International Journal of Innovation Scientific Research and Review
Vol. 04, Issue, 12, pp.3692-3705, December 2022
Available online at http://www.journalijisr.com
SJIF Impact Factor 4.95

IJISRR

ISSN: 2582-6131

Research Article

CYBERSECURITY, FACIAL RECOGNITION, AND ELECTION INTEGRITY

***Donald L. Buresh, Ph.D., Esq.**

Morgan State University.

Received 15th October 2022; Accepted 16th November 2022; Published online 20th December 2022

ABSTRACT

This paper discusses the relationship between cybersecurity, facial recognition, and election integrity. The article highlights cybersecurity issues and then explains facial recognition technology in depth. The essay points out that blind reliance on facial recognition technology and algorithms is not a substitute for integrity when counting votes. The paper notes that facial recognition software has significant failings, particularly when attempting to identify people of color. The reason is that facial data sets typically lack a sufficient number of faces of people of color to ensure that their identification is accurate, not yielding false positives or false negatives. Transparency and accessibility are critical when identifying individuals using biometric technology and counting votes so that the votes of the people who decide to vote are counted. There is no royal road when election integrity is concerned. In the end, election integrity is dependent on individuals of integrity who are dedicated to ensuring that the will of the People is heard.

Keywords: Accessibility, Cybersecurity, Election Integrity, Facial Recognition, Individual Privacy, Nothing to Hide, Transparency, Vote Counting.

INTRODUCTION

This paper discusses the relationship between cybersecurity, facial recognition, and election integrity. The article highlights cybersecurity issues and then explains facial recognition technology in depth. The essay points out that blind reliance on facial recognition technology and algorithms is not a substitute for integrity when counting votes. The paper notes that facial recognition software has significant failings, particularly when attempting to identify people of color. The reason is that facial data sets typically lack a sufficient number of faces of people of color to ensure that their identification is accurate, not yielding false positives or false negatives. Transparency and accessibility are critical when identifying individuals using biometric technology and counting votes so that the votes of the people who decide to vote are counted. There is no royal road when election integrity is concerned. In the end, election integrity is dependent on individuals of integrity who are dedicated to ensuring that the will of the People is heard.

CYBERSECURITY CONSIDERATIONS

This section of the paper discusses the general characteristics of cybersecurity. Its purpose is to define cybersecurity and then describe the harms that cybersecurity seeks to prevent. The essay highlights the values embedded in cybersecurity law while attempting to differentiate privacy from cybersecurity.

Definition of Cybersecurity Law

According to Techopedia, cyber law is "the area of law that deals with the Internet's relationship to technological and electronic elements, including computers, software, hardware, and information systems (IS)."[1] Cyber laws help avert or decrease damages from cybercriminal activities by defending communications, freedom of speech, information access, intellectual property, and privacy concerned with Internet uses such as cell phones, email, and websites using both the hardware and software features of computing devices.[2] The explosion of Internet traffic has resulted in a significant increase in legal issues in the United States and worldwide.[3] Cyber laws vary by jurisdiction and country,and the legal outcome ranges from fines to imprisonment.[4]

Harms that Cybersecurity Law Seeks to Limit

The purpose of cybersecurity laws is to alleviate and mitigate harm to individuals.[5] This harm typically involves privacy violations, such as the disclosure of email messages and personally identifiable information that may be detrimental or embarrassing to an individual.[6]Harms that cybersecurity laws attempt to prevent identity theft and identity fraud, where these terms refer to any crime whereby an individual wrongfully procures and employs the personally identifiable information of another person through fraud or deception, usually for financial gain.[7]

The second type of harm is concerned with the theft of corporate trade secrets that are stored in an information system, where a trade secret is a commercially valuable information that is known to a limited group of individuals and where reasonable efforts are made to keep the information secret, such as confidentiality agreements between business partners and employees.[8] If a trade secret is acquired, used, or disclosed in a way that is opposed to honest commercial practices by unauthorized individuals, such an act is considered a violation of trade secret protection acts.[9] Cybersecurity laws may also try to thwart threat actors from sabotaging corporate

[1]Techopedia Staff, *Cyberlaw*, TECHOPEDIA(n.d.), *available at*https://www.techopedia.com/definition/25600/cyberlaw.

[2]*Id.*
[3]*Id.*
[4]*Id.*
[5]Jeff Kosseff, *DefiningCybersecurity Law*, 103 IOWA L. REV. 985 (2018), *available at* https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/.
[6]*Id.*
[7]DOF Staff, *Identity Theft*, UNITED STATES DEPARTMENT OF JUSTICE (n.d.), *available at*https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.
[8]WIPO Staff, *Trade Secrets: What Is a Trade Secret?*, WORLD INTELLECTUALPROPERTYORGANIZATION(n.d.), *available at*https://www.wipo.int/tradesecrets/en/.
[9]*Id.*

information systems. Hackers have been known to employ several methods to pilfer corporate information, including phishing, social engineering, ransom ware, cyber stalking, employment of botnets, and distributed denial of service (DDoS) attacks.[10] Aside from personal harm, embarrassment, and the chilling effects on free speech, there are harms associated with reduced market value, operational slowdowns, a decline in business reputations, reduced public confidence, and the symbolic victory of the perpetrators.[11]

Finally, the third harm cybersecurity laws seek to uphold is the theft of government confidential information or secrets. This is also known as espionage, or "the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company."[12] Espionage traditionally occurs among nation-states, where countries may be adversaries or even allies. Espionage is gathering military, political, commercial, or other secret information using spies, illegal monitoring machines, and electronic devices.[13] Espionage activities are usually aggressive and illicit.[14]

Values Embedded in a Cybersecurity Law

According to Kosseff, the five fundamental questions that assess the underlying values of cybersecurity laws are (1) What is being secured?; (2) Where and who is doing the securing?; (3) How is the securing being accomplished?; (4) When is the securing being done?; and (5) Why is the securing taking place?[15] Cybersecurity laws and practices are primarily aimed at keeping safe data that are on computer systems and networks.[16] Although data, systems, and networks possess some economic or other value, cybersecurity laws and practices mainly protect an organization's integrity, functionality, and reliability that rely on such data, systems, and networks.[17]Cybersecurity laws and practices safeguard the "lives and happiness of the human beings who depend upon them."[18]

Difference Between Privacy and Cybersecurity

In the United States, privacy law began with the 1890 Harvard Law Review article by Warren and Brandeis.The authors professed that privacy as a liberty right is "the right to be let alone."[19] Warren and Brandeis pointed out that the purpose of their article was to "consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[20] Warren and Brandeis observed that the law of nuisance and defamation were not adequate protections because these laws did not "protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[21]Warren and Brandeis opined that no law stopped the publication of information about individuals. [22]At the time, the Boston Brahmins, or the elite of the 1890s Boston high society, wanted their personal information to stay private. [23]Warren and Brandeis advocated that laws should exist to ensure that the publication of personally identifiable information remains confidential.[24]

In contrast to privacy, cybersecurity refers to the "body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access."[25] Cybersecurity can also be thought of as information technology security. [26] Information technology security is defined as "a set of cybersecurity strategies that prevent[] unauthorized access to organizational assets such as computers, networks, and data."[27] Information technology security preserves the integrity and confidentiality of sensitive or personal information by obstructing its access by mature and sophisticated threat actors.[28]

The difference between privacy and cybersecurity is that privacy is a right, probably a fundamental right, whereas cybersecurity is a collection of technologies, processes, and practices. Cybersecurity is not a right, and privacy is not a set of technologies, processes, and practices. They are as different as apples and oranges. In other words, the intersection of privacy and cybersecurity is empty.

