Securitization and Surveillance in 2019

Present Threats to Our Privacy and Civil Liberties

Securitization is the combined oversimplification and exaggeration of complex national security-related policy concerns. In recent decades, the U.S. government has exploited sociopolitical anxieties to justify a disproportionate response to terrorism at home and abroad. As a securitized community, Arab Americans face discriminatory national security policies and inordinate threats to constitutional rights, particularly those stemming from the First and Fourth Amendments.

Excessive surveillance of targeted communities, including Arab Americans and American Muslims, is one example of securitization in the domestic sphere. While the U.S. government has justified serious transgressions of constitutional rights in defense of national security throughout its history,[1] this dynamic has only intensified since the tragic terrorist attacks on 9/11. National security frameworks, new surveillance technologies, and dragnet immigration policies have each posed distinct challenges to the civil rights and civil liberties of securitized communities.

Section 215 and the USA Freedom Act

After the terrorist attacks on 9/11, Congress authorized new national security measures that increased the federal government's mass surveillance capabilities beyond the two existing mechanisms, the Foreign Intelligence Surveillance Act (FISA) of 1978 and Executive Order 12333.[2] Both the USA PATRIOT Act of 2001 and the FISA Amendments Act (FAA) of 2008 authorized further incursions into Americans' privacy. In accordance with FISA, the Foreign Intelligence Surveillance Court (FISA Court) reviews individual requests from the U.S. government to conduct surveillance relating to "foreign intelligence" within the United States.[3] Section 215 of the USA Patriot Act of 2001 expanded FISA Court-authorized surveillance to include "bulk collection" of Americans' communications and other data.[4] Section 215 created a secret law through FISA in which the government could collect any data "relevant" to terrorism.[5]

In 2013, the whistleblower Edward Snowden disclosed the National Security Agency's (NSA) bulk collection of Americans' call records, or telephony metadata, under Section 215 of the Patriot Act.[6] Following this shocking abuse of power, Section 215 and other provisions of the USA Patriot Act expired on June 1, 2015. However, Congress passed the USA Freedom Act the next day, which restored Section 215 and others in a modified form.[7] The USA Freedom Act prohibited bulk collection of all American's telephony metadata, requiring increased accountability and transparency of U.S. government surveillance activities, while extending certain provisions of the Patriot Act to December 2019.[8]

Section 215 authorities will expire with the sunset of the USA Freedom Act on December 15, 2019.[9] While the Freedom Act made significant advances in protecting the constitutional right to privacy, those reforms were not sufficient. The opaque and overbroad nature of Section 215 jeopardizes the privacy and civil liberties of Americans. It is unclear if Section 215 has any procedures to prevent discrimination, which is concerning given the government's history of wrongly surveilling individuals and groups based on their race,

1600 K St, NW Suite 601 | Washington, DC 20006 | (202) 429-9210 | www.aaiusa.org

religion, or political views.[10] More transparency is also needed regarding how often protected First Amendment activities are surveilled under Section 215. Although the Freedom Act was intended to prevent bulk collection under the Patriot Act, evidence suggests that it has not achieved this goal. In 2017, the government received 534 million records of Americans' phone calls based on only 40 surveillance targets.[11]

Section 215 is ineffective in its mission to improve national security. As of 2014, Section 215 surveillance had not contributed uniquely to preventing a single terrorist attack.[12] There is no evidence to suggest that the changes made in 2015 have increased its effectiveness. Rather, since 2018, the NSA has been deleting call detail records due to "technical irregularities."[13] News reports suggest that the NSA has halted its collection of telephony metadata altogether, however, the NSA has not confirmed this and still has legal authority under Section 215.[14] With rapid technological advancement has come the increased use of encrypted messaging. The collection of call data appears to be not only ineffective, but also irrelevant.

