U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY
SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT

HEARING CHARTER

Privacy in the Age of Biometrics

Wednesday, June 29, 2022
11:00 am EDT
Zoom

PURPOSE

The purpose of this hearing is to evaluate the privacy implications of biometrics technologies. The hearing will seek to define the problem space for privacy and biometrics and technical strategies for balancing privacy and security based on use cases. Members and witnesses will discuss research opportunities in privacy enhancing technologies for biometric applications and their potential to address privacy risks. They will consider a recent high-profile court case involving facial recognition technology and the privacy risks of its use without appropriate guardrails. They will also review the current Federal uses of biometric technologies and discuss strategies to ensure appropriate privacy protections in those applications.

WITNESSES

- **Ms. Candice Wright**, Director, Science, Technology Assessment, and Analytics, U.S. Government Accountability Office
- **Dr. Charles H. Romine**, Director, Information Technology Laboratory, National Institute of Standards and Technology (NIST)
- **Dr. Arun Ross**, Professor, Department of Computer Science and Engineering, Michigan State University; Site Director, NSF Center for Identification Technology Research

OVERARCHING QUESTIONS

- What are the privacy implications of various biometric technology applications?
- How do federal agencies that use biometrics approach privacy and data security?
- How can new technologies and best practices address privacy concerns associated with biometric recognition, collection, and storage?
- How can the federal research enterprise help support an appropriate balance the public goods of security and privacy?

WHAT ARE BIOMETRICS?

The International Standards Organization (ISO) defines “biometric characteristic/biometric” as a biological and behavioral characteristic of an individual from which distinguishing, repeatable biometric features can be extracted for the purpose of biometric recognition. It defines "biometric recognition," often referred to simply as "biometrics," as automated recognition of individuals based on their biological and behavior characteristic. Biometric modes include face, fingerprints, voice, iris, vein, behavioral biometrics, and genetics (including DNA).[1] There are also multimodal biometric systems which collect more than one biometric data point, e.g. a finger print and an iris. Biometric data can be used for:

- **Verification (1:1) –** an application seeks to verify whether a person is who they claim to be.
- **Identification (1:many) –** an application seeks to identify an unknown individual by comparing their biometric data to a (often very large) database and uncover a potential match.
- **Characterization** – primarily an application for facial recognition technology, characterization collects images to identify broad demographic information (e.g. age, race, gender) but does not seek to connect the biometric data to a specific identity.
- **Detection** – artificial intelligence encounters the biometric data point (i.e. a face or a voice) and detects "this is a human" or "there are four humans in this image," but does not seek to connect the biometric data to a specific identity.

PRIVACY AND BIOMETRICS

Violations of privacy with biometric systems can occur when:

- Biometric data is collected, stored, or used without an individual's knowledge or consent
- Biometric data that is collected, stored, or used by an organization is accessed by someone within the organization for unauthorized and/or inappropriate uses
- Biometric data is exposed to third parties by the organization that manages and/or collects that data.

Several high-level concepts and discrete strategies for biometrics management support privacy:

- **Data minimization.** This principle is articulated in the European Union's privacy rule, the General Data Protection Regulation. It states that "the amount of personal data that needs to be processed for a specific purpose must be kept minimal."[2]
- **Data security.** Even if the organization that captures and uses biometric data has strong systems for avoiding violations of privacy, if it does not have strong data security practices, biometric data can be stolen or exfiltrated and abused by third parties.
- **Purpose Specification.** In a 2019 report, the Department of Homeland Security's Data Privacy and Integrity Advisory Committee (DPIAC) recommended that data intended for any particular DHS screening program should not be transferred, shared or used for other purposes, whether private-sector (e.g. marketing) or government (e.g. law enforcement).[3]

[1] https://www.biometricsinstitute.org/what-is-biometrics/

[2] https://ieeexplore.ieee.org/document/9481149

[3] https://www.dhs.gov/sites/default/files/publications/Report%202019-01_Use%20of%20Facial%20Recognition%20Technology_02%2026%202019.pdf

