Developments We're Watching For in 2019

Dechert's Data Privacy and Cybersecurity Group

Dechert LLP

The year 2018 was significant for developments related to privacy and cybersecurity law and policy. Many of these developments — concerns about facial recognition technology, massive data breaches, increased cybersecurity threats, biometric data captured by wearable devices and, of course, the Internet of Things — pose real legal challenges to government regulators and courts.

In this summary, Dechert's Data Privacy and Cybersecurity group highlights the data privacy, cybersecurity and competition issues of interest to our clients that we have been following and will continue to watch as 2019 unfolds.

Fundamental Shifts in the Regulatory Landscape

Three overarching regulatory trends related to data usage and management made themselves heard in 2018 and will continue to play out in 2019.

The first of these trends is the move towards a more regulated online world in the United States. The second of these trends is concerned with how political and philosophical differences among nation-states — some of these among trading partners and political allies with similar values underlying their systems, others between and among states whose differences are more fundamental in nature — will impact the Internet and Internet governance. The third — which some observers might argue is a subset or even a byproduct of the second — is increased antitrust scrutiny of the "tech economy" and the collection of "Big Data," especially in the EU.

The move towards a more regulated online world in the United States

When the online revolution began, government and industry in the U.S. jointly focused on preventing regulations that could impede the Internet's growth as an engine of commerce and communication. Now that the Internet is ubiquitous and our understanding of its capabilities — and of the challenges our increasing reliance on the network poses to society and security — have matured, public perceptions and attitudes have markedly changed. The question in 2019 and the next few years will no longer be "should" our use of the network be regulated, but "how" should it be regulated, for what purposes, and how to balance regulatory efficacy against the economic value our online infrastructure creates for the economy worldwide. Cybersecurity and privacy concerns are at the center of this conversation, along with concerns about the trustworthiness of Internet content, freedom of speech and whether the medium can be made safer for users in general, particularly for more vulnerable populations like children.

How political and philosophical differences among nation-states will impact the Internet and Internet governance

The most serious of these differences center on how freely data should flow internationally among states, and how much control individual governments should be able to exercise over information made available through the Internet to their citizens. It is these differences, and not technology, that pose the greatest threat to the Internet's continued usefulness as an international tool for commerce and communication. Will nations be able to resolve these differences, or are we heading inevitably towards the creation of a so-called "splinternet," where blocs of like-minded nations with compatible legal systems construct their own technological sandboxes? How will an Internet with geographical borders work? What strategies will international businesses need to develop to navigate an online environment altered to preserve cultural and political differences among nations?

Increased Antitrust Scrutiny of the "Tech Economy" and the Collection of "Big Data," Especially in the EU

As data's importance to the world's economy increases, some observers have begun to question whether particular players in the information economy who collect, store and transfer data have too much control over who has access to that data. In terms of government regulators, the EU has been and likely will continue to be the forerunner in this debate about the role of digital platforms and the power of data gathering. Having already imposed two record fines on Google (which has appealed these determinations), EU authorities have additional investigations pending that focus on alleged misuses of third party data. Whether competitors should have access to data collected by rivals is an issue antitrust authorities may be forced to address at some point, but a uniform response to concerns about so-called "data monopolies" is unlikely, certainly in the near term. Ultimately, businesses will look for an appropriate global compliance standard in a fragmented enforcement landscape.

The importance of data privacy in European competition law is also likely to continue in relevant merger cases and monopoly investigations. A German decision concerning data privacy infringements allegedly committed by Facebook as a social network monopoly is expected in early 2019 and may yet highlight additional antitrust compliance concerns for businesses. The claims combine elements of antitrust, privacy, and consumer protection in a novel way, as they target Facebook's harvesting of personal data through the Facebook button on third-party websites.

How Will the GDPR Be Enforced?

The most visible challenge attributable to differences in regulatory regimes applicable to accessing and using personal data, certainly for U.S. companies doing business in the EU, is posed by the need to comply with the EU's General Data Protection Regulation ("GDPR"), which went live in May 2018. For professionals concerned with data protection compliance, the past few years went by in a blur as companies rushed to digest the GDPR's new rules and meet the deadline for complying with this complex regulation.