CYBERSECURITY THREATS

In the second section, threat actors are defined when the reasons why threat actors attempt to gain unauthorized access to systems are outlined. The meaning of cybersecurity for an organization is examined, and the benefits of strong cybersecurity are listed. In particular, solid cybersecurity means safety. Finally, the article points out that all cyber threats are serious because they jeopardize the personally identifiable information of an entity's customers, clients, employees, and other stakeholders.

Threat Actors

A threat actor, also known as a malicious actor or bad actor, is an "entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact -- an organization's security."[29] Threat actors can be external or internal to an organization or a partner.[30] External threat actors do not have privileges within a company, while internal threat actors and partner threat actors may possess a previously existing level of trust or privilege within an entity. A threat actor may be an individual or an organization, where the actions of a threat actor may be intentional or accidental and where the purpose of the action may be purposefully malicious, negligent, or benign.[31]External threat actors are of particular concern because they are common and because the harm they create can be quite severe.

[10]Panda Security Staff, *Types of Cybercrime*, PANDA SECURITY (n.d.), *available at*https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/.
[11]Jeff Kosseff, *supra*, note 5.
[12]*Espionage*, MERRIAM-WEBSTER DICTIONARY (n.d.), *available at* https://www.merriam-webster.com/dictionary/espionage.
[13]*Espionage*, ENCYCLOPEDIA BRITANNICA (n.d.), *available at*https://www.britannica.com/topic/espionage.
[14]*Id.*
[15]Jeff Kosseff, *supra*, note 5.
[16]Shannon Vallor, & William J. Rewak, *Introduction to CybersecurityEthics*, SANTA CLARA UNIV. (n.d.), *available at*https://pdf4pro.com/download/an-introduction-to-cybersecurity-ethics-module-author-668084.html.
[17]*Id.*
[18]*Id.* at 4.
[19]Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARVARD L. REV. 193, 193 (1890), *available at*https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.
[20]*Id.* at 197.
[21]*Id.* at 206.
[22]*SeegenerallyW*arren &Brandeis, *supra* note 19.
[23]*Id.*
[24]*Id.*
[25]Juliana De Groot, *Whatis Cyber Security?Definition, Best Practices & More*, DATA INSIDER (October 5, 2020), *available at*https://digitalguardian.com/blog/what-cyber-security.
[26]*Id.*
[27]Cisco Staff, *What Is IT Security?*, CISCO SYSTEMS, INC. (n.d.), *available at*https://www.cisco.com/c/en/us/products/security/what-is-it-security.html.
[28]*Id.*
[29]Ivy Wigmore, *Threat Actor*, TECH TARGET (Jan. 2016), *available at*https://www.techtarget.com/whatis/definition/threat-actor.
[30]*Id.*
[31]*Id.*

External threat actors can be divided into commodity threat actors and advanced threat actors.[32] A commodity threat actor is a threat actor capable of launching a wide attack with the intention of seeking as many targets as possible. An advanced threat actor focuses on an organization using advanced persistent threat (APT) technology to achieve access to a network while remaining undetected for significant periods so that they may steal data at their leisure.[33] Another type of threat actor is a hacktivist, or individuals or groups of individuals that employ the same tools as financially-motivated cybercriminals. Hacktivists attempt to detect vulnerabilities in systems to gain unauthorized access or use DDoS attacks to negatively impact individuals, brands, companies, and government agencies. [34]The reasons why a threat actor might try to gain unauthorized access to (or disrupt the functioning of) a computer or network are geopolitical, profit or financial gain, ideological, ideological violence, satisfaction, and discontent or gripe[35] Other reasons include intellectual property theft, malicious intent, incompetence, negligence, malcontent, curiosity, fun or just because it can be done, no reason whatsoever[36]

The Meaning of Cybersecurity for an Organization

Cybersecurity protects Internet-connected systems, including hardware, software, and data, from cyber threats.[37] Cybersecurity safeguards individuals and organizations against unauthorized access to data centers and computer systems.[38] Strong cybersecurity that stands against a malicious attack that aims to access, alter, delete, destroy, or extort an entity's systems can prevent or mitigate such a potential event.[39] With strong cybersecurity comes confidence in a corporate reputation and trust in customers, developers, employees, and partners.[40]

The meaning of cybersecurity for an organization lies in its benefits. Those benefits include:

- Protection against cyber attacks and data breaches;
- Security for data and networks;
- Deterrence of unauthorized user access;
- Reduced recovery time following a breach;
- Safeguarding end-users and endpoint devices;
- Compliance with federal and state regulations; and
- Continuity of entity operations.[41]

The advantage of solid cybersecurity is that it may protect, safeguard, deter, or mitigate threat actors from employing malware, ransom ware, social engineering phishing, spear phishing, insider threats, distributed denial of service attacks, advanced persistent threats, man-in-the-middle attacks, botnets, drive-by-download attacks, exploit kits, and malvertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC) and zero-day exploits.[42]

Basically, to an organization, strong cybersecurity means safety. However, the cost of that safety, like the cost of freedom, is eternal vigilance. An organization cannot merely sit on its laurels. It must be forever watchful for cyber threats, as one never knows when they will appear.

The Most Serious Cyber Threats to an Organization and the Response

There is no such thing as a most severe cyber threat to an organization. All cyber threats are serious. If a cyber threat were the most serious, it would be the cyber threat that an organization is currently facing and attempting to mitigate. As stated above, such cyber threats include malware, ransom ware, social engineering phishing, spear phishing, insider threats, distributed denial of service attacks, advanced persistent threats, man-in-the-middle attacks, botnets, drive-by-download attacks, exploit kits, malvertising, vishing, credential stuffing attacks, cross-site scripting (XSS) attacks, SQL injection attacks, business email compromise (BEC) and zero-day exploits.[43] Each of these cyber threats is serious and could potentially and significantly disrupt the workings of an organization. Every one of these cyber-attacks is important.

FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology is virtually everywhere. Technopedia observed that facial recognition has many applications, including airport surveillance at kiosks and social media engines.[44] It is a controversial technology because its use poses profound questions in balancing security versus privacy rights, where the issue is where facial recognition applications can be safely and legally employed.[45] Sample wrote that facial recognition applications are prodigious, and new applications are emerging daily.[46] For example, a video doorbell can inform a resident who is at their door, provided they have uploaded a photograph of the visitor's face.[47] Facial recognition systems can identify missing persons and catch hourly employees that falsify the hours spent in an office.[48] Advertisers are now employing facial recognition technology to create electronic billboards that are tailored for individuals based on their age, mood, and sex.[49] The fact is that facial recognition technology will only intensify as the future unfolds.

Definition of Facial Recognition Technology

According to Kaspersky Labs, facial recognition is a "way of identifying or confirming an individual's identity using their face.[50]Facial recognition systems can employ photos, videos, or real-time pictures of people that can be used to identify them.[51] The Electronic Frontier Foundation (EFF) defined facial recognition as "a method of identifying or verifying an individual's identity using their face."[52] The EFF observed that law enforcement might employ facial

[32]*Id.*
[33]*Id.*
[34]*Id.*
[35]CCC Staff, *Introduction to the Cyber ThreatEnvironment*, CANADIAN CENTRE FOR CYBERSECURITY (Jun. 29, 2021), *available at* https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.
[36]Sentinel One, *Threat Actor Basics: The 5 Main Threat Types*, SENTINEL ONE BLOG (September 9, 2019), *available at*https://www.sentinelone.com/blog/threat-actor-basics-understanding-5-main-threat-types/.
[37]Sharon Shea, Alexander S. Gillis, & Casey Clark, *WhatisCybersecurity?*, TECHTARGET (n.d.), *available at*https://searchsecurity.techtarget.com/definition/cybersecurity.
[38]*Id.*
[39]*Id.*
[40]*Id.*
[41]*Id.*
[42]*Id.*
[43]*Id.*
[44]Technopedia Staff, *Facial Recognition*, TECHNOPEDIA (Aug. 24, 2021), *available at* https://www.techopedia.com/definition/32071/facial-recognition.
[45]*Id.*
[46]Ian Sample, *Whatis Facial Recognition - And How Sinister Is It?*, THE GUARDIAN (Jul. 29, 2019), *available at*https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.
[47]*Id.*
[48]*Id.*
[49]*Id.*
[50]Kaspersky Labs Staff, *Whatis Facial Recognition – Definition and Explanation*, KASPERSKY LABS (n.d.), *available at*https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition.
[51]*Id.*
[52]EFF Staff, *Street-Level Surveillance*, ELECTRONIC FRONTIER FOUNDATION (Oct. 24, 2017), *available at*https://www.eff.org/pages/face-recognition.

recognition software on mobile devices such as cell phones to identify individuals when the police stop them.[53] According to the American Civil Liberties Union (ACLU), facial recognition systems are computer programs that "analyze images of human faces to identify them."[54]The ACLU observed that facial recognition systems are not like other biometric systems because a facial recognition system can be employed for general surveillance that uses public video cameras.[55] Facial recognition systems can passively record a person's face, where the recording does not involve the individual's knowledge, consent, or participation.[56] This last characteristic of facial recognition technology has significant legal consequences because the question that naturally arises is whether one possesses property rights to their image when one is out in public. Under current law, when an individual is publicly among other people, they have no reasonable expectation of privacy and hence, no property rights to their facial image.[57]

How Does Facial Recognition Technology Work?

Before an artificial intelligence (AI) application can perform facial recognition, the software must understand what a face is.[58] This is achieved by employing a deep neural network, where millions of faces are at a known position, and then the application decides where the face is.[59] The neural network is typically a convolutional neural network, where the information is collected and processed using a non-linear mathematical transformation.[60] Over time, the AI software improves and eventually can spot a face, thereby mastering the facial detection step.[61]

The next step is the recognition step. Facial recognition technology employs a second neural network, where it is given many faces and learns how to distinguish one face from another.[62] Some AI facial recognition applications measure the distances between an individual's eyes, nose, mouth, and other physical characteristics.[63] Other facial recognition software employs abstract features of a person's face. The result is a vector for each face, where a vector is a mathematical entity with direction and magnitude that is used to identify an individual by determining the position of one point in space relative to another.[64]

The results are impressive. From 2014 to 2018, the failure rate fell from 4 percent to 0.2 percent.[65] However, the performance failure rate statistics depend on ideal conditions, where a crisp and clear image is compared to a high-quality photograph.[66]In the real world, where there the conditions are less than perfect, images can be blurred. Individuals may look in a different direction, wear a scarf or medical mask, or be older than their reference photograph.[67] These factors tend to reduce the accuracy of the identification. In particular, most AI facial recognition software has problems distinguishing twins.[68]

A Technical Limitation of Facial Recognition Technology

As previously stated, when the recording conditions are less than ideal, AI facial recognition applications have difficulty identifying an individual. Given the current pandemic, one issue that is of particular importance is the software's ability to recognize a face when a person is wearing a medical mask.[69] According to the National Institute of Standards and Technology (NIST), the sheer volume of people covering their faces to reduce Covid-19 from spreading is reducing the performance of facial recognition applications.[70] The NIST reported that the error rates are between five and 50 percent when attempting to match masked faces with unmasked faces.[71] After extensive digital research, the NIST concluded that the AI facial recognition software was never designed to address masked faces.[72] Presuming that the pandemic is a temporary phenomenon, the software should be able to adjust to this new facial environment over time.

What Organizations Use Facial Recognition Technology?

