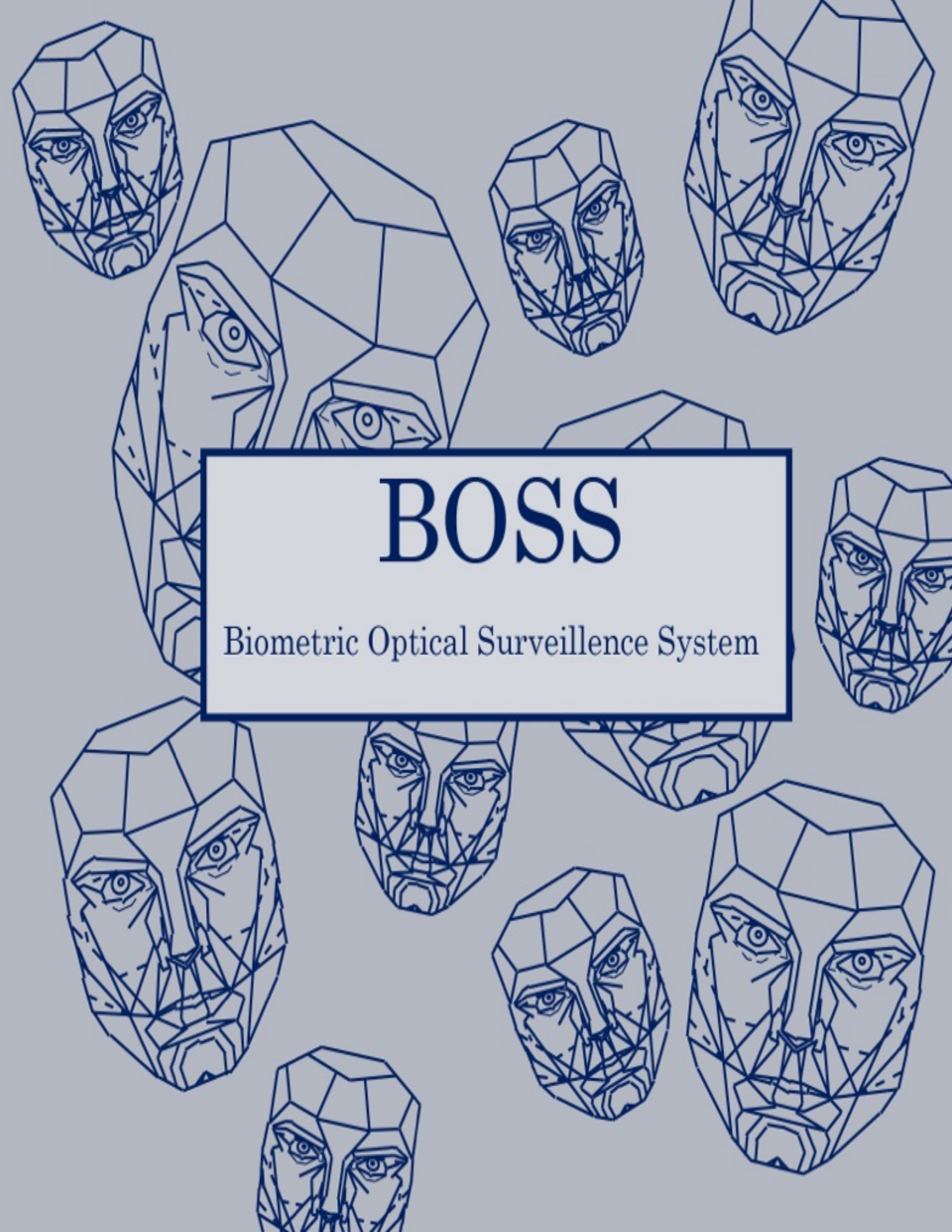
BOSS
Biometric Optical Surveillence System

Abstract

This paper summarizes facial recognition technologies' (FRT) history, current trends in FRT research, surveys FRT's implementations by the governmental and commercial sectors, and contextualizes the first purchase of a facial recognition system called Biometrical Optical Surveillance System (BOSS) by a federal agency, the Department of Homeland Security.

BOSS is in an exploratory phase and has no delineated uses. As such, this paper will also touch on technical limitations and privacy concerns of FRT's unregulated implementation in society for surveillance and security.

Introduction

Our project looks at the Biometric Optical Surveillance System produced by Electronic Warfare Associates as a lens into government supported facial recognition technologies. We track the government's involvement in the development of automated facial recognition and report on all current, publicly available information about BOSS, which was acquired and tested by Homeland Security in 2010 and 2012 respectively.

As part of this study, we look at the commercialization of the biometrics industry, the growth of private facial recognition technology companies, and these companies' relationships to government agencies. Moreover, we investigate different implementations of facial recognition technologies and survey concerns of futurists and privacy advocates who forecast its misuse.

