PROTEGRITY

Data Privacy Is Good for Business

By Albert McKeon

DATA PRIVACY IS GOOD FOR BUSINESS. IT REALLY IS.

It can't be a slogan for a company website but ignored in practice. Protecting the privacy of customers, clients, employees, and all others who are connected to the data under your control is a sound business practice–and a profitable one, too.

To start, the creation of a data-privacy culture–which can happen only when data is properly secured and managed–is now a top priority of lawmakers. More than a dozen U.S. state governments are currently drafting, or are about to vote on, compliance legislation, building on a foundation of established regulations such as GDPR, HIPAA, PCI DSS, and Sarbanes-Oxley. Further, it is high on the list of expectations of consumers, who often don't mind sharing their personal information for commercial purposes, as long as the organization that uses their data respects individual privacy.

Much is made of the power and potential of data, so it's no surprise there is widespread support for codifying how it is used and secured. Protected data allows organizations to pursue, without worry of running afoul of regulations, AI-supported analytics and machine learning, DevOps and containerization, IoT, and many traditional digital applications for sales, operations, customer satisfaction, development, production, employee productivity and engagement.

Look at what Amazon does with data. Its retail business aggregates and analyzes the browsing and sales data of millions of customers, often anticipating what a shopper wants before she knows she wants it. The company also makes sense of data from a vast catalog of inventory, data from nearly 200 fulfillment centers, and the tracking data of the more than two million packages it annually ships–all to ensure consumers have choice when shopping and that their deliveries come when promised.

Similarly, startups, dreaming of becoming the next Amazon, rely mostly on shared data about their markets, competitors, and prospective customers to build their empires. They analyze the data for trends, upswings, shortcomings, and deficiencies in a drive to be the "next new thing."

Make no mistake: The sharing of data, when it's properly protected, can lead to gains in retail, finance, healthcare, academia, energy, and other fields. For instance, public data helped deliver COVID-19 vaccines when a laboratory in China sequenced the novel coronavirus and publicly released the data, allowing laboratories around the world to develop vaccines based on the genome sequence.

When properly managed and protected, data transforms organizations from engines that could to engines that can innovate, satisfy customers, lead markets, and command the attention of Wall Street.

But the underlying thread to that success is ***data protection and, by extension, data privacy***.

Data Privacy Breeds Success

Data privacy isn't a software function, a button you can press to make everything alright. No, data privacy comes only with hard work (and the help of technology). It requires the creation of a top-to-bottom culture of data security. Only when data is properly secured and managed can it be kept private, and effectively useless should it be ***accessed in a breach.***

Organizations that have been ahead of the privacy curve can testify to the gains they're making with data because of the confidence they have in data protection. ***Seventy percent of organizations*** surveyed by Cisco said they have seen "significant" business benefits–including operational efficiency, agility, and innovation–from prioritizing data privacy.

Cisco also found that GDPR-ready companies have ***shorter sales delays***–roughly three weeks as opposed to more than five weeks for those that aren't compliant–because they're actively addressing data-privacy concerns. They are also less likely to feel the impact of a data breach because sensitive data is protected and probably encrypted in some way: Compliant organizations had 79,000 records affected in data breaches, as opposed to 212,000 records for those that had a breach and weren't fully compliant.

Despite overwhelming pressure to prioritize data privacy, and despite overwhelming evidence of its advantages, many organizations can't get there because they say they don't have the time, resources, or knowledge to abide by data-privacy regulations. A primary reason for this struggle is they can't make heads or tails of their data, with often overworked administrators and IT personnel unable to determine where it all is and what should be categorized as sensitive. Most would agree data protection and privacy are noble undertakings, but also daunting ones for organizations, regardless of size and scale, to handle on their own.

Nevertheless, organizations really can't afford to wait much longer, for compliance will only get more complicated, amounts of data will only increase, and more customers will expect nothing but the most stringent privacy. Consider: Sixty-one percent of consumers say they're at least somewhat ***willing to share personal information*** with an app in exchange for more transparency and control over their data.

