April 5, 2024

Re: Comments on the Preparation of the Report on the Civil Rights Implications of Facial Recognition Technology

To the U.S. Commission on Civil Rights:

I. INTRODUCTION

The Commission has requested public comment "on the civil rights implications of Facial Recognition Technology (FRT)," including "how FRT is developed, how it is being utilized by federal agencies, emerging civil rights concerns, and safeguards the federal government is implementing to mitigate potential civil rights issues."[1] The Electronic Frontier Foundation (EFF) is pleased to submit these comments.

The EFF is the leading nonprofit organization defending civil liberties in the digital world, with over 30,000 members. Founded in 1990, EFF's mission is to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF champions users through impact litigation, policy analysis, grassroots activism, and technology development.

The EFF supports a ban on governmental use of face recognition technology (FRT), based on its unreliability and threat to privacy, racial justice, free expression, and information security.[2] In support of our position, we've released research papers,[3] and advocated before legislatures[4] and courts[5] regarding the dangers of FRT. Because our

---

[1] Notice of Comm'n Public Briefing and Call for Public Comments, *Civil Rights Implications of the Federal Use of Facial Recognition Technology*, 89 Fed. Reg. 15546 (Mar. 8, 2024), https://www.federalregister.gov/documents/2024/03/04/2024-04581/sunshine-act-meeting-notice.

[2] *E.g.*, Nathan Sheard and Adam Schwartz, *The Movement to Ban Government Use of Face Recognition* (May 5, 2022), https://www.eff.org/files/2020/04/20/face-off-report-2020_1.pdf.

[3] *E.g.*, Jennifer Lynch, *Face Off: Law Enforcement Use of Face Recognition Technology* (Apr. 2020), https://www.eff.org/files/2020/04/20/face-off-report-2020_1.pdf.

[4] *E.g.*, Hayley Tsukayama, *Stop This Dangerous Bill That Would Normalize Face Surveillance in California* (April 21, 2023), https://www.eff.org/deeplinks/2023/04/stop-dangerous-bill-would-normalize-face-surveillance-california; Matthew Guariglia, *Enough is Enough. Tell Congress to Ban Federal Use of Face Recognition* (Apr. 4, 2023), https://www.eff.org/deeplinks/2023/04/enough-enough-tell-congress-ban-federal-use-face-recognition.

[5] *E.g.*, Karen Gullo, *Victory! New Jersey Court Rules Police Must Give Defendant the Facial Recognition Algorithms Used to Identify Him* (June 7, 2023),

faces are often exposed and, unlike passwords or pin numbers, cannot be remade, governments and businesses, often working in partnership, are increasingly using our faces to track our whereabouts, activities, and associations.

In these comments, EFF will demonstrate that governments should be banned from using FRT because FRT: (1) is not reliable enough to be used in determinations affecting constitutional and statutory rights or social benefits; (2) is a menace to social justice as its errors are far more pronounced when applied to people of color, members of the LGBTQ+ community, and other marginalized groups; (3) threatens privacy rights; (4) chills and deters expression; and (5) creates information security risks.[6]

II. DISCUSSION

1. Lack of Reliability

Forensic technology is often called into question years down the line, demonstrating the deficiency of governmental agencies and the legal system for determining its reliability.[7] Here, studies have not demonstrated that FRT has the appropriate level of accuracy to be used by the government or used to make decision affecting constitutional and statutory rights.

To discuss the inaccuracies of FRT, it's important to understand how it works. Two common uses are to see if a specific photo of a face (often called a "probe photo") matches: (1) a photo of any face in a database (like when law enforcement runs a face captured by a surveillance camera with databases of other faces); or (2) a photo of a particular face (like when your phone's unlock mechanism tries to match its view of your face with the stored imprints of your face). These are often called "face identification" and "face verification." Other types of FRT use a person's face, for example, to track their movements or try to guess their demographics or emotions, without necessarily

---

https://www.eff.org/deeplinks/2023/06/victory-new-jersey-court-rules-police-must-give-defendant-facial-recognition.

