

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

Privacy and Civil Liberties Oversight Board

on

Notice of Public Forum on Domestic Terrorism

87 Fed. Reg. 19,536

April 25, 2022

---

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Privacy and Civil Liberties Oversight Board’s (PCLOB) Notice of Public Forum on Domestic Terrorism.<sup>1</sup> EPIC staff plan to attend the June meeting and to submit more detailed comments following the meeting. EPIC applauds the PCLOB’s decision to scrutinize the government’s approach to domestic terrorism and consider the risks that domestic terrorism investigations pose to privacy, civil liberties, and safety.

EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.<sup>2</sup> EPIC has particular interest in issues related to national security and surveillance. EPIC has engaged with the PCLOB since it was first formed in 2004. In

---

<sup>1</sup> 87 Fed. Reg. 19,536, [https://documents.pclob.gov/prod/Documents/EventsAndPress/b2b6a3c4-0988-4ad4-ba62-4ccd68b6ef3e/Public%20Forum%20Notice%203.25.2022%20\(Final\).pdf](https://documents.pclob.gov/prod/Documents/EventsAndPress/b2b6a3c4-0988-4ad4-ba62-4ccd68b6ef3e/Public%20Forum%20Notice%203.25.2022%20(Final).pdf).

<sup>2</sup> See EPIC, *About Us*, <https://epic.org/about/>.

that time, EPIC has provided extensive comments to the Board on EO 12333, FOIA procedures, and “defining privacy,” among other topics.<sup>3</sup>

EPIC submits comments now to suggest several issues that are of particular importance and should be prioritized at the June meeting. EPIC urges the PCLOB to consider the implications of investigative practices and tools that have been used in the course of domestic terrorism investigations, including facial recognition, aerial surveillance, fusion centers, and the government’s bulk acquisition of personal information from data brokers.

**I. The Oversight Board should examine the use of facial recognition in domestic terrorism investigations and recommend a ban on law enforcement use of facial recognition.**

Facial recognition is a powerful and dangerous technology underpinning modern mass surveillance. For years, EPIC has focused on stopping face surveillance and limiting collection and use of other biometric information. Facial recognition can be used to exploit the vast supply of video and images collected via aerial surveillance, public and private security cameras, cell phones, and the internet. And facial recognition has been used repeatedly in attempts to identify protesters, journalists, and ordinary individuals. Even if perfectly accurate, and perhaps even more so if perfectly accurate, facial recognition technology chills free expression, triggers over-policing, and destroys privacy in public. No facial recognition system available today is perfectly accurate or free from racial bias, and the use of these systems by law enforcement has already led to wrongful arrests

---

<sup>3</sup> Comments of EPIC to the Privacy and Civil Liberties Oversight Board, Request for Public Comment on Activities Under Executive Order 12333 (June 16, 2015), <https://epic.org/privacy/surveillance/12333/EPIC-12333-PCLOB-Comments-FINAL.pdf>; Jeramie D. Scott, Nat’l Sec. Counsel, EPIC, Prepared Statement for the Record Before the Privacy and Civil Liberties Oversight Board (Jul. 23, 2014), [https://archive.epic.org/news/privacy/surveillance\\_1/EPIC-Statement-PCLOB-Review-12333.pdf](https://archive.epic.org/news/privacy/surveillance_1/EPIC-Statement-PCLOB-Review-12333.pdf); Comments of EPIC to the Privacy and Civil Liberties Oversight Board, Freedom of Information, Privacy Act, and Government in the Sunshine Act Procedures (July 15, 2013), [https://epic.org/open\\_gov/EPIC-PCLOB-FOIA.pdf](https://epic.org/open_gov/EPIC-PCLOB-FOIA.pdf); Letter from Marc Rotenberg, EPIC President, & Khaliah Barnes, EPIC Administrative Counsel, to PCLOB on “Defining Privacy,” at 4 (Nov. 11, 2014), available at [https://epic.org/open\\_gov/EPIC-Ltr-PCLOB-Defining-Privacy-Nov-11.pdf](https://epic.org/open_gov/EPIC-Ltr-PCLOB-Defining-Privacy-Nov-11.pdf).

that have disproportionately targeted Black men. EPIC advocates for a ban on the use of facial recognition for surveillance.

