Key Privacy Developments In Trump's First 150 Days

By **Jaipat S. Jain**

Law360, New York (June 23, 2017, 10:18 PM EDT) -- This article tracks chronologically certain key privacy law developments during the first 150 days of the Trump administration.

Jaipat S. Jain

Executive Order Withdrawing Privacy Act Protections for non-U.S. individuals

Within days of assuming office, President Donald Trump issued an executive order titled "Enhancing Public Safety in the Interior of the United States" with a view to remove constraints on Federal agencies engaged in executing U.S. immigration laws.[1] As part of the executive order, the president directed federal agencies to exclude from the protections of the Privacy Act of 1974, as amended,[2] personally identifiably information of individuals who are not U.S. citizens or lawful permanent residents.

The Privacy Act seeks to balance the government's need to maintain information about U.S. citizens and lawful permanent residents with the rights of U.S. individuals to be protected against unwarranted invasions of their privacy by federal agencies. It set forth an enforceable code of conduct with respect to information that may be collected, maintained, used or disseminated by a federal agency and the conditions under which disclosure may be made by it without prior written consent of the concerned individual. Further, it provides U.S. individuals the rights of access to and correction of records maintained on them by federal agencies. Individuals covered by the Privacy Act have the right to bring legal action against a federal agency for breach of the protections afforded by the act.

The Privacy Act protects only U.S. individuals. However, shortly after its enactment, the federal agency charged with the oversight of its implementation, the U.S. Office of Management and Budget, issued comprehensive guidelines under which it encouraged federal agencies to treat PII of all individuals, regardless of immigration status, as "if they were, in their entirety, subject to the Act" except that non-U.S. individuals did not have the right of judicial review accorded U.S. individuals.[3]

The U.S. Department of Homeland Security, the principal agency charged with implementation of the immigration laws, followed the OMB guidance as did other federal agencies.[4] In 2007, the DHS issued policy guidance under which it explicitly extended certain Privacy Act protections to visitors and other aliens in the United States.[5] The decision was partly motivated by the inherent difficulty in tracking an individual's current immigration status, given that it was amenable to change as a result of naturalization or adjustment.

Over the years, federal agencies have collected information about foreign students, workers, asylum seekers and undocumented people such as those known as "dreamers," who were brought to the United States as children. The Obama administration, for example, collected information about "dreamers" with the goal of helping them avoid deportation through its 2012 Deferred Action for Childhood Arrivals program. Following the executive order, advocates for DACA stopped recommending "dreamers" to apply under DACA or to share information about themselves with federal agencies.[6]

Following the issuance of the executive order, the DHS also revised its 2007 policy by issuing DHS Privacy Policy Guidance Memorandum No. 2017-01.[7] Under the 2017 policy, while PII of all individuals will continue to be obtained and handled in accordance with Fair Information Practice Principles, only U.S. individuals will be accorded access and other protections of the Privacy Act and other applicable laws such as the Federal Records Act of 1950[8] and the E-Governance Act of 2002.[9]

The executive order marks a significant shift in long-standing privacy and data security policy and practice of the U.S. However, it has certain limitations. First, neither it nor the 2017 policy forecloses use of the Freedom of Information Act[10] by any person, including non-U.S. individuals, for obtaining access to records not exempt under FOIA. Second, the executive order does not mandate the collection of any new or additional data specifically targeted at determining citizenship status when not otherwise required under any existing law, a point also noted by the DHS in the 2017 policy.[11] Finally, because the extension of Privacy Act protections to certain citizens of the European Union following the invalidation of the U.S.-EU Safe Harbor was done pursuant to a statute, the Judicial Redress Act of 2015 (the "JRA"),[12] the executive order should not affect its operations. Note here that the enactment of the JRA was a condition for the European Union to establish the Privacy Shield; any actual or perceived weakening of the JRA would adversely affect its adequacy as a protocol for flow of EU data into the U.S.

