The Heritage Foundation

CONGRESSIONAL TESTIMONY

Facial Recognition Technology: Examining Its Use by Law Enforcement

Testimony before
Subcommittee on Crime, Terrorism, and Homeland Security[1]

United States House of Representatives

July 13, 2021

Kara Frederick
Research Fellow, Technology Policy
The Heritage Foundation

My name is Kara Frederick. I am a Research Fellow for Technology Policy at The Heritage Foundation. The views I express in this testimony are my own and should not be construed as representing any official position of The Heritage Foundation.

Background

Technology has long outpaced attempts to govern it. Facial recognition technology (FRT) is no different. In a world saturated with sensors, a projected 6 billion people with access to the Internet will generate between 80 zettabytes and 90 zettabytes of data worldwide by 2025. [2] In four years, approximately 80 billion devices will be connected to the Web, creating profuse surveillance opportunities.[3] Nearly every facet of the daily life of an individual is already logged and captured—wittingly and unwittingly—by the sensors and digital applications in the new information environment.

And the barriers to entry are becoming lower and lower. In April 2019, *The New York Times* built a facial recognition "machine"—on the back of Amazon's commercial facial recognition service—that detected more than 2,750 faces in a nine-hour period, in a single park in the New York City borough of Manhattan alone, for approximately $60.[4]

Federal and state government agencies—particularly law enforcement—have wasted no time harnessing this potential. From 2011 to 2019, an internal FBI unit that provides facial recognition capabilities facilitated 390,186 searches of 153,636 photos.[5] A 2021 Government Accountability Office report indicated that 20 out of 42 federal agencies that employ law enforcement officers own or use FRT systems.[6]

The expansion of such use will continue as a stated public safety imperative. Specifically, FRT is currently used for entry at borders (Global Entry), Transportation Security Administration checkpoints (CLEAR), and more than 20 sports stadiums. Certain applications are legitimate: Success stories include the detection of Maryland's *Capital Gazette* shooter in 2018 and the detention of at least three individuals using false passports at Dulles International Airport in the Washington, DC, area that same year.[7]

But the potential for abuse by agents of the state is high. Risks include: false positives generated by inaccurate algorithms, data security vulnerabilities to hacks and leaks, curtailment of civil liberties and

individual privacy, the outsourcing of surveillance to unaccountable private companies, and the potential integration of facial recognition data with other personally identifiable information through the expansion of mass surveillance.

Technical Challenges and False Positives

FRT development is beset with technical challenges. These systems repeatedly misidentify minorities, deliver high false-positive rates, and evince algorithmic bias. In 2020, a test by the National Institute of Standards and Technology (NIST) revealed higher false positive rates for African American females among existing facial recognition algorithms.[8] The same test also discovered higher false match rates for Asian and African American faces relative to images of Caucasians. An earlier NIST test revealed that these systems misidentify African Americans at rates five to 10 times higher than white individuals.[9] As such, an over-reliance on imperfect technology can lead to wrongful scrutiny and potential violations of individual liberties.[10]

Data Security

Extensive use of FRT systems makes data security risks—vulnerability to hacks and leaks—of heightened concern due to the immutable nature of biometrics. In 2019, Department of Homeland Security subcontractor Perceptics was subject to a "malicious cyber attack," which compromised approximately 184,000 traveler images from the Customs and Border Patrol's facial recognition pilot program. At least 19 of these images were posted to the dark web.[11] In the United Kingdom in 2019, hackers exploited a biometric security firm Suprema's tool Biostar 2, spilling facial recognition data and other biometric data into the open.[12] Surveillance start-up Clearview AI, with its more than 2,400 law enforcement partners, also admitted in February 2021 that its client list was hacked.[13]