EPIC works on many fronts to oppose the rollout of new facial recognition systems, enact bans on facial recognition at all levels of government, and cabin other biometrics to limited and transparent use. In 2020, EPIC and a coalition of 40 consumer, privacy, and civil liberties organizations urged the Oversight Board to recommend suspending the use of facial recognition systems across the federal government.<sup>4</sup> Also in 2020, EPIC and a coalition of privacy and civil liberties groups opposed a rulemaking by the Department of Homeland Security (DHS) that would have massively expanded the use of biometrics across the agency.<sup>5</sup> After comments and outreach to the Biden Administration, the policy was reversed in 2021.<sup>6</sup> That same year, EPIC organized a campaign to investigate and shutter a secretive facial recognition system in the Washington, DC, metropolitan area that was used to identify at least one Black Lives Matter protester.<sup>7</sup> After EPIC raised the issue, the facial recognition system was shut down.<sup>8</sup> EPIC recommends that the Oversight Board perform a thorough review of the use of facial recognition for domestic terrorism investigations and should endorse a ban on law enforcement use of facial recognition technology.

---

<sup>4</sup> Letter from 40 consumer, privacy, and civil liberties organizations to the PCLOB on suspending the use of facial recognition systems (Jan. 27, 2020), <https://epic.org/wp-content/uploads/privacy/facerecognition/PCLOB-Letter-FRT-Suspension.pdf>.

<sup>5</sup> Comments of EPIC to the Department of Homeland Security, Collection and Use of Biometrics by U.S. Citizenship and Immigration Services (Oct. 13, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-DHS-BiometricNPRM-Oct2020.pdf>.

<sup>6</sup> Hamed Aleaziz, Biden Is Going To Scrap A Trump-Era Plan To Force Immigrants To Submit Eye Scans, Voice Prints, And DNA, BuzzFeed News (May 7, 2021), <https://www.buzzfeednews.com/article/hamedaleaziz/biden-scraping-trump-immigration-biometrics-plan>.

<sup>7</sup> Coalition Letter to the Metropolitan Washington Council of Governments on the NCR-FRILS Facial Recognition System (Apr. 28, 2021), <https://epic.org/wp-content/uploads/privacy/facerecognition/Coalition-Letter-MWCOG-NCRFRILS-Apr2021.pdf>.

<sup>8</sup> Letter from Chuck Bean to EPIC on Shutting Down the NCR-FRILS Facial Recognition System (May 14, 2021), <https://epic.org/wp-content/uploads/privacy/facerecognition/MWCOG-Letter-Ending-NCRFRILS.pdf>.

For further information, please contact EPIC's Facial Recognition subject-matter experts, Jeramie Scott and Jake Wiener at [jscott@epic.org](mailto:jscott@epic.org) and [wiener@epic.org](mailto:wiener@epic.org).

## **II. The Oversight Board should examine the use and abuse of aerial surveillance in domestic terrorism investigations.**

EPIC applauds the Oversight Board's thoughtful approach to the use of new technologies in domestic terrorism investigations outlined in the Notice of Public Forum and suggests that both manned surveillance via aircraft and unmanned drone surveillance are topics of particular importance. Aerial surveillance devices, including drones, can be equipped with sophisticated imaging technology that provides the ability to obtain detailed photographs of terrain, people, homes, and even small objects. Law enforcement and national security agents have deployed drones that carry cell-site simulators, high-resolution cameras, infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers.<sup>9</sup> Drones are regularly used at the border and have been increasingly used domestically. In 2020, numerous federal agencies including the Department of Homeland Security and the National Guard used aerial surveillance to monitor protesters.<sup>10</sup> EPIC urges the Oversight Board to investigate the use of aerial surveillance.

EPIC was the first privacy organization to identify and oppose the threat of drone surveillance. Today, EPIC is engaged on a variety of fronts to shape drone policy, prevent and roll back aerial surveillance programs, and address the growing dangers of corporate drone use. In the past, EPIC has fought for transparency in government/industry drone policy planning projects and used the Freedom of Information Act to uncover government use of drones. EPIC previously used the Freedom of Information Act to obtain documents detailing the capabilities of the drones used by Customs and Border Protection as well as information about a new blimp aerial surveillance system

---

<sup>9</sup> EPIC, *Drones and Aerial Surveillance* (2022), <https://epic.org/issues/surveillance-oversight/aerial-surveillance/>.