[6] For these same reasons, EFF supports strict regulation of private use of face recognition, including requirements of minimization and opt-in consent, enforceable by a private right of action. *E.g.*, Adam Schwartz, *Sen. Merkley Leads on Biometric Privacy* (Aug. 4, 2020), https://www.eff.org/deeplinks/2020/08/sen-merkley-leads-biometric-privacy.

[7] Spencer S. Hsu, *FBI admits flaws in hair analysis over decades*, Wash. Post (April 18, 2015), https://www.washingtonpost.com/2015/04/18/39c8d8c6- e515-11e4-b510-962fcfabc310_story.html; National Research Council, *Forensic Analysis: Weighing Bullet Lead Evidence* (2004), https://doi.org/10.17226/10924; Office of the Inspector General of the U.S. Dept. of Justice, *A Review of the FBI's Handling of the Brandon Mayfield Case* (March 2006), https://oig.justice.gov/sites/default/files/archive/special/s0601/final.pdf.

verifying or identifying a particular person; government should not use these types of FRT, either.[8]

Face recognition technology may include all or some of the following steps: (1) probe photo capture (choosing or creating the photo of the face to be identified such as selecting the still capture from a video); (2) photo editing (altering or changing the probe photo); (3) creation of a facial template (creating a "face vector" with FRT software, which is a purportedly unique imprint of the face); (4) selecting comparison data (choosing a group or database of face photos for comparison to the probe photo); and (5) algorithmic search (attempting to use FRT software to match the probe photo facial template to facial templates of the photos in the comparison data set).[9]

Errors, both human and technical, abound in every step in the process. The quality, angle, lighting, and resolution of the probe photo all impact accuracy, and yet, many law enforcement agencies that employ FRT lack quality standards for the probe photo.[10] Photo editing will alter the face template, and the face template will differ depending on the FRT software used, directly contravening the assertion that face recognition is based on unchangeable biometric information.[11] The various databases, which may include data from DMVs and local and federal law enforcement agencies, will affect the accuracy based on the quality and characteristics of the photos in those sets, as well as the demographics represented in them. Even for the demographic that FRT is least inaccurate at matching, there are errors with devastating results: Harvey Murphy Jr., a white man, was wrongfully arrested due to FRT misidentification, and then sexually assaulted while in jail.[12]

Two different types of inaccurate conclusions from FRT can result: false positives and false negatives. False positives are misidentifications: the FRT determined there is a likely match even though the match photo is not of the same person as the one in the probe image. False negatives are missed identifications: the FRT failed to find a match

---

[8] Bennett Cyphers et al., *Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-time Tracking, and More* (Oct. 7, 2021), https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification; Adam Schwartz et al., *Face Recognition Technology: Commonly Used Terms* (Oct. 7, 2021), https://www.eff.org/deeplinks/2021/10/face-recognition-technology-commonly-used-terms.

[9] Electronic Frontier Foundation, *Street Level Surveillance*, *Face Recognition*, https://sls.eff.org/technologies/face-recognition.

[10] Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com/.

[11] Electronic Frontier Foundation, *supra* note 9.

[12] Drew Harwell, *Man sues Macy's, saying false facial recognition match led to jail assault*, WASH. POST (Jan. 22, 2024), https://www.washingtonpost.com/technology/2024/01/22/facial-recognition-wrongful-identification-assault/.

when one existed. As discussed in the next section, these errors are especially pronounced for people of color, members of the LGBTQ+ community, and other marginalized groups.[13]

Existing FRT has not undergone the extensive testing necessary to determine the likelihood it produces these errors, and variance in error rate among demographic groups, and are therefore unsuitable for government use. The National Institute of Standards and Technology (NIST) conducts tests on available FRT but participation in these tests is voluntary, and many vendors' products have not been tested. Existing testing often uses identification documents and other clear, high-quality frontal images, as opposed to the kinds of probe photos the government agencies typically encounter in practical usage, such as surveillance camera images where the subject is blurry, looking away from the camera, poorly lit, partially obscured, or edited.[14] As such, the testing results allow comparisons *between* different software, but don't offer a good picture of the accuracy of facial recognition algorithms in real-world circumstances.