According to Kaspersky Labs, facial recognition software is used by law enforcement, airports, border control, finding missing persons, reducing retail crime, improving retail experiences, banking, marketing, advertising, healthcare, tracking student or worker attendance, recognizing drivers, and monitoring gambling addictions.[73] One use of facial recognition software was in the news recently when it was revealed that the United States military employed such applications to identify Afghans who worked for America.[74] Unfortunately, some of this technology ended up in the hands of the Taliban.[75]

Garvie and Moy observed that Detroit, Michigan, possesses a real-time video feed near a woman's healthcare clinic, where the feed goes directly to local law enforcement.[76] Orlando, Florida, began testing facial surveillance in December 2107, which ran until January 2019.[77] Other American cities are also using facial recognition software for various purposes.[78] Individual use of facial recognition applications includes helping individuals who are legally blind, finding missing persons, and preventing identity theft at ATMs.[79]

Advantages and Disadvantages of Using Facial Recognition Technology

The problem with arguing for or against using facial recognition technology is that both arguments are moot. It is a *fait accompli*. Facial recognition applications are here to stay. It does not matter whether one is for or against facial recognition technology. No laws

[53]*Id.*
[54]ACLU Staff, *Facial Recognition Technology*, AMERICAN CIVIL LIBERTIES UNION (n.d.), *available at*https://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.
[55]*Id.*
[56]*Id.*
[57]*Katz v. United States*, 386 U.S. 954 (1967) (see Justice Harlan's concurrence), *available at*https://supreme.justia.com/cases/federal/us/389/347/.
[58]Ian Sample, *supra*, note 46.
[59]*Id.*
[60]Technopedia Staff, *supra*, note 44.
[61]Ian Sample, *supra*, note 46.
[62]*Id.*
[63]*Id.*
[64]*Id.*
[65]*Id.*
[66]*Id.*
[67]*Id.*
[68]*Id.*

[69]NIST Staff,*NIST LaunchesStudiesintoMasks' Effect on Face Recognition Software*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Jul. 27, 2020), *available at* https://www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software.
[70]Id.
[71]Id.
[72]Id.
[73]Kaspersky Labs Staff, supra, note 50.
[74]Eileen Guo, &HikmatNoori, This Is the Real Story of the Afghan BiometricDatabasesAbandoned to the Taliban, MIT TECH. REV.(Aug. 30, 2021), *available at*https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/.
[75]Id.
[76]Clare Garvis, & Laura M. Moy, America underWatch: Face Surveillance in the United States, GEORGETOWN L. CTR. FOR PRIV. AND TECH. (May 16, 2019), *available at*https://www.americaunderwatch.com/.
[77]Id.
[78]Id.
[79]Face First Staff, 21 Amazing Uses for Face Recognition, FACE FIRST (n.d.), *availableat*https://www.facefirst.com/blog/amazing-uses-for-face-recognition-facial-recognition-use-cases/.

prevented the technology from coming into existence, and there will likely be no laws passed by either the federal or state governments that will ban its use because the technology has been embraced by federal and state agencies and corporate entities alike. In technology and business, if something is not forbidden, it is permitted. Too much money has already been spent on implementing the technology in various scenarios. The most that could ever be achieved at this point is for legislation to direct the evolution of the technology according to perceived societal privacy values, including corporate and governmental goals. Thus, the remainder of this essay will focus on the advantages and disadvantages of facial recognition technology along with a single legal issue with the hope that by understanding the benefits, costs, and legal considerations, one can guide the technology accordingly.

Advantages of Using Facial Recognition Technology

According to Kaspersky, the advantages of using facial recognition software are:

- ***Increased security*** – Governments can use facial recognition to identify terrorists and known criminals.[80]
- ***Reduced crime*** – Facial recognition makes it easier to find burglars, thieves, and trespassers, where the knowledge that facial recognition software is employed may act as a deterrent.[81]
- ***Removing bias from stop and search*** – Currently, society is concerned over stops and searches that cannot be justified. The technology allows people to be identified automatically rather than using a less than perfect human process.[82]
- ***Faster processing*** – Currently, it only takes a few seconds for an AI application to recognize a face. In this era of advanced cyber-attacks, speed is critical to ensure proper individual identification.[83]
- ***Greater convenience*** – As facial recognition technology dominates the economic landscape, firms can be assured of effective and efficient customer identification.[84]
- ***Integration with other techno****logies* – Most facial recognition applications are compatible with and integrated into most security systems.[85]

Disadvantages of Using Facial Recognition Technology

Again, according to Kaspersky, the disadvantages of employing facial recognition technology include:

- ***Surveillance*** – The issue here is that many members of society fear that facial recognition technology will be used to limit individual freedoms and catch criminals.[86]
- ***Scope for error***– Facial recognition data is not free from error. The AI applications could be used to charge people with crimes that they did not commit due to a slight change in the camera angle or the appearance of the person being surveilled.[87]
- ***Breach of privacy***– This is an ethical and legal issue because governments are well-known for storing pictures of citizens without their consent. The legal mechanisms to control such governmental activities are slowly being implemented. The European Union (EU) recently passed the General Data Protection Regulation regulating privacy violations.[88] There is currently no comprehensive privacy law in the United States, even though a small minority of states have passed their own privacy laws.[89][90]
- ***Massive data storage*** – Because facial recognition software is dependent on machine learning technology to achieve accurate results, large amounts of data storage are required. Small and medium-sized companies may not have the financial resources to store the necessary data. Such companies may have to pay substantial fees to third-party vendors.[91]

Legal Issues Associated with Facial Recognition Technology

A significant legal issue associated with facial recognition technology is whether an individual has property rights to the information that may be gathered about their face. In other words, does the data collector own the facial recognition data, or does an individual own the facial recognition data? It should be remembered that facial recognition data is biometric information that can be employed to identify individuals uniquely.

In *Carpenter*, the police used cell phone metadata to arrest and convict Carpenter and his partners in crime for stealing cell phones and then reselling them.[92]The majority opinion of the Supreme Court opined that Carpenter had a reasonable expectation of privacy in his cell phone metadata.[93] It was a 5-4 decision with four separate dissents. In essence, Justices Alito, Kennedy, and Thomas argued that Carpenter possessed no privacy rights without property rights because cell phone metadata is owned by the cell phone providers, not the cell phone users.[94] However, Justice Gorsuch took a different stance. He felt that the cell phone providers were bailees and that the cell phone metadata was the property of the cell phone owners.[95] Although currently, not law, Justice Gorsuch's dissent is relevant in analyzing who owns the facial biometric data that is collected by taking a picture of a person's face.

Simply stated, it is readily apparent that one owns the characteristics of one's face. This fact seemingly needs no support. If Justice Gorsuch's argument is applied, the data collected by facial recognition belongs to the person, not the company collecting the data. This is the fundamental issue with facial recognition data and the software that collects it. We own our faces, and we should have the right to decide how the facial recognition gathered should be used.

