West Coast Publishing

Ban Biometric Recognition File 1 Public Forum April 2023

Research assistance by Kinny Torre

Thanks for using our Policy, LD, and Public Forum evidence and Breaking Down Barriers Instructional Materials.

Please don't share this material with anyone outside of your school

including via print, email, dropbox, google drive, the web, etc.

We're a small non-profit; please help us continue to provide our products.

Contact us at jim@wcdebate.com

www.wcdebate.com

WEST COAST DEBATE

Public Forum

Finding Arguments in this File

Use the table of contents on the next pages to find the evidence you need or the navigation bar on the left. We have tried to make the table of contents as easy to use as possible.

Using the arguments in this File

We encourage you to be familiar with the evidence you use. Highlight (underline) the key lines you will use in the evidence. Cut evidence from our files, incorporate your and others' research and make new files. File the evidence so that you can easily retrieve it when you need it in debate rounds. Practice reading the evidence out-loud; Practice applying the arguments to your opponents' positions; Practice defending your evidence in rebuttal speeches.

Use West Coast Evidence as a Beginning

We hope you enjoy our evidence files and find them useful. In saying this, we want to make a strong statement that we make when we coach and that we believe is vitally important to your success: DO NOT USE THIS EVIDENCE AS A SUBSTITUTE FOR YOUR OWN RESEARCH. Instead, let it serve as a beginning. Let it inform you of important arguments, of how to tag and organize your arguments, and to offer citations for further research. Don't stagnate in these files--build upon them by doing your own research for updates, new strategies, and arguments that specifically apply to your opponents. In doing so, you'll use our evidence to become a better debater.

Copying West Coast Evidence

Our policy gives you the freedom to use our evidence for educational purposes without violating our hard work.

- You may print and copy this evidence for those on your team.
- You may not electronically share nor distribute this evidence with anyone other than those on your team unless you very substantially change each page of material that you share.

For unusual situations, you can e-mail us at jim@wcdebate.com and seek our consent.

Ordering West Coast Materials

1. Visit the West Coast Web Page at www.wcdebate.com
2. E-mail us at jim@wcdebate.com
3. Fax us at 877-781-5058

Visit our web page!

www.wcdebate.com

Table of Contents

Resolved: The United States Federal Government should ban the collection of personal data through biometric recognition technology.

Topic Analysis

Topic Essay

This topic considers the ethics and efficacy of biometric recognition technology for companies, the state, and people living in and outside of the US. Biometric recognition technology gathers biological traits of individuals, authenticates data of a particular user to match specific measurements, and then, ideally, conclusively identifies (or rejects) the user as who they claim to be in the world. You are incredibly likely to already use biometric recognition technology in the banality of life i.e., devices that utilize fingerprint and facial recognition. Proponents of biometric technology tout its security and accuracy as the best in the world, yet opponents critique the insecurity of the databases as well as the nefarious uses of such deeply personal data. These issues are considered in this file.

For the Pro's opening, this file centers the issues of surveillance and data insecurity to argue for the banning of the collection of personal data through biometric recognition technology. The Surveillance State contention argues, through a historical perspective, that the US has a history of extending its security and surveillance apparatuses to further persecute and criminalized marginalized populations—particularly, but not limited to, poor communities of color. In other words, the use of biometric recognition technology is used by the state to amplify histories of racial and class bias. There is also room in the literature to argue about the racist coding that leads to racist yet seemingly neutral application of biometric surveillance. The second contention argues that, while the use of biometric data may be the most accurate and perhaps the most secure for identification, the storing of the data is a pandora's box. With hacking of large databases--like the Equifax scandal--as well as the largely permanent nature of one's biological traits, the risk of a data leak or breach could permanently destroy people's financial lives.

For the Con's opening, this file utilizes the concerns of crime and policing, as well as terrorism, to defend the use of biometric recognition technology. While the waves of police and prison abolition are again at a recent high, from the Con's perspective, the rising crime rates as well as the lack of objectivity within policing necessitate the use of biometric technology. Specifically, cities that once banned biometric recognition technology have now repealed those bans in an attempt to crackdown on violent crime. Additionally, biometric technology, like any other tool, can be used to make policing more accurate and the police more accountable because they can utilize objective and accurate information. The second contention discusses the rise of domestic terrorism in the US as well as its transnational nature. As a result, the US, as it does with other types of information for counterterrorism, ought to be working with other countries to share biometric data.

