Nine Data Privacy Trends to Watch in 2021

Focal Point Insights
December 10, 2020

In a turn of events that no one could have predicted, 2020 has become a year for the history books. Companies began the year rushing to comply with the California Consumer Protection Act (CCPA). In March, they were forced to transition to a fully remote workforce due to the global pandemic and reconfigure how personal data was being access and/or shared in this new normal. Many companies had to strengthen their virtual private networks (VPNs) to better secure this surge of remote workers. Now, many are looking ahead to a year filled with uncertainty, strict regulations, and more change.

Many companies are also still transitioning their workforces and trying to adapt to the new business normal while still complying with regulations and reducing privacy risks. In 2020, data privacy became an even greater concern among consumers as they had to move even more of their professional and personal lives online.

So, what changes can we expect in 2021, and will these become the new normal for privacy? Here are the nine key trends we believe will shape the world of privacy in 2021.

1. Data protection regulations around the world will increase.

Since the introduction of the General Data Protection Regulation (GDPR) in 2018, more than 60 jurisdictions around the world have enacted or proposed a privacy or data protection law, including Brazil, Japan, Thailand, and various states around the U.S. This past year saw a record-breaking cadence in the proposal for and adoption of these modern privacy regulations. So much so, that it is projected that 65% of the world's population will have its personal information covered under a privacy regulation by 2023, up from just 10% today.

While the U.S. lacks a substantial federal privacy law, if proposed state privacy laws pass, 57% of the U.S. could soon be covered. Recently, California approved of

the California Privacy Rights Act (CPRA), which will further increase the data protection regulations of the California Consumer Rights Act (CCPA). As consumers continue to demand the protection of their personal data, and data privacy violations continue to make headlines (like with the video sharing app TikTok), countries around the world will likely either strengthen existing regulations or issue new standards to address these concerns.

In response to the privacy allegations against TikTok, China unveiled a new data security initiative they believe could serve as a global standard for data security. In the initiative, China called on other countries to put an end to activities that jeopardize personal information and to oppose mass surveillance. As privacy violations garner more attention, and consumers become more involved in the protection of their personal data, the number of data privacy regulations around the world will increase and strengthen throughout 2021.

2. Companies will need to focus on third party risk management.

In today's interconnected world, practically all organizations depend on third-party service providers or vendors to operate efficiently. From supply chains and manufacturers to staffing companies and IT support services, organizational reliance on third parties continues to increase. Despite this dependency, only 35% of organizations consider their third-party risk management to be effective.

With data breaches being an average of $700,000 more expensive when a third party is involved and over 63% of breaches attributed to third party vendors, this type of an attack can be devastating to an organization. Even well-known companies like General Electric, Instagram, and T-Mobile have suffered from a third-party data breach in the past year, exposing thousands of records.

Consumers expect companies to hold their third-party vendors to a higher standard to keep their personal data from being exposed. In July 2020, the Court of Justice of the European Union (CJEU) invalidated the Privacy Shield agreement – a cross-border data transfer mechanism 60% of companies relied on – for failing to protect the privacy of its citizens' data. More and more privacy frameworks are also creating requirements companies must follow when sharing consumers' personal information with third parties. Even the recently approved California Privacy Rights Act (CPRA) looks to further increase an organization's responsibility for how third parties use, share, or sell personal information.

For these reasons, we'll likely see a heavy focus on third party risk management in 2021 as businesses become more critical of their third-party relationships to prevent any potential risk to their organization.

3. Data privacy transparency will be a top priority for consumers.

With large scale data breaches like the one at Equifax and ClixSense exposing the personal information of millions of people, consumers are growing more concerned about their privacy and are willing to act to protect it. A study by Cisco found that over 50% of consumers would switch companies simply because of their data policies or data sharing practices. Companies that fail to protect consumer data will lose the trust of their customers and drive them to seek another company where they feel more comfortable sharing their personal information.

Building trust through transparency is not a quick process, but doing so can be a key differentiator, especially since the global pandemic has disrupted consumer buying habits. However, by 2023, those companies that do earn and maintain digital trust with their consumers will see a 30% increase in their digital commerce profits compared to their competitors.

4. More companies will invest in privacy technology.

From the CCPA to the GDPR, keeping up with new and existing global data privacy regulations can be a challenge. As each new regulation is passed, it is easy for companies to feel overwhelmed with compliance efforts and consumer requests for personal information. To keep pace with the ever-changing regulatory landscape in 2021, more companies will start to invest and integrate privacy-enhancing technologies into their compliance programs.

These privacy-based technologies and tools (e.g., homomorphic encryption, obfuscation, de-identification, etc.) can fill various data governance needs, including automating compliance processes, creating advanced data mapping services, and even reviewing and fulfilling consumer requests. In addition, by utilizing these privacy-based technologies, organizations can set up workflows that combine project management with compliance, increasing team collaboration and communication and centralizing privacy and risk management functions.