Data Privacy is the New Norm

The days of collecting and using others' data without consequence are over. As just about every function of life for people and businesses is touched by digital applications and tools, there has been a marked shift toward protecting the privacy of individuals. There is now an accepted list of sacred information that must be protected at all costs: Social Security numbers, dates of birth, financial information, addresses, phone numbers, and any other personally identifiable information (PII).

Although regulations that safeguard credit-card data (***PCI DSS***) and healthcare information (***HIPAA***) had been in place for years, the implementation of GDPR (***General Data Protection Regulation***) in 2018 set a worldwide expectation that sensitive data–no matter how it is used and stored–must be preserved to minimize intrusion of privacy and lessen misuse. GDPR codified a set of standards for how organizations, regardless of location, should handle the data of European citizens, including the requirement that personal data should be anonymized. GDPR was so sweeping that companies outside of the EU nonetheless honor it just to avoid unforeseen entanglements.

Since GDPR went into effect, several countries (including Australia and Brazil) and U.S. states (including California with its ***Consumer Privacy Act***, or CCPA, and Virginia with its ***Consumer Data Protection Act***, or CDPA) have enacted data-privacy regulations aimed at safeguarding consumer data and ensuring privacy. They join a long list of other regulations that have enshrined data privacy: the New York SHIELD Act, GLBA, COPPA, and the Fair Credit Reporting Act, along with the well-known HIPAA and PCI-DSS. The list will only get longer; in the wake of Virginia passing CDPA in early 2021, a U.S. House bill was introduced to create a national standard for digital-privacy rights.

Data and Data Breaches Will Only Increase

Just as organizations try to make sense of the long list of privacy laws, they're simultaneously contending with a steady increase of data itself.

IDC predicts that by 2025, ***175 zettabytes (or 175 trillion gigabytes) of new data*** will have been created around the world. IDC also predicts that between 2020 and 2022, enterprise data could annually ***increase 42 percent***. Domo expects that in 2020, for every person on Earth, ***1.7 MB of data will be created*** every second. Since the COVID-19 pandemic began and forced scores of people to work from home, organizations have seen a ***46-percent increase in the number of items*** identified on enterprise endpoints as sensitive data, either PII or PHI.

The costs of not properly safeguarding data, particularly sensitive data that falls under privacy laws, will paralyze any organization that can't make data protection an ingrained, iterative process that runs across all business lines.

For one, regulatory fines can be steep. GDPR can nick anywhere from 10 to 20 million Euros, or from two to four percent of total global turnover. But the potential financial consequences of ineffective data security don't stop there. Organizations incur all sorts of other costs after a data breach, including money spent on a forensics investigation, public relations, and the inadvisable practice of paying ransomware. The average total ***cost of a breach was $3.86 million***, according to IBM.

Inevitably, almost every company suffers a data breach. A Dell survey in 2020 indicated that ***63 percent of businesses*** had suffered a breach within the past year. More than three billion people had their personal data stolen in just two of the top 15 biggest breaches of the 21st century, while the smallest incident since 2000 involved the data of a mere 134 million people, according to CSO.

The list of high-profile hacks runs long. Most recently, the personal information of 533 million Facebook users was stolen from the social media site and leaked on a popular hacker forum. The leak put out in the open users' full names, phone numbers, email addresses, and biographical information, allowing hackers of all abilities to leverage the sensitive data for ill-gotten gain.

How organizations protect their data before a breach determines how much, if any, sensitive data is unprotected and susceptible to misuse. That's why governments are holding organizations accountable for how they protect data and, thus, preserve privacy. By 2023, ***65 percent of the world's population*** could have its personal data covered under modern privacy regulations.

PII and PCI DSS: More Than Similar Acronyms

It's easy to confuse or conflate PII and PCI DSS. While the two acronyms are similar–and both pertain to protecting the privacy of data–they are actually different.

PII stands for person identifiable information. It's a category of information that organizations must, by regulation, keep out of the public domain, not to mention the hands of hackers. The list of PII runs long:

- Name
- Date of birth
- Social Security number
- Email address
- Cellphone number
- IP address
- Log-in account name and password
- Bank account number
- Credit-card information
- Health records
- Driver's license and passport numbers
- Biometric record

While there is overlap, PCI DSS focuses on the credit-card portion of that information. Shorthand for the Payment Card Industry Data Security Standard, it sets standards for the storing, processing, and transmitting of cardholder data. (Protegrity's Chief Security Strategist, Ulf Mattson, was a member of the task forces that helped create PCI DSS and, before that, Visa CISP.)

