THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

Law Enforcement Facial Recognition Is a Powerful Surveillance Technology In Need of Independent Checks and Limits

The Constitution Project (TCP) is a bipartisan, not for profit organization in Washington, D.C. TCP's mission is to safeguard constitutional rights and values when they are threatened by our government's criminal justice and national security practices, and to strengthen our system of checks and balances. In recent years, TCP has issued comprehensive reports on video surveillance, police militarization, and police body cameras, as well as policy analyses and recommendations on law enforcement location tracking and foreign intelligence surveillance. TCP is actively working to examine how emerging surveillance technologies impact constitutional rights and values, and to develop protections for those rights that account for new risks while preserving reasonable and legitimate government needs.

For additional information or questions about TCP's facial recognition policy, please contact Jake Laperruque, Senior Counsel, The Constitution Project, at jlaperruque@constitutionproject.org.

I. Facial recognition is a powerful technology and will only grow more pervasive

Facial recognition is a powerful and invasive technology that, if left unchecked, represents a unique and truly alarming threat to privacy and civil liberties. Generally, facial recognition technology allows software to take an image of an individual's face and make a "face print;" a unique identifier of that person based on their facial features. It also allows software to scan a face – or a series of faces in a crowd – and run those faces against pre-existing face prints to identify a match. Current technology can scan for a match against tens of millions of pre-identified faces per second.[1] And the technology is ever-improving in its speed and sophistication.

Despite being largely absent from public debate and scrutiny, facial recognition is already frequently used by law enforcement and affects an immense number of Americans. According to the Georgetown Law Center on Privacy and Technology, one in two American adults are already enrolled in a law enforcement facial recognition network, and at least one in four police departments have the capacity to run face recognition searches.[2] In 2016 the Government Accountability Office reported that the FBI facial recognition unit (FACE Services) ran on average 4,055 searches per month over the past 4.5 years.[3]

Additionally, capabilities for "real-time" facial recognition are rapidly developing. Real-time facial recognition involves not the matching of a single, particular face from a pre-designated photo or video against a database of face prints, but rather continuous scanning of *all* faces on video feeds, to identify them and see if they match face prints on pre-selected lists.

The growing frequency of law enforcement video surveillance will significantly augment the power of facial recognition technology. Video surveillance has long presented privacy issues,[4] but we are now seeing a mass expansion of law enforcement video surveillance in a variety of areas. Law enforcement

---

[1] *See*, Francis Bea, Digital Trends, *Goodbye, Anonymity: Latest Surveillance Tech Can Search Up to 36 Million Faces Per Second* (March 25, 2012), *available at* http://www.digitaltrends.com/cool-tech/goodbye-anonymity-latest-surveillance-tech-can-search-up-to-36-million-faces-per-second/.

[2] *See*, Clare Garvie et al., Georgetown Law Center on Privacy & Technology, *The Perpetual Line-Up* (Oct. 18, 2016), *available at* https://www.perpetuallineup.org/.

[3] *See*, U.S. Government Accountability Office, GAO-16-267, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy* (May 2016), *available at* http://www.gao.gov/assets/680/677098.pdf.

[4] *See*, The Constitution Project, *Guidelines for Public Video Surveillance* (2007), *available at* http://www.constitutionproject.org/pdf/Video_Surveillance_Guidelines_Report_w_Model_Legislation4.pdf.

CCTV surveillance has been expanding for years, and will likely continue to do so.[5] Aerial surveillance, such as the "Persistent Surveillance" program in Baltimore, provides a new method of near-ubiquitous video surveillance. The vendor managing the Baltimore program hopes to expand to other cities in the near future.[6]

Most importantly, police body cameras have the potential to exponentially increase the scale of law enforcement video surveillance, and accordingly, the power of facial recognition.[7] In cities with large police forces, if officers are deployed with body cameras it will dwarf pre-existing video surveillance capability. For example, the Chicago "Blue Light" police CCTV system, viewed as controversial for its large scale, contains an average of 13 cameras per square mile.[8] If all Chicago police officers are equipped with body cameras in the near future, it will create on average an additional 50 law enforcement cameras per square mile.[9]