By 2021, Gartner estimates that roughly 70% of organizations will integrate automation technologies to increase employee productivity, and that by 2022, privacy-driven spending on compliance tooling will increase to more than $8 billion worldwide. As the privacy landscape grows more challenging, innovative technology will be part of the solution in 2021.

5. Privacy teams may be required to do more with less.

The Covid-19 pandemic forced many organizations to quickly scale their operations, transition employees to a work-from-home environment, and respond to the sudden economic downturn. At first, 65% of business leaders reported an increase in compliance budget costs to cope with the immediate changes brought on by the pandemic. But now, over 81% of business leaders are feeling pressured to lower overall costs.

With the focus now on cost optimization, many organizations are looking for ways to consolidate and reduce compliance efforts for all non-revenue programs like privacy. Privacy teams will now be required to navigate the regulatory landscape and defend against privacy risks with fewer resources than ever. Fortunately, taking advantage of innovative automation technologies and leveraging industry-recognized frameworks like the NIST Privacy Framework can help. In addition, engaging other business functions like Audit and Security can help privacy teams evolve and adapt

6. More organizations will incorporate privacy frameworks.

As seen above, data privacy regulations are spreading both nationally and internationally. With the growing momentum towards regulations and harsher penalties for noncompliance, we'll see more organizations start to incorporate privacy frameworks to help them manage compliance in 2021 and beyond.

Leveraging a privacy framework like the NIST Privacy Framework or ISO/IEC 27701:2019 can help organizations create a foundation for building a strong privacy program, offering structure and guidance for managing privacy risk. According to the IAPP, roughly 56% of organizations are moving towards a single privacy strategy, and respected well-known frameworks like the NIST Privacy framework can help.

A privacy framework can also help:

- Meet evolving data privacy regulations and laws
- Achieve compliance while adjusting to changing requirements
- Support compliance initiatives without duplicating efforts
- Reduce costs and increase efficiency of the privacy program

7. There will be a significant increase in data subject requests and complaints.

The introduction of various data privacy regulations around the globe gave consumers more control over their data. With the number of data breaches growing exponentially each year, consumers are starting to become more data aware and want to know exactly who has access to their personal information. As consumers continue to exercise their right to know, update, delete, and even restrict the processing of the personal information businesses have stored about them, we will see a significant increase in data subject requests and complaints in the coming year.

The Information Commissioner's Office (ICO) has already seen a 50% increase of data protection complaints since the introduction of the GDPR with over a third related to Data Subject Access Requests (DSARs). Yet, even though the ICO has provided some leeway for responses to DSARs (normally 30 days) due to the Covid-19 pandemic, organizations are still expected to provide the same privacy and security measures as in normal circumstances. In the U.S., enforcement will soon become a bigger topic of conversation as the CPRA will form an enforcement body where consumer requests will be investigated, a model other states may follow in the near future.

8. Navigating the Privacy Shield invalidation will continue to be a challenge.

In a highly disruptive ruling, the Court of the European Union (CJEU) dismantled the Privacy Shield agreement between the European Union (EU) and the United States in July 2020. The CJEU determined that the adequacy agreement failed to protect the privacy of its citizens' data. Thousands of companies then had to quickly find an alternative data transfer method that adequately protects personal data across borders.

Companies can take advantage of standard contractual clauses (SCCs), binding corporate rules (BCRs), and derogations, but currently these are not long-term solutions. While the European Commission has confirmed it is working on updating SCCs and bringing them in alignment with the GDPR, a timeline has not been announced. Facebook has already been ordered by the Irish Data Protection Commission (IDPC) to stop data transfers between the US and the European Union.

With the future unknown on a legislation that covers these data transfers, companies will continue to face data transfer challenges in 2021.

9. The adoption of long-term remote workforce plans.

At the start of the Covid-19 pandemic, organizations around the world were forced to abruptly change the way their businesses operate. Suddenly in an economic crisis and employees working from home, companies were tasked with modernizing their infrastructure and protecting against privacy threats, while adapting their compliance efforts to keep up with regulatory requirements.

Although businesses began to reopen and employees started returning to work, there has been an overall shift towards keeping a more permanent remote work solution. Many big firms like Facebook and Google have already extended their work from home policies until at least Summer 2021.

If companies are to fully transition to a more long-term remote workforce, compliance programs will need to be updated to protect against data storage issues, the increase in transfers of personal data, and the higher likelihood of a data breach due to phishing attacks. But, with employees scattered across states, time zones, and offices, organizations will start to utilize the benefits of a fully (or even partially) remote workforce and start adopting long-term plans in 2021.

Looking Ahead

The only constant in life is change, and 2020 was a year filled with it. While businesses were forced embrace a new normal this past year, 2021 will continue to be a year of transition. Not only will data privacy regulations continue to evolve, but so will privacy risks, complications, and technologies. Companies that fully embrace these changes will be better prepared going into 2021 and create a more secure and safe data privacy landscape.