Staying Compliant with Global Tech Regulations

In July 2020, the Court of Justice of the European Union (EU) invalidated the EU-U.S. Data Protection Shield under the verdict "Schrems II," due to concerns over the potential for surveillance by U.S. government agencies. Prior to Schrems II, U.S. companies relied on this Privacy Shield to conduct trans-Atlantic data transfers in compliance with the EU's General Data Protection Regulation (GDPR). On March 25, 2022, the EU Commission and the U.S. government proposed the new "Trans-Atlantic Data Privacy Framework" (TADPF) to address concerns raised by the Schrems II decision. Separately, in December 2020 the European Parliament and Commission also proposed the Digital Services Act (DSA) and the Digital Markets Act (DMA), which, respectively, seek greater accountability for online platforms, including regarding illegal and harmful content, and implement new standards that regulate business practices to create greater market competition. **RANE** spoke with **Constantine Karbaliotis, Counsel at nNovation LLP.,** and **Matthew Bernstein, Founder and Information Governance Strategist at MC Bernstein Data,** to better understand how businesses can navigate increasing regulations on the transfer and processing of consumer personal data. Additionally, the experts will provide an introductory review of two critical new EU regulations on 'Big Tech'.

WHAT TO KNOW

The above legislation highlights two main tracks of EU regulation. In the first, an evolving trans-Atlantic framework regulates the management and transfer of customer data between the United States and Europe. The main EU concern is that U.S. intelligence agencies have too much access to personal data. The second is about protecting EU consumers from harmful content and seeks to bring more competition to a market that has been traditionally dominated by a few large, U.S-based companies. Although related in some ways, they have different objectives. While data privacy has historically been more regulated in Europe than in the United States, more recently, the U.S. federal and state governments have been developing more legislation to improve consumer data protection and increase digital market competition. Armed with greater resources, regulators have begun to look at areas where personal data plays a role in commerce, as seen with the following regulation.

EUROPEAN UNION REGULATION

Europe has been at the forefront of privacy and tech regulation, having enacted the data privacy and protection regulation known as the General Data Protection Regulation (GDPR) in 2016 which came into force in 2018, which governs the way in which personal data is used, processed, and stored. In December 2020, the European Commission proposed the Digital Services Act (DSA) to implement new EU-wide standards that ensure accountability for online platforms regarding illegal and harmful content. These standards were agreed to on April 23, 2022, and will apply to all online services within the EU. The law will also be complemented by the Digital Markets Act (DMA), which takes effect on January 1, 2024, and seeks to reign in anti-competitive

business practices.

- The DSA places obligations on large platforms and search engines to prevent the misuse of their systems by employing independent audits of risk management systems, creating safeguards for minors, and adapting to public health and security crises. The DSA framework includes "EU-wide due diligence obligations that will apply to all digital services that connect consumers to goods, services, or content, including new procedures for faster removal of illegal content and goods," as well as protections for users' fundamental rights online. For online intermediary services, such as internet access providers, domain name registrars, online marketplaces, social media platforms, large online search engines, cloud computing, and web-hosting services, the DSA stipulates those obligations will depend on their role, size, and impact within the online ecosystem.
- The EU also agreed to the "Digital Markets Act" (DMA) in April 2022. While the DSA is aimed at policing online content, the DMA is intended to create greater competition in the tech marketplace and curb the market dominance of large tech platforms. The DMA applies to large companies that provide "core platform services," such as social media networks and large search engines, and have a market capitalization or annual turnover (revenue) of at least €75 billion. Companies that have at least 45 million monthly end-users in the EU and more than 10,000 annual business users will fall within the scope, including tech giants such as Google and Apple.
- Within the DMA, large online platforms are defined as "gatekeepers" for having durable and strong economic and intermediation positions with businesses. According to the DMA, gatekeepers must allow business users to access the data that is generated through their usage of the platform, promote the users' products and services (even if they compete with those of the gatekeepers), and conclude contracts with customers outside the gatekeeper's platform, and must allow third parties to inter-operate with the gatekeeper's services. Gatekeepers are also obligated to "provide companies advertising on their platform with the tools and information necessary for advertisers and publishers to carry out their own independent verification of their advertisements."

