epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 30, 2017

The Honorable Michael McCaul, Chairman
The Honorable Bennie Thompson, Ranking Member
U.S. House Committee on Homeland Security
Port of Los Angeles Administration Building
425 South Palos Verdes St.
San Pedro, California

Dear Chairman McCaul and Ranking Member Thompson:

We write to you regarding the upcoming hearing on "Examining Physical Security and Cybersecurity at Our Nation's Ports."[1] EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. We are particularly interested in the privacy problems associated with systems of government surveillance.[2]

EPIC has expertise regarding maritime surveillance. EPIC pursued a Freedom of Information Act (FOIA) lawsuit against the Department of Homeland Security concerning the Nationwide Automatic Identification System (NAIS), a system designed with the support the U.S. Coast Guard to promote boating safety that the DHS has transformed into a surveillance network monitoring vessels, including recreational vehicles operated by U.S. citizens. On March 28, 2016, after successfully obtaining nearly 2,500 pages of documents on NAIS, EPIC settled the case.[3] EPIC uncovered documents in which the DHS claimed that boaters have "no expectation of privacy with regard to any information transmitted" about the location of their boats.[4] It was a remarkable assertion that would come as a surprise to the vast majority of boaters in this country who pursue recreational boating. Ralph Naranjo, a widely regarded mariner, author, and former Vanderstar Chair at the U.S. Naval Academy, expressed dismay that "a

[1] *Examining Physical Security and Cybersecurity at Our Nation's Ports*, 115th Cong. (2017), H. Comm. on Homeland Security, https://homeland.house.gov/hearing/examining-physical-security-cybersecurity-nations-ports/ (Oct. 30, 2017).
[2] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html; EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/, Statement of EPIC, "*Unmanned Aircraft Systems: Innovation, Successes, and Challenges,*" Hearing Before S. Comm. on Commerce, Science, and Transportation, United States Senate, Mar. 13, 2017, https://epic.org/testimony/congress/EPIC-SCOM-Drones-Mar2017.pdf.
[3] EPIC v. USCG - Nationwide Automatic Identification System, https://epic.org/foia/dhs/uscg/nais/.
[4] https://epic.org/foia/dhs/uscg/nais/EPIC-15-05-29-USCG-FOIA-20151030-Production-1.pdf#page=2

sailor's Good Samaritan effort to share location data will automatically enroll them in a data bank that tracks all of their movements." [5]

This Committee recently passed the "Border Security for America Act,"[6] which would dramatically expand surveillance capabilities along the northern and southern borders of the U.S. The bill seeks "to achieve situational awareness and operational control of the border" with surveillance technology, including a biometric exit data system at U.S. seaports.

Many of the techniques that are proposed to enhance border surveillance have direct implications for the privacy of American citizens. And as these techniques are adopted, the likelihood is that they will be deployed further and further and from the border unless Congress establishes meaningful safeguards. For example, facial recognition poses significant threats to privacy and civil liberties. It can be done covertly, remotely, and on a mass scale. Additionally, there are a lack of well-defined federal regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous and near-effortless identification eliminates individual's ability to control their identities and poses a specific risk to the First Amendment rights of free association and free expression. The use of facial recognition at seaports has real consequences for U.S. citizens as well as non-U.S. citizens. All people entering the U.S., including U.S. passport holders, could be subject to this new screening technique.

The Privacy Act normally limits the government's ability to collect personal data, but the "Border Security for America Act," would exempt the Department of Homeland Security from compliance with the Privacy Act. Biometric data would be combined with other Federal databases. EPIC opposes government databases of personal data that fail to comply with federal privacy laws. The Privacy Act of 1974 requires all federal agencies that maintain a system of records to publish the details of such record systems in the Federal Register. The publication must describe the intended uses of the system, the policies and practices governing the records, and the procedures agencies must follow to give individuals access to their records. The E-Government Act of 2002 requires agencies to perform Privacy Impact Assessments ("PIA"). PIAs are required when "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form" or "initiating a new collection of information" that contains identifiable information. The "Border Security for America Act" would strip away these important safeguards that protect the privacy of U.S. citizens.

EPIC understands that enhanced surveillance techniques may be part of the discussion over border security.[7] EPIC writes to warn that enhanced surveillance at the border will almost

---

[5] Ralph Naranjo, *Big Brother on the Water: The Coast Guard's Maritime Domain Awareness Program Chips Away at our Boating Freedoms*, Practical Sailor, Feb. 2011, at 28, http://www.practical-sailor.com/issues/37_2/features/Is_AIS_Chipping_Away_at_Our_Freedoms_10135- 1.html.

[6] H.R. 4548.

[7] Samantha Schmidt, *Border wall with Mexico won't be built 'from sea to shining sea,' DHS secretary says*, Washington Post, April 6, 2017,

certainly sweep up the personal data of U.S. citizens. Before there is any new deployment of surveillance at the U.S. border, an assessment of the privacy implications should be conducted. Additionally, deployment of surveillance technology should be accompanied by new policy and procedures and independent oversight to protect citizens' rights. And any law enforcement agency that uses surveillance tools should be prepared to comply with all current laws, including any open government laws. The privacy assessments, policies and procedures, and oversight mechanisms should all be made public.

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Subcommittee on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
EPIC Policy Director

/s/ Jeramie Scott
Jeramie Scott
EPIC National Security Counsel

/s/ Christine Bannan
Christine Bannan
EPIC Policy Fellow

https://www.washingtonpost.com/news/morning-mix/wp/2017/04/06/border-wall-with-mexico-wont-be-built-from-sea-to-shining-sea-dhs-secretary-says/.