Currently the Department of Homeland Security has not outlined a scope for implementing BOSS. DHS officially stated in a publication released 17 December 2012 that "BOSS technology will not be integrated into the existing STIDP[1] technology suite. Department of Homeland Security Science and Technology Directorate Human Factors Division is testing the technology as a standalone system to better understand the limitations of facial recognition using stereoscopic recognition techniques." The document also called BOSS an "advantageous technology" with potential implementations for national security. Therefore, the paper will consider the different applications of facial recognition to national security threat prevention.

[1] Standoff Technology Integration and Demonstration Program (STIDP) is a U.S. Department of Homeland Security program for countering explosives attacks at large public events and mass transit facilities Other technologies for consideration in this suite are infrared, millimeter-wave, and video analytics technologies for detecting person- borne improvised explosive devices at a public arena (Knudson, Kemp, Lombardo).

Context and Content

In a survey of policy considerations facing facial recognition technology, Introna and Nissenbaum (2009) posit that increased mobility and globalization mean individuals are less associated with their local contexts. As such, organizations and states rely on more accurate and reliable identity markers to track increasingly mobile individuals. Consider international banking and or border control offices implementing fingerprinting and e-passports. Whereas traditional identity managers such as biographical or attributed identifiers such as birthdate, social security numbers or addresses are falsifiable, biometric identity markers such as fingerprints, iris prints, or "face prints" seem more reliable because the human body "doesn't lie." (Introna and Nissenbaum, 2009).

Biometrical identity markers such as iris prints and fingerprints are less falsifiable than addresses and social security numbers, but they also have intrusive collection procedures. Facial recognition technology, however, identifies individuals using a unique, largely unchanged feature - a human face - and can operate from a distance. As such, since the advent of facial recognition technology research, it "promised" more flexibility and accuracy than existing identity management systems. This is exciting to not only security agencies in government, but to many industries - casinos, banks, hospitals, marketers, security system providers, to name a few.

Facial recognition technology was first developed in the 1960s at Panasonic Research in Palo Alto. The research was largely funded by the Department of Defense to gain "technological superiority" during the cold war (Gates 2013). It promised to target combatants from a distance. Woodrow Wilson Blesdoe, of Panasonic Research in Palo Alto, first manually entered key points from the face into a computer to match one image to another in a database. These key points

included the corners of the eyes and mouth, top of the nose, and hairline. Into the late 60s and 70s this system of "feature extraction" became automated. A computer algorithm could be trained to pick out these features on an image of a human face.

Throughout the 1970s researchers worked to refine picture processing and facial recognition for broader purposes such as biomedical imaging and x rays, nuclear physics and satellite images. They also programmed the computer to better detect a non-frontal facing facial images. In the late 1970s, scientists introduced the system to locate and rank images based verbal input from a human operator. Facial recognition drew from computer science, engineering and statistical methods to extract features and calculate facial matches.

Into the late 1980s and 1990s scientists relied on three main types of algorithms to perform automated facial recognition (Chellappa, Rama, Pawan Sinha, P. Jonathon Phillips, 2010). The first of these is Principal Component Analysis (PCA), which is also called the use of *eigenfaces*. These algorithms simplify the image from 2 dimensional samples by compressing data down to a 1 dimensional array. PCA work best with frontal photographs. Alternatively, Linear Discriminant Analysis algorithm puts faces into classes based on similarity. This system relies on a statistical model to assign similarity scores. This reduces the sample space of images from the total database down to smaller sets to compare alike facial images. Lastly, Elastic Bunch Graph Matching uses specific nodes on the faces to make an elastic map of the distances of facial features. This method is really good for accounting for light, pose, etc. However it is difficult to pinpoint the exact point of features on the face, so a combination the first two methods above are sometimes first used to normalize and pare down potential matches before an Elastic Bunch Graph Matching algorithm (Blackburn, Miles, Wing, Shepard 2006).

Many companies, in liaison with universities, developed separate systems using various databases to train their algorithms. Thus, in 2000, the National Institute of Standards and Technology (NIST) started a series of Facial Recognition Vendor Tests (FVRTs) to establish the facial recognitions' technical capabilities. The FVRT in 2006 noted face recognition in 2D and 3D had improved by one order of magnitude since 2002, and in the most recent US Government evaluation conducted in 2010, the identification rate was 93% for the best commercial facial recognition systems (Chellappa, et. al. 2010).

Currently, facial recognition technologies are implemented in many ways, and fall in two main categories:

(1) **verification**: Verification involves an identity check to make sure an individual is permitted into a organizations property (physical or online space). The image is captured and needs to make a *one-to-one* match to the images enrolled into the database. There are only two possible outcomes: positive (permitted) or negative (denied). This system considers a face as a visual password for entry into a protected space.