Aside from protecting PII, banks, credit-card companies, and other organizations that handle financial data must also safeguard:

- Cardholder name
- Permanent account number (PAN)
- Card expiration date
- Service code
- Data in a card's magnetic strip or chip
- Card PIN/Card PIN blocks
- CVC/CVC2

It's Not Easy Safeguarding Data

Responsible businesses believe their customers, clients, and employees have a right to privacy–they value those relationships, after all. Unfortunately, success in safeguarding privacy, now and in the future, won't be guaranteed simply by a desire to do so.

A *TechRepublic survey* showed companies struggling with the complexity of GDPR (18 percent), lacking the proper technology (eight percent), or adhering to a business model that relies on user surveillance but not the protection of data itself (eight percent). What's more, according to TechRepublic, 37 percent of companies do not have a dedicated privacy team, while 44 percent have no more than five employees dedicated to the task. Another survey found organizations with the resources might be spending too much on compliance: a *$3.5 million annual cost* that includes, on average, 22 dedicated employees working on security and privacy audits.

Companies often find their well-intentioned data-privacy practices blocked by "data liabilities." For instance, the requirement to keep a customer's data in his home country, where regulations might differ from another country, prevent a unified approach to privacy. They're also stymied when sharing data across business lines. Also, when they extract data from acquired companies, they find the data can't be unlocked from siloes, preventing them from uniformly protecting it. And troubles arise when data from disparate systems can't be merged because the data protection methods and conflicting policies of different applications and systems limit access.

Access to sensitive data, in a deidentified state, is critical to serving customers, projecting sales and revenue, developing and manufacturing products, monitoring the condition and safety of machinery, managing the productivity of employees and deciding whether to hire more people, and forecasting financial markets and industries. Basically, every business function is tied to the safe access of data.

Because some organizations are uncertain about which data needs to be kept private, it can seem like an impossible feat to ensure all sensitive data elements are encrypted and that protection aligns with compliance regulations. Fortunately, data-protection technology makes it possible.

Beware Those Data Liabilities

Companies often find their well-intentioned data-privacy practices blocked by "data liabilities":

- Keeping data in a person's home country
- Sharing data across business lines
- Data that is locked in siloes
- Disparate systems create disparate data protection polices and methods

It All Starts with Managing Data Protection

When organizations can easily manage and see where sensitive data is–whether in the cloud or on-premises–they are in the best possible position to make sound choices on how to best protect data. With the help of a *comprehensive data-protection platform*, they can see where data resides and what its purpose is. From there, they can choose from a variety of data-protection methods, including the tokenization and encryption processes that hide, or pseudonymize, elements of data; or the privacy models that strip elements of data out of data sets, effectively anonymizing some data elements so data scientists and third parties can never access the sensitive data.

With this detailed level of control, companies can select a type of protection that best suits business objectives. A *retailer*, for example, can pseudonymize aspects of a customer's personal information so that a customer service representative sees a name and address but only meaningless digits and characters in place of a Social Security number–a step that should soothe the customers who are concerned about privacy. Similarly, by choosing to anonymize certain data–whether it's PII, PHI, or PCI–organizations can point to how, even if the larger data set is ever breached, the sensitive data is unusable.

Data Security Begets Data Privacy–and Big Gains

Sound data security-practices create robust data-privacy outcomes. Businesses can extract value from sensitive data while ensuring the privacy of customers and employees is preserved. When organizations rely on a data-protection platform that can cohesively protect data wherever it is and however it is accessed, they are able to safeguard privacy across the enterprise.

Security and privacy allow businesses to use sensitive data to fuel advanced analytics, machine learning, and AI, even as those initiatives migrate to cloud environments. They can innovate responsibly, knowing they have laid the foundation for a mature privacy practice that allows them to be on the side of people and business, simultaneously, without sacrificing one for the other.

