ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

September 26, 2017

Senator John Cornyn
Subcommittee on Border Security and Immigration, Chairman
517 Hart Senate Office Building
Washington, DC 20510

Re: S. 1757 re border surveillance technology - OPPOSE

Dear Sen. Cornyn:

The Electronic Frontier Foundation (EFF) opposes many provisions in your bill, the Building America's Trust Act (S. 1757).[1] Any new statutory authority given to the government to ensure border security must be carefully balanced to ensure that it does not overreach and violate the privacy of the people it intends to protect.

In EFF's view, this bill does not achieve that balance. Instead, it expands biometric and other high-tech surveillance of U.S. citizens and foreign visitors at and near the U.S. border without regard to essential civil liberties. We look forward to working with you on changes that would ensure Constitutional protections for all Americans.

EFF is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy rights in the digital world. EFF was founded in 1990 and has over 38,000 members.

1. Biometric Data Collection at the Border

S. 1757 would require the Department of Homeland Security (DHS) to complete a plan within six months to establish a biometric exit data system.[2] After two years, it would also require DHS to implement this plan at our nation's busiest international airports, seaports, and land crossings.[3] In doing

[1] https://www.congress.gov/115/bills/s1757/BILLS-115s1757pcs.pdf.
[2] Sec. 418(a)(1) on pp. 129-30.
[3] Sec. 418(a)(2) on p. 132.

so, DHS would be required to make every effort to collect "multiple modes of biometrics."[4]

As you know, DHS already has an existing and continually expanding program of facial recognition screening of all travelers—U.S. citizens and foreign citizens alike—who take certain outgoing flights from U.S. airports. EFF opposes this program.[5]

S. 1757 would entrench and expand DHS's current facial recognition border screening program, and expand it to collect other forms of biometric data. EFF opposes this for the following reasons:

1. Privacy - Facial recognition is a unique threat to our privacy. We cannot hide our faces in public, and it is difficult to change our faces.

2. Accuracy - Facial recognition has significant accuracy problems, especially as to people of color.

3. Theft – As we have seen with other government data breaches, data thieves might steal DHS's biometric information, and use it to steal our identities and stalk us.

4. Misuse – Government employees may misuse DHS's reservoir of biometric data.

5. Improper Sharing – DHS might share with other government agencies the biometric information it seizes from travelers.

6. Mission Creep - DHS might expand the ways it uses its biometric system, from just identifying travelers, to also screening them against other potentially problematic databases. Arrest warrant databases, for example, are riddled with error, and include many people accused of minor offenses.

In sum, EFF calls on Congress to end DHS's current program of biometric border screening, not entrench and expand it.

[4] Sec. 418(h) at p. 137.
[5] https://www.eff.org/deeplinks/2017/08/end-biometric-border-screening.

2. DNA Screening of Immigrants

S. 1757 would require DHS to collect "biometric information" from "any individual filing an application, petition, or other request for immigration benefit or status." This could include collection of DNA, as well as fingerprints, iris prints, and voiceprints.[6]

EFF opposes such dragnet collection of biometric information from immigrants.[7] Government collection of DNA raises special privacy concerns, above and beyond other biometric screening, because DNA contains highly sensitive information about familial history and health issues.[8]

Even though this provision of S. 1757 does not invade the privacy of U.S. citizens, it is still highly troubling. First, biometric privacy is a basic human right, regardless of citizenship status. Second, as shown by DHS's existing program of biometric screening of travelers flying out of the U.S., government programs that begin by screening foreign citizens often expand to U.S. citizens. Third, foreign nations may respond to this U.S. program by imposing biometric screening on visiting U.S. citizens.

3. Biometric Data Sharing

S. 1757 would require DHS to share its biometric information about immigrants with the FBI, the Defense Department, and the State Department.[9] It also would require DHS to store its voiceprints and iris scans of immigrants in a manner that is compatible with state and local law enforcement systems,[10] which would facilitate DHS sharing of its biometrics collection with state and local agencies.

EFF opposes this distribution of immigrants' biometric information throughout our federal, state, and local law enforcement agencies. The greater the distribution of this highly sensitive information, the greater the risks of mission creep, theft, and employee misuse.

---

[6] Sec. 305(a)(1) on p. 151.
[7] https://www.eff.org/document/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond.
[8] https://www.eff.org/foia/dna-collection.
[9] Sec. 305(b) on p. 152.
[10] Sec. 205(a) on p. 128.

4. Screening Social Media of Visa Applicants

S. 1757 would require DHS, to the greatest extent possible, to "review the social media accounts of visa applicants" from "high risk countries."[11]

As you know, the State Department currently screens the social media of certain visa applicants, and DHS screens the social media of visitors from China as well as from citizens from Visa Waiver Program countries. All of these screening programs ask the applicant to disclose their social media handles or identifiers.