UNITED STATES REGULATION

'Big Tech' is also starting to face greater scrutiny in the United States - both at the federal and state level. This year, the U.S. Senate will likely vote on "The American Innovation and Choice Online Act," which, if passed in its current form, would forbid tech platforms from favoring their own products and services over those of their competitors. In addition to prohibiting companies' misuse of data, this proposed legislation constitutes a move in using historic antitrust laws against what some see as more modern threats to competition embodied in 'Big Tech.' Various states have also tackled the issue of consumer data privacy.

- On June 3, 2022, bipartisan U.S. federal lawmakers introduced a new data privacy bill, "The American Data Privacy and Protection Act," which would be the first data privacy proposal to receive bicameral support, establish a strong national framework to protect consumer data privacy and security, and grants

Americans broad protections against the discriminatory use of personal data. The framework, which has been in discussion for 20 years, aims to "[strike] a meaningful balance on issues that are critical to moving comprehensive data privacy legislation through Congress." The House Energy & Commerce Committee is scheduled to hold a legislative hearing on June 14.

- The American Innovation and Choice Online Act would prohibit big firms like Amazon, Apple, Facebook, and Google from "self-preferencing" their products and services over those of their rivals on their platforms, which the bill's sponsors see as anti-competitive. Recent cases targeting tech giants have tested existing antitrust laws, and tech-regulation advocates say new laws are needed to protect competition and consumers. Sen. Amy Klobuchar (D-MN), the legislation's sponsor, said that the American Innovation and Choice Online Act reflects a growing awareness that existing competition laws need to be updated for the digital era.
- The states of California, Colorado, Utah, Virginia, and now Connecticut, have individually enacted their own consumer data privacy laws. While the "California Consumer Privacy Act of 2018" (CCPA) is already in effect, the "California Consumer Privacy Rights Act" (CPRA), the "Colorado Privacy Act," Utah's "Consumer Privacy Act," Virginia's "Consumer Data Protection Act," and Connecticut's "Data Privacy Act," are all set to take effect in 2023. Most of these laws overlap when addressing a consumer's right to access, correct, and delete personal information as well as opt-out from the collection and sale of personal data. Other common provisions require online platforms to provide a privacy policy that describes the types of personal information being collected, what information is being shared with third parties, and how consumers can request changes to their information.

WHAT TO THINK ABOUT

While some of this legislation will have varying business consequences depending on location and industry, the recently negotiated "Trans-Atlantic Data Privacy Framework" (TADPF) will have widespread implications for business between the United States and Europe. In particular, companies will be able to undergo a self-certification process, as established by the U.S. Department of Commerce, that will enable them to safely transfer EU citizens' personal data to the US. It is expected that the TADPF will contain similar language to its predecessors regarding the handling and transfer of personal data. While **Bernstein** points out that the self-certification process is not a new concept, **Karbaliotis** advises that businesses conduct transfer impact assessments as enforcement will continue while the TADPF is under consideration.

- **Karbaliotis** points out that the upcoming TADPF will supersede the "Privacy Shield" and "Safe Harbor," the two previous frameworks that regulate trans-Atlantic data transfers. He says the TADPF has been viewed with skepticism by commentators who believe the framework does not sufficiently address the question of U.S. national surveillance laws and he believes that "without resolving the issue of what is acceptable in terms of spying on friends, we're never going to see a resolution." There are also challenging issues with the application of privacy rights under the U.S. constitution

solely to residents of the United States, which is viewed by EU commentators as ultimately dooming any trans-Atlantic arrangements.

- **Karbaliotis** believes the framework should be viewed as moving towards a broader common understanding of how personal information should be handled and protected, not just between the EU and the U.S., but among all countries that want to engage in the free flow of data. He notes that national surveillance authorities will need to abide by the accepted framework that enables the free flow of data and ensure confidence that the rules under which they have collected the data will apply regardless of where the data goes.
- **Karbaliotis** points out that while the TADPF is under deliberation, enforcement will continue for organizations that are already under the Privacy Shield as indicated by their transfer impact assessments. As organizations are currently conducting transfer impact assessments to reassure their European customers, **Karbaliotis** says he doesn't think there will be any pause in enforcement.
- **Bernstein** notes that a self-certification process had already existed under the Privacy Shield. He explains that the suspension of the Privacy Shield was not based on shortcomings with companies' self-certification or actions but rather due to EU concerns over the U.S government's ability to access sensitive information. He explains that between the advent of the Privacy Shield and the introduction of the TADPF, the EU introduced its GDPR. While the TADPF's self-certification requirements may replicate most of the language from its predecessors, **Bernstein** says he's tracking whether new aspects related to the GDPR will be added.