Broadband Privacy Rules Gutted

In rare exercise of its authority under the Congressional Review Act of 1996, as amended,[13] to disapprove rules adopted by federal agencies within 60 legislative days of assuming office, the 115th Congress disapproved 11 rules,[14] including the broadband privacy rules adopted six months earlier by the Federal Communications Commission.[15]

The broadband privacy rules[16] sought to apply to broadband internet service providers the privacy standards similar to those applicable for nearly two decades to telecommunications common carriers under the Communications Act of 1934, as amended.[17] Under Section 222 of Title II of that act, telecommunications carriers have a duty to protect the confidentiality of proprietary information of customers and not disclose such information to any person (other than as permitted under the act in connection with providing services to the customer) without the prior written consent of the customer. Broadband internet service providers were treated as "information service" providers exempt from regulation under the Communications Act. Oversight of their privacy policies and practices rested solely with the Federal Trade Commissionunder its unfair and deceptive acts and trade practices authority [18]

The FCC sought to wrest control from the FTC over the regulation of broadband service providers. Its previous attempts to do so, however, failed for want of express statutory authority.[19] In 2015, in its third such attempt, it succeeded when its Open Internet Order[20] was upheld by the Federal Circuit.[21] Under that order, the FCC reclassified broadband service as a telecommunications service subject to Title II of the

Communications Act. That success paved way for it to propose the broadband privacy rules in 2016.

In proposing the broadband privacy rules in 2016, the FCC noted that broadband service providers had access to vast amounts of information about their customers including when they were online, where they were physically located, how long they stayed online, what devices they used, what websites they visited, and what applications they used. Besides, they had access to personal information of each of their customers. The broadband provider, according to FCC, sat at a privileged place in the network as a "gatekeeper" between the customer and the rest of the internet, uniquely placed to collect and use "an unprecedented breadth" of electronic personal information of its customers with little or no regulation over their privacy practices.[22]

Days before it issued its notice of proposed rule-making in March 2016, the FCC entered into a settlement with Cellco Partnership d/b/a/ Verizon Wireless[23] following its investigation into whether Verizon failed to disclose to consumers that it was inserting a unique, nonremovable, fool-proof "perma cookie" into their internet activities. Verizon obtained several patents for unique identifier header "(UIDH")[24] and launched targeted advertising programs called Verizon Selects and Relevant Mobile Advertising that were offered to advertisers on the promise of their ability to associate UIDH with customers' proprietary network information as well as other customer demographic and interest information so that advertisers could more precisely target advertising content to specific customers.[25]

According to the settlement, FCC's investigation found that although Verizon began inserting UIDH into consumers' internet traffic as early as December 2012, it did not disclose the practice until October 2014. It was not until March 2015, over two years later, that Verizon first updated its privacy policy to include information about UIDH. The FCC's investigation also found that at least one of Verizon advertising partners used UIDH for unauthorized purposes to circumvent consumers' privacy choices by restoring deleted cookies.

News reports indicated that at around the time Verizon was exploiting UIDH, at least one other major broadband service provider, AT&T, acknowledged having experimented with similar technologies and marketing programs.[26] Note here that the Verizon settlement came on the heels on a record $7.4 million settlement a Verizon affiliate entered into with the FCC for its failure to notify phone customers of their privacy rights prior to conducting thousands of marketing campaigns.[27]

The broadband privacy rules sought to regulate the privacy and data security policies and practices of broadband service providers. While issuing the rules, the FCC stated that its objective was to ensure that broadband customers had choice, greater transparency and strong security protections for their personal information collected by broadband internet service providers. According to the FCC, the rules were designed to provide consumers more control over the use of their personal information together with a framework of consent required for broadband service providers to use and share customers' personal information that was calibrated to the sensitivity of the information. The FCC noted that its approach was consistent with other privacy frameworks, including the FTC's and the administration's Consumer Privacy Bill of Rights.

The broadband privacy rules were vehemently opposed by large internet service providers and associations representing advertising companies. In addition to filing review petitions before the Federal Circuit, these organizations and associations lobbied Congress for their rollback.[28]

On April 3, 2017, the president signed the congressional resolution disapproving the rules. The next day, the new chairman of the FCC, Ajit Pai, and the acting chair of the FTC, Maureen Ohlhausen, wrote a joint op-ed piece for the Washington Post.[29] In it they stated: "Let's set the record straight: First, despite hyperventilating headlines, Internet service providers have never planned to sell your individual browsing history to third parties. That's simply not how online advertising works. And doing so would violate ISPs' privacy promises. Second, Congress' decision last week didn't remove existing privacy protections; it simply cleared the way for us [FCC and FTC] to work together to reinstate a rational and effective system for protecting consumer privacy."[30]

Two other developments in this regard are notable. First, the FCC has issued a notice of proposed rule-making seeking to roll back the 2015 Open Internet Order and return to the "light-touch regulatory framework" that existed prior to that order.[31] Second, 11 Republican senators have introduced a bill to take away the FCC's regulatory authority that allowed it to make net neutrality rules.[32]

