epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Department of Homeland Security Data Privacy and Integrity Advisory Committee

October 27, 2020 Meeting and New Tasking

November 10, 2020

The Electronic Privacy Information Center ("EPIC") submits these comments in response to the October 27, 2020 meeting of the Department of Homeland Security ("DHS") Data Privacy and Integrity Advisory Committee ("DPIAC").[1] EPIC writes now to expand on oral comments provided at the meeting.

The Chief Privacy Officer tasked the DPIAC to provide "written guidance on best practices to ensure the effective implementation of privacy requirements for information sharing across the DHS enterprise."[2] EPIC calls on the DPIAC to perform a thorough investigation of fusion centers in response to that tasking. Specifically the DPICAC should 1) create a public report detailing the use of facial recognition technology by fusion centers, including the privacy and civil liberties risks created by this usage; 2) urge DHS to ban the use of facial recognition by fusion centers; 3) review data minimization and retention requirements at fusion centers and determine whether fusion centers are complying with those requirements; and 4) consider whether DHS's continued support of fusion

[1] 85 F.R. 63568, https://www.federalregister.gov/documents/2020/10/08/2020-22240/dhs-data-privacy-and-integrity-advisory-committee.
[2] Agenda for Data Privacy and Integrity Advisory Meeting (Oct. 27, 2020), https://www.dhs.gov/sites/default/files/publications/dpiac_october_27_public_meeting_agenda_for_web_20201022.pdf.

centers is justified in light of the minimal amount of actionable intelligence they produce and the magnitude of privacy and civil liberties harms they create.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving the Privacy Act safeguards enacted by Congress.[3] EPIC also has a sustained interest in DHS's biometrics policies and practices.[4] EPIC previously urged DPIAC to advise CBP to halt the implementation of its facial recognition program.[5]

I. Background

DHS's Information Sharing Environment is composed of four elements: the National Network of Fusion Centers, the Nationwide Suspicious Activity Reporting Initiative, the National Terrorism Advisory System, and the "If You See Something, Say Something" campaign.[6] Of these

[3] *See, e.g.*, Comments of EPIC to the Department of Homeland Security, Correspondence Records Modified System of Records Notice, Docket No. DHS-2011-0094 (Dec. 23, 2011), http://epic.org/privacy/1974act/EPIC-SORN-Comments-FINAL.pdf; Comments of EPIC to the Department of Homeland Security, 001 National Infrastructure Coordinating Center Records System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2010-0086, DHS-2010-0085 (Dec. 15, 2010), http://epic.org/privacy/fusion/EPIC_re_DHS-2010-0086_0085.pdf; Comments of EPIC to the Department of Homeland Security, Terrorist Screening Database System of Records Notice and Notice of Proposed Rulemaking, Docket Nos. DHS-2016-0002, DHS-2016-0001 (Feb. 22, 2016), https://epic.org/apa/comments/EPIC-Comments-DHS-TSD-SORN-Exemptions-2016.pdf.

[4] *See e.g.*, Comments of EPIC to the Transportation Security Administration, Intent to Request Revision of Agency Information Collection Activity Under OMB Review: TSA PreCheck, Docket ID: TSA-2013-0001 (June 22, 2020), https://epic.org/apa/comments/EPIC-TSA-PreCheck-FRT-Comment-June2020.pdf; Comments of EPIC to the Department of Homeland Security, Agency Information Collection Activities: Biometric Identity, Docket No. 1651-0138 (Jul. 24, 2018), https://epic.org/apa/comments/EPIC-CBP-Vehicular-Biometric-Entry-Exit-Program.pdf; EPIC v. CBP (Biometric Entry/Exit Program), https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html (EPIC obtained a report which evaluated iris imaging and facial recognition scans for border control); EPIC Statement to U.S. House Committee on Homeland Security, "Border Security, Commerce and Travel: Commissioner McAleenan's Vision for the Future of CBP" (Apr. 24, 2018), https://epic.org/testimony/congress/EPIC-HHSC-CBP-Apr2018.pdf.

[5] Comments of EPIC to the Data Privacy and Integrity Advisory Committee, December 10, 2018 Meeting, Docket No. DHS–2018–0066 (Dec. 10, 2018), https://epic.org/apa/comments/EPIC-Comments-DHS-DPIAC-Face-Rec-Report-Dec-2018.pdf.