Civil Liberties and Individual Privacy

Regarding individual liberties, the FBI is leading the way in the use of FRT for domestic surveillance through its Facial Analysis, Comparison, and Evaluation (FACE) Services Unit and the Next Generation Identification–Interstate Photo System (NGI-IPS).[14] Such pervasive use raises questions over undue privacy infringements. In just one example, an FBI special agent used a facial comparison tool to scan a suspect's girlfriend's social media accounts which led to the suspect's arrest in connection with the January 6th event at the Capitol over three months later. To expand the hunt for American citizens in the Capitol on January 6th, local law enforcement ran 129 facial recognition searches through Miami's police team alone in response to the FBI's call for investigative leads in early January.[15] The private company employed by these Miami police, Clearview AI provides the ability to sift through its 3 billion image database scraped from social media sites and other corners of the Internet. On January 7th, Clearview AI saw their searches increase 26 percent.[16]

Outsourcing Surveillance and the Fourth Amendment

Reports that the Biden Administration intends to expand its outsourcing of domestic surveillance to private companies and contractors[17] unencumbered by constitutional strictures are also troubling.[18] Although government entities like the Department of Homeland Security have long used firms like social media aggregator Babel Street to identify patterns in publicly available information, a renewed push to "make use of outside expertise" for domestic spying portends potential Fourth Amendment violations.[19] Further, scandals such as IBM's 2019 use of millions of photos from unwitting citizens on the photo hosting site Flickr should not engender public trust in this type of data collection by private companies.[20] After a challenge from the American Civil Liberties Union (ACLU), even Twitter and Facebook cut off social media monitoring start-up Geofeedia's access to their products in 2016 due to its invasive practices.[21]

Mass Surveillance

Such impulses to expand and outsource domestic surveillance can lead to more pervasive methods of monitoring by law enforcement. Multiple data sources can be aggregated and synchronized to allow governments to look for patterns in citizen's behavior, and even potentially identify political dissidents. Now, faster networks with lower latency like 5G provide quick transmission and higher throughput to handle increased data flows. More compute power and compute options, such as cloud or edge computing, to sort and process the data are advancing in concert. Developments in machine

learning and sophisticated analytics that extract value from data are also growing exponentially.[22] These improvements fit together in mutually reinforcing ways. Smart city initiatives may eventually combine these developments into regional panopticons that monitor citizens at the municipal level.

Indeed, the United States is currently testing plans for the basic building blocks of large-scale surveillance. Before the initiative was abandoned under public pressure in 2021, the City of Baltimore announced the deployment of a pilot program for wide-area motion imagery in December 2019, which would provide nearly 90 percent coverage of the city with three aircraft flying simultaneously. Baltimore Police Commissioner Michael Harrison claimed Baltimore would be "the first American city to use this technology in an attempt to solve and deter violent crime."[23] Similarly, predictive policing, or the use of large data sets to predict and attempt to prevent crime "upstream" of its execution, is used in dozens of American cities via the California-based company PredPol.[24]

Even municipalities without a law enforcement remit in the United States are getting in on the game, using the COVID-19 pandemic as a justification for the deployment of expanded surveillance measures. In early 2021, Peachtree Corners, Georgia, became the first U.S. city to use AI-driven "smart" cameras to monitor social distancing and use of masks.[25]

Technical issues, hard cyber vulnerabilities, and the impulse to expand surveillance notwithstanding, FRT systems—especially *live* systems—are easily abused for political aims (e.g., to monitor political dissenters at rallies or individuals based on their ethnic makeup).

This political targeting using FRT is already demonstrable worldwide. Facial recognition purveyed the path for ethnic targeting in the western region of Xinjiang by Chinese authorities, where 1.5 million Uighers are imprisoned in reeducation camps, often through the use of FRT systems.[26] In Hong Kong, democratic protesters fearing a Chinese-style surveillance state cover their faces and use lasers to thwart monitoring by police.[27] In Russia, officials reportedly used FRT to identify and arrest dissidents, including journalists, professors, and photographers, at April 2021 protests in support of the now-detained Russian opposition leader Alexei Navalny.[28]