ISSUES COLLECTING FACIAL RECOGNITION DATA

This section addresses some issues with the collection of facial recognition data. The so-called "nothing-to-hide" (NTH) argument is

[80]Kaspersky Labs Staff, *supra*, note 50.
[81]*Id.*
[82]*Id.*
[83]*Id.*
[84]*Id.*
[85]*Id.*
[86]*Id.*
[87]*Id.*

[88]Donald L. Buresh, *A Comparison Between the European and American Approaches to Privacy*, 6 INDONESIAN J. OF INTL AND COMP. L. 2, 253-281 (2019), *available at*https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=.
[89]Donald L. Buresh, *Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?*, 38 SANTA CLARA UNIV.: HIGH TECH L. J., *available at* https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.
[90]Kaspersky Labs Staff, *supra*, note 50.
[91]*Id.*
[92]Donald L. Buresh, *The Meaning of Justice Gorsuch's Dissent in Carpenter v. United States*, 43 AMERICAN JOURNAL OF TRIAL ADVOCACY 1 55-103 (2019), *available a*t https://heinonline.org/HOL/LandingPage?handle=. hein.journals/amjtrad43&div=7&id=&page=.
[93]*Id.*
[94]*Id.*
[95]*Id.*

explained, highlighting several problems. The NTH argument is quite pervasive when discussing privacy because individuals tend to favor security over privacy. The NTH argument tends to be glossed over a number of issues, such as how facial recognition data is used once collected, mainly secondary use of the data. The section also discusses data privacy protection in the United States and the European Union.

The "Nothing to Hide" Argument

According to Solove, theNTH argument is a retort or a primary argument when balancing privacy against security.[96] In the most persuasive form, it argues that the "privacy interest is generally minimal to trivial, thus making the balance against security concerns a foreordained victory for security."[97] The argument pervades widespread discussion about privacy and security issues. The NTH argument is essentially stated by individuals that feel that they are doing nothing wrong or criminal, and therefore, they do not care if the government monitors their activities. However, these same individuals care that people have something to hide, such as criminals or terrorists, who are caught and receive their comeuppance. The problem with the argument is that people have something to hide, which could be their social security number, health records, credit card bills, or even their naked body. After all, people do wear clothes that hide their nakedness.[98]

Problems with the "Nothing to Hide" Argument

There are a variety of problems with the NTH argument. First, there is information that people might want to conceal merely because it is embarrassing or they do not want other people to know about it.[99] According to Solove, privacy is a collection or protection against related social problems.[100] Second, most people believe that the underlying assumption regarding privacy is that it is about hiding bad things. In other words, privacy is about hiding a wrong.[101] The problem with this argument is that it perceives privacy as secrecy or a form of concealment. However, according to Solove, disguising something from a government agency, such as the National Security Agency (NSA), is equivalent to hindering surveillance, where personal information is swept up to identify and prevent terrorist activities.[102]

The NTH argument focuses mainly on information collection issues. A particular data item that could be collected may be harmless when viewed by itself. However, when aggregated to form a cogent whole, gathering innocent individual data items may be something to hide.[103] This is the allure of data mining, or the discovery of harmless data that, when assembled, reveals a picture that an individual may not want to be broadcast to the world.

Another issue with the NTH argument is the exclusion problem, where "people are prevented from knowing how their information is being used, as well as barred from being able to access and correct errors in that data."[104] The issue here is that organizations such as the NSA gather massive amounts of data without an individual ever determining whether the data collected is accurate. This issue has more to do with government agencies' power and structure than with the NTH argument.[105]

A related problem is secondary use, where secondary use is the use of data obtained for one reason and then employed for another purpose without a user's consent.[106] The problem is that once personal information is released to another person, that individual loses control of how that data will be employed. An organization could employ the data obtained without any limit on accountability regarding how the data are used. According to Solove, it is hard to assess the danger in this situation.[107]

The critical misunderstanding is that the NTH argument perceives privacy as equivalent to secrecy or the right to hide things.[108] The problem with the NTH argument is that it searches for a visceral rather than a structural type of injury. In other words, the NTH argument is looking for a physical injury, such as broken bones or even death. However, in many instances, privacy is endangered not by one egregious act but by a slow, never-ending collection of almost negligible acts that accumulate into a harmful whole.[109] In addition, a violation of privacy may not result in embarrassment, humiliation, or physical injury but go against an individual's privacy. Solove provided the example of Chase Manhattan Bank selling personal customer information in contradiction to its privacy policy.[110] The court opined that there was no harm and, thus, no violation of privacy.

Finally, according to Solove, security in its totality should not be weighted in its entirety against privacy. Instead, the marginal change in security should be balanced against privacy to provide a more accurate picture of what is occurring.

Data Privacy Protection in the United States

The data privacy and protection regime in the United States is a series of federal and state laws. From the federal perspective, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a significant cybersecurity law. HIPAA generated national standards to protect sensitive patient health information from exposure without a patient's consent. The HIPAA Privacy Rule deals with disclosing protected health information regarding individuals by organizations subject to the rule.[111] Next, the Gramm-Leach-Bliley Act (GLBA) of 1999 is another primary cybersecurity law. It is also known as the Financial Modernization Act (FMA) of 1999 because it addresses how financial institutions control individual private information.[112]Finally, the Federal Information Security Management / Modernization (FISMA) is the third primary cybersecurity law in the United States. The FISMA Act of 2002 was included in the E-Government Act (EGA) of 2002. FISMA of 2014 amended FISMA of 2002 by reinforcing the employment of continuous monitoring systems while reducing the overall reporting requirements and focusing an agency on the compliance and reporting of breaches in security. FISMA of 2014 also required the Office of Management and Budget (OMB) to revise

[96]Daniel J. Solove, *"I've Got Nothing to Hide" and OtherMisunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 747 (Feb. 7, 2007), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.
[97]*Id.* at 747.
[98]*Id.* at 750.
[99]*Id.* at 752.
[100]*Id.* at 763.
[101]*Id.* at 764.
[102]*Id.* at 765.
[103]*Id.* at 766.
[104]*Id.* at 766-67.
[105]*Id.* at 767,
[106]*Id.*
[107]*Id.*
[108]Id. at 768.
[109]*Id.* at 769.
[110]*Id.* at 770.
[111]CDC Staff, *HealthInsurancePortability and AccountabilityAct of 1996 (HIPAA)*, CENTERS FOR DISEASE CONTROL AND PREVENTION (Sep. 18, 2018), *available at*https://www.cdc.gov/phlp/publications/topic/hipaa.html.
[112]Gary Kranz, *Gramm-Leach-BlileyAct (GLBA)*, TECHTARGET(Jun. 2021), *available at*https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act.

OMB. Circular A-130 promoted changes in reporting as technology progressed.[113]

On the state level, it has only been recently that state law entered the privacy and protection arena, ready to defend the privacy rights of its citizens. The California Consumer Privacy Act (CCPA),as amended by the California Privacy Rights Act, safeguarded the personal information of California consumers independent of what economic sector the data originated.[114][115] Another statute is the Virginia Consumer Data Protection Act (VCDPA) which, on March 2, 2021, Governor Ralph Northam signed into law.[116] The third statute is Colorado's Privacy Act (CPA) which became law on July 8, 2021.[117] Nevada and Maine have also passed privacy laws, but these laws are not nearly as comprehensive as the privacy laws in California, Virginia, and Colorado.[118] It remains to be seen whether the United States Congress will pass a comprehensive privacy law.

