SQUIRE PATTON BOGGS

Election 2020:

Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation

US – November 13, 2020

By Kristin Bryan, Lydia de la Torre, Glenn A. Brown and Aaron Garavaglia

The US is in the process of completing its 59th presidential election and electing its 46th president. A change in administrations is inevitably accompanied by a change in executive priorities.

Assuming that Vice President Biden is sworn in as President on January 20, 2021, the area of data privacy will likely be of particular focus under the Biden Administration, with consequences for data privacy litigation. Some top of mind questions regarding the anticipated impact a Biden presidency may have in this area are addressed below. Specifically, we anticipate that a Biden Administration will likely focus on the passage of federal data privacy legislation, renegotiate conditions for EU data transfers to the US, reintroduce a cybersecurity coordinator to the White House and increase FTC enforcement activity. Of course, several of these issues are contingent upon which party will come to control the Senate, a question that will not be answered until the two runoff elections in Georgia are completed in early January 2021.

Will a Biden Administration Be Interested in Pursuing Privacy Legislation?

It is anticipated that the Biden Administration will likely see pursuing privacy legislation as a high priority. This is consistent with Vice President-elect Kamala Harris' track record and interest in privacy-related topics during her career as California Attorney General and US Senator.

As Attorney General, Harris was very active in the privacy space. During her tenure, privacy issues related to the rise of mobile devices were of particular concern. In January 2013, her office issued a report (Privacy on the Go: Recommendations for the Mobile Ecosystem) and pushed tech giants to agree to certain principles to provide creative and forward-looking solutions that give consumers greater transparency and control (Joint Statement on Principles). It was also during Harris' tenure that the Privacy Enforcement and Protection Unit of the California Attorney General's Office was created to enforce laws related to cyberprivacy, as well as identity theft and data breaches. That office is currently responsible for the enforcement of the California Consumer Privacy Act. Additionally, in 2015, Harris also secured settlements with several large companies related to their privacy practices. Notably, one of these settlements required the company at issue to hire a Chief Privacy Officer, the first time such a provision has been included in a settlement with the California Department of Justice.

What Might Be Expected for the Biden Administration's Priorities?

For obvious reasons, one of the main priorities of the Biden Administration will be to revitalize the US economy. This priority will run up against global data privacy considerations, however, in light of developments this past summer . In July 2020, the Court of Justice of the European Union invalidated the EU-US Privacy Shield, a framework designed to facilitate transatlantic data transfers (you can see our webinar on the topic here). In the aftermath of this decision, the regulatory burden and associated risks have significantly increased for companies transferring EU personal data to the US in line with the EU General Data Protection Regulation. The legal issues involved include US surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) (Section 702), Executive Order 12333 (E.O. 12333) and Presidential Policy Directive 28 (PPD-28). A Biden Administration opens the door to potential reconsideration of, or modifications to, both E.O. 12333 and PPD-28, which could pave the way for agreement on a new transatlantic framework for the transfer of EU personal data to the US.

Many observers have also predicted that the Biden Administration will reestablish a cybersecurity coordinator position within the White House. The White House Office of Cybersecurity, established in 2009, was eliminated under the Trump Administration and the position's responsibilities were largely shifted to the new Cybersecurity and Infrastructure Security Agency. The Biden Administration will likely reinstate many of these responsibilities at the White House level.

Will We Finally See Federal Privacy Legislation and What Impact Would This Development Have in the Area of Litigation?

In terms of immediate priorities, dealing with the public health and economic crises brought about by the COVID-19 pandemic is likely to dominate the initial years of the Biden Administration, but the resolution of these issues may lead to the enactment of related privacy legislation.

Efficiently controlling the spread of the virus has involved, and will continue to involve, tracking and tracing cases, which require data collection and processing activities that involve privacy risks. During 2020, these risks caught the attention of Republicans and Democrats alike, which led to a bill introduced by Republicans in the Senate (S. 3663 – The COVID-19 Consumer Data Protection Act of 2020) and a bill introduced by Democrats in the House (H.R. 6866 – The Public Health Emergency Privacy Act). Although both bills remain pending, should control of the Senate switch during the next Congress, it is plausible that the bill introduced by the Democrats will receive renewed attention. The interest in enacting privacy legislation as to COVID-19-related information is likely to resurface in 2021 and may lead to new requirements for both government entities and organizations in the private sector, including companies collecting employee health data and guest or visitor screening data.

