LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

5 Global Data Protection Trends To Watch In 2022

By **William Long and Francesca Blythe** (January 3, 2022, 12:03 PM EST)

William Long

Francesca Blythe

A recent discussion with Elizabeth Denham and Claudia Berg of the U.K. Information Commissioner's Office[1] provided ample food for thought on the direction in which data protection regulation both in the U.K. and internationally is headed, including key trends to watch for in data protection.

These key trends will be important for international companies as they consider their data strategies wherever they may be based and include:

- A growing call for international collaboration on data protection;
- A trend toward data localization in an increasingly global technology world;
- Dealing with the rise of cyberattacks, in particular through ransomware;
- The development of regulating emerging technologies, such as artificial intelligence; and
- The role of regulators in an age of global technological innovation.

Global Convergence and the Potential for More International Collaboration on Data Protection Legislation

Regulators like the ICO are increasingly seeing an appetite for international collaboration on data protection laws in order to support international data transfers and to further innovation. This effort has been driven by a recent convergence in objectives and mandate among global forces in data protection.

This can be seen most prominently through the June 2021 Group of Seven summit held at Carbis Bay, U.K., and the 2019 Group of Twenty summit held in Tokyo, which both had the same theme: "to allow a free flow of data with trust."

There is also a global awareness that we need new data protection legislation as well. For example, the U.K. government has proposed reforms on data protection law in its recent "Data: A New Direction" white paper, while China's new data law, the Personal Information Protection Law came into force on

Nov. 1. In the U.S., many states are developing their own data privacy laws, such as with the California Consumer Privacy Act.

Moreover, there is recognition that, given the pace of innovation we are seeing with technology, a nation-by-nation or state-by-state approach can only take us so far. Former U.K. Information Commissioner Elizabeth Denham, for instance, has advocated for a form of data Bretton Woods, whereby we rethink data protection in the way that Bretton Woods rethought global financial systems toward the end of World War II.

International Data Transfers, Data Localization and Consequences of Brexit

We have already seen some signs of a trend toward data localization — the idea that nations are putting up barriers to international data transfers as opposed to allowing a free flow of data across borders.

This can be seen most obviously through the idea of "adequacy," which originates from the European Union. An adequate jurisdiction is one that the EU considers to be providing an equivalent level of data protection to the level that EU legislation offers. Such a jurisdiction benefits from the free flow of data in and out of the EU.

Countries deemed inadequate must implement safeguards like standard contractual clauses, or SCCs, instead. The U.K. was handed an adequacy decision this year, and there has been much debate about whether this status will continue, especially in light of the U.K.'s ambitious plans to reform its data protection regime and potentially move away from certain EU standards.

Further, the U.K. has suggested that it wishes to add more countries to its adequate list of jurisdictions, including potentially the U.S. This marks a departure from the European Commission's previous determination that the U.S. was effectively an adequate jurisdiction under the EU-U.S. Privacy Shield framework, but the EU's Court of Justice in the July 2020 Schrems II case invalidated that determination.

The U.K.'s decision to walk its own path can further be seen in the area of SCCs. Until now, the U.K. had adopted the EU's set of SCCs. However, post-Brexit, it has decided not to adopt the latest set of EU SCCs that were published in June 2021.

Instead, the U.K. has drafted its own set of new U.K. standard contractual clauses — referred to as an international data transfer agreement — which are expected to be released shortly. It will be interesting to see how this trend of digital sovereignty will cut against the themes of international collaboration discussed above.

Data Breaches Fueled by New Form of Cybercriminality

Cybersecurity and data breach reporting obligations remain key issues for both businesses and regulators such as the ICO. The seriousness of cybersecurity attacks was brought into focus when the U.K.'s national health service became the subject of such an attack in 2017.

More generally, it has been widely reported that ransomware attacks have increased significantly over the last two years. In light of these issues, the ICO, like many regulators, is looking to focus resources on more serious cybersecurity attacks and ransomware rather than dealing with more minor accidental data breaches.

The U.K. government has also recognized the cost of overreporting, and its new "Data: A New Direction" white paper is considering the need to only report material breaches.

However, drawing the line with reporting obligations can be difficult, as even simple data breaches can have serious consequences. For example, the ICO has highlighted the recent incident in which an email mistakenly revealed Afghan interpreters' contact details, which potentially threatened their safety.

These are important developments for international businesses, including those in the U.S., that are handling U.K. and EU data. They reflect a possible shift in the U.K. position away from that of the EU on certain key data privacy issues, such as data breach notifications.

If these proposals are carried out, it means that international businesses will need to fine-tune data breach response plans as the test for notification of data breaches in the U.K. may differ from the test as applied in other EU member states.

Emerging Technologies: The Challenges of Regulating AI, Machine Learning and Facial Recognition

The governance of emerging technologies, such as AI, machine learning and facial recognition technology, will be a huge priority for all players in data privacy and cybersecurity in the years to come.

AI and other related technologies are increasingly both discussed and invested in, with large tech players like Facebook Inc. investing in the metaverse and Google LLC putting more resources into its AI entity "DeepMind."

The ICO, like other international regulators, recognizes a need to support innovation through digital development while ensuring appropriate regulation is in place. The form of that regulation is still to be determined, in particular whether AI regulation should be centralized to cover all industries, as in the proposed EU AI regulation, or decentralized at an industry level, as with regulation of AI in driverless cars through automobile industry regulation.

Support of emerging technologies and innovation can also take place through clear and practical guidance from regulators. For example, the ICO has produced an AI toolkit that explains how to develop and deploy AI in a way that is data law compliant, and it has produced a recent paper on facial recognition technology in public places.

The ICO is also promoting the use of so-called "Sandboxes," whereby new technologies are reviewed by the regulator for data law compliance before they are released on the marketplace. This approach ties in with the U.K. government's recent publication of its national AI strategy, which further emphasizes unlocking the use of AI as opposed to overregulating it.

The Role of Regulators in an Age of Global Technological Innovation

With data becoming more crucial to every industry, the U.K. government is calling for the widening of the ICO's mandate, a proposal that has been supported by the ICO itself. U.K. government proposals have suggested that the ICO should have due regard for principles like public safety, economic growth and competition under statute.

This can be seen as another sign of a trend toward a pro-growth and pro-innovation approach that many governments and international regulators in Europe, the U.S. and elsewhere are grappling with.

Practically speaking, this wider and pro-innovation mandate may make international data flows, especially between the U.K. and U.S., easier.

Ultimately, the real trade-off in the future, for the ICO, for regulators in the U.S. and in other countries, will be how to foster technological innovation while at the same time protecting the privacy and security of individuals and society through appropriate regulation.

So, where does this leave regulators and international business? It is clear that we are in a time of profound global change where both regulators and international businesses need to assess new technologies, risks and opportunities.

For regulators, there has never been a greater need to cooperate globally on agreed objectives and principles to regulation of data. And for international businesses, there has never been a greater need to understand trends in data protection regulations globally and, more fundamentally, that data is the key asset class of the future.

William Long is a partner and a global co-leader of the privacy and cybersecurity practice at Sidley Austin LLP.

Francesca Blythe is a senior associate at the firm.

[1] On Sept. 21, Sidley Austin LLP.partners Alan Raul and William Long engaged in a fireside chat with Elizabeth Denham and Claudia Berg of the United Kingdom Information Commissioner's Office.