2. Threat to Racial and Social Justice

Accuracy of FRT depends heavily on demographics, with higher error rates when the subjects are people of color, women, members of the LGBTQ+ community, and children and the elderly.

NIST's 2019 report revealed that false positive rates were generally higher for those from West and East Africa and East Asia than for Eastern European subjects; for women than men; and for the elderly and children.[15] Other studies yielded similar results, finding that commercially available FRT performed "best on Caucasian testing subsets" and "worst

[13] Patrick Grother et al., *FRVT Part 3: Demographic Effects*, NISTIR 8280 (2019), pp. 2-3, https://doi.org/10.6028/NIST.IR.8280 [hereinafter NIST Demographics Study]; John J. Howard et al., *Quantifying the Extent to Which Race and Gender Features Determine Identity in Commercial Face Recognition Algorithms*, DEP'T OF HOMELAND SECURITY, https://www.dhs.gov/sites/default/files/publications/21_0922_st_quantifying-commercial-face-recognition-gender-and-race_updated.pdf.

[14] Patrick Grother et al., *Face Recognition Vendor Test (FRVT) Part 2: Identification*, NISTIR 8271 Draft Supplement (Sep. 2023), https://pages.nist.gov/frvt/reports/1N/frvt_1N_report.pdf.

[15] NIST Demographics Study, *supra* note 13, at 2-6.

on Asian and African" ones.[16] FRT errors are also pronounced for Black women[17] and trans and nonbinary people.[18]

These FRT inaccuracies are not academic—they cause a growing number of wrongful arrests. In addition to the case of Mr. Murphy, at least one Black woman and five Black men have been arrested for crimes they did not commit due to FRT errors. Their names are Porcha Woodruff,[19] Michael Oliver,[20] Nijeer Parks,[21] Randal Reid,[22] Alonzo Sawyer,[23] and Robert Williams.[24] Every arrest of a Black person carries the risk of excessive or even deadly police force, making FRT a threat to Black lives. Use of FRT also poses a threat to Black people's equal opportunity to access public accommodations: a public skating rink erroneously expelled a Black patron, Lamya Robinson, on the basis

---

[16] Wang Mei et al., *Racial Faces in-the-Wild: Reducing Racial Bias by Information Maximization Adaptation Network* (Jul. 27, 2019), https://arxiv.org/pdf/1812.00194.pdf.

[17] Jay Buolamwini, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[18] Amrita Khalid, *Facial recognition AI can't identify trans and non-binary people*, QUARTZ (Oct. 16, 2019), https://qz.com/1726806/facial-recognition-ai-from-amazon-microsoft-and-ibm-misidentifies-trans-and-non-binary-people.

[19] Kashmir Hill, *Eight Months Pregnant and Arrested After False Facial Recognition Match*, N.Y. TIMES (Aug. 6, 2023), https://www.nytimes.com/2023/08/06/business/facial-recognition-false-arrest.html.

[20] Elisha Anderson, *Controversial Detroit facial recognition got him arrested for a crime he didn't commit*, DETROIT FREE PRESS (Jul. 10, 2020), https://www.freep.com/story/news/local/michigan/detroit/2020/07/10/facial-recognition-detroit-michael-oliver-robert-williams/5392166002/.

[21] John General and Jon Sarlin, *A false facial recognition match sent this innocent Black man to jail*, CNN (Apr. 29, 2021), https://www.cnn.com/2021/04/29/tech/nijeer-parks-facial-recognition-police-arrest/index.html.

[22] Sudhin Thanawala, *Facial recognition technology jailed a man for days. His lawsuit joins others from Black plaintiffs*, ASSOCIATED PRESS (Sep. 24, 2023), https://apnews.com/article/mistaken-arrests-facial-recognition-technology-lawsuits-b613161c56472459df683f54320d08a7.