[6] Dep't. of Homeland Sec., *Information Sharing* (Aug. 14, 2018), https://www.dhs.gov/information-sharing.

elements, fusion centers, in particular, merit focus given their history of privacy and civil liberties issues and their role in collecting and distributing information of questionable value.

Fusion centers are billed as the "collaborative effort of two or more agencies that provide resources, expertise, and information to the center with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity."[7] Centers are intended to "fuse" a broad range of data from local law enforcement, local public services, the federal government, and the private sector to create "meaningful, and actionable intelligence and information.[8] In practice this amounts to facilitating access to databases and information that local, state, or federal law enforcement could not otherwise use. Despite the billing, fusion centers have never performed much "true fusion": "analysis of disparate data sources, identification of intelligence gaps, and pro-active collection of intelligence against those gaps which could contribute to prevention is occurring."[9]

Fusion centers nationwide are now in compliance with DHS's model, despite substantial privacy and civil liberties violations. From 2007-2015 DHS was engaged in developing fusion centers from loose information sharing groups to dedicated, fully resourced and staffed centers.[10] In 2015 DHS declared that the National Fusion Center Network had "matured".[11] Fusion centers now employ roughly 3,000 people nationwide, mostly local/state law enforcement and DHS agents.[12]

---

[7] Bureau of Justice Assistance, Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, Department of Justice (Aug. 2006), https://epic.org/privacy/fusion/report.pdf.
[8] Todd Masse, Siobhan O'Neil, John Rollins, Cong. Rsch. Serv., RL34070, Fusion Centers: Issues and Options for Congress at 6 (Jul. 6, 2007), https://epic.org/privacy/fusion/crs_fusionrpt.pdf (quoting Dept. of Just., Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era, (Aug. 2006)).
[9] *Id.* at i.
[10] Dept. of Homeland Sec., *2015 National Network of Fusion Centers Final Report* i-ii (April 2016), https://www.dhs.gov/sites/default/files/publications/2015%20Final%20Report%20Section%20508%20Compliant.pdf.
[11] *Id.* at 17.
[12] Dept. of Homeland Sec., *2018 National Network of Fusion Centers Final Report* (2018), https://www.dhs.gov/sites/default/files/publications/2018_national_network_of_fusion_centers_final_report.pdf.

Every fusion center has access to at least one classified federal database, despite only 67% of employees who need federal clearances having one.[13]

Fusion centers consistently experiment with advanced intelligence gathering and identification systems. At least 10 fusion centers have facial recognition capacities.[14] According to the latest ICE Privacy Impact Assessment, any fusion center that partners with ICE may use facial recognition to search ICE's substantial databases, as well as the fusion center's own databases.[15] Fusion center's own databases contain photo entries from fusion center partners, including local law enforcement and private sector partners.[16] ICE itself solicits profiles for facial recognition from local law enforcement, federal agencies, and commercial vendors.[17] Fusion centers have recently run facial recognition programs without any privacy policy, despite DHS requirements.[18] Little is known about the use of facial recognition by fusion centers. DPIAC should thoroughly review the past and present use of facial recognition systems by fusion centers and analyze the privacy and civil liberties risks created by this usage. The resulting report should be made available to the public.

II. Fusion centers have a documented history of privacy and civil liberties violations.

Early this year a report based on "court records, federal legislation, policy documents, interviews, news reports" and FOIA documents detailed the substantial surveillance of protected

---

[13] *Id*.
[14] Ryan Mac, Caroline Haskins, and Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, Buzzfeed News (Feb. 27, 2020), https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.
[15] Dept. of Homeland Sec., DHS/ICE/PIA-054 ICE Use of Facial Recognition Services at 13 (May 13, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-frs-054-may2020.pdf.
[16] *Id*.
[17] Aaron Boyd, *ICE Outlines How Investigators Rely on Third-Party Facial Recognition Services*, Nextgov (Jun. 2, 2020), https://www.nextgov.com/emerging-tech/2020/06/ice-outlines-how-investigators-rely-third-party-facial-recognition-services/165846/.
[18] Tom Schuba*, CPD using controversial facial recognition program that scans billions of photos from Facebook*, other sites, Chi. Sun Times (Jan. 29, 2020), https://chicago.suntimes.com/crime/2020/1/29/21080729/clearview-ai-facial-recognition-chicago-police-cpd.