Interest in privacy legislation has been steadily increasing at the federal level over the past few years.

In April 2020, the Congressional Research Service released a report that compared various consumer privacy bills introduced in Congress. The report concluded that most of the bills follow similar approaches by: (1) recognizing individuals' rights to control their personal information; (2) requiring a defined class of entities to take steps to respect those rights; and (3) creating procedures to enforce those requirements. The three key differences focus on: (1) which federal agency would have enforcement power; (2) whether the federal legislation should preempt state privacy laws; and (3) whether the bills should provide a private right of action.

Following the April 2020 report and as the current Congress comes to a close, the Senate has taken steps that should put fresh privacy legislation on the agenda of the next Congress. On September 23, 2020, the Committee on Commerce, Science and Transportation held a hearing entitled Revisiting the Need for Federal Data Privacy Legislation. In anticipation of that meeting, on September 17, 2020, Republican senators introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability (SAFE DATA) Act. In parallel, the Democrats have introduced the Consumer Online Privacy Rights Act (COPRA).

Depending on which party will take control of the Senate, the data privacy litigation landscape could be upended by preemption issues raised by federal data privacy legislation. In the absence of comprehensive federal legislation, privacy law has proliferated at the state level. Three states – California, Nevada and Maine – have signed data privacy legislation, while similar legislation has been introduced in at least seventeen states, with the majority of bills pending in committee. Additionally, at least six states have assembled joint task forces to consider data privacy issues. Based on the number of state privacy bills that are currently pending, it is conceivable that more than half of the states could enact divergent privacy laws over the next few years. With a potential statutory hodgepodge looming, preemption becomes a serious issue.

The proposed SAFE DATA Act would broadly preempt state privacy laws (with significant impacts, to say the least, on privacy litigation). By contrast, COPRA views federal privacy legislation as a "floor," and would allow states to enact stricter privacy standards if they elect to do so. Should the Democrats gain control of the Senate, the Biden Administration will likely be inclined to sign off on COPRA, thus minimizing the impact of federal preemption. Should Republicans maintain control, several outcomes are possible. As one example, the Biden Administration and Democrats may compromise on the preemption provision, sacrificing it to move the legislation forward. Of course, it is possible that federal privacy legislation will continue to remain in limbo.

The ability of the Biden Administration to work with the Congress to find a path for resolving these differences will be a key factor in determining whether comprehensive privacy legislation can be enacted at the federal level.

What Impact Will the Biden Administration Have on the FTC?

The Biden Administration will also likely have a significant impact on the FTC's enforcement priorities, as it is anticipated there will be increased FTC enforcement activity. This increased enforcement may have ripple effects in privacy litigation. One example concerns litigation alleging negligence *per se* under state law. Generally, negligence *per se* is a theory whereby an act is negligent as a matter of law solely on the basis that it violates a statute or regulation. To put it otherwise, negligence *per se* bypasses the traditional "reasonable person" standard by focusing upon three issues, which are whether: (1) the defendant violated a statute or regulation that sets forth a standard of care; (2) the plaintiff is a member of the class that the statute or regulation is designed to protect; and (3) the plaintiff suffered an injury that the statute or regulation was designed to prevent. Some courts have already expressly held that a violation of Section 5 may serve as the basis of a negligence *per se* claim. *Perdue v. Hy-Vee, Inc.*, 455 F. Supp. 3d 749, 760-61 (C.D. Ill. 2020). Accordingly, with an increase in enforcement, the data privacy landscape for suits involving private parties may also shift.

Contacts

Kristin L. Bryan
Senior Associate
T +1 216 479 8070
E kristin.bryan
@squirepb.com

Glenn A. Brown
Of Counsel
T +1 678 272 3235
E glenn.brown
@squirepb.com

Lydia de la Torre
Of Counsel
T +1 650 843 3227
E lydia.delatorre
@squirepb.com

Aaron C. Garavaglia
Associate
T +1 202 457 6436
E aaron.garavaglia
@squirepb.com