[23] Khari Johnson, *Face Recognition Software Led to His Arrest. It Was Dead Wrong*, WIRED (Feb. 28, 2023), https://www.wired.com/story/face-recognition-software-led-to-his-arrest-it-was-dead-wrong/.

[24] Drew Harwell, *Wrongfully arrested man sues Detroit police over false facial recognition match*, WASH. POST (Apr. 13, 2021), https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/.

of FRT misidentification.[25] Indeed, the intersectional danger is that folks who occupy multiple demographics where FRT has high error rates – like being both Black and a woman – will suffer the most.[26]

Even if face recognition technology was always accurate, or at least equally inaccurate across racial groups, it would still have an unfair racially disparate impact. Surveillance cameras are over-deployed in neighborhoods of color, making those residents more likely to be subjected to FRT. Face recognition is just the latest chapter of what FTC Commissioner Alvaro Bedoya has called "the color of surveillance."[27] Indeed, FRT harkens back to "lantern laws," which required people of color to carry candle lanterns while walking the streets after dark, so police could better see their faces and monitor their movements.[28]

3. Violation of Privacy

Like other biometric surveillance programs that collect, store, share, and combine sensitive and unique data, FRT poses critical threats to our human right to privacy.[29] Our biometrics are unique to each of us, can't be remade, and are easily accessible. FRT takes the privacy risks to a new level because it is so difficult to prevent the collection of an image of your face. Most of us expose our faces in public every day we walk out our front door. Moreover, our faces are easily accessible on social media, often linked to our names and other personal information, even if we have not personally posted or shared the photographs at issue. With the proliferation of surveillance camera networks in public spaces, FRT can facilitate the quick, cheap, and easy tracking of where we've been, who we've been with, and what we've been doing.[30]

---

[25] Whitney Kimball, *Black Teen Kicked Out of Roller Rink Because Its Face Recognition Tech Screwed Up, Predictably*, GIZMODO (Jul. 16, 2021), https://gizmodo.com/black-teen-kicked-out-of-roller-rink-because-its-face-r-1847306558.

[26] NIST Demographics Study, *supra* note 13, at 47.

[27] Shahid Buttar, *Alvaro Bedoya Highlights the Critical Connection between Civil Liberties and Civil Rights* (Apr. 25, 2019), https://www.eff.org/deeplinks/2019/04/dennis-chavez-memorial-lecture-alavaro-bedoya-highlights-critical-connection

[28] Claudia Garcia-Rojas, *The Surveillance of Blackness: From the Trans-Atlantic Slave Trade to Contemporary Surveillance Technologies*, TROUTHOUT (Mar. 3, 2016), https://truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police/.

[29] U.N. Gen. Assembly, *International Covenant on Civil and Political Rights*, 999 U.N.T.S. 171 (1966), https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[30] Bennett Cyphers et al., *supra* note 8.

Government use of face recognition also raises Fourth Amendment concerns. In recent years, the U.S. Supreme Court has repeatedly placed limits on invasive government uses of cutting-edge surveillance technologies to track our movements, like GPS devices and cell site location data.[31] Face surveillance can likewise track our movements and allows for covert, remote, and mass surveillance, far beyond the fears of the drafters of the Fourth Amendment.[32]

4. Chilling the Right to Expression

The accumulation of easily identifiable photographs and usage of FRT deters the exercise of free speech and freedom of association protected by the First Amendment, including anonymous speech, private conversations, confidential receipt of unpopular ideas, gathering news from undisclosed sources, and confidential membership in expressive organizations. For example, FRT allows faceprinting from photographs of crowds at political protests – photos which police can easily take themselves, collect from surveillance cameras, find in online social media, or seize from protesters.