In 2019, we should learn more about how EU data protection authorities actually will use their significantly enhanced powers to respond to complaints and reports about how personal data is being handled by businesses subject to the GDPR. Activity under the new regime has begun: the EU recently announced that more than 95,000 GDPR complaints have been filed with national data protection authorities since the regulation took effect in May of last year. On January 21, 2019, France's data protection authority, the CNIL, levied its first fine under the GDPR and the largest such fine under the Regulation imposed so far — a fine of 50 million Euros assessed against Google for violations of the GDPR's provisions on transparency and data subject consent. Google has said it will appeal the CNIL's decision.

The GDPR issues we will be watching this year include:

- What measures will data protection authorities expect to see implemented when determining whether companies can demonstrate compliance with the GDPR's provisions? What deficiencies will be considered particularly problematic? In assessing penalties, how much will a business's good faith efforts to comply be taken into consideration? Will there be opportunities for dialog with data protection authorities on compliance issues before penalties are assessed?
- How significant will fines be? How frequently will they be issued and for what kinds of conduct?
- What role will "stop processing orders" play with regard to enforcement?
- How uniform will the decisions of the several individual data protection authorities be on various issues? What role will instrumentalities of the EU Commission play in promoting uniformity?

– Will we see businesses and individuals bringing damage claims against data controllers and processors pursuant to Article 82 of the GDPR, which allows recovery of damages for data protection violations in certain instances?

A panel of Dechert data privacy practice group members addressed some of these GDPR questions in a webinar entitled, GDPR: The First Six Months. In addition, we expect increasing attention to be paid this year to how the GDPR should be applied to uses of blockchain technology. A Dechert OnPoint specifically addressing these issues will be published in February.

Data Protection and the Brexit Conundrum

The United Kingdom's plan to withdraw from the EU was thrown into disarray recently when Parliament rejected the withdrawal plan negotiated by Prime Minister Theresa May. Since that rejection, questions have intensified about what to expect from the UK's privacy regime in the event of a "no deal" Brexit — that is, a withdrawal without a negotiated agreement between the EU and UK. If the current deadline for withdrawal from the EU holds, businesses will need to have answers to these questions by March 29, 2019.

If Parliament does ultimately approve the Prime Minister's withdrawal plan in some or other form (which remains a possibility at the time of writing), EU law, including the GDPR, will continue to apply in the UK during a Transition Period, running until at least December 31, 2020. With regard to data protection, May's agreement assumes that during the Transition Period, the EU and UK will take the steps necessary to facilitate EU adoption of an adequacy decision that will allow data to continue to flow freely between the UK and EU after the Transition Period. With the uncertainty as to definitive rejection by the UK Parliament of the Prime Minister's proposal, however, plans for an orderly transition from data governance under the EU's data protection scheme to an independent but cooperative UK regime are in flux.

One thing is clear: even if there is a "no deal" Brexit, the GDPR would be incorporated into UK law by the European Union (Withdrawal) Act 2018 and will therefore remain the core law on data protection in the UK. However, whether data transfers from the EU to the UK under a "no deal" scenario could continue in such circumstances without additional measures would be dependent on the EU making an adequacy decision in relation to the UK. The process of negotiating a new adequacy or similar agreement could take years, during which companies would have to rely on other means of legally facilitating data transfers, such as binding corporate rules or standard contractual clauses. (Earlier this year, a group of our colleagues explored the issues raised on the data protection front by the possibility of a "no deal" Brexit and potential responses to such an environment in a Dechert OnPoint, available here.)

Will UK-EU plans for cooperation on data protection issues be a casualty of the continuing Brexit frictions? What strategies should companies subject to the GDPR doing business in the UK or with UK companies use to navigate through these divisions until the tensions surrounding the UK's re-definition of its relationship with the EU are resolved?

Will the US Enact National Data Protection Legislation?