- **Notification and consent.** Control over one's personal information though knowledge and active decision-making is a fundamental privacy principle, in part because what may be sensitive information to one individual may not be considered sensitive to another.[4] Consent is a significant challenge for many uses of biometric technology in public spaces (i.e., concerts, grocery stores, and airports), where data subjects are often not meaningfully able to consent to the collection and use of PII.
- **Limiting persistence.** Biometric systems can be designed to automatically destroy biometric data after it has been used for its intended purpose or after a specified period.
- **Noninvertibility.** Biometric systems often use cryptographic techniques to turn outputs, such as fingerprints and facial images, into digital templates and store those, rather than storing the actual image of the physical feature itself. Noninvertibility means it would be impossible to "reverse" the template to restore the physical image from it.
- **Revocability.** Privacy-protective biometric systems can ensure that digital templates can be completely revoked and replaced if the template were compromised or stolen.[5]
- **Nonlinkability.** Nonlinkability means it would not be possible to successfully match two separate templated fingerprints or images from the same person, making it harder to track an individual's activities over time and space.[6][7]
- **Avoiding promiscuous capture.** Biometric systems can be refined to ensure they only collect data from individuals who have opted in and not incidentally from other individuals nearby or in the background.

FEDERAL AGENCY USERS OF BIOMETRICS

The U.S. government has used biometrics for security and law enforcement purposes since the 1960s, if not earlier. With the development and refinement of new technologies, including new uses for artificial intelligence, federal biometrics programs have increased significantly over the past decade, both in the variety of modes and in the scope and sophistication of applications. A recent survey conducted by the U.S. Government Accountability Office found that in Fiscal Year 2020, of 24 federal agencies surveyed, 18 were using facial recognition technology.[8]

Three primary statutes govern the federal government's use and management of Americans' biometric information insofar as biometrics are a type of "record" about American citizens and resident aliens: the Privacy Act of 1974, the E-Government Act, and the Federal Information Security Modernization Act (FISMA). In accordance with these Acts, NIST issues Federal Information Processing Standards (FIPS) that govern federal computer systems.

On May 22, 2007, the OMB Deputy Director for Management under President George W. Bush issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." It defined PII as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, ***biometric records***, etc. alone, or when combined with other personal or identifying information..." The

[4] https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/consent_201605/

[5] https://www.researchgate.net/publication/339720956_On_the_Unlinkability_of_Fingerprint_Shell

[6] https://www.researchgate.net/publication/339720956_On_the_Unlinkability_of_Fingerprint_Shell

[7] https://ieeexplore.ieee.org/document/7192825

[8] https://www.gao.gov/products/gao-21-526

Obama Administration revoked and replaced M-07-16 with a new Memorandum, M-17-12, which changed the definition of PII. But it seemed to maintain that biometrics are a type of PII when they can be used to distinguish or trace the identity of an individual.[9]

BIOMETRIC PRIVACY AND THE FEDERAL SCIENCE ENTERPRISE

National Institute for Standards and Technology: Housed within the Department of Commerce, NIST has conducted research on, supported the development of standards for, and conducted technology testing and evaluation of biometrics since the technology field was dawning around the 1960s. These efforts are not primarily focused on privacy, but NIST's Information Technology Laboratory (ITL) also leads general research, standards, and testing efforts related to privacy enhancing technologies that can be applied to biometrics applications or more broadly. NIST is responsible for promulgating the standards that govern Federal computer systems, called the Federal Information Processing Standards (FIPS), in accordance with the *Federal Information Security Modernization Act* (Public Law 113-283).[10] These standards and guidelines are developed when there are no acceptable consensus-based alternatives or solutions for a particular government requirement. NIST has promulgated several FIPS standards for biometrics technologies used by Federal agencies as well as general standards for identity management, cybersecurity, and privacy that would impact federal biometrics systems. Beyond federal standards, ITL is also the accredited standards development organization for data format standards that enable the interchange of biometric data.[11]