EFF opposes these programs and calls on DHS and the State Department to end social media screening of foreign visitors. They threaten the digital privacy and freedom of expression of innocent foreign travelers, and the many U.S. citizens who communicate with them. Moreover, the government has not shown that such information collection will be effective at combating terrorism.[12]

The existing DHS and State Department social media monitoring programs do not demand passwords (though former DHS Secretary Kelly floated this possibility[13]). This bill, however, opaquely requires DHS to monitor "social media accounts." It is unclear if this means public information accessible with a social media handle, or private information accessible with a social media password. EFF opposes both forms of social media monitoring, but doing so with a password is worse.

EFF is also troubled by the bill's focus on "high risk countries." The bill empowers the DHS Secretary to determine which countries are "high risk" based on "any" criteria the Secretary deems "appropriate."[14] It is all too likely that DHS would use these broad authorities to practice "extreme vetting" of the social media of visitors from Muslim nations.

---

[11] Sec. 434 on p. 365.
[12] https://www.eff.org/deeplinks/2017/06/no-state-department-social-media-surveillance; https://www.eff.org/deeplinks/2016/08/us-customs-and-border-protection-wants-know-who-you-are-twitter-its-flawed-plan; https://www.eff.org/deeplinks/2017/04/no-screening-social-media-handles-chinese-visitors?page=8.
[13] https://www.eff.org/deeplinks/2017/04/tell-dhs-social-media-passwords-should-not-condition-entry.
[14] Sec. 434(b)(3) on p. 366.

Thus, EFF opposes the social media screening provision of S. 1757.

5. Drones Near the Border

S. 1757 would require DHS[15] and the Defense Department[16] to deploy drones at the U.S. border, but does not limit the path of the drones or attempt to minimize information collected about innocent bystanders.

Drones can capture personal information, including faces and license plates, from all of the people on the ground within the range and sightlines of a drone. Drones can do so secretly, thoroughly, inexpensively, and at great distances.

Millions of U.S. citizens and lawful permanent residents live close to the U.S. border. Deployment of drones at the U.S. border will invariably capture personal information from vast numbers of U.S. persons. Troublingly, the bill has no provisions regarding the retention, use, and sharing of the personal information that these drones will capture from U.S. persons. EFF opposes the unfettered use of drones in unspecified areas.

6. ALPRs Near the Border

S. 1757 would require U.S. Customs and Border Protection (CBP) to upgrade all of its existing automatic license plate readers (ALPRs) located "on the northern border and southern border on incoming and outgoing vehicle lanes," and would authorize spending $125 million for this purpose.[17] It also would require a pilot program using ALPRs at "land ports of entry or checkpoints."[18]

It is unclear whether the bill's ALPR surveillance would be limited to cars that actually cross the U.S. border, or would also apply more broadly to cars at CBP's many interior checkpoints, some of which are located as far as 100 miles from the border.[19] The associated pilot program applies to

[15] Sec. 103(b) on p. 13; Sec. 104(a) at p. 15.
[16] Sec. 111(b)(1) on pp. 39-40.
[17] Sec. 204(a) & (d) on pp. 127-28.
[18] Sec. 204(b) on p. 127.
[19] http://www.gao.gov/new.items/d09824.pdf.

"checkpoints." If CBP spent $20,000 per ALPR,[20] it could acquire more than 6,000 ALPRs with $125,000,000, which is far more ALPRS than CBP needs to secure our nation's approximately 150 land border crossings.[21] Many kinds of ALPRs are portable, and might be moved from border crossings to interior checkpoints.

Again, millions of U.S. citizens and lawful permanent residents live close to the U.S. border. They routinely drive through CBP interior checkpoints on their way to work and school, though they have not recently crossed the U.S. border and have no plans to do so. These U.S. persons should not be subjected to ALPR surveillance merely because they live near the border.

ALPRs collect massive amounts of sensitive location information about identifiable law-abiding people.[22] Therefore, EFF is concerned about the proliferation of these devices, and opposes the ALPR provisions of S. 1757.

* * *

Thank you for considering EFF's objections to S. 1757. If you have any questions, please do not hesitate to email me at adam@eff.org, or to call me at (415) 436-9333, extension 176.

Sincerely,

Adam Schwartz

[20] https://www.eff.org/sls/tech/automated-license-plate-readers/faq#faq-How-much-do-ALPR-systems-cost,-and-how-are-law-enforcement-agencies-paying-for-them.

[21] https://en.wikipedia.org/wiki/List_of_Mexico%E2%80%93United_States_border_crossings.
https://en.wikipedia.org/wiki/List_of_Canada%E2%80%93United_States_border_crossings.

[22] https://www.eff.org/document/neal-v-fairfax-county-eff-amicus-brief.