Data Privacy and Protection: What Businesses Should Do

Kiersten E. Todt

Data privacy and protection should be priorities for every business, large or small, regardless of sector or geographic location. Data collection is now a critical component of all business operations, whether it is client data to perform a simple service or enterprise data to ensure operations of critical infrastructure. In today's operating environment and with the continued expansion of the digital economy, data are a critical corporate asset. Despite the functionality and importance of data, it is difficult to encourage businesses to protect data on their own.[2]

But, this data protection challenge does not mean the US should leap to regulation. When I served as the Executive Director of the independent, bipartisan Commission on Enhancing National Cybersecurity in 2016, the Commission examined how to secure the Internet of Things (IoT) devices, recognizing the increasing interdependencies that were growing at that time and which have only been growing exponentially since 2016. The Commission ultimately determined that the best approach was to allow market forces to create incentives for companies to secure IoT devices; companies would define their business case for why "secure to market" should trump "first to market." If those market forces fail and companies do not take appropriate steps to secure IoT devices, then regulation should be introduced.

Businesses find themselves singing this refrain as they struggle to secure today's digital economy. One primary obstacle is that businesses do not know how to evolve their thinking on security to align with trends in technology and innovation. They use traditional, historical models of thinking when it comes to security, models that previously had physical components at their core. This environment no longer exists. Digital infrastructure and digital interdependencies define our economy and our threat environment, creating challenges, like privacy, that require new thinking and new approaches.

Kiersten E. Todt is currently the President and Managing Partner of Liberty Group Ventures, LLC and advises senior executives and Boards on cyber risk management, including the development and execution of tabletop exercises; she also provides strategic advice and counsel to senior leaders in industry and government. She is the Managing Director of the Cyber Readiness Institute, which convenes senior leaders of global companies to help small and medium-sized enterprises improve their cybersecurity. Ms. Todt is the Scholar in Washington, DC of the University of Pittsburgh Institute for Cyber Law, Policy, and Security and most recently served as the Executive Director of the Presidential Commission on Enhancing National Cybersecurity. She has served in senior positions in the White House and in the United States Senate, where she drafted components of the legislation that created the U.S. Department of Homeland Security.

As businesses seek to understand how best to protect and secure data, we need to recognize and understand the influence of technology platforms, like Facebook, Google, Twitter, and YouTube, which are collecting and aggregating data at unprecedented rates and in exponential quantities than we have ever known. The US struggles to address the power of these technology platforms because we are not defining them accurately. These companies are not "just" technology platforms, as their General Counsel's asserted on Capitol Hill in 2017 and their senior executives have done so repeatedly since then. These companies have become a sector critical to the functioning and security of our nation and must act with the responsibility and accountability that we demand of other sectors critical to our nation's well-being.

Before 9/11, the US created categories of critical infrastructure, including telecommunications, finance, and energy, that the government determined were essential to our nation's economic and national security. Even as the digital economy exploded over the past fifteen years, US security policies have continued to focus on these traditional industries. As interdependencies among infrastructure are growing, the lines defining what is and is not critical are blurring. The definition of critical infrastructure must evolve and align with the growth of the digital economy and its potential impact on our national security.

Technology platforms were developed to innovate, make actions easier, faster, more convenient, and to create global connections. But the technologies have grown at a rapid pace and are now much more ubiquitous than what their original business models intended them to be. Companies are beginning to acknowledge that with the power of their technologies comes newfound responsibilities. The cybersecurity failures of the last few years (e.g., Target, Sony, the U.S. Office of Personnel Management, Equifax, Marriott, Facebook) have forced the U.S. Government and businesses

to re-examine and re-define what is critical in today's environment. In the aftermath of these events, the importance of protecting critical information has become more apparent, yet, the nation continues to fail at making protecting critical information a priority.