New Surveillance Technology

Technological advances have expanded the government's surveillance toolbox. The nation's law enforcement agencies have increased their use of drones, which pose a great threat to privacy rights if not properly regulated. Drones may be equipped with facial recognition software, infrared technology, and speakers that can monitor personal conversations. Capable of mass tracking of vehicles and people, drones can also be small enough to go unnoticed in private spaces.[15] State and local police departments can also track individuals' locations by obtaining data from mobile carriers.[16] Law enforcement has access to automatic license plate readers: small high-speed cameras that can be mounted on police cars and objects like road signs. These readers capture and collect the license plate number, date, time, and location of every scan, and store this information in databases, often indefinitely.[17] State motor vehicle agencies have high-quality photographs of most citizens, which can be used to train facial recognition technology to create yet another method of surveillance.[18]

Securitized communities are particularly threatened by unregulated surveillance technologies. This is evidenced by the current and proposed use of surveillance technology at our borders. U.S. Customs and Border Protection (CBP) officers use the technologies described above, in addition to other methods of surveillance. The Department of Homeland Security (DHS) has created a security and tracking program known as the Automated Targeting System (ATS). ATS assigns algorithm-generated risk assessment scores to travelers who cross the border.[19] These algorithms, which are also used in our criminal justice system,[20] are highly susceptible to racial bias and can lead to unjust targeting of innocent civilians.

Immigration Vetting

During his campaign, President Trump promised "extreme vetting" of immigrants and a "total and complete shutdown of Muslims entering the country."[21] Within days of being in office, he signed an executive order now known as the Muslim Ban, which barred travelers, refugees, and immigrants from several Muslim-majority countries.[22] In February 2018, Trump established the National Vetting Center (NVC), which introduced unprecedented levels of collaboration and collocation of intelligence information across federal agencies.[23] According to the Cato Institute, this increased investment in the U.S. vetting system is unnecessary. Between 2002 and 2016, "the chance of an American being killed in an attack committed by a terrorist who entered as a result of a vetting failure was 1 in 328 million per year."[24]

The NVC threatens the rights and civil liberties of almost anyone interacting with the border, whether they are U.S. citizens, lawful permanent residents, or people from other countries. President Trump has mandated continuous screening of immigrants to identify potential threats and generate leads for deportation.[25] U.S. Citizenship and Immigration Services (USCIS) will monitor, collect, and retain social media information to use in decisions regarding entry, removal, and changes in immigrant status.[26] Individuals identified by the Trump administration as members of "risky populations" must hand over five years of phone number, email and social media history as a condition of their visa application.[27] Additionally, the Visa Lifecycle Vetting Initiative, led by U.S. Immigration and Customs Enforcement (ICE), will create a new centralized database that will store immigrants' information such as court documents, license plate tracking data, and social media data.[28] This database will serve the Trump Administration's goal of continuous surveillance of immigrants, a policy that is both discriminatory and ineffective.

1600 K St, NW Suite 601 | Washington, DC 20006 | (202) 429-9210 | www.aaiusa.org

Endnotes

1 *See generally Korematsu v. United State*s, 323 U.S. 214 (1944). *See also* Nadine Frederique, COINTELPRO, Encyclopedia Britannica (Jul. 21, 2016), https://www.britannica.com/topic/ COINTELPRO.

2 Mark Jaycox, *A Primer on Executive Order 12333: The Mass Surveillance Starlet*, Electronic Frontier Foundation (Jun. 2, 2014), https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet. *See also* Electronic Privacy Information Center, Executive Order 12333 (accessed Apr. 27, 2019), https://epic.org/privacy/surveillance/12333.

3 For a comprehensive review of the FISA Court, *see* Elizabeth Goitein and Fiza Patel, *What Went Wrong with the FISA Court*, Brennan Center for Justice (Mar. 18, 2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

4 Brennan Center for Justice, Foreign Intelligence Surveillance (FISA Section 702, Executive Order 12333, and Section 215 of the Patriot Act): A Resource Page (last revised Sept. 28, 2017), https://www.brennancenter.org/analysis/foreign-intelligence-surveillance-fisa-section-702-executive-order-12333-and-section-215. *See also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Patriot) Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), *available at* https://www.congress.gov/bill/107th-congress/house-bill/3162.

5 American Civil Liberties Union, *Unleashed and Uacountable: The FBI's Unchecked Abuse of Authority*, at 5 (Sept. 2013), *available at* https://www.aclu.org/sites/default/files/field_document/unleashed-and-unaccountable-fbi-report.pdf.

6 The term metadata refers to non-content-based communications information. See Scott F. Mann, *Fact Sheet: Section 215 of the USA PATRIOT Act,* Center for Strategic and International Studies (last revised Feb. 27, 2014), https://www.csis.org/analysis/fact-sheet-section-215-usa-patriot-act.

7 Elizabeth Goitein, *USA Freedom Act and the Surveillance Reform that Almost Was*, Just Security (May 1, 2015), https://www.justsecurity.org/22624/usa-freedom-surveillance-reform.