(2) **identification**: In identification, individual faces are compared to a closed-set or open-set of data. Unlike verification, identification is a *one-to-many* match. When an unknown facial image is captured, the database images in the closed-set are each ranked. A human operator will set the threshold that the images must pass to be ranked. A human operator also picks from a final match from the first-rank matches. Matching a face to an open-set of data is much more difficult because the researcher does not know if the unidentified face image exists in the data base or not (Introna & Nissenbaum, 2009). Some companies use the identification feature to identify individuals on a watch list, a VIP list, or even to track large crowd flows.

BOSS is an identification system, meaning it makes a one-to-many match, and would most probably need to run searches in an open-set data. As such, privacy advocates voice concern over DHS conducting indiscriminate scans in public places. The Department of Homeland Security took privacy concerns into consideration during their first controlled experiment in 2013 to test BOSS' accuracy. DHS released a "Privacy Impact Assessment Update for the Facial Recognition Data Collection Project." This document put forth the mandate that "DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of [privacy]...There should be no system the existence of which is a secret" (Wolfhop & Cantor 2013). It can be assumed that the DHS would operate BOSS as an overt surveillance system in large crowds and at airports. However, would the general public know whether their faces are in the database? Many privacy advocates are concerned about the lack of clear description of *who* DHS is scanning crowds for. Furthermore, once a random citizen is identified, DHS could easily link to the citizens other data for any reason, which also threatens privacy.

Research Approach

This project began with a *New York Times* article from February 1, 2014 entitled "When No One Is Just A Face in the Crowd." The article surveyed facial recognition in society and mentioned international airports tracking frequent flyers arriving and leaving a country using facial recognition.

As a group of international graduate students, the implications for facial recognition at border security and to protect national interests caught our attention. Searching "border security" and "facial recognition" revealed a slew of articles suggesting 9/11 could have been prevented had facial recognition technologies been effectively monitoring airport security. This bold claim piqued interest and slight suspicion. Could this be true? Is the US government acting upon these claims to prevent future acts of terror? We then chose to approach the project with these following questions:

(1) How the United Stated government using facial recognition for border control?
(2) Is facial recognition being used for national security?
(3) How is facial recognition use by government being regulated?
(4) How will the use of these technologies affect the lives of ordinary American citizens and foreign nationals?

We began this process by identifying a distinct technology recently tested by the Department of Homeland Security named Biometrical Optical Surveillance Systems. BOSS was already being tested for future use so it is not a completely hypothetical technology.

We approached the Science and Technology Public Affairs officers of the US Department of Defense and Department of Homeland security for an expert interview on the acquisition and testing process. Although they were unable to interview, they pointed us to academics with notable work in facial recognition technology. We were also able to access several RFPs and public reports about BOSS technology published by DHS.

Having a sense of the state of BOSS technology, and knowing it was a 3D stereoscopic technology, we then took a deep dive into literature from a variety of disciplines about facial recognition technology. We read papers from communications, computer science, statistics, policy and law, and several articles in popular media framing the debate on facial recognition use in society. This helped explain the content and social shaping of Facial Recognition technology.

Finally we read multiple chapters from recent books on the evolution of biometrics and the rise of biometric identity management in a data-centric world.

Component Summary

Poster: The design of the poster required us to distill the many steps of facial recognition technologies down to sizable bites. There are a diverse number of algorithms, facial features, and research methods. Furthermore, the newest advances in facial recognition, including the use of 3D stereoscopic images and skin texture analysis, could each take up a poster. Thus we decided the poster should summarize the broader process facial recognition follows and add details specific to the inception of BOSS. We know from Department of Homeland Security documents that BOSS creates 3D facial signatures using two images captured by two individual cameras. However, we do not know the exact facial points that the algorithm relies on.

In terms of design and aesthetics, the poster and handout espoused a few main themes: neutrality, symmetry, precision, and detailed procedures.

Neutrality: Facial recognition technology's advocates have added to the myth that technology is "apolitical." Many pro-FRT members of the biometrics industry propose using algorithms implies technological neutrality in identifying criminals or terrorists. The plain grey background, slim lines, clerical blue and orange color scheme, and overall modesty of our poster design draws from this myth.

Symmetry: Our poster layout is purposefully as symmetrical as possible. In fact, the human face is rarely symmetrical and human-to-human recognition relies on identifying this asymmetry. Our poster eliminated irregularity so as to emphasize the "machine thinking" aspects of facial recognition technology.

Precision: This theme relates to symmetry. We chose thin lines and hard corners to emphasize the desired precision with which facial recognition technology operates. Our design choices shy away from rounded objects or filled spaces.