While authoritarian powers like China are at the bleeding edge of using FRT for internal control, the demonstrated inclination by governments to expand these powers in democratic nations renders the slope a slippery one. Right now, the United States' system offers guardrails against such use in the form of sufficient rule of law protections, openness, a free press, independent judiciary, and engaged citizenry. For example, a wave of grassroots bans against the use of facial recognition by government entities materialized in 2019 and 2020. As of January 2020, 10 state legislatures introduced bills to limit, study, or generally increase transparency surrounding the use of facial recognition.[29] Cities in California like Oakland and San Francisco, as well as Massachusetts municipalities like Brookline, Somerville, and Cambridge have enacted bans on the use of facial recognition technology by local law enforcement and city officials.[30] And as of early 2020, Indiana, Maryland, Michigan, New Hampshire, New Jersey, South Carolina, and Washington were considering varying forms of restrictions and regulation.[31] The ACLU is suing Clearview AI, and its Illinois arm filed a 2018 lawsuit against the Chicago Police Department to publicize its use of social media monitoring software.[32]

However, trendlines are foreboding. The United States nearly matches China in its surveillance coverage, with one camera for every 4.6 people, compared to China's one for 4.1 individuals.[33] Other Western democracies are expanding their use of surveillance technologies with an eye toward harnessing the latest tech developments. In January 2020, the United Kingdom's Metropolitan Police force announced it would use Live Facial Recognition to immediately identify potential suspects in real time, employing technology in areas "where intelligence suggests [they] are most likely to locate serious offenders."

Combined with near-historic low levels of public trust in the U.S. government to do "what is right," the unfettered deployment of these technologies by

government entities will continue to strain the health of the body politic without immediate and genuine safeguards.[34]

The Way Forward

To further distance itself from such practices and mitigate abuse, programmers in the United States should design with privacy in mind and continue to improve face recognition algorithms in order to mitigate false positives and increase accuracy. *We must take the time to get it right.*

To govern these technologies, U.S. lawmakers should incentivize transparency and openness, including data security and privacy protection laws that standardize collection, retention, and sharing of user data. The debate over public safety and privacy trade-offs in our republic provides an opportunity for the United States to articulate the right way to embed technology with privacy protections from the outset, in addition to maintaining a strong system of checks and balances to redress privacy infringements that do occur.

To constrain abuse and bound expansion by government agencies, a secure and privacy-protecting framework for the use of digital data obtained by FRT is requisite. To do so, Congress should:

Establish a federal data protection framework with appropriate standards and oversight for how U.S. user data is collected, stored, and shared by government entities—federal, state, and local—that use FRT. This framework should incentivize consistent, open, and transparent data practices by all law enforcement agencies. The initial focus of the effort should:

- Establish clear policies on data retention, such as time limits and the prohibition of infinite data storage.
- Categorize biometric data as "sensitive data" with additional protections, including limited interoperability to compartmentalize access between state and local law enforcement and federal entities, as well as between individual law enforcement bodies. Similar measures should be taken to stymie data integration practices with other government-collected, shared, stored, transferred or purchased biometric data to prevent mass surveillance.

Ensure any U.S. identity management system used by government actors is secure and reliable, based on proper standards and measurements, and in accordance with NIST guidelines.[35]

- Mandate built-in data privacy protections for U.S. identity management systems. This "privacy by design" concept builds in safeguards for users in the design phase of technology development. This can be done by utilizing new methods of encryption and/or differential privacy, decentralized models of data storage, or federated models of machine learning for these systems.[36]
- Test and evaluate specific algorithms used by these entities on an annual basis to mitigate false positives and help increase accuracy.[37]
- Consider recommendations that require NIST to share false-positive rates for minority groups when using one-to-many algorithms and when one photo is compared to many photos to identify a potential lead, as recommended by Heritage Foundation Visiting Fellow Brian E. Finch.[38]

Enforce data protection inspections and oversight among all parties.[39]

Update current timelines for publishing and updating all federal agencies' Privacy Impact Assessments and System of Records Notices to require dissemination every six months of program use. Submit efficacy reports on the use of FRT systems by government entities and results (e.g., wrongful arrest rates and generation of investigative lead that led to successful prosecution, etc.)