8 Cindy Cohn and Randy Reitman, *USA Freedom Act Passes: What we celebrate, what we mourn, and where we go from here*, Electronic Frontier Foundation (Jun. 2, 2015), https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebratewhat-we-mourn-and-where-we-go-here. *See also* Kate Tummarello, *Debunking the Patriot Act as it Turns 15*, Electronic Frontier Foundation (Oct. 26, 2016), https://www.eff.org/deeplinks/2016/10/debunking-patriot-act-it-turns-15.

9 Robert Chesney, *Three FISA Authorities Sunset in December: Here's What You Need to Know*, Lawfare (Jan. 16, 2019), https://www.lawfareblog.com/three-fisa-authorities-sunset-december-heres-what-you-need-know.

10 *Supra* note 5, at 14-15.

11 Office of the Director of National Intelligence, Office of Civil Liberties, Privacy, and Transparency, *Statistical Transparency Report Regarding the Use of National Security Authorities, Calendar Year 2017*, at 28 (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf.

12 Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and the Operations of the Foreign Intelligence Surveillance Court*, at 155 (Jan. 23, 2014), *available at* https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

13 Charlie Savage, *N.S.A. Purges Hundreds of Millions of Call Records*, N.Y. Times (Jun. 29, 2018), https://www.nytimes.com/2018/06/29/us/politics/nsa-call-records-purged.html.

14 Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. Times (Mar. 4, 2019), https://www.nytimes.com/2019/03/04/us/politics/nsa-phone-records-program-shut-down.html.

15 American Civil Liberties Union, Domestic Drones (accessed Apr. 27, 2019), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones.

16 American Civil Liberties Union, Location Tracking (accessed Apr. 27, 2019), https://www.aclu.org/issues/privacy-technology/location-tracking.

17 American Civil Liberties Union, Automatic License Plate Readers (accessed Apr. 27, 2019), https://www.aclu.org/issues/privacy-technology/location-tracking/automatic-license-plate-readers.

18 American Civil Liberties Union, Face Recognition Technology (accessed Apr. 27, 2019), https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.

19 American Civil Liberties Union, Border Security Technologies (accessed Apr. 27, 2019), https://www.aclu.org/other/border-security-technologies.

20 Mitch Smith, *In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures*, N.Y. Times (Jun. 22, 2016), https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html

21 Jessica Taylor, *Trump Calls for "Total and Complete Shutdown of Muslims Entering" U.S.*, NPR News (Dec. 7, 2015), https://www.npr.org/2015/12/07/458836388/trump-

1600 K St, NW Suite 601 | Washington, DC 20006 | (202) 429-9210 | www.aaiusa.org

calls-for-total-and-complete-shutdown-of-muslims-entering-u-s.

22 Nick Miroff, *Trump Is Creating a Vetting Center. Is it 'Extreme' Enough to End His Travel Ban?* Washington Post (Apr. 23, 2018), https://www.washingtonpost.com/world/national-security/trump-is-creating-a-vetting-center-is-it-extreme-enough-to-end-his-travel-ban/2018/04/22/6ab109fa-43fd-11e8-baaf-8b3c5a3da888_story.html?noredirect=on&utm_term=.faa970bc6283.

23 Chinmayi Sharma, *The National Vetting Enterprise: Artificial Intelligence and Immigration Enforcement*, Lawfare (Jan. 8, 2019), https://www.lawfareblog.com/national-vetting-enterprise-artificial-intelligence-and-immigration-enforcement.

24 David Bier, *Extreme Vetting of Immigrants: Estimating Terrorism Vetting Failures*, CATO Institute (Apr. 17, 2018), https://www.cato.org/publications/policy-analysis/extreme-vetting-immigrants-estimating-terrorism-vetting-failures#fullhttps://www.cato.org/publications/policy-analysis/extreme-vetting-immigrants-estimating-terrorism-vetting-failures#full.

25 *Supra* note 22. *See also* Memorandum on Optimizing the Use of Federal Government Information in Support of the National Vetting Enterprise, National Security Presidential Memorandum/NSPM-9, DCPD No. 201800078 (Feb. 6, 2018), *available at* https://www.whitehouse.gov/presidential-actions/presidential-memorandum-optimizing-use-federal-government-information-support-national-vetting-enterprise.

26 *Id.*

27 *Id.*

28 *Id.*

1600 K St, NW Suite 601 | Washington, DC 20006 | (202) 429-9210 | www.aaiusa.org