In addition, in January 2020, NIST published the *NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management.*[12] The voluntary Framework does not include tailored guidance specific to biometrics, but it includes definitions and best practices around discrete privacy concepts. As of January 2022, it had been downloaded 65,000 times. NIST has been working to expand this popular framework by providing resources for its application to meet state privacy law requirements and promote adoption by small businesses.[13]

Department of Homeland Security: In 2015, DHS issued a Biometrics Strategic Framework: 2015-2025 which articulates a vision of "strengthen[ing] national security while respecting privacy and civil liberties."[14] The Science & Technology Directorate (S&T) at DHS performs testing and evaluation of biometric applications at the Maryland Test Facility in order to simulate the performance of a technology in specific operational use cases. However, there is no requirement for the results of these studies to be considered by DHS in procurement decision-making. S&T held a Biometric Technology Rally with industry participants in June 2021 and is currently accepting submissions for the next rally, planned for September 2022.[15] The FY2022 Budget provided $5.95 million for Biometrics and Identity Management activities within S&T.[16]

[9] https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

[10] The Federal Information Security Modernization Act (FISMA), 113th Congress, P.L.113-283.

[11] https://www.nist.gov/programs-projects/ansinist-itl-standard

[12] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.01162020.pdf

[13] https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

[14] https://www.hsdl.org/?view&did=786880

[15] https://www.dhs.gov/science-and-technology/news/2022/05/20/st-calls-submissions-2022-biometric-tech-rally

[16] https://www.dhs.gov/sites/default/files/2022-03/Science%20and%20Technology%20Directorate_Remediated.pdf

National Science Foundation: Since 2002, NSF has funded the Center for Identification Technology Research (CITeR), an Industry-University Cooperative Research Center (IUCRC) led by Clarkson University, at about $400,000 per year. The NSF Award search engine shows NSF has 91 active awards related to "biometric(s)," primarily through the Directorate on Computer and Information Science and Engineering (CISE), as well as 34 active awards related to "facial recognition." Only a handful of these appear to have a focus on privacy. However, NIST does support a great number of privacy-related projects not specific to biometrics that could nonetheless yield lessons learned for biometric applications.

Office of Science and Technology Policy (OSTP): On June 9, 2022, OSTP released a request for information on Advancing Privacy-Enhancing Technologies.[17] In October 2021, OSTP published a broad Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.[18] The RFI generated 130 responses, largely from researchers and research institutions, privacy advocacy groups, and biometrics companies.[19]

CURRENT SCIENCE COMMITTEE LEGISLATION ON BIOMETRICS PRIVACY

H.R. 4609, the *NIST for the Future Act,* broadly authorizes NIST's privacy work for the first time. Specifically, it authorizes NIST to formalize a measurement research program to inform the development of best practices, benchmarks, methodologies, procedures, and voluntary technical standards for biometric identification systems.[20] The covered modalities include, but are not limited to, fingerprints, voice, iris, face, vein, behavioral biometrics, genetics, and multimodal biometrics. Among other things, the bill instructs NIST to:

- Establish common definitions and characterizations for biometric identification systems, including privacy and consent.
- Study the use of privacy-enhancing technologies and other technical protective controls to facilitate access to public data sets for biometrics research.
- Write performance standards and guidelines for high-risk biometric identification systems, including facial recognition systems, accounting for various use cases, types of biometric identification systems, and relevant operating conditions.

The Committee marked up and favorably reported H.R. 4609 on February 18, 2022. Its provisions have been included in the *America COMPETES Act* currently being conferenced with the Senate.

In n addition, on May 3, 2022, the Committee marked up and favorably reported H.R. 847, the *Promoting Digital Privacy Technologies Act*. H.R. 847 authorizes research on privacy enhancing technologies at NIST and NSF and directs the Networking and Information Technology

[17] https://www.federalregister.gov/documents/2022/06/09/2022-12432/request-for-information-on-advancing-privacy-enhancing-technologies

[18] https://www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

[19] https://www.ai.gov/rfi/2022/86-FR-56300/Biometric-RFI-2022-combined.pdf

[20] https://docs.house.gov/billsthisweek/20220131/BILLS-117HR4521RH-RCP117-31.pdf. See section 10226, p 211.

Research and Development Program (NITRD) to perform a coordinating role for these activities. It passed the House on May 12, 2022.[21]

Clearview AI

Clearview AI is a facial recognition software company that scrapes billions of existing photos from the internet, including social media sites, in order to make virtually any person traceable on its site. In March 2022, Clearview AI announced that its "index of faces" included 20 billion images and that it was on track to have 100 billion images in its database by the end of the year. Clearview conducted this activity without the knowledge or consent of individuals and in violation of many companies' terms of service (e.g., Facebook), which forbid scrapping personal information from their websites. The Committee on Science, Space & Technology sent two letters to Clearview AI in 2020 following a massive cybersecurity breach of Clearview's list of clients and source code. Chairwoman Johnson and Chairman Foster urged the company to submit its algorithm to NIST's Facial Recognition Vendor Test following the news that Clearview obtained a contract with U.S. Immigration and Customs Enforcement.[22] Clearview complied with this request.[23]

In May 2020, ACLU sued Clearview under the Illinois Biometric Information Privacy Act (BIPA).[24] BIPA is the most protective biometrics privacy law in the country, forbidding the collection of residents' faceprints without explicit consent. Unlike many other state or federal privacy laws, BIPA allows Illinoisans who have been affected by the law to sue if companies violate their rights under the law. A settlement was reached May 9, 2022. It permanently bans Clearview, nationwide, from making its faceprint database available to most businesses and other private entities. Clearview must cease selling access to its database to any entity in Illinois, including state and local police, for five years.[25] Clearview must also give residents of Illinois the opportunity to opt out of appearing in Clearview search results.[26]

The settlement under BIPA is the first U.S.-based legal victory against the Clearview, but other countries have taken action against what they deem a violation of their citizens' privacy rights. Italy and Britain levied fines against Clearview totaling $9.3 million and $21.1 million (USD) respectively.[27,28] Canada and Australia have deemed Clearview's activities illegal.[29,30] Platforms

[21] https://www.congress.gov/bill/117th-congress/house-bill/847/actions

[22] https://science.house.gov/news/press-releases/chairs-johnson-and-foster-issue-statement-on-clearview-ais-new-contract-with-us-immigration-and-customs-enforcement

[23] https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf

[24] https://www.aclu.org/cases/aclu-v-clearview-ai

[25] https://www.washingtonpost.com/technology/2022/05/09/clearview-illinois-court-settlement/

[26] https://privacyportal.onetrust.com/webform/1fdd17ee-bd10-4813-a254-de7d5c09360a/a465fd9c-58d4-4793-b5e0-959619d71be7

[27] https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/

[28] https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

[29] https://www.nytimes.com/2021/02/03/technology/clearview-ai-illegal-canada.html

[30] https://www.reuters.com/business/cop/australia-says-us-facial-recognition-software-firm-clearview-breached-privacy-2021-11-03/

such as Facebook, Twitter, and Google have also raised challenges, issuing cease and desist orders for image scraping contrary to their terms and conditions.[31]

Since 2020, Clearview has held contracts with federal agencies totaling $584,047.[32] Thousands of police departments across the United States utilize this technology, either through formal contracts or, prior to the settlement under BIPA, via free trials offered to individual police officers. Pursuant to the Illinois settlement, Clearview can no longer offer these free trials in the United States. However, access to Clearview's database is granted to individuals working at contracting agencies at the discretion of the agency's administrators, and Clearview does not audit individual users or searches to ensure that users are law enforcement officers conducting searches germane to active investigations.[33]

[31] https://slate.com/technology/2020/02/youtube-linkedin-and-others-serve-clearview-ai-with-cease-and-desist-letters.html
[32] https://www.usaspending.gov/recipient/8cbe9b49-79af-44f4-3eb5-87296ee4a591-C/latest
[33] https://www.washingtonpost.com/washington-post-live/2022/04/27/transcript-path-forward-facial-recognition-technology-with-hoan-ton-that/