What Biden Presidency May Mean For Data Privacy Litigation

By **Lydia de la Torre, Glenn Brown and Kristin Bryan** (November 30, 2020)

Lydia de la Torre

Glenn Brown

Kristin Bryan

The U.S. 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 President-elect Joe Biden is sworn in as president on Jan. 20, 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 U.S., reintroduce a cybersecurity coordinator to the White House and increase Federal Trade Commission enforcement activity.

Of course, several of these issues are contingent upon which party will come to control the U.S. Senate, a question that will not be answered until the two runoff elections in Georgia are completed in early January.

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 U.S. 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[1] and pushed tech giants to agree to certain principles to provide creative and forward-looking solutions that give consumers greater transparency and control.[2]

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 privacy, 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 U.S. economy. This priority will run up against global data privacy

considerations, however, in light of developments this past summer.

In July, the Court of Justice of the European Union invalidated the EU-U.S. privacy shield, a framework designed to facilitate transatlantic data transfers. In the aftermath of this decision, the regulatory burden and associated risks have significantly increased for companies transferring EU personal data to the U.S. in line with the EU General Data Protection Regulation.

The legal issues involved include U.S. surveillance under Section 702 of the Foreign Intelligence Surveillance Act,[3] Executive Order No. 12333[4] and Presidential Policy Directive 28.[5] A Biden administration opens the door to potential reconsideration of, or modifications to, the latter two, which could pave the way for agreement on a new transatlantic framework for the transfer of EU personal data to the U.S.

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.[6] and a bill introduced by Democrats in the U.S. House of Representatives.[7]

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.

The interest in comprehensive privacy legislation has been steadily increasing at the federal level over the past few years. In the absence of comprehensive federal legislation, privacy law has proliferated at the state level. Three states — California, Nevada and Maine — enacted data privacy legislation during the 2018-2019 cycle, while similar legislation was introduced in at least 17 other states. Additionally, at least six states assembled joint task forces to consider data privacy issues.

In April, the Congressional Research Service released a report[8] 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 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 Sept. 23, the Committee on Commerce, Science and Transportation held a hearing.[9] In anticipation of that meeting, on Sept. 17, Republican senators introduced the Setting an American Framework to Ensure Data Access, Transparency, and Accountability, or SAFE Data, Act. In parallel, the Democrats have introduced the Consumer Online Privacy Rights Act, or COPRA.[10]

On Nov. 3, California voters overwhelmingly voted to enact Proposition 24, the California Privacy Rights Act, or CPRA, a new ballot measure that updates the California Consumer Privacy Act. The CPRA pushes the state already stringent requirements even further ahead of the rest of America when it comes to data privacy legislation. Proposition 24's passage adds to California's reputation as the state that pioneers progressive privacy laws that the rest of the country later adopts and becomes a major consideration in terms of potential federal legislation.

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.

The proposed SAFE DATA Act would broadly preempt state privacy laws — with significant impacts, to say the least, on privacy litigation — and, even if it passes the Senate, the expectation is that it will struggle to gain support in the house as the California representation is unlikely to support a bill that, in practice, will reduce the rights of California residents particularly since those rights were enacted through a ballot initiative that received the overwhelming support of their constituents.

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.

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.

Of course, it is possible that federal privacy legislation will continue to remain in limbo.

It would be an understatement to declare that national data privacy legislation, if enacted, has the potential to completely revolutionize data privacy litigation. At the moment, there is a patchwork of state laws — with California, New York and Illinois among some of the states with privacy laws having broad impact — as well as other industry-specific laws at the federal level for health care, financial institutions, consumer credit and others.

Of the states with privacy laws on the books, including in the context of data breaches, some lack a private right of action and may only be enforced by the state attorneys general. Accordingly, under the current regime, the privacy rights of individuals, including the right to seek vindication of their privacy rights in court, vary depending on residency.

If a federal privacy law is passed that preempts existing state laws, it may increase the rights of consumers and he correlated obligations of organizations who live in states that currently do not provide comprehensive privacy protections.

However, it would also displace the various state laws that have supported the rapid expansion of data privacy litigation in recent years potentially reducing the rights afforded to individuals who live in states that, like California, currently offer strong protections.

On the other hand, if a federal privacy law does not preempt existing state laws, it will increase the complexity of the existing patchwork of legal requirements and, potentially, allow for overlapping federal and state fines in the event of violations.

If the federal law does not allow for a private cause of action, its effectiveness enforcement is likely to be left to federal and state agencies which will require additional funding to effectively policy its application. If it does allow for a private cause of action, it will fuel the already active litigation landscape and potentially double existing exposure by adding federal causes of action to existing state requirements unless the private right of action is coupled with some form of preemption

In any event, large numbers of entities would find themselves having to address a new area of regulatory and litigation risk if a federal privacy bill is enacted.

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 and push up the already steep fines.

Increased FTC 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.[11] Accordingly, with an increase in enforcement, the data privacy landscape for suits involving private parties may also shift.

In addition, if a federal privacy bill is enacted during the Biden administration, it is expected that the FTC will take the main role in terms of enforcement and rulemaking, which will require additional funding for the agency and potentially an update of its rulemaking process, which is currently extremely onerous.

Lydia de la Torre and Glenn Brown are of counsel, and Kristin Bryan is a senior associate, at Squire Patton Boggs LLP.

Squire Patton associate Aaron Garavaglia contributed to this article.

[1] Privacy on the Go: Recommendations for the Mobile Ecosystem at https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/privacy_on_the_go.pdf.

[2] Joint Statement on Principles at https://oag.ca.gov/system/files/attachments/press_releases/n2630_signed_agreement.pdf.

[3] Section 702 at https://www.eff.org/702-spying.

[4] E.O. 12333 at https://www.archives.gov/federal-register/codification/executive-order/12333.html.

[5] PPD-28 at https://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities.

[6] S. 3663 – The COVID-19 Consumer Data Protection Act of 2020 at https://www.congress.gov/bill/116th-congress/senate-bill/3663?q=%7B%22search%22%3A%5B%22COVID-19+Consumer+Data+Protection+Act+of+2020%22%5D%7D&s=1&r=1.

[7] H.R. 6866 – The Public Health Emergency Privacy Act at https://www.congress.gov/bill/116th-congress/house-bill/6866?q=%7B%22search%22%3A%5B%22Public+Health+Emergency+Privacy+Act%22%5D%7D&s=2&r=1.

[8] Report at https://crsreports.congress.gov/product/pdf/LSB/LSB10441.

[9] Revisiting the Need for Federal Data Privacy Legislation at http://team.ssd.com/dept/bdm/department/Communications/Forms/AllItems.aspx?RootFolder=%2Fdept%2Fbdm%2FDepartment%2FCommunications%2FMedia%20Activity&FolderCTID=0x01200073EB95DB97A5BE49B87DB844781E5D4B&View=%7bFF7EB409-79CD-45D5-A2EB-D212BA92ABD7%7d.

[10] Consumer Online Privacy Rights Act at https://www.congress.gov/bill/116th-congress/senate-bill/2968/text.

[11] Perdue v. Hy-Vee, Inc., 455 F. Supp. 3d 749, 760-61 (C.D. Ill. 2020).