The prospect of this flood of new body-worn cameras – mobile, inconspicuous, and pervasive – incorporating facial recognition appears inevitable. Police can already review and apply facial recognition technology to body camera video uploaded after an officer's shift is complete. And vendors are rapidly moving to add real-time facial recognition capabilities to body cameras. The Australian police body camera vendor Strategic Systems Alliance already incorporates facial recognition technology into its device.[10] Its CEO, Travis Reddy, boasts, "As I wear this and walk around, *it's checking all the faces I walk past* … and notifying me if any of those people are on my watch list."[11] Taser, America's largest body camera vendor, has committed to adding facial recognition technology to its devices in the near future.[12] Taser vice president Steve Tuttle once suggested that with these combined technologies one day "every cop will be RoboCop."[13] The ability to activate facial recognition for mass real-time scans throughout a city creates major risks for privacy and due process rights.

II. Facial recognition presents serious risks to privacy and civil liberties

Facial recognition is a highly powerful technology that creates serious risks to privacy and civil liberties. Facial recognition can identify individuals absent any notification or consent, creating risks of overbroad use and abuse, including the cataloging and targeting of First Amendment activities.

Constitutional implications of the right to privacy in public places are shifting based on the emergence of new technologies. As Justice Sonia Sotomayor's concurring opinion in *United States v. Jones* highlighted, technological advances are changing the long-standing assumption that there is no reasonable expectation of privacy in public. Unrestricted use of new surveillance technologies could, "by making available at a relatively low cost such a substantial quantum of intimate information about any person

---

[5] Kate Dailey, BBC News Magazine, *The rise of CCTV surveillance in the US* (April 29, 2013), *available at* http://www.bbc.com/news/magazine-22274770.

[6] Monte Reel, Bloomberg, *Secret Cameras Record Baltimore's Every Move From Above* (August 23, 2016), *available at* https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.

[7] *See*, The Constitution Project, *Guidelines for the Use of Body Worn Cameras by Law Enforcement* (December 2016), *available at* http://www.constitutionproject.org/wp-content/uploads/2016/12/BodyCamerasRptOnline.pdf.

[8] *See*, Jake Laperruque, The 2016 Cato Surveillance Conference, *Ways to Use and Misuse Facial Recognition With Police Body Cameras* (December 14, 2016), *available at* https://cdn.cato.org/archive-2016/cc-12-14-16-06.mp4.

[9] *Id*.

[10] *See* Martin Kaste, NPR, *Stealth Mode? Built-In Monitor? Not All Body Cameras Are Created Equal* (Nov 2, 2015), http://www.npr.org/sections/alltechconsidered/2015/10/30/453210272/stealth-mode-built-in-monitor-not-all-body-cameras-are-created-equal.

[11] *Id* (emphasis added).

[12] *See*, Jake Laperruque, Slate, *Should Police Bodycams Come With Facial Recognition Software?* (November 22, 2016), *available at* http://www.slate.com/articles/technology/future_tense/2016/11/should_police_bodycams_come_with_facial_recognition_software.html.

[13] *Id*.

whom the Government, in its unfettered discretion, chooses to track...[,] alter the relationship between citizen and government in a way that is inimical to democratic society."[14] Facial recognition technology could create this type of power imbalance in an unprecedented way.

Facial recognition, specifically real-time facial recognition, raises the specter of law enforcement circumventing location tracking limits**.** Because location tracking is a controversial practice that impacts privacy rights—especially in documenting individuals' presence at sensitive locations—it is subject to limits. In particular, law and administrative policy require judicial approval for use of GPS trackers and stingrays, and for acquisition of cell-site location data.

Real-time facial recognition could evade these protections. With sufficient cameras, real-time facial recognition could potentially scan faces across a city, pinpoint hundreds of individuals' location within seconds, and track them continuously without any devotion of law enforcement man power. Because this process would not be tied to any judicial authorization or requirements, there would be no limit to ensure that targets of such location tracking are suspected of wrongdoing. Such an action would violate privacy rights, and bypass requirements that would otherwise apply to invasive investigative techniques.