First Amendment activities by fusion centers.[19] A Chicago area fusion center known as the Chicago Prevention and Information Center ("CPIC") monitored anti-ICE protests in 2018, reports on those protests were sent to DHS.[20] CPIC receives reports from Chicago Police Departments on "any significant or newsworthy event" in the city with a particular emphasis on "strikes, labor-management incidents, or union controversies".[21] The same fusion center in Chicago had no privacy policy in place for using facial recognition technology yet continued to use Clearview AI.[22] Similar surveillance was discovered at a Memphis fusion center that monitored protests in 2017, targeting activists and journalists.[23]

a. Fusion centers have failed to implement meaningful oversight.

At CPIC, alerts which identified individuals primarily based on ethnicity were flagged as "unreliable" but still passed on to DHS.[24] These alerts were eventually cancelled, but only after analysts had used them as justification to collect information on individuals. A review of years of internal privacy audits at CPIC found "small changes to internal regulations, but a near-blanket rubber stamp of CPIC's activities".[25] Both Congressional and NGO reports on fusion centers have found them to be poorly regulated, prone to Constitutional violations, and providing little if any actionable intelligence.[26]

---

[19] Open the Government, *The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers* (Mar. 26, 2020), https://www.openthegovernment.org/dhs-fusion-centers-full-report/.
[20] *Id*.
[21] *Id*.
[22] *Id.* citing Chicago Sun-Times.
[23] *Id*.
[24] *Id*.
[25] *Id*.
[26] *See* S. Permanent Subcommittee on Investigations, 112th Cong. Federal Support for and Involvement in State and Local Fusion Centers: Majority and Minority Staff Rep. (Oct. 3, 2012), https://www.hsgac.senate.gov/imo/media/doc/10-3-2012 PSI STAFF REPORT re FUSION CENTERS.2.pdf., *and* Open the Government, *The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers* (Mar. 26, 2020), https://www.openthegovernment.org/dhs-fusion-centers-full-report/.

A 2012 report from the bipartisan Committee on Homeland Security and Governmental Affairs Senate Investigations Subcommittee found that DHS's involvement with fusion centers has "not produced useful intelligence to support Federal counterterrorism efforts."[27] The report found that fusion centers were not serving their asserted role: providing DHS with timely counter-terrorism information. Instead, fusion centers staff were focused on local law enforcement, entirely unsupervised in their use of federal funds, minimally trained, and almost never held responsible for providing incorrect or irrelevant information.[28]

In 2012 there was little to no oversight of employees drafting Homeland Intelligence Reports ("HIRs"), the primary intelligence product of fusion centers. During the period the Subcommittee reviewed, 118 of 574 draft reports were cancelled as either irrelevant, lacking useful information, or in breach of privacy/civil liberties protections.[29] The Committee found that intelligence was "of uneven quality – oftentimes shoddy, rarely timely, sometimes endangering citizens' civil liberties and Privacy Act protections, occasionally taken from already-published public sources, and more often than not unrelated to terrorism."[30] Only 94 of the 368 approved HIRs could be associated with terrorism, and the majority of those were either outdated, duplicative, or based on publicly available information.[31]

The Subcommittee sharply criticized DHS's fusion center program for failing to sanction reporting officials who repeatedly produce inappropriate HIRs.[32] The failure to supervise compounded a years-long failure to provide adequate training on privacy and civil liberties protection to DHS employees. Until 2012 DHS required only five days of training for employees

[27] S. Permanent Subcommittee Report at 1.
[28] *Id*.
[29] *Id.* at 31-2.
[30] *Id.* at 27.
[31] *Id.* at 39-45.
[32] *Id.* at 45-47.

assigned to fusion centers, and of that, only four hours were dedicated to privacy and civil liberties.[33] DHS did not rely only on federal employees to manage data from fusion centers. Instead, DHS often hired contract employees from private companies to draft and review intelligence reports, resulting in high volumes of low-quality reporting and undertrained contract staff.[34] When HIRs were found to violate privacy or civil liberties standards those reports were retained years after being "cancelled".[35] DHS retained information on U.S. persons well in excess of the time allowed under either the Privacy Act or even the department's internal oversight procedures.

The Committee concluded that up to $1.4 billion in federal funding had produced little useful counter-terrorism intelligence and had not stopped a single attack.[36] Most fusion centers did not prioritize counter-terrorism, and some performed no counter-terrorism functions at all. The Committee called for Congress to clarify the purpose of federal funding to support fusion centers and on DHS to tailor funding for federal needs.[37] Within the agency, the Committee recommended improved training, oversight from DNI, more disclosure to Congress, and adherence to privacy and civil liberties requirements. Eight years later, little, if anything, has changed.[38] In light of their lack of value and the risk they pose to privacy and civil liberties, DHS's fusion center program should be shut down.

b. Fusion centers monitored Black Lives Matter protests this summer.