Detailed procedures: Facial recognition algorithms follow step-by-step procedures to create a face stamp. For this reason we wanted our poster to go through the step-by-step procedure from image capture to database match.

Video and Interview: We encountered difficulty securing either an academic or government official to speak about this technology. We emailed 12 different academic and spokespeople, which points to how diverse the field is but also how nascent FRT use is for government purposes. We eventually found a researcher from the University of West Virginia to discuss the wide scope of facial recognition technologies. Although he didn't work on BOSS in particular, he was able to elaborate on the process of feature extraction and creating 3D face prints using 2D images.

Online: Our website espouses the same design principles as our poster. Our Twitter presence focused on showing the diversity of voices sounding off on facial recognition. We retweeted and posted information from the corporate sector, government sector, privacy and security companies, independent journalists, and universities. Retweets ranged from USA users to the UK to India. We hoped to show the breadth of concern around facial recognition. It is closely tied to other privacy and surveillance concerns after the revelation of governments' massive collection of citizen data.

Conclusion and Further Research

Our group found facial recognition *is* being tested for national security but not currently used. BOSS is not currently able to detect faces outdoors and there are still technical difficulties in identifying faces if they are partially covered or in bad lighting. Furthermore, the technology is limited to faces within a 100-meter radius and takes up to 30 seconds to process an image (Walhorfe 2013).

Moreover, there is no current regulation on what images are in a government database (a closed set of criminals vs. an open set of all citizens) or on where and when the Department of Homeland Security can deploy cameras linked to BOSS' facial recognition algorithm. This lack of regulation extends to commercial uses of facial recognition, for example, on smart phones or Google Glass.

Although the use of BOSS may not affect the day-to-day lives of citizens, the lack of guiding regulation protecting an individual's face in a crowd is cause for much debate amongst policy makers and privacy advocates. As the technology proliferates, more awareness will be necessary to generate action from lawmaking bodies.

Appendix- Survey

Target audience:

American adults who may be unaware of BOSS or facial recognition technologies.

Survey Rationale:

The Department of Homeland Security is testing facial recognition technology to automatically recognize known and wanted criminals at airports, border crossings, and large public gatherings. The system being tested, Biometric Optical Surveillance Systems, could potentially also be used for crowd flow analysis and tracking suspicious individuals. There is currently no regulation on the use of the cameras, databases, or spaces in which FRT can be deployed. However, once deployed an average citizen may be in sight of government cameras.

As such, we have designed a short survey to assess American adults' knowledge of facial recognition technology, and their opinions about a system that can instantly scan a crowd for wanted criminals or terrorists.

This survey hopes to assess whether the public is largely supportive or skeptical of such a system. Does the widespread use of FRT make the public feel safer or spied on? Does the public consent to their images in databases alongside criminals? How accurate should a FRT be before it is deployed?

The survey hopes to track public opinion, therefore, most of the questions include a statement followed by a 5-point scale from "strongly disagree" to "strongly agree." By collecting data this way, the researchers hope to gauge how well the use of BOSS technology in public spaces would

be received by the average citizen. Although DHS reports uphold the mandate to inform individuals of any surveillance, this survey asks about instances when the public is under surveillance but not overtly informed in order to see if national security supersedes personal privacy concerns.

Introduction to Survey Taker:

Thank you for agreeing to take a short survey on Facial Recognition Technology. This survey is intended to assess your knowledge about the government's use of this technology. It will also ask your opinions on using surveillance and face tagging systems for public safety. There are 10 questions and should take approximately 5 minutes.

1. Have you heard of "Facial Recognition Technology" before?

Yes

No

2. Should you be notified if you are under camera surveillance in a public place?

Yes

No

Not Sure

3. Do you believe the government has the right to monitor public gatherings on camera?

Yes

No

Not Sure

Please indicate how strongly you agree or disagree for the following questions:

4. The government has the right to scan the crowd for known criminals, even if they are not in the act of a crime.

Strongly Disagree

Disagree

Neutral

5. I am comfortable submitting my photo to a government database for the purposes of national security

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

6. The government should use facial recognition technologies to automatically find individuals with a criminal record in the crowd

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

7. Facial recognition technologies should be used in foreign countries to identify known targets or enemy combatants.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

8. Individuals need to be informed if there are any cameras in my vicinity linked to image databases owned by the government.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

9. Individuals should not be informed if there are any cameras in my vicinity linked to image databases.

Strongly Disagree

Disagree

Neutral

Agree

Strongly Agree

10. How accurate should Facial Recognition technologies be at matching faces before being used by the government or law enforcement to ID individuals in a crowd?

100%

95-99%

90-94%

85-89%

80-84%

70-89%

60-79%

50-59%