Wilson says pandemic underscores need to establish privacy rules for 'Big Tech'

Official Statement | 18 May 20 | 20:50 GMT

In Brief

MLex Summary: Christine Wilson, a Republican member of the US Federal Trade Commission said in the full text of a media opinion piece shared with MLex that the Covid-19 pandemic underscores the need for comprehensive federal privacy legislation. "Covid-19 presents new and complex choices about tech companies' collection, dissemination and application of users' data. Rather than take chances on companies' ability to intuit the appropriate course, Congress should provide the guardrails. The health, privacy, and Fourth Amendment rights of Americans are at stake," Wilson wrote.

Text of Wilson op-ed follows in full:

Covid-19 Underscores Need for Comprehensive Privacy Legislation

By Christine Wilson

After years of vilifying pharmaceutical and technology companies, the pandemic-stricken globe now looks to them with hope. The role of Big Pharma is obvious: find treatments, cures and vaccines. The role of Big Tech is less clear – and requires guidance from Congress.

Many view technology, in the form of comprehensive contact tracing, as key to safely reopening our economy and recovering a sense of normality in our social interactions. But the pandemic has not erased concerns about tech companies' handling of consumer privacy. Indeed, it heightens those concerns, as government omnipotence combines with private sector omniscience.

As a Commissioner at the Federal Trade Commission, I am familiar with Big Tech and Big Pharma. I voted to sue Facebook and YouTube for privacy violations, and Martin Shkreli for unlawful conduct that increased drug prices astronomically. While enforcing the competition and consumer protection laws is central to my FTC role, I have also sworn to support and defend the Constitution.

The Fourth Amendment protects American citizens from government overreach, but the “reasonable expectation of privacy” test applied in Fourth Amendment cases links the arenas of government action and commercial data collection. In the commercial arena, consumers have become accustomed to surrendering extensive data through their daily use of phones, computers, digital assistants and other connected devices. This phenomenon has inevitable spillover effects in the legal arena – if citizens know and accept that nothing is private, then they have no reasonable expectation of privacy, and the Fourth Amendment gets eviscerated.

The Supreme Court has limited the warrantless tracking of Americans through GPS devices placed on their cars and through cellphone data voluntarily handed over by mobile network operators. GPS data has proven helpful in fighting the spread of Covid-19; it also could be used to piece together evidence of violations of stay-at-home orders. As Chief Justice John Roberts wrote in Carpenter, “With access to [cell-site location information], the government can now travel back in time to retrace a person’s whereabouts… Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years.”

History has taught us repeatedly that sweeping security powers granted to governments during an emergency persist long after the crisis has abated. Just last week [May 13], the Senate refused to prohibit the federal government from obtaining warrantless access to third-party data collection of Americans’ web browser and search history information. This development further undermines any expectation of privacy that Americans would otherwise have in their data. As Slovak lawmaker Tomas Valasek has said, “It doesn’t just take the despots and the illiberals of this world… to wreak damage.”

Several governments around the world, from Taiwan to Poland, have required people infected with or exposed to the novel coronavirus to download smartphone apps to facilitate enforcement of quarantine restrictions.

State action has not gone entirely unchallenged; Israel’s Supreme Court ruled late last month that the country’s parliament must pass legislation for the internal security service to use individuals’ mobile data for contact tracing. “The state’s choice to use its preventative security service for monitoring those who wish it no harm, without their consent, raises great difficulties and a suitable alternative, compatible with the principles of privacy, must be found,” the court said. “We must take every precaution to ensure that the extraordinary developments with which we are dealing these days do not put us on a slippery slope in which extraordinary and harmful toolsare used without justification.”

The UK government on May 4 introduced the National Health Service’s home-grown contacttracing app to the Isle of Wight. Mobile device users choose whether to install the app and to inform it if they have symptoms or a diagnosis of Covid-19. The NHS COVID-19 app relies on Bluetooth technology to determine if one user has been in close proximity for a certain amount of time with another user who has reported possible or confirmed infection.

The U.S. has not yet taken similar steps in its fight against COVID-19, but tech companies are collecting relevant data. As part of its “Data for Good” initiative, Facebook has partnered with universities to distribute a symptom survey to users, with the company’s knowledge of their demographics used to correct for sample bias. Apple and Google are introducing interoperability between iOS and Android devices to support decentralized contact tracing apps from

public health authorities. But a Washington Post poll found that half of the polled smartphone users do not trust tech companies to protect the anonymity of app users who test positive for Covid-19. Voluntary measures will fail if a critical mass of Americans do not participate – which should incentivize both the public and private sectors to demonstrate their trustworthiness.

The FTC recommended that Congress pass comprehensive federal privacy legislation in its first major report on privacy in 2012. I have echoed this long-standing call – in testimony before the US Senate and House, in public speeches, and in articles. The FTC recently confronted the significant limits to its authority in bringing its enforcement action against Facebook. As the district court noted when entering the consent order, “these concerns are largely for Congress.”

Congress’s failure to pass legislation is mystifying: in a toxic political environment infused with strident partisanship, the need for a comprehensive privacy regime is one issue on which both parties and all stakeholders agree. In recent months, Congressional drafts were released with fanfare. None was perfect, but for too long, on data security and privacy, we have let the perfect be the enemy of the good.

In the absence of comprehensive privacy legislation, coronavirus researchers have justified using mobile device data provided by companies by citing prior customer consent. But the assumption that consumers have given informed consent – particularly for quarantine compliance monitoring during a pandemic – is undermined by studies showing users have little understanding of the actual scope of data collection and deployment. Moreover, click-through consent does not end the conversation about privacy rights. Lengthy fine-print disclosures are insufficient, especially if assent is framed as altruism to aid public health.

To address at least the current pandemic, five Republican senators on May 7 introduced coronavirus-specific privacy legislation. A week later, two Democratic senators offered their own version of such a law. These bills agree on some core issues, including the need to obtain affirmative express consent rather than infer consent from inaction; the obligation to provide an effective way to revoke consent; and enforcement by the FTC under its authority against unfair or deceptive practices and by state attorneys general.

But the proposals diverge on some of the same points that previously held up passage of a baseline privacy law: whether the federal law preempts state law; whether consumers should have a private right of action to obtain damages; and whether this right can be subject to binding arbitration. That these bills are not bipartisan does not inspire confidence in their likelihood of getting passed. In any event, a narrow privacy bill dealing only with the conditions of the pandemic, which we pray will soon pass, is far less preferable than comprehensive legislation that will provide broad guidance for years to come.

Covid-19 presents new and complex choices about tech companies’ collection, dissemination and application of users’ data. Rather than take chances on companies’ ability to intuit the appropriate course, Congress should provide the guardrails. The health, privacy, and Fourth Amendment rights of Americans are at stake.

Tags

Subjects: Data Security
Industries: Digital Industries, Health, Information Technology, Pharmaceutical
Regulators/Courts: Other Courts, US Courts
Jurisdictions: North America, USA
Issuing entity(ies): Christine Wilson
Document Type: Statement

Related case file(s)

Data Security - Covid-19 (US)