* * * * * * * * * * * * * * * * * * *

The Heritage Foundation is a public policy, research, and educational organization recognized as exempt under section 501(c)(3) of the Internal Revenue Code. It is privately supported and receives no funds from any government at any level, nor does it perform any government or other contract work.

The Heritage Foundation is the most broadly supported think tank in the United States. During 2018, it had hundreds of thousands of individual, foundation, and corporate supporters representing every state in the U.S. Its 2018 operating income came from the following sources:

Individuals 67%
Foundations 13%
Corporations 2%
Program revenue and other income 18%

The top five corporate givers provided The Heritage Foundation with 1% of its 2018 income. The Heritage Foundation's books are audited annually by the national accounting firm of RSM US, LLP.

---

[1]The concepts and recommendations throughout this testimony are drawn from the author's previous working papers and publications, including but not limited to: Center for a New American Security, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," September 3, 2020, https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem (accessed July 12, 2021), and Center for a New American Security, "Democracy by Design," December 15, 2020, https://www.cnas.org/publications/reports/democracy-by-design (accessed July 12, 2021), as well as the author's media appearances from 2019–2021.

[2]David Reinsel, Jon Gantz, and John Rydning, "Data Age 2025: The Digitization of the World From Edge to Core," International Data Corporation *White Paper* No. US44413318, November 2018, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf (accessed July 12, 2021), and News release, "The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast," International Data Corporation, June 18, 2019, https://www.idc.com/getdoc.jsp?containerId=prUS45213219 (accessed July 12, 2021).

[3]David Goldfein, keynote address, Air Force Association Air Warfare Symposium Orlando, Florida, February 23, 218, https://www.af.mil/Portals/1/documents/csaf/CSAF_AFA_Orlando-23Feb18.PDF (accessed July 12, 2021), and Gil Press, "IoT Mid-Year Update from IDC and Other Research Firms," *Forbes*, August 5, 2016, https://www.forbes.com/sites/gilpress/2016/08/05/iot-mid-year-update-from-idc-and-other-research-firms/#16ec3e8355c5 (accessed July 12, 2021).

[4]According to *The New York Times* article, not every one of the 2,750 faces detected is necessarily unique. Sahil Chinoy, "We Built an 'Unbelievable' (but Legal) Facial Recognition Machine," *The New York Times*, April 16, 2019, https://www.nytimes.com/interactive/2019/04/16/opiniohttps://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.htmln/facial-recognition-new-york-city.html (accessed July 12, 2021).

[5]Gretta L. Goodwin, Director Homeland Security and Justice, "Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains," testimony before the Committee on Oversight and Reform, U.S. House of Representatives, June 4, 2019, https://www.gao.gov/assets/gao-19-579t.pdf (accessed July 12, 2021).

[6]Government Accountability Office, "Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks," GAO-21-518, June 29, 2021, p. 1, https://www.gao.gov/products/gao-21-518 (accessed July 12, 2021).

[7]U.S. Customs and Border Patrol, "Dulles CBP's New Biometric Verification Technology Catches Third Impostor in 40 Days," October 2, 2018, https://www.cbp.gov/newsroom/national-media-release/dulles-cbp-s-new-biometric-verification-technology-catches-third (accessed July 12, 2021).

[8]National Institute of Standards and Technology, "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects," NISTIR 8280, December 2019, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (accessed July 12, 2021).

