



February 19, 2013

VIA FACSIMILE

U.S. Department of Homeland Security
Science and Technology Directorate
Washington, D.C. 20528
Acting FOIA Officer/Public Liaison: Katrina Hagan
Phone: 202-254-6819
Fax: 202-254-6178

Dear Ms. Hagan:

This letter constitutes a request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC").

EPIC seeks documents concerning the development and deployment of Biometric Optical Surveillance Systems ("BOSS") technology by the Department of Homeland Security.

Background

On December 17, 2012, the Department of Homeland Security Science and Technology Directorate ("S&T") released a new Privacy Impact Assessment ("PIA") regarding its BOSS technology, which is "a facial recognition technology that matches 3D signatures from captured facial images with enrolled images stored in the system database."¹

According to the S&T PIA:

The BOSS technology consists of two cameras capable of taking stereoscopic images of a face and the back end Remote Matching System ("RMS"). Stereoscopic images are two images of the same object, taken at slightly different angles that create an illusion of 3-dimensional depth from the 2-dimensional images. The cameras transfer the pair of images to the RMS via fiber optic or

¹ Privacy Impact Assessment Update for the Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests, Dec. 17, 2012, available at: www.dhs.gov/.../PIAs/privacy_pia_st_stidpboss_dec2012.pdf

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

wireless technology. The RMS then processes and stores the two images into a 3D signature, which is the mathematical representation of the stereo-pair images that the system uses for matching. Using the BOSS facial recognition algorithms, the signature is matched against a locally stored database created from volunteers, using a combination of mathematical and statistical analysis.

BOSS is capable of capturing images of an individual at 50-100 meters in distance. The system can capture images of subjects participating from a specific distance, or be set up in a way that tracks and passively captures frontal face images of an individual as he/she moves in front of the camera.

Privacy Impact Assessment Update for the Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests, Dec. 17, 2012 at 3.²

According to its PIA, S&T plans to test this technology in a variety of scenarios, including “a single test subject, multiple test subjects, a single passive test subject, or multiple passive test subjects walking through the test bed.”³ The developer of the technology, Pacific Northwest National Laboratory (“PNNL”) will work with “a local 6,000-seat venue (the Toyota Center located in Kennewick, Washington) to serve as a long-term testbed for the project. Since 2008, the use of the Toyota Center involved integrating and conducting tests on technologies developed or acquired by PNNL under contract to support the STIDP test objectives. The Toyota center provides representative crowd dynamics using a relatively small venue with a simple footprint.”⁴

Widespread deployment of facial recognition technology carries with it a number of privacy and security concerns.⁵ Facial recognition data is personally identifiable information and improper collection, storage, and use of this information can result in identity theft or inaccurate identifications.⁶ Additionally, an individual’s ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security that facial recognition technology erodes.⁷ Finally, ubiquitous and near-effortless identification eliminates individuals’ ability to control their identities, posing special risk to protestors engaging in lawful, anonymous free speech.⁸ The U.S. Supreme Court has repeatedly upheld the right to engage in political speech

² *Id.*

³ *Id.*

⁴ *Id.*

⁵ *Biometric Identifiers*, ELEC. PRIVACY INFO. CTR.<http://epic.org/privacy/biometrics/>; Electronic Privacy Information Center Comments to the Federal Trade Commission, *Face Facts: A Forum on Facial Recognition*, Jan. 31, 2012, *available at* <http://www.ftc.gov/os/comments/facialrecognitiontechnology/00083-82624.pdf>.

⁶ *Id.* at III.C.

⁷ See Erik Larkin, *Electronic Passports May Make Traveling Americans Targets, Critics Say*, PC World (Apr. 11, 2005 4:00 AM), https://www.pcworld.com/article/120292/electronic_passports_may_make_traveling_americans_targets_critics_say.html.

⁸ See Jeffrey Rosen, *Protect Our Right to Anonymity*, N.Y. TIMES, Sept. 12, 2011.

anonymously.⁹ For these reasons, it is vital that the deployment of facial recognition technology be done transparently and thoughtfully.

The DHS recognized several of these risks associated with increased use of facial recognition technology in its Privacy Impact Assessment.¹⁰

Documents Requested

EPIC requests copies of the following agency records:

1. All contracts with the PNNL and any other researchers or companies for the development of BOSS technology;
2. All statements of work associated with BOSS technology; and
3. All technical specifications related to BOSS technology.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information ...” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.” 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

EPIC is “primarily engaged in disseminating information.” *American Civil Liberties Union v. Department of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

As discussed above, the widespread use of facial recognition technology has serious privacy implications, including implications for legitimate exercise of First Amendment rights.

Request for "News Media" Fee Status

EPIC is a “representative of the news media” for fee waiver purposes. *EPIC v. Department of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003). Based on our status as a “news media” requester, we are entitled to receive the requested record with only duplication fees assessed. Further, because disclosure of this information will “contribute significantly to public understanding of the operations or activities of the government,” any duplication fees should be waived.

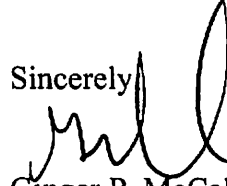
⁹ See, e.g., *Buckley v. American Constitutional Law Foundation*, 525 U.S. 182 (1999); *Talley v. California*, 362 U.S. 60 (1960); *NAACP v. Alabama*, 357 U.S. 449 (1958).

¹⁰ Privacy Impact Assessment Update for the Standoff Technology Integration and Demonstration Program: Biometric Optical Surveillance System Tests, Dec. 17, 2012, available at: www.dhs.gov/.../PIAs/privacy_pia_st_stdipboss_dec2012.pdf.

Conclusion

Thank you for your consideration of this request. As 28 C.F.R. § 16.5(d)(4) provides, I will anticipate your determination on our request within ten (10) calendar days. I can be contacted at 202-483-1140 x 102 or foia@epic.org.

Sincerely

A handwritten signature in black ink, appearing to read 'Ginger P. McCall', written in a cursive style.

Ginger P. McCall
Director
EPIC Open Government Project