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

Biden Term Could Spell Sanctions, Boost Data Transfer Deal

By **Ben Kochman and Allison Grande**

Law360 (November 8, 2020, 5:26 PM EST) -- Joe Biden's presidency could lead to tougher sanctions for state-backed actors who target the U.S. with cyberattacks and carve out an easier path for a key trans-Atlantic data transfer deal, industry experts say.

The next four years are also likely to feature stronger privacy enforcement by the Federal Trade Commission and consistent messaging from the White House about cybersecurity threats, as well as enhanced cooperation with other countries on those issues.

Biden won the presidency Saturday with projected victories in Pennsylvania and Nevada, and while President Donald Trump is continuing to fight the results in court, the former vice president said he was moving forward with his transition plans so he would be ready to hit the ground running on Inauguration Day in January.

Here's a breakdown of some major privacy and cybersecurity policies that the president-elect and his administration could implement when he takes office in January.

Stiffer Sanctions for Cyberattacks

A Biden Justice Department is expected to continue the trend of calling out adversaries for destructive cyberattacks, and it's possible "name and shame" indictments of state-backed attackers will more often be accompanied by deeper punishments such as economic sanctions.

In a July blog post, Biden vowed to use "all appropriate instruments of national power and make full use of my executive authority to impose substantial and lasting costs on state perpetrators" who interfere in U.S. elections. Punishments could include financial sanctions, asset freezes or the mounting of retaliatory cyberattacks, he wrote.

The Justice Department under Trump has accused state-backed actors of a series of headline-grabbing attacks, including last month, when authorities charged six Russians with some of the most destructive cybercrimes ever, including the 2017 NotPetya malware attack that targeted Ukraine's power grid but ended up infecting computers worldwide — including at BigLaw giant DLA Piper. That attack caused roughly $10 billion in damage.

Some critics, including Democrats in Congress, have called for the Treasury Department to take

the further step of issuing economic sanctions on the purported Russian military officers accused of carrying out the attack.

Trump's Treasury Department did sometimes issue sanctions alongside DOJ indictments, including for two Russian nationals accused of leading a decadelong, international hacking and bank fraud scheme that facilitated the theft of more than $100 million.

But some industry attorneys, including those who served in the Obama administration, have called for U.S. officials to more consistently issue sanctions as part of a multi-pronged deterrence strategy.

"The Justice Department under Trump has made great strides in investigating nation-state cyber activity, but additional costs need to be imposed," said Ed McAndrew, a partner at DLA Piper and former federal cybercrime prosecutor.

"I think the Biden administration would be more aggressive in imposing financial costs to malicious cyber activity, and specifically with sanctions," McAndrew added.

EU Privacy Shield Pact

The European Union's highest court shook up the trans-Atlantic data transfer landscape in July when it invalidated the popular Privacy Shield that more than 5,300 companies relied on to legally move personal data from the EU to the U.S.

The European Commission and U.S. Commerce Department quickly vowed to negotiate a replacement, and Biden's administration is likely to make restoring this pathway a priority.

"In order for Privacy Shield to be renegotiated, the U.S. must have an administration that is interested in enhancing global trade and is seeking to facilitate global interoperability among the privacy laws," said Miriam H. Wugmeister, partner and co-chair of Morrison & Foerster LLP's privacy and data security practice. "While the Biden administration will have many priorities, enabling the exchange of information between the EU and the U.S. will likely be on the list."

The European Court of Justice cited concerns over the ability of U.S. intelligence authorities to gain unfettered access to EU citizens' transferred data as the primary concern driving its decision to strike down the pact.

Crafting a new arrangement will require the U.S. to assuage these surveillance worries, and a Biden administration is likely to receive a stronger reception than its predecessor to these efforts.

"Under a Biden administration, there's likely to be a lot more willingness to try to have the government reassume the role as a trusted country and more commitment to various rules that will give the EU government much more comfort," said Sherrese Smith, vice chair of the data privacy and cybersecurity practice at Paul Hastings LLP. "Everyone understands that some data transfer solution needs to be put in place and that our global economy depends on it."

More Focus on Russia

As president, Joe Biden will likely follow the lead of law enforcement and intelligence agencies in calling out Russia for interference in U.S. elections, industry attorneys say.

"Despite the exposure of Russia's malign activities by the U.S. intelligence community, law enforcement agencies and bipartisan congressional committees, the Kremlin has not halted its efforts to interfere in our democracy," Biden warned in his July blog post.

Trump, by contrast, has repeatedly contradicted the intelligence community's conclusions about Kremlin-backed malicious cyber activity, most notably that Russian military hackers interfered in the 2016 U.S. elections by hacking into Democratic National Committee servers and stealing emails that were later leaked and published.

Perhaps most strikingly, Trump issued a rebuke to the intelligence community in 2018, when, after meeting with Russian leader Vladimir Putin, he attempted to cast doubt on a unanimous assessment from the FBI, CIA, National Security Agency and Office of the Director of National Intelligence that Russia was behind the attacks.

"I have President Putin, he just said it's not Russia. I will say this: I don't see any reason why it would be," Trump said after meeting with Putin in Helsinki, Finland.

Trump also appeared several times to downplay the threat of cybersecurity in general during his presidency, despite the U.S. Department of Homeland Security and FBI's consistent warnings that cybercriminals, including those backed by nation-states, are targeting hospitals, local governments and businesses of all sizes.

Most recently, at an Oct. 19 rally in Tucson, Arizona, Trump told the crowd, "Nobody gets hacked," in a puzzling comment made while referencing C-SPAN political editor Steve Scully, who admitted to lying about hackers taking over his Twitter feed.