Broadband Privacy Legislation Proposed in 28 States

Following the rollback of the broadband privacy rules, bills have been introduced in at least 28 states, including three in New York, that seek to protect the privacy rights of customers in their state.[33]

Each of the three New York bills[34] seeks to impose an affirmative duty on internet service providers to keep customer data confidential, obtain customer consent before sharing sensitive personal information with any third party, and not penalize any customer who declines consent. One of the bills requires ISPs to provide customers with its privacy policy that includes the ISPs data collection and use practices, third-party relationships, purpose of data collection and the process for customers to exercise control over its personal information. Under one of the bills, breach of the provisions is a misdemeanor; in another, breach results in a civil penalty and the attorney general has a right to injunctive relief; and in the third, customers have a private cause of action against the ISPs. One of the bills also imposes data security obligations on the ISPs.

Ironically, the specter of multiple and varying state laws may compel the broadband service providers to lobby Congress to legislate and create a level playing field.

Privacy Shield Remains Under the Lens

The Congress and Trump administration will have more immediate pressure to act, however, from privacy and data protection authorities from the European Union. The U.S.-EU Privacy Shield, launched Aug. 1, 2016, and now self-certified by over 2,200 companies engaged in transatlantic data transfer, is due for annual review.

On April 6, 2017, the European Parliament adopted a strongly worded resolution deploring certain recent U.S. actions it perceived as adversely affecting the privacy and data protection rights of its citizens.[35] The resolution, among other things, deplored the rollback of broadband privacy rules, and noted with "great concern" that the Privacy and Civil Liberties Oversight Board charged with analyzing and reviewing counter-terrorism programs and policies, and ensuring that they adequately protected privacy and civil liberties, had lost its quorum on Jan. 7, 2017, and the president had not nominated any new board member.

It noted that the Privacy Shield did not prohibit the collection of bulk data for law enforcement purposes and expressed "alarm" over the revelation that Yahoo had conducted surveillance activities on emails upon request of the National Security Agency and the Federal Bureau of Investigation as late as 2015, that is, one year after Presidential Policy Directive 28[36] was adopted and during the negotiation of the EU-U.S. Privacy Shield. It called on the commission to take all necessary measures to ensure that the Privacy Shield afforded the protections to which EU citizens were entitled.

The Parliament's resolution echoes various other dissenters in the EU who have challenged the Privacy Shield, in court[37] and in other EU forums.[38] In its most recent plenary meeting held on June 7-8, 2017, the Article 29 Working Party, the body comprised of representative of data protection authorities of EU members, adopted a letter addressed to the commission in which it called on the commission to "ensure that the U.S. authorities are able to constructively answer concerns on the concrete enforcement of the Privacy Shield decision" during the September 2017 annual review.[39] It reserved the rights to write its own review report.

Privacy Genie Is Out of the Bottle

Whether it is legislative activism at the state level and efforts of broadband service providers to seek congressional intervention to preempt that, or the pressure from European Union and the businesses relying on the effective continuation of the Privacy Shield, the Trump administration will not be able to put the privacy genie back into a bottle. 2017 may well be one of the most momentous years yet in the area of privacy regulation in the United States.

Jaipat S. Jain is a partner at Lazare Potter & Giacovas LLP in New York. He chairs the Privacy Law Subcommittee of the Information Technology and Cyber Law Committee of the New York City Bar Association.

[1] Executive Order No. 13,768 dated Jan. 25, 2017. Available at https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

[2] 5 U.S.C. §552a.

[3] Circular A-108, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28951 (July 9, 1975).

[4] Examples for the Department of Justice include the following systems: Executive Office of Immigration Review Records (EOIR) Records, INTERPOL (USNCB) Records, and International Prisoner Transfer Case Files/ International Prisoner Transfer Tracking Records. Examples for the Department of State include Visa Records and Refugee Case Records.

[5] DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of

Information on Non-U.S. Persons, Memorandum No. 2007-1, as amended. Available at https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2007-1.pdf

[6] The advocacy group, Immigration Equality, for instance, prominently writes on its website: "At this time, Immigration Equality does not recommend that you file for DACA if you have never done so before." See http://www.immigrationequality.org/get-legal-help/our-legal-resources/path-to-status-in-the-u-s/daca-deferred-action-for-childhood-arrivals/

[7] DHS Privacy Policy Guidance Memorandum/ DHS Privacy Policy Regarding Collection, Use, Retention and Dissemination of Personally Identifiable Information, dated April 27, 2017. Available at https://www.dhs.gov/publication/dhs-privacy-policy-guidance-memorandum-2017-01.