Research confirms that government surveillance deters Americans from engaging in public debate and to associate with others whose values, religion, or political views may be considered unpopular.[33] This is partially based on the long-studied phenomenon of the "spiral of silence"— the significant chilling effect on an individual's willingness to publicly disclose political views when they believe their views differ from the majority.[34]

Since expressive activities often depend on freedom from surveillance, participants may reasonably fear that FRT will facilitate retaliation from police, employers, and neighbors. This fear is borne out in practice. We have seen law enforcement agencies across the country used FRT to identify protesters for Black lives.[35] These include the U.S. Park

---

[31] *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (CSLI); *United States v. Jones*, 565 U.S. 400 (2012) (GPS).

[32] Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407, 415 (Dec. 2012).

[33] Jon Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L. J. 1, 119 (Sep. 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2769645.

[34] Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. QUARTERLY, 296–311 (2016), http://journals.sagepub.com/doi/pdf/10.1177/1077699016630255.

[35] This phenomenon is not limited to the United States. https://restofworld.org/2024/facial-recognition-government-protest-surveillance/.

Police,[36] the U.S. Postal Inspection Service,[37] and local police in Baltimore,[38] New York City,[39] Pittsburgh,[40] Miami,[41] and other locales in Florida.[42]

5. Security Risks from Collection and Retention of FRT Data

All government data is at risk of breach by outsiders and misuse by insiders, and there are heightened concerns for biometric data like face data because of its unchanging character.

The number of security breaches from external actors against the government demonstrates that it is not safe for the government to collect and retain face recognition data. From government agencies like DHS to private entities like Equifax, data regarding Americans have been targeted by wrongdoers including those backed by foreign

---

[36] Justin Jouvenal and Spencer S. Hsu, *Facial recognition used to identify Lafayette Square protester accused of assault*, WASH. POST (Nov. 2, 2020), https://www.washingtonpost.com/local/legal-issues/facial-recognition-protests-lafayette-square/2020/11/02/64b03286-ec86-11ea-b4bc-3a2098fc73d4_story.html.

[37] Government Accountability Office, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021), https://www.gao.gov/assets/gao-21-518.pdf.

[38] Geofeedia, *Baltimore County Police Department and Geofeedia Partner to Protect the Public During Freddie Gray Riots*, https://www.aclunc.org/docs/20161011_geofeedia_baltimore_case_study.pdf.

[39] James Vincent, *NYPD used facial recognition to track down Black Lives Matter activist*, THE VERGE (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[40] Juliette Rihl, *Emails show Pittsburgh police officers accessed Clearview facial recognition after BLM protests,* PUBLICSOURCE (May 20, 2021), https://www.publicsource.org/pittsburgh-police-facial-recognition-blm-protests-clearview/.

[41] Connie Fossi, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC MIAMI (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/.

[42] Joanne Simpson and Marc Freeman, *South Florida police quietly ran facial recognition scans to identify peaceful protestors. Is that legal?*, SOUTH FLA. SUN SENTINEL (Jun 26, 2021), https://www.sun-sentinel.com/2021/06/26/south-florida-police-quietly-ran-facial-recognition-scans-to-identify-peaceful-protestors-is-that-legal/.

governments.[43] In fact, the faceprints of 184,000 people were stolen from a vendor of U.S. Customs and Border Protection.[44]

The information security risk also comes from inside the government: on many occasions, government employees have improperly and unlawfully used information retained by the government. For example, a 2011 state audit of law enforcement access to driver information in Minnesota revealed "half of all law-enforcement personnel in Minnesota had misused driving records."[45] Likewise, NSA staff improperly used government data for "LoveInt" – information about significant others.[46] And a 2016 *Associated Press* investigation found that "[p]olice officers across the country misuse confidential law enforcement databases to get information on romantic partners, business associates, neighbors, journalists and others for reasons that have nothing to do with daily police work."[47]

Misuse by government workers is especially problematic because many of the recorded examples involve men targeting women. For example, the AP study found officers took advantage of access to confidential information to stalk ex-girlfriends and look up home addresses of women they found attractive. [48] Similarly, a study of England's surveillance camera systems found the mostly male operators used the cameras to spy on women.[49] In

---

[43] Jack Stubbs et al., *U.S. Homeland Security, thousands of businesses scramble after suspected Russian hack*, REUTERS (Dec. 14, 2020), https://www.reuters.com/article/global-cyber-idUSKBN28O1Z3; Tara Bernard et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. TIMES (Sep. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html.