Perhaps more disturbingly, facial recognition could be used to target specific locations and events, including those involving exercise of First Amendment rights. Police could take video nearby religious ceremonies, protests, or political rallies, and use facial recognition to create a face print of every participant and catalog their activities. Facial recognition being used in this manner is not a far-fetched concern. In recent years law enforcement has targeted such events for surveillance,[15] and during his confirmation, Attorney General Jeff Sessions refused to rule out using advanced surveillance technologies to target and catalog individuals engaging in protests, religious activities, or political rallies.[16] A 2010 FBI presentation explicitly highlighted the ability to use facial recognition to identify participants at presidential campaign rallies.[17]

Beyond identification, police could also target sensitive events and locations, running facial recognition scans to find any participants with an outstanding warrant, and arrest them as a form of selective persecution and to discourage participation. Agency rules and practical limits are not sufficient to prevent this type of abuse.[18] Even if the government does not engage in such activities, the mere threat of their occurrence could chill First Amendment protected activities.

Finally, absent restrictions on the category of offenses for which facial recognition can be used for, the potential exists for "arrest at will authority." Many cities have significant numbers of active arrest warrants for minor, non-violent crimes. For instance, a 2015 Department of Justice investigation reveals that Ferguson, Missouri had active, outstanding municipal arrest warrants – mostly for minor offenses such as unpaid fines for traffic violations – for 16,000 people in a municipality with population of

---

[14] *See United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

[15] *See e.g.*, George Joseph, The Intercept, *Exclusive: Feds Regularly Monitored Black Lives Matters Since Ferguson* (July 24, 2015), *available* at https://theintercept.com/2015/07/24/documents-show-department-homeland-security-monitoring-black-lives-matter-since-ferguson/; *see also*, The American Civil Liberties Union, *Factsheet: The NYPD Muslim Surveillance Program*, *available at* https://www.aclu.org/other/factsheet-nypd-muslim-surveillance-program?redirect=factsheet-nypd-muslim-surveillance-program.

[16] Sen. Richard Blumenthal, *Nomination of Jeff Sessions to be Attorney General of the United States Questions for the Record* (January 17, 2017), *available at* https://www.judiciary.senate.gov/imo/media/doc/Sessions%20Responses%20to%20Blumenthal%20QFRs.pdf.

[17] *See*, Richard W. Vorder Bruegge, Federal Bureau of Investigations, *Facial Recognition and Identification Initiatives*, p 4, *available at* https://www.eff.org/files/filenode/vorder_bruegge-facial-recognition-and-identification-initiatives_0.pdf.

[18] To quote Chief Justice John Roberts "Probably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols." *Riley v. California*, 573 U.S. ___ (2014).

21,000.[19] Facial recognition technology could provide officers with notification any time they are in vicinity of an individual with a warrant for a minor, arrestable offense. Officers could exercise this power to selectively target protesters, minorities, or an individual with whom they simply have a negative interaction.

III. In light of these serious risks, facial recognition should be subject to independent checks and limits

In light of these various risks, it is essential that independent checks and limits be placed on law enforcement use of facial recognition. Independent court oversight prevents abuse, and ensures that invasive surveillance activities are properly limited to individuals where appropriate cause exists to suspect criminal wrongdoing.

There should be court approval, using a probable cause standard, for two types of facial recognition uses: First, to scan and identify a specific face in a photo or video; and second, to develop a face print of a specific face at a given location, for the purpose of creating a profile based on presence at a place or event for future use, a serious risk if cataloging sensitive activities or interactions. In both situations, particularization should be required: the government should be required to obtain court approval for each individual face that the technology is to be used for, and mass face identification scans should not be permitted. Such rules would prevent circumvention of existing limits on the investigative process, and thwart identification and targeting of individuals for exercising First Amendment-protected activities.

"Real-time" continuous scanning of cameras for the faces of certain suspects and dangerous persons should be subject to additional limits, for several reasons. Unlike the above situations that are particularized, this would involve scans of *all* individuals – absent suspicion – to determine if they match with a designated suspect. And whereas the previous situations apply to a static moment in time, this type of surveillance would be continuous for a prolonged period of time.[20] Finally, while the above situations would only apply to a single camera – or perhaps a small set of cameras identifying the same face from different angles – this type of surveillance could simultaneously apply to thousands of cameras throughout a large geographic area.

