ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Privacy Now: What in the [Privacy] World is Happening?

Technology, Privacy, and eCommerce

2021 is off to a hot start when it comes to privacy legislation around the world. After a year focused on elections and a pandemic, it seems as if the lawmakers and authorities are ready to move quickly back into privacy and data protection laws. Although March seems particularly active with the California appointments and passage of Virginia's law, there have been multiple developments in the past few months with more to come.

Here are some of the more significant data protection law developments already in place, as well as some to watch for in the near future.

UK GDPR

The European Commission published two draft Adequacy Decisions for the United Kingdom on Feb. 19, 2021, one for the General Data Protection Regulation and one for the Law Enforcement Directive. We are awaiting the opinion by the European Data Protection Board, which is anticipated in some circles to be a negative opinion based on the United Kingdom's surveillance activities and emphasis on business relationships, as seen by its recent job announcement for the Information Commissioner's Office (ICO). This opinion is non-binding on the Commission and is expected in April.

Context

The bridge to transition from the European's General Data Protection Regulation (GDPR) to an adequacy decision is on its (alleged) last extension through June 2021. This bridge permits personal data to continue to flow freely from the European Economic Area to the United Kingdom. Meanwhile, the UK's GDPR has gone into effect. In conjunction with its Data Protection Act 2018, and with only

a few changes, such as to limit the provisions to one country, the UK GDPR mirrors its European counterpart.

Practical effect

The UK GDPR is much like the EU GDPR, and controllers will need to appoint a UK representative if they are not physically established in the United Kingdom regardless of whether the controller is physically established in the European Union or has an EU representative appointed. If the representative for the European Union is in the United Kingdom, another will need to be appointed within the European Union. This is the same for nominating a supervisory agency. If the controller had selected the ICO as its EU agency, it would need to select another in the European Union. Any data transfer mechanisms used for the European Union will need to be re-evaluated for the United Kingdom. Data transferred before Jan. 1, 2021 will remain subject to the provisions of the EU GDPR (the “frozen GDPR”), and data transferred starting this year will be subject to the UK GDPR.

California Consumer Privacy Act

The California Consumer Privacy Act saw new regulations come into effect March 15. These mainly comprise requirements for offline notices, guidance on icons for opting out, and specifications for making opt-outs and rights requests easy for consumers.

However, an announcement was also made appointing the first board to the new California Consumer Privacy Agency, established under the Consumer Privacy Rights Act (CPRA), which passed as a ballot initiative in this past November 2020 election. The board is responsible for selecting the leadership and staff for the new agency, which will be effective Jan. 1, 2023.

Context

California was the first state in the US to pass comprehensive privacy legislation in 2018. After multiple amendments in both 2019 and 2020, as well as several rounds of regulations, the CCPA is currently in effect. About 60 class action lawsuits have been filed and the Attorney General’s office issued warning letters in July to companies allegedly not following the CCPA.

The CCPA was the first omnibus privacy law in the United States and is expected to influence other state laws. It covers controversial aspects like individual rights, a private right of action, and the "selling" of data with a broad definition of selling including benefits other than monetary gain. Some of these elements mimic the EU GDPR yet diverge in others. Under the new CPRA, the privacy protection agency is new. It is yet to be seen what effect this will have on privacy enforcement and activity, but it is anticipated to be very active.

The big focus for the AG’s office appears to be more on individual rights, including notice and opting out provisions. However, under the CPRA, companies will need to perform annual audits and submit them to the new agency. The concept of sharing data under the CPRA will add a level of complexity, especially in adTech.

Practical actions

If you are subject to the CCPA, get your data governance program into alignment. If you are also

subject to the GDPR, leverage your current activities and identify the critical differences. If you did not take compliance with the GDPR seriously, because perhaps on a risk-based level, you have minimal exposure, complying with the CCPA may be a way to also shore up your GDPR compliance. Consult a privacy professional, legal counsel, and invest in privacy compliance software that may make your compliance more streamlined and cost-effective. Identify your processing activities for sales of personal data, but also sharing under the CPRA.

Virginia Consumer Data Protection Act

In a surprising move, Virginia passed its Consumer Data Protection Act, which goes into effect Jan. 1, 2023. This new act carries many similarities to the CCPA and to the GDPR, but several notable differences. There are individual rights, but no 12-month look-back period like the CCPA and no private right of action.