Securing and optimizing privacy protection protocols around those data should be a critical function of any organization that holds data and, even more so, when a company holds sensitive data, such as personal DNA or personally identifiable information (PII). Traditional approaches to securing data typically have been driven by the mission of the organization and how it relates to protecting critical infrastructure. However, in today's environment, almost all organizations and businesses are part of a value chain connected to critical infrastructure. Therefore, data privacy and protection need to be a priority for all enterprises.

Many organizations are unaware that the data they hold can be access points to critical operations and functions, unrelated to their business. We cannot assume that all businesses that hold enormous amounts of critical data will voluntarily take the disciplined steps necessary to protect those date. The solution is two-pronged:

1) Companies need to be educated that, regardless of the mission of their organization (i.e., pizza parlor or public utility), some or even most of the data they hold are critical and needs to be protected. Companies have to make risk management decisions, based on their corporate mission and functions, regarding how much they invest protecting their data. A public utility, for example, will invest more in the protection and security of its data than a pizza parlor.

2) Companies must know the voluntary steps they can and should take to protect their data. All types of data are not equal. Companies need to understand the data they have and identify what is critical and what should be prioritized to ensure they are appropriately protected.

As large and small businesses worldwide try to understand the impact of the growing and interdependent digital economy, the European Union (EU) has stepped in with a heavy regulatory hammer. The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy that also addresses the export of personal data outside the EU and European Economic Area (EEA). Through this regulation, the EU has asserted that when it comes to security and privacy, organizations need regulation and the threat of stiff financial penalties to do the right thing. GDPR has been in effect for a year, and the world is learning from the European experience and beginning to look at data privacy and protection in the context of GDPR. Some US sectors already are using GDPR as a de facto standard. Additionally, the state of California worked off GDPR to shape the California Consumer Privacy Act, which was signed into law in June 2018 (effective in 2020). Under the GDPR, every business that brushes against the European Union has a privacy agreement.

GDPR forces companies to conduct due diligence on the data they hold and how they are protecting them. But it is not enough in the EU to be GDPR-compliant. As with most original drafts, GDPR needs editing, and it will take a while for the edits to be approved and then enacted. In the meantime, the secondary (negative) impacts of GDPR–on small businesses, on the necessary and vital collection and retention of threat data, to name a few–are growing.

What should companies be doing to protect privacy and data? Let's start with privacy. Privacy is a concept that, in the digital economy, has become jargon, and it is a concept that varies widely depending on the culture. For example, the US approach to privacy, which originated in the Bill of Rights, is much more liberal than that in other countries, such as Germany. The US has a broad range of what it will accept regarding data privacy, based on how that information is used. In the US and certain other western countries, some assert their desire for privacy, but what they are actually asserting is a desire for control over their information. Those who truly care about their privacy would not allow social media tracking applications that let others know where they are at any given moment or feel comfortable posting on the World Wide Web personal photos of and information on children or families in private locations. What many people in these countries care about is control of their data, not necessarily the absolute privacy of their data.

Prudent businesses that are mindful of these widely varying interpretations of privacy are creating a baseline level of privacy that protects the volumes of data they collect and retain. Before presenting approaches for protecting data, it is important to recognize that this aggregation of data at unprecedented rates in our world's history also means that an element of any efficient privacy policy and data protection policy should be the elimination of data that is no longer needed. Our muscle memory on data demands that we focus on data retention and on the concern that we will somehow lose data that we will need in the future. Because data accumulation often is unlimited, a critical component of data privacy and protection policies is the regular review of data that can and should be deleted. In the past, we were forced to shred paper when we no longer needed documents because of the restrictions of physical space. The dawning of digital files makes it too easy to keep everything, which becomes a significant risk to the protection and security of data. Developing a sound and active policy on data deletion is a salient and necessary part of any effective privacy and data protection policy.

The three critical elements of a comprehensive business data protection plan are:

1) data inventory;

2) public projection of data privacy and protection policies; and,

3) incident response.