For the Pro's rebuttal strategy, their arguments center around the tenuous of biometric security as well as the necessity of trust for effective policing. The pro can argue that, as with the case of the Taliban in Afghanistan, biometric databases are high value targets for terrorist groups that seek to crackdown against dissidents. Additionally, beyond arguing that there has been a steady decrease in crime over the years, biometric recognition technology, when utilized police, amplifies the historically low levels of trust in policing institutions. As a result, crime goes underreported and vigilantism continues to increase, especially when biometric technology amplifies histories of discrimination.

For the Con's rebuttal, the strategy is centered around improving instead of abolishing the use of a tool. Specifically, most of the literature that discusses biometric technology call for the effective use of state regulations but not the banning of biometric surveillance. The effective regulation of biometric recognition technology from its application to the storage of its data, is key to its efficacy. From here, the

Con can use arguments from the Opening speech about how much of the critiques of biometrics are based in slippery slope fallacies or unlikely worse case scenarios.

For the Pro's closing strategy, I would recommend utilizing both contentions. The Surveillance State arguments project a dystopian near-future that destroys the foundations of democracy. This is a systemic impact with societal implications but, the needs of democracy may by trumped by the needs to safety. As a result, when paired with the Insecurity contention, provide the means to mitigate the Con's solvency and, at best, turn the arguments against them. Finally, the Insecurity contention can be collapsed to provided that the closing the Final Focus frames it through an invisible threshold in which a 1% probability is sufficient for a pro ballot given the irreversible stakes.

For the Con's closing strategy, I would also recommend synthesizing both contentions. The Crime contention is designed to mitigate the moral claims about racialized violence by providing a practical way to hold police accountable. So, when paired with the rising rates of domestic terrorism e.g.., White nationalism, would be able to turn the entirety of the Pro's contentions. The Crime and Terrorism contentions also function on an invisible threshold and, especially with the latter, have opportunities for high magnitude claims.

Definitions

Biometric Recognition Technology

Biometric recognition technologies are technologies that identify a person based on some aspect of their biology

Mohammad Dastbaz et al., Dastbaz is the Dean and Pro Vice Chancellor at Leeds Beckett University (LMU), faculty of Arts, Environment and Technology, 2013,

"Emerging Technologies and the Human Rights Challenge of Rapidly Expanding State Surveillance Capacities" https://www.sciencedirect.com/topics/computer-science/biometric-technology

Biometric technologies generally refer to the use of technology to identify a person based on some aspect of their biology. Fingerprint recognition is one of the first and original biometric technologies that have been grouped loosely under digital forensics. With the ever-growing number of video surveillance cameras mushrooming in large cities, the use of the data captured by these cameras has been at the center of a number of privacy and human rights storms. Following the 9/11 terrorist attack, the use of facial recognition, especially in crowded places, as a means of detecting possible threats has been debated widely. The way the technology works is straightforward. CCTVs in streets, public places, and office buildings record images 24/7, sophisticated algorithms then carry out a matching exercise with an existing database of images of potential "villains" or "targets." A match will trigger enhanced surveillance and possible future and further action. For the system to be effective, the matching database should be as wide and comprehensive as possible. It is not surprising to note that to put such a database together security agencies never (at least we cannot identify any evidence) consult or seek permission to keep people's records in their data centers. Furthermore routine phishing activities through the Internet and social networks provide a fertile ground for not only a simple one-dimensional set of data (photos and other personal data) but potentially three-dimensional datasets of associated friends, links, habits, and quite often current location. In early August 2012, Michael Bloomberg, Mayor of New York, and Ray Kelly (NYPD Commissioner) unveiled a new police surveillance infrastructure developed by Microsoft called the Domain Awareness System, which links existing police databases with live video feeds from a variety of different sources.