While compliance with the TADPF may threaten business models that rely on the sale and usage of personal data, **Karbaliotis** says businesses can be transparent and establish trust with their consumers by providing preference and consent management. **Bernstein** advises that businesses focus on working with their consumer base as a whole, avoiding the collection of unneeded personal data and targeting individuals, while implementing good privacy practices.

- For companies concerned about potentially losing access to valuable data on their customers, **Karbaliotis** says that organizations can create preference and consent management tools and processes to empower consumers and ensure they are in control when more stringent rules are developed. Providing consumers with the choice to update their preferences prevents the option from being a binary 'yes' or 'no,' but instead is a more nuanced and transparent approach. "The goal here is to be transparent, provide options, and establish trust, so that the consumer will still leave their data with you and that way, the information is retained," he says.
- **Karbaliotis** advises companies to take a different approach in engaging with stakeholders and consumers by providing this transparency and granularity, and "this is perhaps the strongest way in which organizations can be ready for whatever comes."
- **Bernstein** says online advertising is one business sector that will struggle with these new obligations. Social media platforms that are built around a revenue

model that uses and sells personal data will find that "noncompliance could threaten that business model." **Bernstein** points out that, for any business using consumers' personal data, compliance with the new obligations will also create awareness and implementation costs. "The first is an awareness cost for your company to understand data privacy implications, and the second is an implementation cost to change data controlling and processing to comply with regulation."

- **Bernstein** says that targeting specific individuals with tailored advertising is a real issue for some companies and this will continue to be a problem for their compliance with data privacy laws. Some companies are interested in what their customers individually want, "which is exactly the problem as it's personally identifiable information." However, most companies are interested in what their customers, collectively, want – in order to improve products and marketing – and that can be compatible with good data privacy practices.

WHAT TO CONSIDER

Businesses can navigate increasing regulations on 'Big Tech' as well as the transfer and processing of consumer personal information by taking stock of their data and mapping it out from a compliance perspective. While **Karbaliotis** recommends selecting a good existing framework as a starting point to implement a data privacy program, **Bernstein** suggests that businesses examine their obligations (not just consumer data subjects' rights) and focus on what compliance might mean from an operational standpoint.

- **Karbaliotis** points out that the new framework addresses the larger issue, which is fundamental information management and good data governance. He says that most organizations do not know where their consumer data is flowing after its collection, nor do they have the appropriate technological capacity in place to govern this information. As organizations have neither updated nor properly documented the development of their systems, **Karbaliotis** says, "data inventory and mapping will be fundamental for compliance with these upcoming obligations."
- **Karbaliotis** explains that poor information and data governance leads to poor privacy. He explains that many organizations will need to get a handle on their own information governance to understand what is being done with the data before they are able to support these obligations, which are still subject to change over time. Moreover, he says another issue is data retention; most organizations increase their data storage capacity rather than remove irrelevant information, which increases the likelihood that a potential breach will cause blowback because more data can potentially be compromised.
- **Karbaliotis** recommends that "companies select a good framework and start moving towards it." He explains that the fundamentals of good privacy are generally the same, though there may be different requirements, for example, as to how much notice must be given in the event of a breach. He says, "it's important to build off of the foundational elements of knowing where your data is, how it's moving, who has access to it, and how to propagate corrections or deletions,

which are fundamentals regardless of the nuances of any particular privacy law."

- **Bernstein** suggests that businesses establish a data privacy program and plan as a key step to mitigate the risks of regulatory enforcement and reputational damage. He points out that the GDPR explicitly calls for giving credit to companies that show good faith and a reasonable attempt at addressing compliance measures.
- **Bernstein** recommends that businesses examine the obligations and focus on what compliance might mean from an operational standpoint. He says companies should conduct a 'walk-across' to analyze the operational commonalities of the various global data privacy laws. He says most data privacy laws are focused on similar concerns (notice, consent, and how the data is processed and shared), "so companies need to select a framework that can respond to all these different laws." Therefore, companies should introduce a framework that will allow for easier review of different laws that may come in the future, depending on geography and sector. Going forward, this framework will ensure that the business will be able to assess and adapt to the complex and changing regulatory environment, he says.

