Published on *The National Law Review* https://natlawreview.com

Managing Data Privacy in the COVID-19 Environment – Navigating the Challenges of a Pandemic in 2021

Article By:

Chanley T. Howell

Last year, the COVID-19 pandemic brought about a global market disruption across multiple industries, and manufacturers expect the pandemic to continue to affect the automotive industry through 2021. The pandemic has not slowed the technological innovations in the industry or the pace of increasing regulation affecting data privacy and security. In the midst of the pandemic, we saw significant changes to the privacy landscape, including a steady rise in California Consumer Privacy Act (the CCPA) litigation by private citizens, a successful ballot measure amending the CCPA to include significant new obligations for companies that often mirror those of the European General Data Protection Act (GDPR), and a major decision from the Court of Justice of the European Union in the so-called “Schrems II” impacting personal data transfers between the EU and the U.S., all of which impacts the automotive industry. As we have seen in recent years, consumer demand is driving the industry towards greater privacy protections and it is not likely to slow down.

2020 and the pandemic brought about changes not only to the regulatory environment, but also to business operations, with substantial periods of remote operations, implementation of tracking tools collecting sensitive health information from workforce employees, and fully remote automotive purchases changing the landscape of consumer interaction. Without notice or sufficient time to plan, companies were forced to shift abruptly to a remote work environment, exposing new vulnerabilities and creating new security risks with the increased usage of personal devices and insecure networks, increased phishing attacks, strained virtual private network resources, and economic impacts across industries limiting resources.

Accordingly, we expect to see in 2021 that a company’s prioritization of budgets will be split between information technology and compliance departments and for any increased spending in resources necessary to address regulatory requirements or risks affecting consumer trust. As industry executives grapple with prioritizing budget constraints while responding to the new business and operational challenges under the pandemic, it is important for executives to keep in mind that noncompliance with privacy and security requirements can result in harsh monetary and legal penalties, including steep fines and potential civil liability, and can result in a loss of consumer trust potentially impacting a brand into the post-pandemic landscape.

As automotive companies tackle budget constraints and a changing regulatory environment with new compliance requirements, executives may find navigating data privacy compliance and security practices difficult. However, we outline below six critical focus areas to ensure the resiliency and security of your organization, to best comply with regulatory requirements, and to maintain consumer trust in the face of ever-changing data privacy laws.

1. Incident Response and Business Continuity Protocols

The pandemic created a colossal challenge globally for companies, which were unprepared for the first lockdown and had to quickly shift resources to ensure business continuity for their workforces in a remote environment. Few, if any, organizations included a global pandemic in their business continuity plans, leaving many companies staggering to respond to the increased demand on infrastructure resources posed by a remote workforce. This impacted the ability of companies at all tiers and in all areas of the automotive ecosystem to continue to effectively and consistently respond to security incidents, and to maintain and manage their cybersecurity practices and procedures. Looking forward, as more local, regional, or national disruptions and lockdowns are expected, automotive companies should ensure their incident response plans and protocols are updated for a remote workforce environment.

2. System Security and Access Controls

As companies shifted entire workforces to a remote environment en masse, companies often realized that the major constraints for organizations were remote-access capacity and access controls to enterprise systems. Many companies found that legacy systems were especially prone to problems with availability, scalability, and performance – all of which are required to run smoothly for effective cybersecurity for the workforce, as well as security for vehicles, connected hardware and components. Looking ahead, we expect companies to continue to prioritize short-term spending on security for remote workers. In addition, companies may consider deploying technologies and solutions that can be quickly adopted, such as cloud solutions and security services vendors; however, we suggest including relevant stakeholders, such as the security team, early in the process to ensure that all security benefits and risks are being considered in any such transition. Remote connectivity should further facilitate security practices, including over-the-air (OTA) updates and patches for vehicle software and electronic components. Companies should also consider enabling multifactor authentication, and updating security monitoring capabilities and log management rules to ensure full visibility despite remote work conditions. The above considerations should be in addition to the core internal and external (product-based) security functions, such as patching, vulnerability management and cyber awareness programs.