Biometric recognition technology conclusively proves the identity of the person through their biological traits

Aman Khanna, VP of Products at ThumbSignIn, a strong authentication provider offering a suite of two-factor and biometric solutions, March 30, **2020**,

"What's the difference between biometric authentication and identity verification?" https://www.biometricupdate.com/202003/whats-the-difference-between-biometric-authentication-and-identity-verification (accessed: 03/070/23)

However, there is a misconception that biometric authentication automatically translates into identifying exactly who the user is. In reality, there's a lot more to identity verification than just being able to match a set of biometrics. One of the biggest issues is the ability to correlate those metrics to a source of real-world identity that has been established and verified by an authority, like the government. That's where identification verification comes in. While biometric authentication might indicate that a person trying to authenticate has the same biometric markers as the person already in the system, identity verification can help conclusively prove that the person is who they say they are out in the real world. How does identification verification work? Traditionally the most common way identity verification has been done is by manually comparing a valid real-world identity document such as a passport or a driver's license with the physically present person. With the maturation of technologies like face recognition, it has become possible to reliably automate such processes. One example of identification verification is a biometric selfie. A biometric selfie would require a user to take a selfie while holding their government-issued driver's license along with a picture of the license itself. When both images are uploaded, the system would then use facial-recognition software to recognize that the photo of the person in the selfie is the same as the photo of the person in the ID, thus establishing the person's official, government-recognized identity.

PRO

Contentions

Surveillance State

Biometric identification technology can be used by police forces to create a state of permanent and omnipresent surveillance

Bernard Marr, Marr is an internationally best-selling author, popular keynote speaker, futurist, and a strategic business & technology advisor to governments and companies, August 19, **2019**

"Facial Recognition Technology: Here Are The Important Pros And Cons"
https://www.forbes.com/sites/bernardmarr/2019/08/19/facial-recognition-technology-here-are-the-important-pros-and-cons/?sh=91a43fc14d16 (accessed: 03/07/23)

The biggest drawback for facial recognition technology in most people's opinions is the threat to an individual's privacy. In fact, several cities have considered or will ban real-time facial recognition surveillance use by law enforcement, including San Francisco, Cambridge, Massachusetts, and more. These municipalities determined the risks of using the technology outweighed the benefits. Police can still use footage from personally owned devices such as Nest cameras to find criminals; it's just not allowing the government entities to use live facial recognition software.

Biometric surveillance disproportionate affect communities of color and marginalized populations

Nicol Turner Lee and Caitlin Chin, Lee is a Senior Fellow for Governance studies and Chin is a fellow at the Center for Strategic and International Studies at Brookings, April 12, **2022**,

"Police surveillance and facial recognition: Why data privacy is imperative for communities of color"
https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ (accessed: 03/07/23)

Governments and private companies have a long history of collecting data from civilians, often justifying the resulting loss of privacy in the name of national security, economic stability, or other societal benefits. But it is important to note that these trade-offs do not affect all individuals equally. In fact, surveillance and data collection have disproportionately affected communities of color under both past and current circumstances and political regimes. From the historical surveillance of civil rights leaders by the Federal Bureau of Investigation (FBI) to the current misuse of facial recognition technologies, surveillance patterns often reflect existing societal biases and build upon harmful and virtuous cycles. Facial recognition and other surveillance technologies also enable more precise discrimination, especially as law enforcement agencies continue to make misinformed, predictive decisions around arrest and detainment that disproportionately impact marginalized populations.

Biometric identification technologies further historical biases against communities of color; only federal regulation can solve.

Nicol Turner Lee and Caitlin Chin, Lee is a Senior Fellow for Governance studies and Chin is a fellow at the Center for Strategic and International Studies at Brookings, April 12, **2022**,

"Police surveillance and facial recognition: Why data privacy is imperative for communities of color" https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/ (accessed: 03/07/23)

Although suspicion toward communities of color has historical roots that span decades, new developments like facial recognition technologies (FRT) and machine learning algorithms have drastically enlarged the precision and scope of potential surveillance.[14] Federal, state, and local law enforcement agencies often rely upon tools developed within the private sector, and, in certain cases, can access massive amounts of data either stored on private cloud servers or hardware (e.g., smartphones or hard drives) or available in public places like social media or online forums.[15] In particular, several government agencies have purchased access to precise geolocation history from data aggregators that compile information from smartphone apps or wearable devices. In the general absence of stronger privacy protections at the federal or state levels to account for such advancements in technology, enhanced forms of surveillance used by police officers pose significant risks to civilians already targeted in the criminal justice system and further the historical biases affecting communities of color. Next, we present tangible examples of how the private and public sectors both play a critical role in amplifying the reach of law enforcement through facial recognition and other surveillance technologies.