For instance, organizations can personalize every customer interaction with secure data. Data privacy optimizes the buyer journey to drive personalized digital experiences, empowers support reps to better engage when customers need help, and enhances every interaction to improve brand affinity–all while ensuring customers' privacy is preserved. By implementing secure AI into customer experience (CX) strategy, customer service, and marketing campaigns, 24 percent of organizations surveyed by the IBM Institute for Business Value said they are able to make quicker, more informed decisions. Fifty-one percent of them said responding to customer demands for more personalized experiences is their number-one reason for adopting AI. But a commitment to protecting customers' sensitive data underpins every CX initiative.

Secure data also accelerates innovation, which, in turn, drives growth. When siloed enterprises acquire businesses–and their data–these walls only exacerbate the challenge of wrangling disjointed data to fuel strategic initiatives. Data-savvy businesses know a unified privacy practice is critical to driving operational efficiencies and unlocking market-expansion opportunities. When privacy prevails, businesses are free to leverage sensitive data, with confidence, to accelerate growth and gain hard-to-win competitive advantage.

Organizations that embed privacy into the design and operation of IT systems, networked infrastructure, and business practices–an approach known as "privacy by design"–are nearly two-and-a-half times more likely to be completely confident in the ability of their privacy teams to ensure data privacy and achieve compliance with new privacy laws and regulations, according to *ISACA*. That confidence pays dividends when data drives business.

Here's what else a focus on data security and privacy–and having a comprehensive, easy-to-manage data-protection platform–does for business:

IT FUTURE-PROOFS AGAINST EVOLVING REGULATIONS

Transparent and effective data security keeps organizations compliant with current regulations–and prepares them to handle future regulations. Organizations already have to make sense of an alphabet soup of privacy laws that cripple progress; but the "soup" will only get thicker. More than 15 state governments–including Alabama, Florida, New Hampshire, Oklahoma, Utah, and Washington–are working on privacy legislation that could add to this complicated mix.

Those distinctions are among the maybe thousands of differences between privacy laws. It's a lot to keep track of. By partnering with a data-protection provider, companies are relieved of the burden of compliance. A comprehensive data-protection platform continuously classifies and discovers data, ensuring that sensitive data within the scope of regulations does not go undetected. Such a platform centralizes the management and enforcement of data-security and privacy policies to ensure sensitive data is consistently protected and aligned with regulations.

IT SIMPLIFIES DATA-SECURITY MANAGEMENT

A data-protection platform advances a cohesive data-privacy strategy across applications, systems, and data siloes, whether on-premises or across hybrid- and multi-cloud environments. This approach reduces the complexity of enforcement and simplifies protection.

IT FACILITATES ACCESS TO SENSITIVE DATA

Again, it's all about having a platform that extends control of data-management to unleash the power of sensitive data, letting it be safely accessed by employees companywide (aka, data democratization). Imagine an ambitious customer service representative who wants to remove a duplicative purchase from a customer's account but can't because restrictive privacy controls won't let him access necessary information. A platform with control allows employees to access elements of data they need to do their jobs, while protecting what has been deemed sensitive. With a platform's fine-grained controls, front-line employees see only the elements of customer information that they should see so they can better serve customers.

IT PROMOTES A MATURE DATA PRIVACY PRACTICE

Enterprises often find their well-intentioned data-privacy practices blocked by the data liabilities that were explained above. A data-protection platform eliminates those many costly blockers by consolidating and standardizing data-protection methods and polices across cloud and on-premises technologies and systems, opening the door to the safe sharing of data across business lines and national borders.

IT PROTECTS COMPANIES FROM COSTLY DATA BREACHES

Breaches are costly–we know that. Beyond that, the reputational damage from a data breach is often incalculable, and it's a risk most companies don't want to take. Trust between businesses and customers creates the underpinnings for high-value relationships that promote brand affinity and deliver value to the bottom line. Privacy, at its core, is fundamental in creating trust, especially when customers are confident that sensitive digital information is safeguarded. Breaches are all but inevitable, unfortunately. A data-protection platform ensures that if data is ever accessed by a hacker or cybercriminal, the sensitive elements will be worthless because they are encrypted, preventing harm to consumers and brand reputation.