The GDPR's influence and the enactment in California of the most ambitious data protection legislation yet adopted by any U.S. state, along with other widely-reported, high profile stories of data breaches and cybersecurity incidents, have raised concerns about the quality of data protection available to U.S. consumers, prompting some in the US. government and various industries to more seriously consider national privacy and data security legislation. Serious obstacles to the adoption of such legislation remain, however, including disagreements on what data management practices any such legislation should mandate, what federal agency should be charged with enforcing such laws (the FTC versus a new agency created solely to focus on privacy and cybersecurity), and on whether any federal legislation enacted should preempt privacy and cybersecurity protections already adopted by the several states. In a Dechert OnPoint, our colleague Greg Luib recently examined the proposals available so far and what effect they might have on any federal legislation ultimately adopted.

Cybersecurity: Where Are We Now?

Cybersecurity will remain a key focus of businesses and government (including government regulators) in the US. Experts agree that threats to US computer networks will increase as attacks become more numerous and the technology behind them increasingly sophisticated.

Given the relative stringency of the GDPR's breach reporting requirements, evolving legal expectations in the US, and market sensitivities to the effects of cyber-attacks, businesses will be expected to respond swiftly and effectively to these threats and to prevent them to the extent possible.

In the past several years, various government actors and private industry have devoted increasing attention to protecting the integrity of computer networks.

In the US, the Trump Administration recently adopted a National Cyber Strategy, and specific federal agencies charged with regulating US businesses that collect and process consumer information (including financial information, health information, and other PII) are pushing these businesses to take measures deemed necessary to protect their customers' data from attack and misuse. Every US state now has some form of breach notification law, and the courts provide redress for breach victims who can prove demonstrable harm.

Recent statutory amendments suggest that the protection of consumer information is viewed as a national security concern. The Foreign Investment Risk Review Modernization Act (FIRRMA), which took effect in August 2018, expanded the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS), an inter-agency body empowered to consider whether foreign investments in and acquisitions of US businesses threaten US national security and thus should be blocked, unwound or subject to mitigating conditions. As a result of FIRRMA, for the first time CFIUS has jurisdiction to review a foreign investment even at a non-controlling level if the targeted US business possesses "sensitive personal data." (Our colleague Jeremy Zucker covers CFIUS issues closely. Read recent Dechert OnPoints regarding CFIUS considerations)

But issues remain. For example, will the federal government set a national standard for responses to breaches of computer networks, or will it choose to continue with the current scheme of state-by-state regulation? Will the FTC or some other federal agency be given more explicit authority to address cybersecurity issues in private industry?

How will the US promote international cooperation on cybersecurity issues? Promoting international adherence to universally accepted standards of conduct in cyberspace is a goal of the Administration's National Cyber Strategy. But the US recently refused to join the Paris Call for Trust and Security in Cyberspace, whose 370 signatories include every member of the EU and 27 of 29 members of NATO. Are there other ways of promoting cooperation on cyberspace issues in the international community?

Data Transfers between the EU and US

Data transfers between entities in the EU and the U.S. were placed at risk by the European Court of Justice's decision in *Schrems*, (which declared the "Safe Harbor" regime invalid), leading to the adoption of the EU-US Privacy Shield, and increased reliance by industries operating internationally on private instrumentalities for data transfers, such as standard contractual clauses. Now, both the private compliance instrumentalities and the Privacy Shield itself are under attack in EU courts by activists claiming that they provide insufficient protection for EU data subjects whose personal data is processed outside the EU, especially in the U.S. EU privacy officials claim in their most recent report to be generally satisfied with how the U.S. is meeting its commitments under the Privacy Shield framework, but concerns about the extent of the U.S. government's compliance with the framework's provisions and its plans to enforce provisions meant to protect the privacy rights of EU data subjects remain. What's in store for the EU and U.S. in this area? And what, if any, effect should these concerns have on determining what kind of national regulation the U.S. adopts with regard to data protection?

Successfully Navigating the Legal Complexities Associated with Cloud Computing

The massive growth in cloud computing continues as more companies and public organizations seek to harness its advantages — cost savings, speed, scalability, performance, security, and redundancy and resilience in the face of cybersecurity risks. Cloud business is increasingly a critical revenue source for major technology companies and they are making significant investments to maintain their dominant market positions. Cloud computing now includes an array of services, including Business Process as a Service (BPaaS), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Database Platform as a Service (DPaaS), which ensures continued competition with smaller scale providers, including start-ups. Moreover, because of data security and privacy concerns, Cloud Service Providers are now offering different cloud platforms, including a public cloud, private clouds, and hybrid models.