However, like with the GDPR, there are requirements for data protection assessments (which the attorney general may request), the concept of controllers and processors of which processors are also subject to enforcement, required data processing agreements, and provisions pushed down to subcontractors. Although there are provisions to identify the sale of personal data like the CCPA, it is limited to monetary gain and not expanded to other benefits.

Context

The passing of this law was a bit of a surprise and there are multiple other states with bills under consideration, most notably Washington, Utah, New York, and Oklahoma. In 2020, many states, including the ones listed here, were poised to pass consumer privacy laws, but other priorities quickly rose to the forefront. Virginia’s passing sends a strong signal that states are ready to take these laws seriously.

Practical actions

Evaluate your exposure to the CDPA whether as a controller or as a processor who has controllers as clients. Identify differences between the various privacy/data protection laws to which you are subject. Consider moving to a framework compliance methodology as opposed to managing by individual laws and one-offs. Engage a knowledgeable privacy professional, legal counsel, and evaluate privacy compliance software solutions (look for expertise and not check-the-box solutions).

US Federal Trade Commission

The FTC announced it has made significant changes to its security orders in three broad areas:

1. Security orders must be more specific and detail the steps companies must take to improve their security practices based on the problems alleged in the complaint.

2. Accountability for third-party assessors is increased by requiring increased rigor, specifically identified evidence supporting conclusions, and the retention of documentation which must be available to the FTC and not withheld under privilege.

3. Security considerations must be elevated to the C-Suite and Board.

For assessors, the FTC will review assessors on a two-year basis to approve or disapprove them to continue as assessors. On the security considerations to the board, the FTC will require annual certifications, similar to other federal requirements.

In addition, the FTC released its 2019 privacy and security update on Feb. 25, 2021, detailing its activities including enforcement and workshops.

Context

The FTC has been the most active enforcement agency for privacy under unfair and deceptive trade practices. There is at least one bill, with favorable support, that would extend the FTC's authority over privacy/data protection activities. There are other federal privacy bills, but as in past years, no guarantee any will pass.

Practical actions

Watch FTC enforcement actions to evaluate specific security actions proposed. If you do not have both privacy and security individuals on your board, you should. Security may be getting more press coverage because breaches matter, but privacy is what drives most laws. They are two equally important areas and companies need both areas of expertise.

US Health Insurance Portability and Accountability Act (HIPAA)

Although not as splashy as many privacy law developments, HIPAA has had some significant activity recently, including the Information Blocking final rule by the Office of the National Coordinator, enforcement discretion on several fronts, the Cybersecurity Safe Harbor, the Cybersecurity Tech Donations Safe Harbor, and proposed revisions to individual rights.

Other developments to watch for in 2021

Australia is reviewing its Privacy Act and should publish findings this year.

Brazil's Lei Geral de Proteção de Dados (LGPD), Latin America's first major data protection law, came into force in September 2020 and enforcement (sanctions) are slated to start August 2021.

Canada's proposed Digital Charter Implementation Act (DCIA) was introduced in November 2020 for the Consumer Privacy Protection Act and would replace the Personal Information Protection and Electronic Documents Act (PIPEDA). It includes a private right of action, penalties and enforcement provisions, and individual rights, among others. In addition, in February, Canada also announced that its Privacy Act (applying to the government) will be reviewed.

China's Standing Committee of the National People's Congress published the first draft of its Personal Information Protection Law for public comment in October 2020. Its goal is to enact one omnibus law and add extraterritoriality, fines, requirements for data protections officers, and cross-border data transfers. More review is expected, but they are trending towards a GDPR-like approach.

New Zealand's Privacy Act 2020 came into force in December 2020, so we should see activity in 2021. The act includes new provisions around cross-border transfers, individual rights, data breach

notifications, and extraterritoriality.

Singapore amended its Personal Data Protection Act (PDPA), adding breach notifications, increased penalties, and changes to its consent requirements.

Conclusion

The items listed above are certainly not everything that is happening; privacy law really is growing rapidly. If you handle any type of personal information, you should be watching this space. But be careful, “personal information” may not carry the same definition where you are located as it does in other countries or states. It is even more critical now to manage your programs in a comprehensive manner.

K Royal

Global Chief Privacy Officer

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.