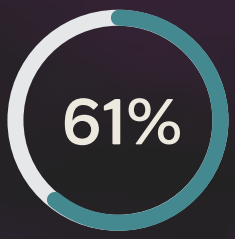
A New Approach to Data-Driven Business Awaits

When data is secure, a world of data-driven rewards is within reach.

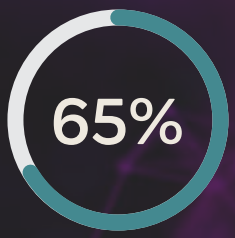
Financial institutions can use, without worry, their customers' data to not only provide traditional banking services but to also try new programs that provide insights meant to help patrons save and make money. They can also use sensitive data to run analytics about new lending programs, insurance offerings, and budget priorities.

Hospitals and healthcare institutions can pursue telemedicine, virtual wellness, medical research, and other initiatives when the patient data

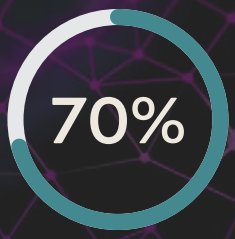
By The Numbers



of consumers are somewhat willing to share personal information with an app in exchange for more transparency and control over their data.



of the world's population will have its data covered under modern privacy regulations by 2023.



of organizations see "significant" business benefits from prioritizing data privacy.

79k

breached data records affected in compliant orgs.

212k

breached data records affected in non-compliant orgs.

Nearly

50%

of organizations point to data privacy and security as their biggest obstacle.

that drives those efforts is completely in sync with HIPAA. As the quick sequencing of the coronavirus demonstrated, the sharing of secure public data can lead to fast advancements that save lives.

Retailers can run personalized marketing and sales campaigns to narrow customer demographics: the latest designer sneakers for young adults in urban and exurban areas, mid-range exercise equipment for middle-class parents, or high-end furniture for owners of secondary homes. Analytics and AI are even making it possible for retailers to incorporate weather data into sales, connecting forecasts to customers' geographic data to send them personalized messages about, say, rock salt availability as a snowstorm barrels down on their neighborhood.

Similarly, HR departments can offer health, wellness, personal improvement, and other employee-focused programs when their workers' personal data stays private. They can also use secure data to analyze employee performance.

Again, people generally don't mind sharing their personal information as long as they can gain from it–and as long as the organization holding their data protects it and respects their privacy. That sentiment was borne out in a *KPMG survey* in which nearly every respondent (91 percent) said corporations should take the lead in establishing corporate data responsibility. Eighty-seven percent of them said data privacy is a human right.

Data security begets data privacy, and data privacy wins the confidence of the data owner. Data-savvy businesses recognize this connection and have created unified data-privacy practices that drive operational efficiencies, optimize customer experiences, and unlock market expansion opportunities. When privacy prevails, businesses are free to leverage, with confidence, sensitive data to grow and beat the competition.

'Alphabet Soup' of Regulations

GDPR: Requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory.

PCI DSS: A data-security standard for organizations that handle debit, credit, and pre-paid cards.

HIPAA: Protects sensitive patient health information from being disclosed without the patient's consent or knowledge.

CCPA: Enhances privacy rights and consumer protection for California residents.

CDPA: A data-protection law that covers privacy rights for Virginia residents.

New York SHIELD Act: Obliges organizations to safeguard the privacy of data of New York residents.

COPPA: Assures children under 13 years of age don't share their personal information on the Internet without the express approval of their parents.

Gramm Leach Bliley Act: Financial institutions must explain their information-sharing practices to customers and safeguard sensitive data.

Fair Credit Reporting Act: Ensures the accuracy, fairness, and privacy of information in consumer credit-bureau files.

Sarbanes-Oxley: Requires the enforcement and communication of formal data-security policies.

Balancing privacy with business ambitions shouldn't be a tightrope act. With a flexible, compliant, and comprehensive data-protection platform–and an all-enterprise focus on data privacy–businesses can walk the walk and prove they can be trusted with data...which, in the end, brings positive business results.