[9]Tom Simonite, "The Best Algorithms Struggle to Recognize Black Faces Equally," *Wired*, July 22, 2019, https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/ (accessed July 12, 2021).
[10]Kashmir Hill, "Wrongfully Accused by an Algorithm," *The New York Times*, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html (accessed July 12, 2021).
[11]Office of the Inspector General for Homeland Security, "Review of CBP's Major Cybersecurity Incident during a 2019 Biometric Pilot," OIG-20-71, September 21, 2020, https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf (accessed July 12, 2021).
[12]Chris Baraniuk, "Biostar Security Software 'Leaked a Million Fingerprints,'" BBC, August 14, 2019, https://www.bbc.com/news/technology-49343774 (accessed July 12, 2021).
[13]"Clearview AI: Face-collecting company database hacked," BBC, February 27, 2020, https://www.bbc.com/news/technology-51658111 (accessed July 12, 2021).
[14]Congressional Research Service, "Federal Law Enforcement Use of Facial Recognition Technology," *Report for Congress*, R46586, October 27, 2020, https://fas.org/sgp/crs/misc/R46586.pdf (accessed July 12, 2021).
[15]Drew Harwell and Craig Timberg, "How America's Surveillance Networks Helped the FBI Catch the Capitol Mob," *The Washington Post*, April 2, 2021, https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/ (accessed July 12, 2021).
[16]Kashmir Hill, "The Facial-Recognition App Clearview Sees a Spike in Use after Capitol Attack," *The New York Times*, January 9, 2021, https://www.nytimes.com/2021/01/09/technology/facial-recognition-clearview-capitol.html (accessed July 12, 2021).
[17]The role of private tech companies in the development and use of facial recognition systems, especially as they contract with law enforcement agencies, cannot be overlooked. These companies currently possess the talent, data, and know-how to make the biggest leaps in technological progress on FRT. Duly, pushes for transparency must also be focused on and conducted with these companies in mind, not solely targeted at government agencies. In fact, according to a Pew study released in 2019, Americans are actually *more* suspicious of what private companies will do with facial recognition than they are of law enforcement. More than half of American adults trust law enforcement to use facial recognition responsibly, compared to the 36 percent that trust tech companies to do so. Aaron Smith, "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly," Pew Research Center, September 5, 2019, https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (accessed July 12, 2021).
[18]Zachary Cohen and Katie Bo Williams, "Biden Team May Partner with Private Firms to Monitor Extremist Chatter Online," CNN, May 3, 2021, https://www.cnn.com/2021/05/03/politics/dhs-partner-private-firms-surveil-suspected-domestic-terrorists/index.html (accessed July 12, 2021).
[19]Ibid.; Ken Dilanian and Julia Ainsley, "DHS Weighing Major Changes to Fight Domestic Violent Extremism, Say Officials," NBC, March 25, 2021, https://www.nbcnews.com/politics/national-security/dhs-weighing-huge-changes-fight-domestic-violent-extremism-say-officials-n1262047 (accessed July 12, 2021); and Maya Villasenor, "The Wild West of Smartphone Data and Surveillance," Council on Foreign Relations, February 1, 2021, https://www.cfr.org/blog/wild-west-smartphone-data-and-surveillance (accessed July 12, 2021).
[20]Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped without Consent," NBC News, March 12, 2019, https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 (accessed July 12, 2021).
[21]Jonah Engel Bromwich, Daniel Victor, and Mike Isaac, "Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says," *The New York Times*, October 11, 2016, https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html (accessed July 12, 2021), and Curtis Waltman, "Meet Babel Street, the Powerful Social Media Surveillance Used by Police, Secret Service, and Sports Stadiums," VICE, April 17, 2017, https://www.vice.com/en_us/article/gv7g3m/meet-babel-street-the-powerful-social-media-surveillance-used-by-police-secret-service-and-sports-stadiums (accessed July 12, 2021).
[22]Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," Center for a New American Security, September 3, 2020, https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem (accessed July 12, 2021).
[23]Tim Prudente, "Federal Appeals Court Rebukes Baltimore Spy Plane Program," *The Washington Post*, June 25, 2021, https://www.washingtonpost.com/local/legal-issues/baltimore-spy-plane-court-ruling/2021/06/25/f61e972c-d5c8-11eb-9f29-e9e6c9e843c6_story.html (accessed July 12, 2021).
[24]Caroline Haskins, "Dozens of Cities Have Secretly Experimented With Predictive Policing Software," VICE, February 6, 2019, https://www.vice.com/en/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software (accessed July 12, 2021).