Insecurity

Biometric databases are vulnerable to attack with the effects lasting forever

Nils Matthiesen, Staff writer for Avira, March 27, **2019**,

"Biometrics really are (in)secure" https://www.avira.com/en/blog/biometrics-really-are-insecure (accessed: 03/07/23)

On top of this, biometrics relies on databases – and these are vulnerable to attack. Here's an example: In the US a database containing the details of government workers was hacked in 2015 and over five million fingerprints stolen. Furthermore, the effects can be forever. Compared to password hacks, in principle the stolen biometric data can be misused for an entire lifetime if it falls into the wrong hands. The problem of not being able to just change this data raises its head once again if hackers steal biometric data and it ends up on the internet because of a database leak.

Biometric data is vulnerable, and the incumbent theft of identities is unresolvable

Yana Welinder, program manager at Carbon, a non-residential fellow at the Stanford Center for Internet and Society and an affiliate at the Berkman Center for Internet and Society at Harvard, July 13, **2016**,

"Biometrics in Banking Is Not Secure" https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure (accessed: 03/07/23)

Hacking of banks and identities is big business. An estimated 17.6 million Americans were subject to identity theft in 2014, mostly through breached bank accounts and credit cards. At this point, bank hackers are probably not looking for biometric data when attacking a bank. But even if it leaks as a by-product of a financial breach, criminals will find ways to abuse biometric data or resell it for further exploitation. And biometric data is more sensitive than other personal information banks store on behalf of their customers because unlike a credit card number (or even a name!), stolen biometric data cannot be replaced: It corresponds to a person's face or fingerprints. In general, financial institutions tend to invest more in security when they are mandated to do so and, even then, their efforts are mostly focused on minimizing their own financial loss. For example, when credit card data is stolen, other personal data of the customer can also be compromised, but credit card issuers do not specifically address that. It can take customers months to resolve various issues that result from identity theft. If the compromised data happens to be biometrics, issues of identity theft may simply be unresolvable. So any regulation of banks' use of biometrics should be designed to impose sufficient financial loss on the banks to incentivize them to design systems that effectively safeguard biometrics.

Traditional password technology is more secure than biometric technology

Yana Welinder, program manager at Carbon, a non-residential fellow at the Stanford Center for Internet and Society and an affiliate at the Berkman Center for Internet and Society at Harvard, July 13, **2016**,

"Biometrics in Banking Is Not Secure" https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-in-banking-is-not-secure (accessed: 03/07/23)

Customers could get better protection with strong, randomly generated passwords that are not reused between different accounts, are frequently updated and are coupled with two-factor authentication. There are now password manager apps like 1Password that help users generate secure passwords for all their accounts and keep track of them. Banks actually often undermine secure passwords by using login software that restricts the use of special characters or prompts customers to answer insecure security questions like "What's your mother's maiden name?" Instead of dabbling in biometrics, banks could focus on software and instructions that push customers to more secure password practices.

Rebuttals

AT: Counter-Terrorism

The threat of terrorism has decreased by 30%

Catrina Doxsee, Doxsee is an associate director and associate fellow for the Transnational Threats Project at the Center for Strategic and International Studies (CSIS), May 17, **2022**,

"Pushed to Extremes: Domestic Terrorism amid Polarization and Protest"
https://www.csis.org/analysis/pushed-extremes-domestic-terrorism-amid-polarization-and-protest#:~:text=The%20total%20number%20of%20domestic,percent%20from%20the%20prior%20year
(accesseD: 03/07/23)

CSIS data also highlighted trends in the number and type of U.S. terrorist attacks and plots. This section analyzes the data in three parts: incidents and fatalities, perpetrator ideology, and types of weapons and targets. Incidents and Fatalities The total number of domestic terrorist attacks and plots decreased from its height in 2020, though 2021 still had the second-highest number of attacks and plots in the past three decades. In 2021, there were 77 terrorist attacks and plots in the United States, a decrease of 30 percent from the prior year.