Data Privacy Protection in the European Union

The European Union (EU) data privacy and protection regime consists of the General Data Protection Regulation (GDPR) and consists of the Data Protection Directive (1995/46/EC), the Data Processing Directive (2002/58/EC), the Data Retention Directive (2006/24/EC), and the GDPR.[119]The GDPR is a set of legal guidelines that address collecting and processing personal information regarding individuals who live and reside in the EU.[120][121] The GDPR applies regardless of where a website is located.[122]Any site accessed by a European citizen must obey the regulation, irrespective of whether an organization markets goods or services to EU residents.[123]The GDPR applies to organizations that do business in the EU.[124]

When comparing the data privacy and protection regime in the United States versus the data privacy and protection regime in the EU, it is evident that the European regime comprehensively encompasses all of the nations in the EU. Also, businesses and entities in the EU are subject to the GDPR. In contrast, in the United States, privacy and protection take a sectored approach, where some sectors are subject to comprehensive privacy legislation, whereas other sectors are not. All businesses in the United States are subject to the Federal Trade Commission (FTC) Act of 1919. Recently, the FTC has valiantly striven to plug the privacy and protection gap by requiring firms to behave as if the United States possessed a comprehensive federal privacy law.[125][126]

INFORMATION, TRANSPARENCY,& ACCESSIBILITY

The purpose of this section is to discuss what constitutes transparency and accessibility. The essay will deal with these two concepts from the perspective of individuals, corporations, and nations. The section will argue that although transparency and accessibility seem to be the norm, the opposite (i.e., confidentiality and secrecy) is of greater interest.

Definition of Information

Merriam-Webster's Dictionary defines information as "knowledge obtained from investigation, study, or instruction."[127] Information is also defined as "the attribute inherent in and communicated by one of two or more alternative sequences or arrangements of something (such as nucleotides in DNA or binary digits in a computer program) that produce specific effects."[128] In other words, it is an intrinsic characteristic of something that is communicated from one party to another party.[129]

Definition of Transparency

According to Black's Online Law Dictionary, transparency is "[a] lack of any hidden agendas with all information being available," the "degree of disclosure is minimum for all verified agreements, practices and dealings," and the "required condition for an open and free exchange."[130] In other words, transparency means that concerning the interactions of various parties, the parties have no hidden agenda.[131] It also means that the degree of unnecessary disclosure is minimized and that among parties, there is a free and open exchange of information.[132]

Definition of Accessibility

Black's Online Law Dictionary defines accessibility as "[t]he ability and ease a customer can access a service, good, associate, or facility," or "the ability to access records on a system or website."[133] Here, a customer is "[o]ne who regularly or repeatedly makes purchases of, or has business dealings witha tradesman or business house."[134][135][136]A customer is also considered "one who has had

[113]NIST Staff, *Federal Information Security ModernizationAct (FISMA) Background*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Updated Sep. 28, 2021), *available at*https://csrc.nist.gov/projects/risk-management/fisma-background.
[114]Donald L. Buresh,*supra*, note 88.
[115]*California PrivacyRightsAct: An Overview*, PRIVACYRIGHTSCLEARINGHOUSE (December 10, 2020), *available at*https://privacyrights.org/resources/california-privacy-rights-act-overview#:~:text=The%20California%20Privacy%20Rights%20Act%20clarifies%20that%20people%20can%20opt,personal%20information%20to%20third%20parties.&text=The%20California%20Privacy%20Rights%20Act%20expands%20this%20to%20cover%20data,includes%20a%20username%20and%20password.
[116]Sarah Rippy, *Virginia Passes the Consumer Data Protection Act*, INTERNATIONALASSOCIATION OF PRIVACY PROFESSIONALS, (Mar. 3, 2021), *available at*https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.
[117]Sarah Rippy, *Colorado PrivacyActBecomes Law*, THE PRIVACYADVISER (Jul. 8, 2021), *available at*https://iapp.org/news/a/colorado-privacy-act-becomes-law/.
[118]Donald L. Buresh,*supra*, note 89.
[119]Anthony K. Haynes, *Global PrivacyRegimes*, CSDP 501 – CYBERSECURITY PUBLIC POLICY SEMINAR (2021), *available at*https://albanylaw.instructure.com/courses/1828/files/145476/download?download_frd=1. PowerPoint Presentation.
[120]Jake Frankenfield, revised by Amy Drury, *General Data Protection Regulation (GDPR)*, INVESTOPEDIA, (November 11, 2020), *available at*https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp.
[121]IT GOVERNANCEPRIVACYTEAM,EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE 11, 11 (2nd ed. 2017).
[122]*Id.*
[123]*Id.*
[124]*Id.*

[125]*In the Matter of TaxSlayer, LLC*, Complaint Docket No. C-2646 (n.d.), *available at*https://www.ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_complaint.pdf.
[126]*In the Matter of Everalbum, Inc*., UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION (May 7, 2021), *available at*https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint.
[127]*Information*, MERRIAM-WEBSTER'SDICTIONARY, (n.d.), *available at*https://www.merriam-webster.com/dictionary/information.
[128]*Id.*
[129]*Id.*
[130]*WhatisTransparency*, BLACK'S LAW ONLINE DICTIONARY, (2016), *available at*http://alegaldictionary.com/transparency/.
[131]*Id.*
[132]*Id.*
[133]*WhatisAccessibility*, BLACK'S LAW ONLINE DICTIONARY, (2016), *available at*http://alegaldictionary.com/accessibility/.
[134]*Aiken Mills v. United States, D.C.S.C*.,144 F.2d 23 (4th Cir. 1944), *available at*https://law.justia.com/cases/federal/appellate-courts/F2/144/23/1547763/.
[135]*Arkwright Corporation v. United States*, D.C. Mass., 53 F.Supp. 359, 361 (D.C. Mass. 1943), *available at* https://casetext.com/case/arkwright-corporation-v-united-states.
[136]*Customer*, BLACK'S LAW DICTIONARY 462 (4th ed. 1968), *available at*https://heimatundrecht.de/sites/default/files/dokumente/Black'sLaw4th.pdf.

repeated business dealings with another."[137][138]Finally, a customer is "[a] buyer, purchaser, or patron."[139] In other words, a customer is a party engaged in an economic transaction. The fact that accessibility is concerned with customers that are involved in an economic transaction will be shown to be quite relevant in the succeeding text.