[25]Alex Whittler, "Peachtree Corners Installs Cameras to Monitor Use of Masks, Social Distancing," Fox News, January 20, 2021, https://www.fox5atlanta.com/news/peachtree-corners-installs-cameras-to-monitor-use-of-masks-social-distancing (accessed July 12, 2021).
[26]Paul Mozur, "One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority," *The New York Times*, April 14, 2019, https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html?utm_source=newsletter&utm_medium=email&utm_campaign=newsletter_axioscodebook&stream=technology (accessed July 12, 2021).
[27]Paul Mozur, "In Hong Kong Protests, Faces Become Weapons," *The New York Times*, July 26, 2019, https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html (accessed July 12, 2021).
[28]Ilya Arkhipov and Jake Rudnitsky, "In Moscow, Big Brother Is Watching and Recognizing Protesters," Bloomberg, May 2, 2021, https://www.bloomberg.com/news/articles/2021-05-02/in-moscow-big-brother-is-watching-and-recognizing-protesters (accessed July 12, 2021).
[29]Kate Conger, Richard Fausset, and Serge F. Kovaleski, "San Francisco Bans Facial Recognition Technology," *The New York Times*, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html?smtyp=cur&smid=tw-nytimes (accessed July 12, 2021); Sarah Ravani, "Oakland Bans Use of Facial Recognition Technology, Citing Bias Concerns," *The San Francisco Chronicle*, July 17, 2019, https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php (accessed July 12, 2021); Sarah Wu, "Somerville City Council Passes Facial Recognition Ban," *The Boston Globe*, June 27, 2019, https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html (accessed July 12, 2021); and Nathan Sheard, "Victory: Brookline Votes to Ban Face Surveillance," Electronic Frontier Foundation, December 20, 2019, https://www.eff.org/deeplinks/2019/12/victory-brookline-votes-ban-face-surveillance (accessed July 12, 2021).
[30]Ibid.
[31]Ibid.
[32]American Civil Liberties Union, "ACLU Sues Clearview AI," May 28, 2020, https://www.aclu.org/press-releases/aclu-sues-clearview-ai (accessed July 12, 2021), and American Civil Liberties Union, "ACLU of Illinois v. City of Chicago," June 21, 2018, https://www.aclu-il.org/en/cases/aclu-illinois-v-city-chicago (accessed July 12, 2021).
[33]Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem."
[34]Pew Research Center, "Public Trust in Government: 1958-2021," May 17, 2021, https://www.pewresearch.org/politics/2021/05/17/public-trust-in-government-1958-2021/ (accessed July 12, 2021).
[35]Kara Frederick, Center for a New American Security, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before Judiciary Subcommittee on Crime and Terrorism, U.S. Senate, November 5, 2019, https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Tesitmony.pdf (accessed July 12, 2021).
[36]Richard Fontaine and Kara Frederick, "Democracy's Digital Defenses," *The Wall Street Journal*, May 7, 2021, https://www.wsj.com/articles/democracys-digital-defenses-11620403161 (accessed July 12, 2021).
[37]Congressional Research Service, "Federal Law Enforcement Use of Facial Recognition Technology," R46586, October 27, 2020, p. 11, https://fas.org/sgp/crs/misc/R46586.pdf (accessed July 12, 2021).
[38]Brian E. Finch, "Addressing Legitimate Concerns About Government Use of Facial Recognition Technologies," Heritage Foundation *Legal Memorandum* No. 274, October 30, 2020, https://www.heritage.org/civil-rights/report/addressing-legitimate-concerns-about-government-use-facial-recognition.
[39]Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors."