasis on usable encryption streamlines the DSAR process by fitting seamlessly into email clients which allows the sender to encrypt the message, as well as attachments containing personal data, with a simple toggle above the body of the email. Users can also leverage additional access controls to ensure that only the intended recipient has access to the data.

Finance: Collecting and Sharing Consumers' NPI for Mortgage Loan Processing

The U.S. mortgage supply chain is a vulnerable target for data breaches. The entire mortgage process—from pre-qualification to closing—requires sharing non-public personal information (NPI), which includes personally identifiable information (PII) such as name, address, and SSN, as well as data needed to conduct a financial transaction (e.g. account numbers and balances) or provide a financial service (e.g. credit report).

Additionally, mortgage processes must comply with a web of consumer and financial data privacy regulations including Gramm-Leach-Bliley Act (GLBA) Regulation P, Consumer Financial Protection Bureau (CFPB), GDPR, CCPA, and other state privacy laws. Compliance isn't the only concern though. Privacy is necessary to foster clients' trust in a transaction with a financial institution.

Traditional approaches to collecting data needed for mortgage processing are time consuming and often involve secure portals that require additional logins, or worse, paper copies of sensitive data. Virtru unlocks seamless, secure NPI sharing workflows throughout the mortgage process to ensure privacy and compliance.

With Virtru for Gmail or Outlook, borrowers, brokers, originators, title companies, and other authorized individuals can easily share sensitive data via email, without the need for additional logins or passwords, and ensure that it remains protected throughout the full mortgage transaction process. End-to-end encryption and access controls ensure true privacy of sensitive data and that regulatory compliance requirements are met. These measures help build client trust and loyalty, as well as the organization's competitive advantage.

Technology: Securing Data Generated by Connected Devices

Living in a "smart" world means that there is a rapidly growing network of connected devices that collect and share data. But, this wave of new smart gadgets comes with a cost: the rapid speed of product development does not always allow enough time for security considerations. And, with so much data flowing in and out of all of these IoT devices, there is a significant privacy concern: data could easily end up in the wrong hands.

Take for example, home security systems, such as video doorbells. These connected devices utilize the IoT to send snapshots of any individual who comes within range or rings the doorbell, straight to a smartphone app. If the home security device does not encrypt this data, a third party—such as the police—could gain access to a consumer's "visitor log," without their prior knowledge or consent, by going straight to the device manufacturer. With encryption, the snapshots/videos would be inaccessible to the manufacturer and therefore all unauthorized third parties, too, ultimately putting control over this sensitive data into consumers' hands.

For ultimate security, each data point must be protected with data-centric encryption and privacy controls that travel with the data from the moment it is created by the IoT device. Encryption protects and isolates data between users, companies, and third-parties with access to the data. and also helps tech companies build trust with consumers when it comes to sharing sensitive information with the right people.

As it turns out, privacy can be great for business. Taking a proactive approach to protecting data in compliance with privacy regulations can help power innovation and growth, protect your bottom line, and ensure that your organization maintains a competitive advantage.

virtru

To learn more about using Virtru to protect sensitive data and ensure privacy for a competitive advantage, get in touch with us. **virtru.com/contact-us**

At Virtru, we empower organizations to unlock the power of data while maintaining control, everywhere it's stored and shared. Our portfolio of solutions and tools—built on our open data protection platform—governs data throughout its lifecycle. More than 20,000 organizations trust Virtru for data security and privacy protection. For more information, visit **virtru.com** or follow us on Twitter at @virtruprivacy.