In the Interest of Individual Privacy

In the United States, privacy law began with the publication of the 1890 *Harvard Law Review* article by Warren and Brandeis, where the authors opined that privacy was a liberty right which is "the right to be let alone."[140] Warren and Brandeis claimed that the purpose of their article was to "consider whether the existing law affords a principle which can properly be invoked to protect the privacy of the individual; and, if it does, what the nature and extent of such protection is."[141] The authors believed that the law of nuisance and defamation were inadequate protections because these laws did not"protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds."[142] The authors asserted that there should be laws blocking the publication of information that individuals believed should be confidential.[143]

The issue addressed by Warren and Brandeis is the issue of privacy versus transparency.[144] Warren and Brandeis argued that individuals have the right to prevent others from gaining access to specific information about themselves.[145] In essence, transparency is the antithesis or the opposite of privacy. From a Hegelian dialectical perspective, where one may be searching for a synthesis between the thesis of privacy and the antithesis of transparency, such a synthesis may be challenging to attain because the synthesis may depend on the type of information under consideration.[146] For example, if a person's social security number or health records are information items under analysis, then society has tipped the scales in the balance of privacy because the benefits of privacy outweigh the benefits of transparency. On the other hand, although an individual might want to maintain the privacy of their address or perhaps the amount of money in their bank account private, the Supreme Court has deemed that a person does not have a reasonable expectation of both types of information.

Misrepresentations

When dealing with transparency, it is crucial to discuss misrepresentations and misdirections. According to Investopedia, a misrepresentation is "a false statement of a material fact made by one party which affects the other party's decision in agreeing to a contract."[147]There are three types of misrepresentations.[148] First, an innocent misrepresentation is "a false statement of material fact by the defendant, who was unaware at the time of contract signing that the statement was untrue."[149] An innocent misrepresentation can usually be corrected by providing additional correct information or permitting recession. Second, negligent misrepresentation is "a statement that the defendant did not attempt to verify was true."[150] In contract law, the remedy is either recession or damages.[151] Finally, intentional or fraudulent misrepresentation is a statement made knowing that the statement was false or made recklessly to induce the other party to engage in a specific behavior.[152] In many instances, it is the last category of misrepresentations that governments indulge in to prevent their citizens and other governments from learning the truth.[153] This type of misrepresentation is also known as misdirection.[154]

Benefits and Costs of Transparency and Accessibility

From a prima facie perspective, the benefits of transparency and accessibility are that the people know the truth regarding a particular matter.[155][156] It is sometimes difficult to place a dollar amount on the value of knowing the truth.[157] When one knows the truth regarding a matter, one is operating based on what is occurring or has occurred, and one can make accurate and precise decisions.[158] In contrast, when the truth is unknown for whatever reason, one is operating using false premises, the effects of which can range from a minor inconvenience to a significant tragedy, depending on the circumstances.[159] Nations and companies can suffer dramatic losses like what is currently happening in Afghanistan.[160] According to recent estimates, thousands of Americans will be stranded in Afghanistan, not to mention the tens of thousands of Afghans that worked with the Americans in the past 20 years and the $83 billion in equipment left in the country.[161] Many people may pay the ultimate price (death) as a cost because of the lack of American transparency.[162]

As for accessibility, please recall the definition above. According to the definition of accessibility, it must be purchased with money.[163] To gain accessibility, one may engage in an economic transaction.[164]

[137]*Lyons v. Otter Tail Power Co.*, 70 N.D. 681, 297 N.W. 691, 693 (1941), *available at*https://cite.case.law/nd/70/681/.
[138]*Gallopin v. Continental Casualty Co*., 290 Ill. App. 8, 7 N.E.2d 771, 774 (1937), *available at*https://casetext.com/case/gallopin-v-continental-casualty-co.
[139]*Nichols v. Ocean Accident &Guarantee Corporation*, 70 Ga.App. 169, 27 S.E.2d 764, 766 (1943), *available at*https://casetext.com/case/nichols-v-ocean-accident-c-corporation/.
[140]Samuel D. Warren, & Louis D. Brandeis,*supra*, note 19.
[141]*Id.* at 197,
[142]*Id.* at 206.
[143]*Id.*
[144]Samuel D. Warren, & Louis D. Brandeis, *supra*, note 19.
[145]*Id.*
[146]*Hegel'sDialectics*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY, (October 02, 2020), *available at*https://plato.stanford.edu/entries/hegel-dialectics/.
[147]*Misrepresentation*, INVESTOPEDIA, (n.d.), *available at*https://www.investopedia.com/terms/m/misrepresentation.asp.
[148]*Id.*
[149]*Id.*
[150]*Id.*
[151]*Id.*
[152]*Id.*
[153]Gordon Adams, *From Vietnam to Afghanistan, all US governments Lie*, THE CONVERSATION, (August 31, 2019), *available at*https://theconversation.com/from-vietnam-to-afghanistan-all-us-governments-lie-128695.
[154]*Misdirection*, MERRIAM-WEBSTER DICTIONARY, (n.d.), *available at*https://www.merriam-webster.com/dictionary/misdirection.
[155]Rebecca Hawk, *5 Benefits of More Transparency in Your Workplace*, THE CENTER FOR ASSOCIATION LEADERSHIP, (n.d.), *available at*https://www.asaecenter.org/association-careerhq/career/articles/talent-management/5-benefits-of-more-transparency-in-your-workplace.
[156]Lee Cataluna, *Honesty vs. Transparency:Which Is Key to SuccessfulGovernment? (Opinion)*, GOVERNMENT TECHNOLOGY, (November 09, 2016), *available at*https://www.govtech.com/opinion/honesty-vs-transparency-which-is-key-to-successful-government-opinion.html.
[157]Terry Treadwell, *What Is the Cost of Truth?*, WOUND CARE LEARNING NETWORK, (n.d.), *available at*https://www.hmpgloballearningnetwork.com/site/wounds/editorial/what-cost-truth.
[158]PETER F. DRUCKER, MANAGEMENT:TASKS, RESPONSIBILITIES, PRACTICES (HarperBusiness 1993).
[159]*Id.*
[160]Scott Ridder, *The Biden Administration'sIncompetence Has Created the Conditions for a Modern Dien Bin Phu in Kabul*, RT, (August 19, 2021), *available at*https://www.rt.com/op-ed/532533-us-troops-remain-afghanistan-hkia/.
[161]Charles Kim, *Pelosi: LeavingMilitary Equipment Behind Is 'WhatHappens' in Withdrawal*, NEWSMAX, (August 18, 2021), *available at* https://www.newsmax.com/politics/pelosi-democrats-biden-war/2021/08/18/id/1032933/.
[162]Laura Jakes, *How Many People in Afghanistan Need to beRescued? The NumberRemains Elusive.*, THE NEW YORK TIMES, (August 24, 2021), *available at*https://www.nytimes.com/2021/08/24/us/politics/afghanistan-evacuations-kabul-airport.html.
[163]*WhatisAccessibility*, *supra*, note 133.
[164]*Id.*