[8] Pub. L. No. 81-754, 64 Stat. 585 (codified as amended in Chapters 21, 29, 31, and 33 of 44 U.S.C.).

[9] 44 U.S.C. §3501 note.

[10] 5 U.S.C. §552.

[11] 2017 policy, at 5.

[12] Pub. L. 114-126 of 2016, codified as 5 U.S.C. §552a note.

[13] Codified as 5 U.S.C. Chapter 8.

[14] Prior to 2017, Congress has exercised its authority to disapprove Federal agency rules only once by Pub. L. 107-5. See https://www.whitehouse.gov/the-press-office/2017/04/05/press-briefing-congressional-review-act

[15] Pub. L. 115-22 of 2017.

[16] Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, 47 CFR Subpart U, 64.2001 et seq., 81 Fed. Reg. 87,274 (December 2, 2016).

[17] 47 U.S.C. §151 et seq

[18] See 15 U.S.C. § 45(a)(1) (prohibiting unfair or deceptive acts or practices in or affecting commerce).

[19] See Comcast Corp. v. FCC, 600 F.3d 642 (D.C. Cir. 2010), and Verizon v. FCC, 740 F.3d 623 (D.C. Cir. 2014).

[20] In the Matter of Protecting and Promoting the Open Internet, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601 (2015) (Title II Order).

[21] United States Telecom Ass'n. v. F.C.C., 825 F.3d 674 (2016).

[22] See In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunication Services, WC Docket 16-106, adopted March 31, 2016. Available at: https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-39A1.pdf

[23] Available at https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf. See also http://webpolicy.org/2014/10/24/how-verizons-advertising-header-works/.

[24] See for instance U.S. Patent Nos. 8,832,436 B2; 8,763,101 B2; 9,264,430 B2. Appl. Nos. 0150312255; 20140380053; 20140325025; 20130318581 and 20130318346.

[25] See, for instance, https://vimeo.com/109847536 and https://vimeo.com/109846832.

[26] See "AT&T Says It's 'Testing' Unique Tracker on Customers' Smartphones, Forbes (Oct. 28, 2014), https://www.forbes.com/sites/kashmirhill/2014/10/28/att-says-its-testing-unkillable-tracker-on-customers-smartphones/.

[27] Copy of the settlement and consent decree is available at: https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1251A1.pdf

[28] Among those who filed review petitions were the United States Telecom Association, American Cable Association, NCTA – The Internet & Television Association, Competitive Carriers Association, and various national advertising associations.

[29] Available at: https://www.washingtonpost.com/opinions/no-republicans-didnt-just-strip-away-your-internet-privacy-rights/2017/04/04/73e6d500-18ab-11e7-9887-1a5314b56a08_story.html?utm_term=.185e1f03e800

[30] Id., paragraph 2.

[31] Restoring Internet Freedom, Notice of Proposed Rule Making, April 27, 2017.

[32] Restoring Internet Freedom Act, Bill S.993, 115th Cong. May 1, 2017.

[33] Will US States Pick Up The Slack Left By Trump-Era Policy Reversals?, Angelique Carson, International Ass'n. of Privacy Professionals, June 13, 2017. Available at https://iapp.org/news/a/will-u-s-states-pick-up-the-slack-left-by-trump-era-policy-reversals/.

[34] A-07495A, A-07236, and A-07191A.

[35] Adequacy of the protection afforded by the EU-US privacy Shield, Resolution of the European Parliament, April 6, 2017. For text, see: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0131+0+DOC+XML+V0//EN&language=EN

[36] The Presidential Policy Directive, Signals Intelligence Activities, PPD-28, Jan. 17, 2014 constitutes Presidential policy instruction governing the safeguarding of personal information collected from signals intelligence activities. Available at https://www.dhs.gov/publication/presidential-policy-directive-28-ppd-28-signals-intelligence-activities-0

[37] See, for instance, Digital Rights Ireland v. Commission, Case T-670/16, available at: http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2016.410.01.0026.01.ENG; and La Quadrature du Net v. Commission, Case No. T-738/16, available at: http://eur-lex.europa.eu/legal-content/it/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ITA

[38] See, for instance, the various statements of the EU Article 29 Working Party available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

[39] Id., for a copy of the letter.