<sup>10</sup> See FOIA Request from EPIC to U.S. Customs & Border Prot. (June 12, 2020), <https://archive.epic.org/foia/cbp/blm-protest-surveillance/EPIC-20-06-12-CBP-FOIA-20200612-Request.pdf>.

developed by Rathyeon that the Army was planning at the time to implement in the Washington DC area.<sup>11</sup> For further information, please contact EPIC’s Aerial Surveillance subject-matter expert, Jeramie Scott at [jscott@epic.org](mailto:jscott@epic.org).

### **III. The Oversight Board should investigate the role of fusion centers in spreading unreliable intelligence on domestic terrorism.**

EPIC has identified fusion centers as particularly dangerous and wasteful outgrowths of counter-terrorism policy that are now being used to investigate domestic terrorism. Fusion centers have a long track record of disseminating inaccurate and biased intelligence reports across the federal government. At the same time, the main work of fusion centers is the policing of poverty, substance abuse, and property crimes that provide no counter-terrorism value. These centers provide state and local police with access to a wide range of surveillance technologies including facial recognition, nationwide automated license plate reader databases, and social media monitoring services. In 2020 fusion centers across the country surveilled racial justice protests and disseminated inaccurate intelligence predicting planned violence by Black Lives Matter protesters.<sup>12</sup> Fusion centers have, since their inception, been a source of abuse and wrongful surveillance as they exist in a nebulous space between state and federal regulation, allowing law enforcement to “policy shop” for the most permissive privacy rules and the least meaningful oversight practices.

EPIC has urged the Department of Homeland Security to conduct a thorough investigation of fusion centers.<sup>13</sup> EPIC staff have carefully reviewed the existing records on fusion centers, including

---

<sup>11</sup> EPIC Spotlight on Surveillance, *DRONES: Eyes in the Sky* (Oct. 2014), [https://archive.epic.org/privacy/surveillance/spotlight/1014/drones.html#\\_ftnref35](https://archive.epic.org/privacy/surveillance/spotlight/1014/drones.html#_ftnref35).

<sup>12</sup> See e.g. 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/>, Ryan Devereaux, *Leaked Documents Show Police Knew Far-Right Extremists Were the Real Threat at Protests, Not “Antifa”*, *The Intercept* (Jul. 15, 2020), <https://theintercept.com/2020/07/15/george-floyd-protests-police-far-right-antifa/>.

<sup>13</sup> Comments of EPIC to the Department of Homeland Security Data Privacy and Integrity Advisory Committee, October 27, 2020 Meeting and New Tasking (Nov. 10, 2020), <https://epic.org/wp-content/uploads/apa/comments/EPIC-DPIAC-Meeting-Oct-2020-Comments.pdf>.

internal fusion center documents, for a detailed report on fusion centers currently in progress. EPIC recommends that the Oversight Board investigate the role of fusion centers in policing domestic terrorism and the effect of providing state and local law enforcement with access to advanced surveillance technologies, particularly on First Amendment protected activities. For further information, please contact EPIC's Fusion Center subject-matter expert Jake Wiener at [wiener@epic.org](mailto:wiener@epic.org).

#### **IV. The Oversight Board should examine government purchases of bulk data from data brokers.**

Government purchases of data are a significant threat to privacy and safety as they enable unlawful end-runs around statutory and constitutional privacy protections, are often drawn from highly unethical sources, and can be used for powerful and untargeted surveillance. In the last decade there has been a significant expansion in the government's collection and use of personal information supplied by data brokers. The U.S. military has purchased access to X-Mode, which runs an SDK that is embedded in apps targeting Muslims.<sup>14</sup> ICE, Customs and Border Protection, the Federal Bureau of Investigation, and the Drug Enforcement Administration have all purchased access to Venntel, which aggregates location data from 80,000 apps, including X-Mode apps.<sup>15</sup> The largest data brokers offer products that merge live location tracking and social media surveillance to offer comprehensive surveillance packages.<sup>16</sup>

---

<sup>14</sup> Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, Vice (Nov. 16, 2020), <https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x>.

<sup>15</sup> Hamed Aleaziz and Caroline Haskins, *DHS Authorities Are Buying Moment-By-Moment Geolocation Cellphone Data To Track People*, BuzzFeed News (Oct. 30, 2020), <https://www.buzzfeednews.com/article/hamedaleaziz/ice-dhs-cell-phone-data-tracking-geolocation>; Joseph Cox, *How an ICE Contractor Tracks Phones Around the World*, Vice (Dec. 3, 2020), <https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps>; Joseph Cox, *The DEA Abruptly Cut Off Its App Location Data Contract*, Vice (Dec. 7, 2020), <https://www.vice.com/en/article/z3v3yy/dea-venntel-location-data>.