[44] Office of the Inspector General, *Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot* (Sep. 21, 2020), https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[45] Chris Francescani, *License to Spy*, MEDIUM (Dec. 1, 2014), https://medium.com/backchannel/the-drive-to-spy-80c4f85b4335.

[46] Ryan Gallagher, *How NSA Spies Abused Their Powers to Snoop on Girlfriends, Lovers, and First Dates*, SLATE (Sep. 27, 2013), https://slate.com/technology/2013/09/loveint-how-nsa-spies-snooped-on-girlfriends-lovers-and-first-dates.html.

[47] Sadie Gurman & Eric Tucker, *Across US, police officers abuse confidential databases*, ASSOC. PRESS (Sept. 28, 2016), https://apnews.com/699236946e3140659fff8a2362e16f43.

[48] *Id.*

[49] Simon Davies, *Little brother is watching you*, INDEPENDENT (Aug. 25, 1998), https://www.independent.co.uk/arts-entertainment/little-brother-is-watching-you-1174115.html (Researchers found that "10 per cent of the time spent filming women was motivated by voyeurism." One researcher noted, "It is not uncommon for operators to make `greatest hits' compilations."); *Man jailed for eight months for spying on woman*

Florida, an officer breached the driver and vehicle database to look up a local female bank teller he was interested in.[50] More than 80 officers accessed driver and vehicle information about a female Florida state trooper to retaliate against her for pulling over a Miami police officer for speeding.[51] In Ohio, officers looked through a law enforcement database to find information on an ex-mayor's wife, along with council people and spouses.[52] And in Illinois, a former police sergeant, who was convicted of murdering one ex-wife and suspected of murdering another, was found to have used police databases to check up on one of his wives before she disappeared.[53]

These security concerns are an additional threat to Americans subject to FRT and further weigh against its use by government actors.

III. CONCLUSION

In sum, government use of FRT is improper given its unreliability and the risks it poses for constitutional and fundamental rights. Thus, we urge a ban on government use of this dangerous technology. Thank you for the opportunity to submit this comment.

Respectfully Submitted,

Hannah Zhao
Staff Attorney
zhao@eff.org
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94104

---

with police camera, THEJOURNAL.IE (Sept. 26, 2014), http://www.thejournal.ie/cctv-police-spying-woman-1693080-Sep2014.

[50] Amy Pavuk, *Law-Enforcer Misuse of Driver Database Soars*, ORLANDO SENTINEL (Jan. 22, 2013), http://articles.orlandosentinel.com/2013-01-22/news/os-law-enforcement-access-databases-20130119_1_law-enforcement-officers-law-enforcers-misuse; Kim Zetter, *Cops Trolled Driver's License Database for Pic of Hot Colleague*, WIRED (Feb. 23, 2012), https://www.wired.com/2012/02/cop-database-abuse.

[51] *Florida Highway Patrol Trooper Who Stopped Miami Cop Sues After Harassment*, NBC MIAMI (Feb. 11, 2014), https://www.nbcmiami.com/news/local/florida-highway-patrol-trooper-who-stopped-miami-cop-sues-after-harassment/1958049/.

[52] Eric Lyttle, *Fairfield County Grand Jury Indicts Two over Misuse of Database for Police*, COLUMBUS DISPATCH (Apr. 24, 2015), http://www.dispatch.com/article/20150424/NEWS/304249775.

[53] Brad Flora, *What Do the Cops Have on Me?*, SLATE (Dec. 4, 2007), https://slate.com/news-and-politics/2007/12/what-the-police-can-learn-when-they-run-a-background-check-on-your-name.html.