Disinformation, Mob Mentality, And Federal Privacy Legislation

FG Law Blog

January 11, 2021
Krishna A. Jani
Philadelphia, PA

Will the disinformation that led to a mob surrounding the Capitol Building help drive federal privacy legislation?

Here's why I think it will.

Disinformation

It is no secret that the internet is rife with information—some legitimate, and, inevitably, some not. In many ways, social media and the rise of new and emerging platforms on which to share information, contribute to the spread of *dis*information. Disinformation is false information that is intended to mislead, unlike *mis*information, which is false information that is spread, regardless of intent to mislead.

Disinformation can be damaging to both individuals and businesses because it can be difficult to discern the difference between evidence-backed information and disinformation. This very issue arguably resulted in thousands of people surrounding the Capitol Building on January 6, 2021 in Washington, D.C.

The Role of the Internet and Social Media

Though many platforms likely contributed to the widespread disinformation that led to a mob storming the Capitol Building, certain platforms have a significantly greater impact. For example, with more than two billion users worldwide, Facebook has unprecedented reach, and that reach has created a near-monopoly on certain types of information and the sharing of that information. For instance, small businesses often rely on Facebook to find customers. Content creators use Facebook to create visibility for their work. Software developers seek to attract customers on the platform. Media outlets use the platform to share news articles. The list goes on.

Platforms like Facebook employ the details of personal profiles to gauge which content it believes a particular user will find enticing. Then, the platform will calibrate the user's feed according to this process in an effort to maximize the amount of time that the user stays online. The result is that the information that appears in our feeds is informed, to at least some degree, by what our friends and network contacts post and consume. It is shaped, by a much larger degree, by the platforms' algorithm.

This is precisely the point at which data privacy, personal autonomy, and democracy intersect.

The Problem and Ways to Avoid the Spread of Disinformation

Disinformation can harm businesses in a myriad of ways. Incorrect news, negative social media posts, and even overtly false consumer reviews can adversely impact a company's bottom line.

Successful companies understand their markets, their customers, and their partners. They also need to understand how their brand is perceived by users of social media. This can be achieved by using in-house technology or hiring an outside firm. By doing so, companies can get advance warning of an individual's or group's efforts to spread disinformation about a given brand. To the extent a business participates in e-commerce and has a social media presence, the business should aim to establish verified accounts on major platforms and use them regularly to establish their markets.

Other tools businesses can use to avoid the spread of disinformation are: self-assessing, preparing for incident response, and communicating directly with their customers. In addition, data ethics should be incorporated into decision-making along with business motivation, technological practicality, and legal compliance.

How Federal Privacy Legislation Could Help

The federal government has no organization to regulate or help quell the spread of disinformation, and there is no one particular person within the government in charge of an overall disinformation policy. The United States needs a comprehensive approach to risk generated by data. Accordingly, any effective federal privacy regime must take into account the process of data throughout the whole lifecycle of data governance.

The business industry has plenty of reasons to support federal privacy legislation. For one, a single piece of comprehensive legislation reduces confusion surrounding compliance. Second, one law to rule them all would likely preempt many of the piecemeal legislative efforts of various states. Lastly, in the wake of the *Schrems II* decision, passing a commercial privacy law would help the atmosphere considerably as negotiations go forward with the European Union with regard to transborder data flows.

It is also worth noting that some of the largest markets in the world are moving toward comprehensive data protection laws, such as China, India, Brazil, and Canada. The adoption of a similar comprehensive law in the United States would solidify the United States' position as a world leader in data privacy.

The goal of any federal privacy legislation should be to preserve the most beneficial aspects of social media platforms while simultaneously protecting individuals and businesses from the platforms' more harmful impacts. Most pending federal legislation include the basics: data access, deletion rights, and portability. The next steps will be to incorporate protections against disinformation.

Krishna A. Jani is a member of Flaster Greenberg's Litigation Department focusing her practice on complex commercial litigation. She is also a member of the firm's cybersecurity and data privacy law practice groups. She can be reached at 215.279.9907 or krishna.jani@flastergreenberg.com.