1. Data Inventory

A key element of protecting data is developing and executing a thorough process for creating a data inventory that prioritizes the business data according to the business mission and sensitivity of data. Critical questions to ask and answer include:

- What data do you hold and where do you keep them (i.e., geographic location and relationships with partners, third-party vendors, and service providers)?
- Who can access your data?
- How are you using your data?
- Do you know where your data is held along your value chain?
- Do you track your data appropriately and effectively?
- What security protocols do your partners, third-party vendors, and product and service providers have in place?
- Can you consolidate where your data are held?
- What data can you delete on a regular basis?
- Do any of your vendors present too much risk?
- Do you have the proper controls in place? Do these controls reflect your data and asset priorities?
- What are your consumers/clients asking/demanding of you regarding data privacy and protection?
- What can (and should) be told to your consumers/clients regarding your data privacy and protection safeguards?

To protect and secure data, businesses must be organized. Businesses need to inventory and prioritize all of their data because it is difficult and costly to protect all data in the same way. Businesses should also pay close attention to administrative privileges and who has access to data, both within the organization and externally (i.e., third-party access). A key component of all human resources functions is a strict policy on the immediate removal of access privileges once an employee is terminated.

There should be certified contractual agreements with all third-party vendors that require a baseline of privacy and protection policies, which align with the business policies. A business needs to map the journey its data takes to understand the vendors it touches and to ensure data protection and privacy are maintained throughout the value chain. A business also needs to know its role in the value chains of other businesses. Additionally, as discussed before, a critical component of data protection is the regular and deliberate deletion of data that is no longer needed. Finally, business data protection policies must align with the demands of the consumer/client, which is why effective and continuous public protection of data privacy and protection is important.

2. Public Projection of Data Privacy and Protection Policies

In crisis communications, how a business communicates its response can be as important as the response itself. If a business inaccurately or ineffectively communicates how it responds, the public reaction can be destructive. Similarly, how a business communicates its prioritization of privacy and data protection policies and how that prioritization aligns with client/customer demands can be almost as important as the policies themselves. These policies cannot exist effectively in a vacuum; their interface with the public is critical to their success and effectiveness. A business needs to think deliberately about how its policies impact and are understood by the public – both in how the enterprise communicates the policies and how it chooses to engage with the public. For example: What privacy options are available on the business website? How much user engagement does a business have? How much attention does the business pay to fulfilling data requests? These factors all play important roles in how effective policies will be. Transparency and ensuring that customers and the public understand how their data are being used and how they are being protected is critical. Greater transparency leads to improved awareness and confidence in customers, which helps businesses serve these customers more effectively.

3. Incident Response

Repeatedly, businesses hear that experiencing a security breach is not a matter of "if" but "when." In the current threat environment, most businesses have experienced some form of security breach. If proper policies are in place and if a resilient strategy for business security is well-executed, then a breach is not a demonstration of failure. In fact, success is more often measured not by what is prevented but by how effectively a business responds to an event. Was it possible to minimize disruption and prevent operations from going offline or, at a minimum, to contain the impact so that other functions were not disrupted? Developing a sound incident response plan is key to the success and effectiveness of privacy and data protection.

A business needs to identify the trigger points for communicating internally, including to its Board of Directors and to its customers and clients. These trigger points should be identified, in advance, to minimize the number of subjective judgment calls during an event. These decisions should be in line with customer expectations. When a crisis or event occurs, especially a significant one, first reports are often wrong. A business needs to have an internal agreement, ahead of time, on the protocols for public statements following an event. An effective template that can be drafted, pre-event, is a statement that outlines the actions the business has taken to be a resilient organization.

CONCLUSION

Data privacy and protection should be priorities for every business, regardless of size, sector, or geographic location. A business needs to know its customers/clients understanding of privacy and what they expect of the business. Regarding data protection, a business should focus on three primary actions: data inventory, public projection of data privacy and protection policies and, incident response. By focusing on these actions, a business will develop a sound, resilient, and robust approach for data privacy and protection. It will also ensure an effective and strategic response when an incident does occur.