<sup>16</sup> Sam Biddle & Jack Poulson, *American Phone Tracking Firm Demo'd Surveillance Powers by Spying on CIA and NSA*, The Intercept (Apr. 22, 2022), <https://theintercept.com/2022/04/22/anomaly-six-phone-tracking-signal-surveillance-cia-nsa/>.

EPIC is investigating how the government buys and uses data through EPIC’s Location Data Project. EPIC has taken actions to stop apps from collecting and selling users’ location data without consent. One success story is EPIC’s case against AccuWeather, which resulted in AccuWeather changing its app to separate location access permissions for app function and for other purposes (i.e., sale to a third-party marketing company).<sup>17</sup> EPIC urges the Oversight Board to investigate the acquisition and use of bulk data, including location data, for domestic terrorism investigations. For further information, please contact EPIC’s Location Data subject-matter experts Megan Iorio and Dana Khabbaz at [iorio@epic.org](mailto:iorio@epic.org) and [khabbaz@epic.org](mailto:khabbaz@epic.org).

**V. The Oversight Board should consider how “Domestic Terrorism” as a category produces differential impacts on racial and other minority groups.**

Finally, EPIC urges the Oversight Board to take a critical approach to the definition of “domestic terrorism” and to consider explicitly how distinguishing such a category may itself exacerbate differential impacts on racial and other minority groups. Since 9/11, the federal government’s classification of “domestic” and “foreign” terrorism has been a classification rooted in race, religion, and ideology. In fact, the Department of Justice has often sidestepped statutory definitions of international terrorism to make designations of foreign or domestic terrorism based on ideology. For example, international terrorism is associated “with designated foreign terrorist organizations”<sup>18</sup>—a majority of which are Islamist<sup>19</sup>—while domestic terrorism includes ideologies such as white supremacy and anti-abortionism.<sup>20</sup> This ideology-based distinction is not only contrary

---

<sup>17</sup> *EPIC v. Accuweather*, No. 2018 CA 001870 B (D.C. Sup. Ct. 2018), <https://epic.org/documents/epic-v-accuweather/>.

<sup>18</sup> Michael German & Sara Robinson, *Wrong Priorities on Fighting Terrorism* 3, Brennan Ctr. for Just. (2018), <https://www.brennancenter.org/our-work/research-reports/wrong-priorities-fighting-terrorism>.

<sup>19</sup> *Foreign Terrorist Organizations*, U.S. Dep’t of State, <https://www.state.gov/foreign-terrorist-organizations>.

<sup>20</sup> German & Robinson, *supra* note 17, at 3.



to federal statutory terrorism definitions,<sup>21</sup> but it is also fictional. In reality, white supremacist violence can be just as transnational as the violence associated with Muslim groups.<sup>22</sup>

The distinction between violence that is considered “domestic” and that which is considered “foreign” matters because the federal government has considered foreign violence to be more threatening than domestic violence, and acts of terrorism committed by Muslims to be more serious than acts of terrorism committed by white supremacists.<sup>23</sup> The distinction also leads to “broader, more secretive, and less accountable” law enforcement investigations for acts of terrorism committed by Muslims.<sup>24</sup> This discrepancy has historically facilitated rights abuses and overcriminalization of Muslims, racial minorities, and immigrants.

Relying on a separate category of domestic terrorism is likely counterproductive to resolving this discrepancy. The creation of an independent category of “domestic terrorism” increases the likelihood that already over-criminalized minority groups will face further targeting by federal law enforcement. The present underenforcement against white supremacist terrorism is not for lack of statutory authority but instead is the result of the federal government’s discretionary de-prioritization of criminalizing white supremacist violence.<sup>25</sup> A greater prioritization of “domestic terrorism” generally will not necessarily remedy this, since the category of “domestic terrorism” also includes acts committed by racial justice protesters or what the federal government previously called “Black

---

<sup>21</sup> 18 U.S.C. § 2331(1), (5) (distinguishing international and domestic terrorism based on whether the activities “occur primarily outside the territorial jurisdiction of the United States”).