Biden, a career elected official who first joined the U.S. Senate in 1972, will be more likely to echo the findings of U.S. authorities on such issues, industry attorneys told Law360.

"I think that the Biden administration would likely be much more open and level with the American people with respect to what the cybersecurity vulnerabilities are," said Aloke Chakravarty, a veteran former federal prosecutor and now partner at Snell & Wilmer LLP.

"The message would be part of the strategy rather than having most of the cybersecurity work happen behind closed doors," he added.

Enhanced FTC Privacy Enforcement

The Federal Trade Commission has continued to aggressively pursue privacy and punish data security missteps during President Donald Trump's tenure. Last year alone, it notched a record $5 billion settlement against Facebook for a string of data misuse scandals and set a high water mark for children's privacy violations with a $136 million fine against Google's YouTube subsidiary.

While Republican Chairman Joe Simons' term isn't set to expire until September 2024, agency leaders typically step aside when a new party wins the presidency. And a shift to a 3-2 Democratic majority would only serve to escalate the agency's already robust enforcement efforts, according to attorneys.

"Democrats have historically taken a more active enforcement role with respect to consumer

protection, including privacy enforcement, and I expect we would see the same under a Biden administration," said Julie O'Neill, a partner in Morrison & Foerster LLP's privacy and data security group.

In recent years, the commission has taken a more cautious approach in pursuing allegedly unfair business practice under Section 5 of the FTC Act, particularly in light of an Eleventh Circuit ruling from June 2018 that threw out an order against LabMD due to a lack of specifics about how proposed data security changes should be implemented.

"We could see the FTC [under a Biden administration] try to push back against that requirement" that these orders need to include more specifics, said Al Saikali, chair of the data security and privacy group at Shook Hardy & Bacon LLP. He said he expected to see an uptick in enforcement actions applying the unfairness prong to data breaches in particular.

A Democrat-led commission is also likely to embrace a broader view of what types of consumer harm are necessary to support its enforcement actions, attorneys say.

"Under President Trump, the FTC has been focused on cases where there was actual, tangible consumer harm," noted Brenda Sharton, co-chair of the global privacy and cybersecurity practice at Dechert LLP. "In the coming years, I would expect a return to a more expansive view of potential companies' adherence to their own policies and privacy programs and cases involving those types of violations."

At the tail end of the last Democratic administration, the FTC reached a settlement with Vizio over claims that it tracked users' viewing habits without their consent. The deal drew a rebuke from the Republican Commissioner Maureen Ohlhausen — who had just been elevated to acting chairman following the 2016 election — for broadly defining what qualifies as sensitive information and consumer harm.

"That enforcement action seemed to be a seed that was planted for the next Democratic administration of the FTC to use as a stepping stone to make expansions such as finding that all web-surfing behavior should be treated as sensitive information that requires opt-in consent," said D. Reed Freeman Jr., a partner at Venable LLP and former FTC staff attorney.

Freeman noted that the current Republican-led FTC is asking more questions, requesting more documents and holding more hearings during its investigations than he's ever seen, and that he wouldn't expect a commission with Democrats at the helm to "be any less aggressive."

There's also a solid chance Congress over the next four years will enact federal privacy legislation that will hand the commission enhanced rulemaking and fining authority for alleged privacy violations, attorneys noted.

"We seem to be closer than we have been before to getting comprehensive consumer privacy legislation, with both the chair and ranking member of the Senate Commerce Committee having released their own substantive privacy drafts during the past year," said Howard Waltzman, a partner at Mayer Brown LLP.

While the parties continue to disagree over whether a federal framework should preempt more stringent state laws and allow consumers to bring lawsuits, "the overall impetus for privacy reform remains," and "there seems to be a bipartisan consensus that while the FTC is a really good privacy

enforcer, they can be even more effective if they have enhanced enforcement authority," Waltzman added.

The Biden administration is likely to be a strong supporter of this initiative, particularly given that during his tenure as vice president, the Obama administration put forth its own white paper proposing a "bill of rights" for protecting consumers' online privacy.

"The impetus for comprehensive privacy legislation under the Biden administration is likely to come from the White House and the U.S. Department of Commerce, where there will be a focus on privacy regulatory policy and a desire to build on the foundation established by the Obama administration's privacy bill of rights," said Alan Charles Raul, the leader of the privacy and cybersecurity practice at Sidley Austin LLP.

No More 'America First' on Cyber Issues

One move Biden is likely to make early in his administration is to restore the role of White House cybersecurity coordinator, tasked with organizing the country's response to cyberthreats, industry attorneys agreed.

The Trump administration axed the position, created by former President Obama, in May 2018, leaving empty what some cybersecurity experts have described as a key post for collaborating with foreign allies on digital threats.

"I think that Biden is an institutionalist and that he will value that role and probably empower it, in part to better engage with our foreign partners," said Chakravarty.

A smoother relationship with the U.S.' allies could lead to discussions at some point in the next four years about international standards for cybersecurity and for cyber warfare, including the thorny question of when and in what circumstances countries should mount offensive cyberattacks.

Both the Biden campaign and Trump administration have endorsed authorizing offensive cyber actions, a strategy that some experts have said carries with it serious risks, as criminal hackers or U.S. adversaries could repurpose weapons released into the digital ecosystem for their own malicious ends.

Cybercriminals in May 2017 used a Microsoft Windows software flaw first discovered by the NSA to launch the global cyberattack known as WannaCry, for example.

A President Biden would be wise, data security attorneys say, to be in constant dialogue with international allies about how best to handle the offensive cyberattack issue and other evolving cybersecurity threats to the country.

"When it comes to cyber activity, America first and America alone is not going to work," McAndrew said.

--Editing by Philip Shea.