Data insecurity makes the risk of biometric identification outweigh the harm

Kelsey Atherton, Atherton is a military technology journalist based in Albuquerque, February 09, **2022**,

"The enduring risks posed by biometric identification systems"
https://www.brookings.edu/techstream/the-enduring-risks-posed-by-biometric-identification-systems/
(accessed: 03/07/23)

Biometric identification systems record immutable personal characteristics in a machine-readable format. When used by governments, they can solve a hard problem: verifying personal identity in a way that cannot be faked. But in doing so, these systems create risks for the people whose data is collected, ranging from how the data is stored to what happens if the collecting agency is not in ultimate possession of the data. The risks posed by the collection and use of biometric data were disturbingly illustrated by the Taliban take-over of Afghanistan late last year, when anti-government forces seized power and inherited a powerful biometric identification system built by the U.S. military. The Handheld Interagency Identity Detection Equipment (HIIDES) system was designed as a way for U.S. forces to be able to easily identify individuals in the field and tell friend from foe. But in the hands of the Taliban, these systems risked revealing the identities of individuals who had worked with American forces, potentially exposing them to reprisal. An unshakeable identification risked becoming a mechanism for revenge, punishment, or exclusion.

AT: Crime

Squo solves: crime rates are decreasing

US Department of Justice, September 28, **2020**,

"FBI Report on Crime Shows Decline in Violent Crime Rate for Third Consecutive Year" https://www.justice.gov/opa/pr/fbi-report-crime-shows-decline-violent-crime-rate-third-consecutive-year (accessed: 03/07/23)

Today, the Federal Bureau of Investigation released its 2019 edition of Crime in the United States, which showed that violent crime decreased nationwide for the third consecutive year. After decreases in both 2017 and 2018, the violent crime rate dropped an additional one percent this past year and the property crime rate decreased 4.5 percent. Since 1930, the FBI has tracked nationwide data on crimes and publishes its compilation each year. Submitting data to the FBI is a collective effort on the part of city, county, state, tribal, and federal law enforcement agencies to present a nationwide view of crime.

Lack of trust in the police is the major driver of gun violence in the US

Abené Clayton, Clayton is a reporter on the Guardian's Guns and Lies in America project, January 21, **2020**

"Distrust of police is major driver of US gun violence, report warns" https://www.theguardian.com/us-news/2020/jan/21/police-gun-violence-trust-report (accesseD: 03/07/23)

The lack of trust between law enforcement and the communities they serve is a major driver of gun violence in cities across the United States, a new report by the Giffords Law Center to Prevent Gun Violence warns. In many American communities, acts of police brutality, over-enforcement targeting small infractions and high numbers of unsolved shootings and homicides have eroded trust, making residents less likely to place their trust in law enforcement and more likely to seek vigilante justice, the researchers note. "Everybody has largely missed the fact that if people can't count on help from the state and its agents, they're going to take care of themselves," says David Kennedy, the director of the National Network for Safe Communities, a violence reduction research center, whose work is referenced throughout the report. "Sometimes taking care of yourself looks like day-to-day gun violence."

CON

Contentions

Crime

Arguments for banning biometric technology are based in logical fallacies; regulations of biometric tech is key to its effective use as well as holding police accountable

Ashley Johnson et al., senior policy analyst at the Information Technology and Innovation Foundation, January 09, 2023,

"Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms" https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/ (accessed: 03/07/23)