<sup>22</sup> Joel Rubin, *Washington Must Treat White Supremacist Terrorism as a Transnational Threat*, Foreign Policy (Jan. 18, 2021), <https://foreignpolicy.com/2021/01/18/washington-must-treat-white-supremacist-terrorism-as-a-transnational-threat> (discussing transnational communications among white nationalists associated with domestic white supremacist violence and highlighting disparities between criminalization of funding of Middle Eastern groups and funding of European groups).

<sup>23</sup> See generally German & Robinson, *supra* note 17.

<sup>24</sup> *Id.* at 4.

<sup>25</sup> *Id.* at 5.



Identity Extremists.”<sup>26</sup> EPIC has worked to uncover and advocate against criminalization of racial justice protesters,<sup>27</sup> including urging the federal government not to fund surveillance of Black Lives Matter protesters.<sup>28</sup> The likelihood that the federal government’s “efforts to counter domestic terrorism” will be used to further criminalize racial justice protesters is exemplified by the FBI’s replacement of “Black Identity Extremists” with “racially motivated violent extremists,” which groups acts committed by white supremacist groups with acts committed by racial justice protesters.<sup>29</sup> In practice, efforts to address “domestic terrorism” generally would fail to address decades of racially motivated criminalization and would instead provide further federal authority for over-criminalization of minority groups.<sup>30</sup>

As such, EPIC urges the Oversight Board to define “domestic terrorism” concretely and to examine separately the government’s “efforts to counter domestic terrorism” in: (1) white supremacist and far-right terrorist contexts, and (2) in contexts concerning acts committed by racial and religious minority groups. For further information, please contact EPIC’s Privacy, National Security, and Immigration subject-matter experts Jeramie Scott and Dana Khabbaz at [jscott@epic.org](mailto:jscott@epic.org) and [khabbaz@epic.org](mailto:khabbaz@epic.org).

---

<sup>26</sup> Michael German, *The FBI Targets a New Generation of Black Activists*, Brennan Ctr. for Just. (June 26, 2020), <https://www.brennancenter.org/our-work/analysis-opinion/fbi-targets-new-generation-black-activists>.

<sup>27</sup> *Privacy & Racial Justice*, EPIC, <https://epic.org/issues/democracy-free-speech/privacy-and-racial-justice>; *EPIC Seeks Documents on Protest Monitoring and Advanced Surveillance Technologies from Federally-Funded Fusion Centers*, EPIC (Mar. 18, 2021), <https://epic.org/epic-seeks-documents-on-protest-monitoring-and-advanced-surveillance-technologies-from-federally-funded-fusion-centers>.

<sup>28</sup> *EPIC, Coalition to Congress: Stop Funding Surveillance Tech Aimed at Peaceful Protesters*, EPIC (June 17, 2020), <https://epic.org/epic-coalition-to-congress-stop-funding-surveillance-tech-aimed-at-peaceful-protesters>.

<sup>29</sup> Faiza Patel, *New Domestic Terrorism Laws Are Unnecessary for Fighting White Nationalists*, Brennan Ctr. for Justice (Oct. 2, 2019), <https://www.brennancenter.org/our-work/research-reports/new-domestic-terrorism-laws-are-unnecessary-fighting-white-nationalists>; Byron Tau, *FBI Abandons Use of Term ‘Black Identity Extremism’*, Wall St. J. (July 23, 2019), <https://www.wsj.com/articles/fbi-abandons-use-of-terms-black-identity-extremism-11563921355>.

<sup>30</sup> See Mary Zerkel, *Why We Should Rethink Calling White Supremacist Violence ‘Terrorism,’* AFSC (Jan. 14, 2021), <https://www.afsc.org/blogs/news-and-commentary/problem-labeling-violence-domestic-terrorism>.

## Conclusion

EPIC applauds the Oversight Board for its new focus on domestic terrorism investigations. These investigations have the potential to cause privacy, civil liberties, and safety harms that are likely to fall heaviest on poor and minority communities, activists, and political dissidents. EPIC looks forward to engaging further with the Oversight Board to support the Board's work in this area.

Respectfully Submitted,

*Alan Butler*

Alan Butler  
EPIC Executive Director

*Jeramie Scott*

Jeramie Scott  
EPIC Senior Counsel

*John Davisson*

John Davisson  
EPIC Senior Counsel

*Megan Iorio*

Megan Iorio  
EPIC Senior Counsel

*Jake Wiener*

Jake Wiener  
EPIC Law Fellow

*Dana Khabbaz*

Dana Khabbaz  
EPIC Law Fellow