3. Assess Security Hygiene of the Remote Workforce

The rapid shutdown early in the pandemic meant that not all departments in an organization were set up for a remote work environment. As additional local, regional, or national disruptions and lockdowns are expected, companies should look to addressing unsecure networks and personal device usage by employees. Looking forward, companies should require that employees install corporate security software onto any personal device prior to connecting to the corporate network and should establish or review remote access firewall rules, including file integrity monitoring and user and entity behavior analytics.

4. Third-Party Risk Management

As we have seen in the fallout from the SolarWinds breach, third parties can be a source of vulnerability for companies. This is a pattern that continues to repeat itself (remember the Target breach back in 2013?). In the SolarWinds breach, hackers were able to infiltrate the systems of SolarWinds' customers through a compromised update of the SolarWinds software. Most companies are not prepared for this type of vendor compromise as software that is digitally signed by the manufacturer (as here, SolarWinds) is inherently trusted by users. This type of risk can be particularly prevalent in the automotive industry due to the large amount of connectivity between organizations in the automotive ecosystem. Looking forward, companies can consider implementing zero-trust networking principles and expanding role-based access controls from users to include applications and servers, and limiting access to applications and servers that are necessary to minimize any potential impact to the corporate system. Companies should continue to implement security measures and practices that work to provide the best cybersecurity, including eliminating vulnerability early at the design stage and continuously monitoring and preparing for new or inevitable security threats.

5. Data Privacy and Compliance Best Practices

As the privacy landscape continues to evolve and become ever-more complex, companies continue to find compliance particularly challenging. For example, as companies have expended significant efforts towards California's CCPA compliance, the new amendment to the CCPA brings with it new obligations on companies operating within and outside of California, including new consumer rights, such as a limited opt-out on the use or disclosure of sensitive personal information except for what is necessary for the company to provide its goods and services, a category that includes geolocation information that may be collected by a vehicle. Cars today are, in essence, computers on wheels – very complex computers, smartphones, tablets and networks rolled into one. Under Schrems II, companies are required to assess on a case-by-case basis whether a data transfer using standard contractual clauses will meet the EU standards. Because privacy and security requirements in developed countries are converging, what happens in the EU can impact (and has impacted) what happens in the U.S. on the automotive regulatory and compliance front. For companies with diverse or widespread operations, understanding how their operations fit into these privacy schemes are crucial for regulatory compliance. Additionally, implementing and maintaining a robust privacy program that is adaptable to specific requirements in different jurisdictions will foster consumer trust and loyalty in a company's brand. That being said, while a robust privacy program may comply with certain notice requirements and consumer rights implemented by privacy laws, it does not protect a company from unauthorized uses or disclosures, and companies should continue to implement security practices that provide the best cybersecurity protection.

6. Customer Expectations

Consumers are becoming more aware of the risks of certain technologies in their automotive products, as shown by the niche industries popping up on Amazon offering faraday cages for key fobs. Companies should begin to distinguish themselves by making privacy and security a priority in their products and making that priority obvious to their consuming market. This will allow those companies to leverage that reputation as product offerings continue to trend towards fully autonomous features. For example, we expect to see this marketing technique utilized by the newest entrant to the automotive industry, Apple, Inc., which is widely known as a design-focused consumer products company. Apple customers are used to a seamless experience across devices with privacy and security by design built into the product, and we expect Apple to leverage its privacy- and security-focused reputation and seamless customer experience to market its automotive offering to

consumers. As the industry moves towards an autonomous vehicle market, a company's privacy and security reputation will be key to adoption of these products by consumers, and the continued brand loyalty of those consumers.

Conclusion

2020 was a year of market disruption and significant challenge to the industry, and 2021 appears to be primed for continuing market conditions leading to a new normal. Budgetary constraints will continue to be a significant factor for companies going into 2021. Companies will need to adjust tactics to do more with smaller budgets while remaining compliant with regulatory requirements. Virtually all facets of an organization, and third parties as well, will need to be involved to properly plan and implement protections, and to prepare for compliance with new and expanding regulations and consumer demands. As consumer expectations continue to drive privacy scrutiny, there is an opportunity to lead the pack in this evolving area, but with new entrants primed to enter the market, that opportunity will not last very long.

National Law Review, Volume XI, Number 91