Some digital rights and civil libertarian organizations, which have a long history of opposing police's use of technology, have tapped into this new wave of public anger with law enforcement to launch new campaigns against law enforcement's use of technology, or "police tech."6 Common criticisms highlight the potential for surveillance, misuse or abuse, and racial or other bias. They also point out the cybersecurity concerns, lack of transparency, and a need to evaluate police tech's effectiveness. While some of these concerns are legitimate, some are born more out of "worst-case scenario" arguments and slippery-slope fallacies and are a smokescreen for police tech bans. This is why many police tech critics conflate legitimate concerns with worst-cases speculation and offer little in the way of solutions to address these concerns other than banning law enforcement from using certain technologies that have the potential to cause harm. But banning this promising set of technologies would cut law enforcement and the general public off from the many substantial benefits of police tech. Moreover, it would eliminate opportunities to use technology to address police violence, bias, and accountability civil rights groups have been working toward. Rather, the Department of Justice (DOJ), state lawmakers, and police departments should accelerate the testing and deployment of police tech while at the same time creating rules, regulations, and best practices for police tech that would protect the public, curtail misuse and abuse, eliminate bias, and ensure transparency and effectiveness.

Biometric data is key to the effective use of police resources to stop crime

Ashley Johnson et al., senior policy analyst at the Information Technology and Innovation Foundation, January 09, 2023,

"Police Tech: Exploring the Opportunities and Fact-Checking the Criticisms" https://itif.org/publications/2023/01/09/police-tech-exploring-the-opportunities-and-fact-checking-the-criticisms/ (accessed: 03/07/23)

Crime forecasting, or predictive policing algorithms, uses historical crime and demographic data and data collected by police patrols and stakeouts, from social media, and by other police technologies such as drones, facial recognition cameras, license plate recognition, and body cameras. The algorithms then identify patterns in criminal activity and predict crime with greater accuracy than human analysis can.11 These predictions give law enforcement the opportunity to deploy their resources more effectively.12 Several studies have evaluated the accuracy and effectiveness of machine learning algorithms at forecasting crime. A review of the available literature conducted in 2019 by researchers from Utrecht University finds mixed results, with some studies showing that predictive algorithms are effective and some showing no statistically significant results. Positive outcomes are mostly associated with algorithms that predict where crime is likely to occur, as opposed to who was likely to commit crime.13 Predictive policing can thus be useful for helping police departments determine where to allocate resources, such as more officers or street cameras.

Rising crime rates necessitate the use of biometric identification

Paresh Dave, Tech Reporter, May 12, **2022**,

"U.S. cities are backing off banning facial recognition as crime rises" https://www.reuters.com/world/us/us-cities-are-backing-off-banning-facial-recognition-crime-rises-2022-05-12/ (accessed: 03/07/23)

Homicide reports in New Orleans rose 67% over the last two years compared with the pair before, and police say they need every possible tool. "Technology is needed to solve these crimes and to hold individuals accountable," police Superintendent Shaun Ferguson told reporters as he called on the city council to repeal a ban that went into effect last year. Efforts to get bans in place are meeting resistance in jurisdictions big and small from New York and Colorado to West Lafayette, Indiana. Even Vermont, the last state left with a near-100% ban against police facial-recognition use, chipped away at its law last year to allow for investigating child sex crimes. From 2019 through 2021, about two dozen U.S. state or local governments passed laws restricting facial recognition. Studies had found the technology less effective in identifying Black people, and the anti-police Black Lives Matter protests gave the arguments momentum. But ongoing research by the federal government's National Institute of Standards and Technology (NIST) has shown significant industrywide progress in accuracy. And Department of Homeland Security testing published last month found little variation in accuracy across skin tone and gender.

Counter-Terrorism

Domestic terrorism has increased by 357%

US GAO, Government Accountability Office, March 02, 2023,

"The Rising Threat of Domestic Terrorism in the U.S. and Federal Efforts to Combat It" https://www.gao.gov/blog/rising-threat-domestic-terrorism-u.s.-and-federal-efforts-combat-it (accessed: 03/07/23)

