Building Consumer Trust in Today's Digital Market
Is Privacy the New Currency in the Digital Economy?

Written By Industry Chief Privacy Officer Dennis Dayman: linkedin.com/in/dennisdayman

Data has powered the growth of the internet for decades by delivering innovative tools and services for consumers and businesses to connect and communicate. Today, the economy is increasingly fueled by the free exchange of data. Global data flows now contribute more to worldwide growth than trade in goods. The U.S. Chamber of Commerce has said that international trade by data flows reached nearly $700 billion in exports from the U.S. and nearly $500 billion in imports.

This continuously growing volume of data presents new challenges—as well as new opportunities—for your organization to build consumer trust. Governments around the world are paying attention to data privacy and responding with new regulations. But relying on regulations alone is simply not enough in an age when data is the currency of our digital economy.

Data flows as the backbone of the economy

Data-driven advertising is one example of how data flow plays an important role in the modern economy by supporting and subsidizing the content and services consumers expect and rely on, including video, news, music, and more. Data-driven advertising also allows consumers to access these resources at little or no cost to them, while enabling small publishers and startup companies to compete in the marketplace against the internet's largest players.

On the global scale, data flow is critical to the trans-Atlantic economic relationship and for all companies large and small across all sectors of the economy. More data travels between the United States and Europe than anywhere else in the world, enabling a $7.1 trillion U.S.-EU economic relationship per the U.S. Chamber of Commerce.

Half of all data flows in both regions are trans-Atlantic transfers. The trans-Atlantic data flows are so critical that to facilitate them, the United States and the European Commission have recently established a Trans-Atlantic Data Privacy Framework. This framework underscores our shared commitment to privacy, data protection, the rule of law, and our collective security, as well as our mutual recognition of the importance of trans-Atlantic data flows to our respective citizens, economies, and societies.

In 2018, Forbes said the amount of data we produce every day is truly mind-boggling. There are 2.5 quintillion bytes of data created each day at our current pace, but that pace is only accelerating with the growth of things like mobile and the Internet of Things (IoT). Over the last two years alone, we have generated 90% of the data in the world and 75% of that data is unstructured. In other words, most of the data is random and difficult to index—and it is presenting new opportunities or problems for marketers, scientists, regulators, and corporate security and operations teams alike.

Building Consumer Trust in Today's Digital Market
Is Privacy the New Currency in the Digital Economy?

Written By Industry Chief Privacy Officer Dennis Dayman: linkedin.com/in/dennisdayman

For security professionals, the increased volumes of data mean you have higher and more profound responsibility to protect your customers' security and privacy, to use the data appropriately, and to ensure that your actions don't inadvertently compromise your customers' wants and needs despite your best intentions. However, if you turn on the TV or open a newspaper (or a tablet) on any given day, the headlines will scream of another company, large or small, that has been targeted or significantly damaged by hackers. How often are you seeing data breach notifications now? They are so commonplace; do you even care anymore?

Regulations matter—but are not enough

Privacy is the currency we pay to engage in our digital ecosystem. We must give up something (personal data) to get something (services) for free. But we also understand that consumers need assurance they can count on the privacy and the safety of their information.

It's clear that governments, attorneys general, federal law enforcement, media, academia, and weary citizens all want answers. Not surprisingly, 2020 became a momentous year for data protection laws around the globe, with new fines levied on companies for security and privacy breaches, as well as new laws created. Some examples of new regulations include:

- Brazil's Lei Geral de Proteção de Dados (LGPD)
- California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)
- Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)
- Thailand's Personal Data Protection Act (PDPA)

All these protections are great, but the regulations have raised concerns that a patchwork of differing frameworks around the world will prove unworkable. Without a consistent global privacy and security standard, the patchwork of laws has resulted in:

- Consumer confusion about what protections they have
- Organizations' failure to meet consumers' expectations about their digital privacy and security choices
- Substantial challenges for businesses trying to comply with these laws

While the law is a powerful element, it cannot alone address the many nuanced scenarios that arise in the digital market. The future technological environment will be made up of an interdependent ecosystem of legislators, corporations, IT developers, and individuals. Each should be equally responsible for shaping this environment, and any imbalance of power risks its sustainability.

Is there an opportunity for businesses?

We need organizations to self-regulate and develop a new ethical approach to handling the personal data they collect. The compliance problem that the disparate laws present for businesses is not likely to disappear anytime soon. And we know that the existing patchwork of privacy laws in the world has not served consumers well and will lead to more unintended consequences and harm.

While these new laws will not be quick in coming—regulations are notoriously slow to adapt to new technological challenges—software companies and their corporate customers shouldn't wait to act. Additionally, taking into consideration the remote workforce now, companies must focus on embedding security processes and technologies into their design and data life cycle as early and as often as possible. They need to connect the resources spent on privacy and security to the volume and complexity of the data they seek to protect.

Many technology designers either put the onus on the users to protect themselves or take the responsibility out of the users' hands in some unexplained way. Users are left with a lack of understanding of what's needed from them, and the result is a dwindling trust in the technology.

But it doesn't have to be like this. Businesses have a big opportunity to build trust in their technology through a people-centric approach to security, and still allow their users to work effectively and securely without limiting the use of data or expecting them to be security or data privacy experts.