Fusion centers engaged in excessive monitoring of protests in the wake of George Floyd's death. The Northern California Regional Information Center ("NCRIC") was nearly exclusively

[33] *Id.* at 47-49. For comparison, U.S. Army intelligence training lasts up to 6 months.
[34] *Id* at 52-4.
[35] *Id* at 57.
[36] *Id* at 83.
[37] *Id* at 106.
[38] *See* Open the Government, *The Cost of Fear: Long-Cited Abuses Persist at U.S. Government-Funded Post-9/11 Fusion Centers*.

focused on monitoring protests between at least May 25 and June 6, 2020.[39] NCRIC staff monitored social media to compile lists of protests and received numerous Suspicious Activity Reports ("SARs") on protesters.[40] One SAR categorized a planned speech on "The Black American Experience" at San Jose State University as "Radicalization/Extremism".[41] NCRIC received numerous requests from local law enforcement for real-time social media monitoring of protests in addition to SARs on protected First Amendment activities.[42]

At the same time across the country, the Maine Information and Analysis Center ("MIAC") was also engaged in protest monitoring.[43] According to the ACLU of Maine, MIAC is "engaged in general law enforcement activities, surveillance of protest activities, collecting and storing information about critics of government policies."[44] Recent reports on MIAC echo the allegations in a federal whistleblower lawsuit filed earlier this year.[45] According to a Maine state trooper alleging retaliation for calling out illegal practices, MIAC "regularly broke privacy laws, overstepped its legal authority and often investigated people associated with lawful protests, sometimes using flimsy legal pretexts—for example, that protesters might litter during a demonstration—to justify prying into private lives."[46]

The recent surge in surveillance of protesters highlights the importance of fusion centers adhering to data retention limits and expediently deleting individual's data. A summer of unrest

---

[39] Micah Lee, *How Northern California's Police Intelligence Center Tracked Protests*, The Intercept (Aug. 17, 2020), https://theintercept.com/2020/08/17/blueleaks-california-ncric-black-lives-matter-protesters/.
[40] *Id*.
[41] *Id*.
[42] *Id*.
[43] *'Blue leaks' include information about police surveillance of Black Lives Matter protests*, WGME News (Jun. 19, 2020), https://wgme.com/news/local/blue-leaks-include-information-about-police-surveillance-of-black-lives-matter-protests.
[44] *Id*.
[45] Matt Bryne, *Maine trooper says he was retaliated against for reporting illegal police surveillance of citizens*, Portland Press Herald (May 14, 2020), https://www.pressherald.com/2020/05/14/maine-trooper-says-he-was-retaliated-against-for-reporting-illegal-police-surveillance-of-citizens/?rel=related#goog_rewarded.
[46] *Id*.

likely swept many new individuals into fusion center databases without their knowledge. In June a hack of web development firm Netsential exposed records from 31 fusion centers and over 200 other law enforcement agencies.[47] Together these events reveal that fusion centers engage in excessive government surveillance and cannot protect individuals' information from data breaches.

III. Conclusion

EPIC urges the Committee to thoroughly investigate fusion centers as part of its mandate to "ensure the effective implementation of privacy requirements for information sharing". Specifically, EPIC urges DPIAC to review fusion centers' use of facial recognition technology. Additionally, EPIC urges the Committee to recommend that DHS standardize and carefully audit data minimization and data retention at fusion centers. DHS should also halt the use facial recognition technology at fusion centers altogether. Facial recognition technology is a substantial threat to privacy, has been shown to be biased, and recent data breaches within DHS have exposed individual's biometric information. Finally, EPIC urges the Committee to consider whether fusion centers as an enterprise are justifiable in light of the limited intelligence value they produce and magnitude of privacy harms they create.

Respectfully Submitted,

Jeramie Scott
Jeramie Scott
EPIC Senior Counsel

Jake Wiener
Jake Wiener
EPIC Law Fellow

[47] Andy Greenberg, *Hack Brief: Anonymous Stole and Leaked a Megatrove of Police Documents*, Wired (June 22, 2020), https://www.wired.com/story/blueleaks-anonymous-law-enforcement-hack/.