Domestic terrorism is on the rise. Several attacks have been widely reported in the last few years. For example, in May 2022, a racially-motivated individual shot and killed 10 people in Buffalo, New York. A 2018 attack on a Pittsburgh synagogue left 11 people dead. All but eight states across the U.S. experienced at least one incident of domestic terrorism between 2010 and 2021. And over the last 10 years, domestic terrorism-related investigations have grown by 357%. Today's WatchBlog post looks at our new report on the rising threat of domestic terrorism and federal efforts to combat it. What do we know about domestic terrorism incidents? Domestic terrorism is generally defined by law as involving criminal acts dangerous to human life on U.S. soil that appear intended to coerce a civilian population or influence or affect the conduct of government. There were 231 incidents (meaning attacks or plots) that met the definition of domestic terrorism between 2010 and 2021, according to DHS. They occurred across the United States, but the greatest number of incidents occurred in states with major metropolitan areas—such as California (Los Angeles, San Diego, and San Francisco), New York (New York City), and Washington, D.C.

Biometric technology is key to combatting all forms of transnational crime

Interpol, The International Criminal Police Organization is an inter-governmental organization that has 195 member countries that fosters collaboration amongst police institutions, June 04, **2014**,

"Innovation in biometric technology key in fighting transnational crime, says INTERPOL Chief" https://www.interpol.int/en/News-and-Events/News/2014/Innovation-in-biometric-technology-key-in-fighting-transnational-crime-says-INTERPOL-Chief (accessed: 03/07/23)

LYON, France – The evolution and expansion of biometric technology is key to combating all forms of transnational crime, law enforcement and private sector partners have heard at the 8th International Symposium on Fingerprints. Organized by INTERPOL's Fingerprint unit, the three-day meeting (4-6 June) brings together some 144 delegates from 63 countries to discuss the latest advances in biometrics and how law enforcement can benefit from new technologies to maximize the opportunities for identifying criminals and solving crimes. Among the delegates attending the meeting is the Minister of Internal Affairs from Moldova, Dorin Recean, accompanied by the Head of NCB Moldova, Fredolin Lecari, who also met with INTERPOL Secretary General Ronald K. Noble and other senior officials to examine ways Moldova can enhance its use of INTERPOL's tools and services to turn back crime and better protect its citizens. Opening the meeting, Secretary General Noble highlighted the significance of global collaboration via INTERPOL's fingerprint and other biometric databases. "In an interconnected world where people cross borders so easily, the need for police to cooperate across borders – especially in sharing fingerprint data – remains very high," said the INTERPOL Chief. "Biometric technology in criminal investigations has evolved greatly, but the need for sophisticated fingerprint recordkeeping and systematic comparisons of these records remains as strong as ever," concluded Mr Noble.

Biometric tools are a powerful counterterrorism tool

Krisztina Huszti-Orban and Fionnuala Ni Aolain, Huszti-Orbán is a Research Fellow at the Human Rights Center at the University of Minnesota Law School and Senior Legal Advisor to the United Nations Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. Aoláin is Regents Professor and Robina Professor of Law, Public Policy and Society at the University of Minnesota Law School, 2020,

"Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" (accessed: 03/07/23)

As such, biometric tools and data can constitute a powerful instrument in the prevention and countering of terrorism and violent extremism by facilitating efficient and targeted responses to threats. This is also reflected in the regulatory efforts by the United Nations Security Council with its resolution 2396 requiring that States "develop and implement systems to collect biometric data" in order to "responsibly and properly identify terrorists, including foreign terrorist fighters" and to do so "in compliance with domestic and international law, including human rights law."

Rebuttals

AT: Surveillance State

The regulation of biometrics is key to its ethical use—the right to safety comes before the right to privacy

Marcus Smith and Seumas Miller, Smith is an associate professor in law at Charles Sturt University and Miller is a Distinguished Research Fellow at the Oxford Uehiro Centre for Practical Ethics, April 13, **2021**,

"The ethical application of biometric facial recognition technology"
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8042627/ (accessed: 03/07/23)

Privacy can reasonably be overridden by security considerations under some circumstances, such as when lives are at risk. After all, the right to life is, in general, a weightier moral right than the right to privacy (Miller and Walsh 2016). Thus utilising facial recognition technology to investigate a serious crime such as a murder or track down a suspected terrorist, if conducted under warrant, is surely ethically justified. On the other hand, intrusive surveillance of a suspected petty thief might not be justified. Moreover, given the importance of, so to speak, the aggregate privacy/autonomy of the citizenry, threats to life on a small scale might not be of sufficient weight to justify substantial infringements of privacy/autonomy, e.g. a low level terrorist threat might not justify citizen-wide biometric facial recognition database. Further, regulation, and associated accountability mechanisms need to be in place to ensure that, for instance, a database of biometric facial images created for a legitimate purpose, e.g. a repository of passport photos, can be accessed by border security and law enforcement officers to enable them to prevent and detect serious crimes, such as murder, but not used to identify protesters at a political rally.

