AMERICAN BANKER®

Congress needs to hurry up on data protection

By Jeremiah Buckley
Published October 30, 2019

Data is the lifeblood of the burgeoning digital economy. The debate about its use — and its protection — is now playing out globally.

As big data, artificial intelligence and machine learning increasingly shape everyday lives, Congress will have some important policy choices to make, weighing how to sustain economic growth while balancing individual rights and corporate responsibility.

Suffusing this debate is the uncomfortable reality that, for all practical purposes, the world's understanding of oneself will be more so based on a digital alter ego: a virtual persona, created and defined by data-driven analytics.

The policy questions often come down to one question: What rights should consumers have to control their digital persona?

The stakes of the debate are high and all too real, but maddeningly abstract. Even a recent American Banker article noted that exactly how legislators move forward on data security has "confounded Congress."

Legislators are aware that the expectations of consumers — or rather, voters — harden with each data breach and perceived corporate misuse of consumer data.

The conversation is beginning to coalesce around what might loosely be identified as a consumer bill of privacy rights, many of which have a foothold in the General Data Protection Regulation and the California Consumer Privacy Act.

At heart is the "right to know," a conceptual declaration that persons should be aware when others collect, store, analyze or process their personal information. This is paired with a related "right to control" disclosure or use of that information.

Then there's the "right to be forgotten" enshrined in the GDPR, which is based on the idea that persons should be able to demand that companies destroy their personal information.

Other attendant rights stem from the fundamentals, such as a consumer's right to ensure their data is accurate and adequately protected — and to be compensated for lost or stolen data. Because two of the chief threats to data privacy are state actors and organized criminal enterprises, consumers also expect government protection.

However, the difficulty lies in the limits and borders of these rights, in their application and enforcement. Even reasonable people are drawing these lines differently.

In the absence of federal legislation, states are rushing to fill a perceived void. California's privacy law (the CCPA) is only the first comprehensive, state-level data protection regime that can purport to parallel GDPR. But it likely won't be the last.

Many state legislatures are developing their own data protection statutes. Some of these deal with privacy while others, data security.

But a balkanized approach to data protection is at odds with the borderless nature of the internet, and has the potential to put a brake on innovation. This demands a national solution in data protection.

Congress was confronted with a similar issue when digital commerce was in its infancy about 20 years ago. States, most notably California, were adopting their own non-uniform electronic signature and record statutes, despite that a uniform state law was in circulation.

Then, as now, a national standard seemed the best solution. But it was not an easy lift. Prompted by concerns that the "digital divide" would allow some citizens to take advantage of electronic commerce, then-President Bill Clinton threatened a veto.

Prospects looked dim until a majority consisting of House Republicans and about 70 New Democrats opted to support the so-called Esign Act, saving it from defeat. That law provided the undergirding for a significant expansion of the use of electronic records, now taken for granted.

The case for a federal data protection statute is now stronger than the case for the Esign Act. But what's at stake is much more complex.

There are questions of individual rights and security as well as

the benefits that digital commerce brings, such as a potential expansion of access to services for the underserved. Perhaps most important, there is the economic consideration of whether the U.S. can continue to lead the global digital revolution without a federal solution.

In the current politically charged environment, it's difficult to determine whether a consensus on the thorny issues surrounding data protection can be achieved. Further, choosing what House and Senate committees will have jurisdiction may get contentious.

And then there is the tough question of which executive branch agency will be principally responsible for rulemaking and enforcement.

Data protection is the type of complex issue that a bipartisan, blue-ribbon panel of experts should assess and make recommendations to lawmakers. The executive branch could also galvanize action by designating a data protection czar with authority to coordinate agency initiatives.

Regardless of how Congress and the administration approach this issue, the important thing is to get started as soon as possible.

Advances in data analytics are proceeding rapidly. Getting this right would be challenging under the best of circumstances, but doing nothing is the same as getting it wrong.

Every citizen has a large stake in how their digital persona is managed. The reputational and economic consequences for every individual deserve serious and prompt attention.

Congress and the administration owe it to all of us to make data protection, in all its aspects, an urgent national priority.

Jerry Buckley is a founding partner of Buckley LLP and over a 40-year career has established himself as an acknowledged leader in financial services law.