Unlike real clouds, cloud data centers have actual physical locations which give rise to thorny legal issues. Differing data protection regimes governing the jurisdictions where data is stored can create regulatory difficulties when governments (including host governments) and non-governmental third parties seek access to data stored at these data sites. Some regimes place restrictions on where their citizens' data may be maintained. For example, some governments require the storage of certain kinds of data within their borders and various levels of access to server technology and data as conditions of doing business in their countries. These differences in approaches to data protection regulation, and measures directed specifically at cloud storage, including legislative enactments like the U.S. Cloud Act and the EU's announcement of its draft e-Evidence Regulation in 2018, will require multinational organizations to be smart and strategic with respect to data residence when they are selecting cloud providers and services.

A Deeper Dive into the Ethics and Policies Governing the Use of Artificial Intelligence

As the uses for artificial intelligence have continued to multiply, so have concerns about how this technology will be used and whether industry and society generally are prepared for the results of its being employed on a much broader scale. AI applications are expected to contribute to advances in government and industry operations and scientific and medical research. Like other technologies that have held great promise and have fascinated us with their potential capabilities, there are concerns that we may be moving forward with AI's deployment without a sufficient understanding of how the technology does what it does, and what changes we can anticipate from its incorporation into a broader spectrum of products and functions.

In 2019 we will be monitoring what developers will do to promote greater understanding of and confidence in AI technology. On the technical side, media reports suggest that developers are focused not only on applications, but also making the processes by which AI reaches its results more transparent and easier to explain. The public and private sector also will be focused on the level of responsibility those who employ AI technology should bear for how uses of their applications may affect others.

The EU has already begun to address some of the policy issues raised by AI deployment through provisions in the GDPR, and through preliminary guidance drafted by an EU committee of experts formed exclusively to ensure that Europe's contributions to the technology's development are ethical and safe. Private sector organizations are also providing guidance on how AI can be deployed ethically, and in ways that can protect people whose interests might be impacted by AI. From a privacy perspective, among other issues, look for increased discussion of how to ensure that AI technology's reliance on vast amounts of data to reach reliable results is consistent with data protection provisions in the EU and other countries.

Contact us

We intend to report on developments in these and other areas of interest as the year progresses. For more information about Dechert's Data Privacy and Cybersecurity practice or to suggest other topics or areas of interest for future reports, contact our practice group leader, Timothy Blank.

Vernon A. Francis
Partner
Philadelphia
+1 215 994 2577
vernon.francis@dechert.com

Ben Barnett
Partner
Philadelphia
+1 215 994 2887
ben.barnett@dechert.com

Timothy C. Blank
Partner
Boston
+1 617 728 7154
timothy.blank@dechert.com

Alec Burnside
Partner
Brussels
+32 2 535 54 33
alec.burnside@dechert.com

Marjolein De Backer
Associate
Brussels
+32 2 535 5414
marjolein.debacker@dechert.com

Dr. Olaf Fasshauer
National Partner
Munich
+49 89 21 21 63 28
olaf.fasshauer@dechert.com

Paul Kavanagh
Partner
London
+44 20 7184 7510
paul.kavanagh@dechert.com

Gregory Luib
Counsel
Washington, D.C.
+1 202 261 3413
gregory.luib@dechert.com

Jennifer McGrandle
Associate
London
+44 20 7184 7800
jennifer.mcgrandle@dechert.com

Sophie Montagne
Associate
Paris
+33 1 57 57 80 47
sophie.montagne@dechert.com

Joshua H. Rawson
Partner
New York
+1 212 698 3862
joshua.rawson@dechert.com

Madeleine White
Associate
London
+44 20 7184 7302
madeleine.white@dechert.com

Jeremy B. Zucker
Partner
Washington, D.C.
+1 202 261 3322
jeremy.zucker@dechert.com

01.31.19