There are many forms that such additional limits could take. First, top law enforcement officers – such as state Attorneys General[21] – could be required to certify that such surveillance is necessary. Second, "real-time" continuous scanning could be limited to situations where an active arrest warrant exists for a violent crime. Third, connection to a legitimate national security threats, or an ongoing threat of death or serious bodily harm, could be required. Fourth, scanning could be limited to specific situations – such as large events or locations like stadiums – where there is heightened risk of harm to a large number of people. A combination of these factors could also be enacted. These restrictions – in addition to court authorization – should effectively reduce the potential for abuse, as well as limit pervasive and mass tracking to situations of absolute necessity.

Finally, given the potential for mass arrests or "arrest at will authority," lawmakers should strongly consider limiting the set of crimes for which any form of law enforcement facial recognition can be used. The most effective way to remedy this concern may be to address overcriminalization issues, but so long as such issues remain ongoing, limiting facial recognition to certain crimes may be necessary to protect

[19] United States Department of Justice Civil Rights Division, *Investigation of the Ferguson Police Department* (March 4, 2015), p 55, *available at* https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/03/04/ferguson_police_department_report_1.pdf.

[20] We do not recommend a specific period of time, but believe existing rules for time limits on orders and renewals for wiretapping and location tracking could provide effective guidance.

[21] Or, for federal use, the U.S. Attorney General or another high-ranking law enforcement official.

civil rights and civil liberties. Such a measure would not be unprecedented; the Wiretap Act proscribes a limited set of crimes for which this surveillance technology may be used, and many complaints have been lodged for use of stingray location tracking for investigation of nonviolent crimes.[22] If a limit is placed on the set of crimes for which facial recognition can be used, policymakers should consider focusing on violent crimes.

IV. Government should maintain a balanced and reasonable approach to facial recognition

Despite the concerns and reservations expressed above, we believe there is a place for facial recognition in law enforcement, so long as it is based on a balanced and reasonable approach. Notably, the limits we recommend would in no way prevent identification of individuals recorded in the act of committing a crime or fleeing the scene. Nor would those limits prevent use of "real-time" facial recognition to identify dangerous fugitives at large and track ongoing national security threats in an unprecedented way. Indeed, even if facial recognition is subject to the limits we recommend, law enforcement would have far more surveillance power than it does today. This is not automatically negative, but does underscore how critical reasonable limits are.

Additionally, exceptions would further provide flexibility for law enforcement to use facial recognition in uncontroversial ways. A consent exception could allow for broader use to find missing persons, and respond rapidly to abductions. Application of emergency exceptions included in virtually all forms of electronic surveillance could ensure that law enforcement could use facial recognition to respond to imminent threats in a timely manner.

As is often the case, even with the most controversial and powerful surveillance technologies, the best approach is a balanced one. Advocating towards extremes – whether outright bans or free and unrestricted use – tends not only to ignore important needs from various stakeholders, but also to be unnecessary. We are concerned by the power of facial recognition technology, and alarmed by the lack of checks in the face of serious potential for abuse. But we believe that appropriately regulating use is both sufficient to address these concerns and in the public interest. We sincerely hope that policymakers will similarly see the utility of this balanced approach and the necessity of viewing law enforcement use of facial recognition with the utmost seriousness, and respond accordingly.

Kami Chavis
Co-Chair, The Constitution Project Committee on Policing Reform
Professor of Law and Director of the Criminal Justice Program, Wake Forest University School of Law

James Trainum
Co-Chair, The Constitution Project Committee on Policing Reform
Criminal Case Review & Consulting; Detective,
Metropolitan Police Department of DC, 1983-2010

Jeffrey Vagle
Co-Chair, The Constitution Project Committee on Policing Reform
Lecturer in Law and Executive Director, Center for Technology, Innovation and Competition, University of Pennsylvania Law School; Affiliate Scholar, Stanford Law School Center for Internet and Society

[22] *See e.g.*, Nicky Woolf, The Guardian, *Lawmakers demand details on federal use of Stingray phone surveillance* (November 9, 2015), *available at* https://www.theguardian.com/us-news/2015/nov/09/congress-stingray-surveillance-jason-chaffetz-elijah-cummings.