Karbaliotis points out that in some jurisdictions, like the EU, governments' views on the collection, storage, and sale of personal data have shifted to become a fundamental human right, which is creating new compliance considerations for companies. **Bernstein** says that proactively taking responsibility and not misusing consumer data encourages consumer trust and regulator confidence. **Karbaliotis** explains that going forward, self-service of preference and consent management will be more organizationally efficient and will ensure consumer trust.

- **Karbaliotis** advises that organizations be accountable stewards of information and avoid waiting on the law. He explains the EU GDPR is responsible for raising consumer expectations globally and organizations that aim to simply comply with the letter of the law without taking more fundamental steps will ultimately fall short. "Being an accountable steward of information means you have to view this from an ethical standpoint and consider doing more than the minimum, you have to take accountability through the whole of your organization for how the data is used and how it's shared," he says.
- **Karbaliotis** explains that in some jurisdictions, personal data is not seen solely as a corporate, but rather a fundamental human right. For example, in the EU, data protection is also protected by Convention 108 of the Council of Europe. Going forward, should similar ideas further spread, self-service of consent and preference management will be more organizationally efficient, create consumer trust, and will allow people to be in control of how their information is used.

Experts expect that the TADPF framework, despite being implemented in the United States through an Executive Order, will likely have staying power beyond the current administration due to bipartisan support in Congress.

- **Karbaliotis** says that previously there has been support from both Democrats and Republicans regarding the need for a federal privacy law. He says, "this will help to solidify the groundings of privacy at the federal level because all the action right now is happening at the state level." While it's hard to know what to expect, **Karbaliotis** notes going forward, "any administration is going to still have to deal with the fact that the U.S. government still needs to support trans-Atlantic data flows."
- **Bernstein** expects companies will see the framework as beneficial, as the Commerce Department and the ministers of trade in the EU hope they will. He sees the risk to its longevity perhaps coming from U.S. officials who may see the TADPF as hamstringing national security and therefore try to delay or revise the framework.
- **Bernstein** says the TADPF has received strong support both politically and commercially and says he believes it will be implemented. He notes that the concerns that prompted Schrems II "were less about how companies were using the data and more about European concerns with U.S. governmental apparatuses having too much access to the personal data."

ABOUT THE EXPERTS

Matthew Bernstein, Founder and Information Governance Strategist at MC Bernstein Data

Matthew Bernstein is the Founder and an Information Management Strategist at MC Bernstein Data, where he leverages his more than 20 years of information management experience to help companies assure compliance with data privacy, regulatory retention, and other information governance requirements. Bernstein specializes in asset management, due diligence, investments, capital markets, and financial modeling.

Prior to his current role, Bernstein held multiple positions – including as a Managing Director and Global Head of Group Information and Records Management - at Deutsche Bank from 2011 to 2018, worked as a Chief Financial Officer at Mortgage Renaissance Investment Trust from 2009 to 2010, a Chief Financial Officer at Mount Kellett Capital Management LP from 2008 to 2009, and as a CFO at RREEF Funds, which was acquired by Deutsche Bank in 2002, from 1986 to 2008.

RANE
Risk Assistance Network + Exchange

Constantine Karbaliotis, Counsel at nNovation LLP

Constantine Karbaliotis is an expert in global privacy compliance and privacy management, with seventeen years' experience in privacy, on both domestic and international levels, combining his legal acumen with understanding of technology and operational challenges. Constantine has fulfilled numerous roles in privacy, first and most recently as a consultant.

Constantine has also acted as privacy officer and leader for two multinational organizations, where he managed the company's internal compliance and the development and implementation of privacy programs, dealing with diverse areas of international privacy and data protection.

During his career, he has also led a team of privacy advisors at a prominent software company serving privacy offices, developing expertise in solutions that support privacy compliance and automation including implementing technologies and processes for major multinationals. Constantine's experience has helped clients build effective privacy programs to comply with Canadian, US and EU legislation (including GDPR), to remain compliant with ever-increasing regulation and expectations.