Regulations prevent the creation of a surveillance state

Osonde A. Osoba and Douglas Yeung, Osoba is the Codirectfor for the Center for Scalable Computing and Analysis, a Senior Information Scientist and Professor atPardee RAND Graduate School, Yeung is the Associate Director of the Management, Technology, and Capabilities Program at RAND Homeland Security Research Division and Faculty member of the Pardee RAND Graduate School, June 17, **2020**

"Bans on Facial Recognition Are Naive. Hold Law Enforcement Accountable for Its Abuse"
https://www.rand.org/blog/2020/06/bans-on-facial-recognition-are-nave-hold-law-enforcement.html (accessed: 03/07/23)

If people distrust police officers' human interactions, how can we ever start to trust them to deploy an imperfect but potentially valuable tool like facial recognition? As a start, we need mechanisms to help independent stakeholders—regulators and the community—detect defects and hold institutions accountable. For instance, facial recognition tools could be made open to the public for independent review. Algorithmic decisions, at either an individual or systemic level, could be open to challenge from the community. Complaint procedures would need to be fair and efficient, without placing undue burden on those reporting suspected abuse.

AT: Insecurity

The flaws with biometric technology should be fixed and not banned outright

Osonde A. Osoba and Douglas Yeung, Osoba is the Codirectfor for the Center for Scalable Computing and Analysis, a Senior Information Scientist and Professor atPardee RAND Graduate School, Yeung is the Associate Director of the Management, Technology, and Capabilities Program at RAND Homeland Security Research Division and Faculty member of the Pardee RAND Graduate School, June 17, **2020**

"Bans on Facial Recognition Are Naive. Hold Law Enforcement Accountable for Its Abuse" https://www.rand.org/blog/2020/06/bans-on-facial-recognition-are-nave-hold-law-enforcement.html (accessed: 03/07/23)

Facial recognition technologies—with the assumptions of their developers embedded in their code—often perform poorly at recognizing women, older people, and those with darker skin. There's little question that these flaws exist. But banning facial recognition isn't necessarily the best response. We do not blind ourselves just because our eyes are imperfect. We learn to calibrate our trust in our vision—or we buy glasses. Technology is not so different. Even systems with known weaknesses remain important for scaling up public services. Many of us file taxes or apply for benefits on the internet, for example, even though we know such sites are vulnerable to inadvertent or malicious disruptions. Facial recognition has useful government applications as well, including airport security screening, contract tracing, and identifying missing children or trafficked people.

Collaboration solves data insecurity

Algride Pipikaite, Algirde is cybersecurity and digital transformation policy expert with a focus on public and private sector engagement and is a lawyer with over a decade of experience in the public and private sectors, September 02, **2021**,

"How to improve security of biometric data" https://www.weforum.org/agenda/2021/09/untangling-the-benefits-and-risks-of-biometrics/ (accessed: 03/07/23)

To avoid situations where biometric data could be exposed or compromised, a close cooperation between government, the private sector and civil society needs to be established. When developing digital identity ecosystems, nations face new cybersecurity challenges to ensure data confidentiality, integrity and availability on an ongoing basis. That is where different actors bring various perspectives that have to be considered and evaluated to prevent any potential harm and damage caused by a misuse, exploit or hack of the system. Managing cyber risk is already a major leadership challenge in public and private sectors. The risks associated with cyberthreats are often opaque, and it is difficult to calibrate the right nature and scale of investment in cybersecurity. Global leaders must think of potential harm caused by misuse or exploit of technology and ensure the measures are in place to use these technologies for good and include a variety of voices when developing them.