Nothing in the definition was said regarding what that monetary price should be, whether it be a nominal or moderate price or a high or excessive price.[165] That decision is left to the details of the transaction. Unfortunately, the economic aspects of accessibility may have the nasty habit of blending into transparency, where to obtain transparency, one must pay a monetary price to get it.[166] This economic barrier to transparency and accessibility may not be what people have in mind when they use these terms.[167]Although, on its face, transparency seems to be a desirable goal and objective, there are real limitations to its implementation. Individuals demand privacy, corporations want confidentiality to prevent potential legal action by the government and competitors, and nations require secrecy to protect its interest. Thus, transparency sounds good, but it should never be forgotten that all that glitters is not gold.

ELECTION INTEGRITY & IDENTITY VERIFICATION

In the 2016 and 2020 presidential election cycles, the accusations of voter fraud have become more pronounced and vitriolic. In the 2016 presidential election, accusations of Russian interference dominated the political landscape.[168] During the election period, Hillary Clinton's campaign was hacked, where Russian agents stole over ten thousand emails from Clinton campaign staffers, including emails from campaign chairman John Podesta.[169] The hackers also gain access to the Democratic Congressional Campaign Committee computer network, according to the special counsel indictment from Special Prosecutor Robert Mueller.[170]In June 2016,DCLeaks.com was launched, where thousands of stolen documents and emails were posted.[171]In July 2018, Mueller indicted twelve Russian nationals for hacking into the federal election systems, claiming they stole personally identifiable information on 500,000 voters from an unnamed state. The hackers visited the websites of counties in Florida, Georgia, and Iowa, as well as penetrating the systems of a voter registration software vendor, and then sent malicious emails to various Florida election administrators.[172] The four years of the Trump administration were plagued with continuous innuendos that Russian interference stole the 2016 election, which promoted the idea that Donald Trump was fraudulently elected.[173]

The 2020 presidential election was also beleaguered with allegations of voter fraud, but this time the claims came from the Republicans rather than the Democrats. Shortly after the 2020 presidential election, Trump claimed that millions of illegal votes prevented him from being elected President.[174] However, 61 of Trump's 64 election challenges failed.[175] Trump's lawsuits asserted claims of voter fraud and illegal polling procedures, including errors with ballots and voting machines. Forty-seven cases were dismissed by Democratic and Republican judges, while eighteen lawsuits were filed in Pennsylvania, focusing on mail-in and absentee voting, extended pre-election deadlines, and technically deficient ballots.[176]The three legal victories in Pennsylvania threw out 270 provisional ballots because the ballots lacked signatures, had separated Election Day provisional ballots from those cast after the election, and had moved back Pennsylvania's deadline for absentee voters to present their voter IDs by three days.[177] One failed suit wanted to block Pennsylvania from certifying seven million votes election results because some counties did not allow voters to fix errors in mail-in ballots.[178]

Voting Principles

Regardless of what one thinks of whether there was voter interference or fraud in the 2016 and 2020 elections, for election integrity to exist must be not only one person one vote but also the individual voting must be legally qualified to vote.[179]One way to ensure that only legally qualified individuals vote is to biometrically identify a person by using fingerprints or facial images.[180] In a biometric verification system, a natural person's biometrics that was previously captured is compared to the current biometric features of that individual.[181]A person claims an identity with a biometric verification system, and their biometric features are captured and compared to previously captured biometric features.[182] The one-to-one comparison decides whether an individual is who they say they are. A biometric verification system is "any means by which a person can be uniquely identified by evaluating one or more distinguishing biological traits."[183] These biological identifiers include fingerprints, facial recognition, hand, and earlobe geometries, iris and retina patterns, voice prints, and written signatures.[184]In a biometric identification system, the individual need not claim an identity. Their biometric features are captured and compared to the features of all their previously captured biometric features stored in a biometric database.[185]Biometric identification is a one-to-many comparison that attempts to determine who the individual is.

Biometric technology can significantly improve voting accuracy when:

- Citizens do not possess reliable and trusted identification documents;
- There is a need to issue voter ID cards that may contain biometric details about the voter;
- Multiple registrations cannot be reliably detected based on high-quality biographical data in the voter register;
- Multiple voting and voter identification at polling stations are significant issues;
- Photos or other biometric features are required at polling stations when it is difficult to determine the identity of citizens based on reliable identification documents; and

[165] *Id.*
[166] *Id.*
[167] *Id.*
[168] Abigail Abrams, *Here'sWhatWe Know So Far About Russia's 2016 Meddling*, TIME (Apr. 18, 2019), *available at*https://time.com/5565991/russia-influence-2016-election/.
[169] *Id.*
[170] *Id.*
[171] *Id.*
[172] *Id.*
[173] Bill Allison et al., *Trump Team'sConflicts and Scandals: An Interactive Guide*, BLOOMBERG (Mar. 14, 2019), *available at*https://www.bloomberg.com/graphics/trump-administration-conflicts/?leadSource=uverify%20wall.
[174] Robby Brod, *TheseRepublicansDid a Deep Dive into 2020 Election Lawsuits, Including in Pa. Here'sWhy Most of ThemFailed*, WITF (Sep. 1, 2022), *available at* https://www.witf.org/2022/09/01/these-republicans-did-a-deep-dive-into-2020-election-lawsuits-including-in-pa-heres-why-most-of-them-failed/.
[175] *Id.*
[176] *Id.*
[177] *Id.*
[178] *Id.*
[179] U.S. Const, amends. XV, XIX, XXIV, & XXVI.
[180] Sven Heiberg, Kristjan Krips, Jan Willemson, &PriitVinkel, *Facial Recognition for RemoteElectronicVotingMissing Piece of the Puzzle or YetAnotherLiability?*,*in*EMERGING TECHNOLOGIES FOR AUTHORIZATION AND AUTHENTICATION,13136. (Springer, Cham. A. Saracino,& P. Mori eds.), *available at*https://doi.org/10.1007/978-3-030-93747-8_6.
[181] PETER WOLF, INTRODUCINGBIOMETRIC TECHNOLOGY IN ELECTIONS, (International Institute for Democracy and Electoral Assistance 2017), *available at*https://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf.
[182] *Id.*
[183] Tech Target Contributor, *BiometricVerification*, TECH TARGET (Jul. 2021), *available at*https://www.techtarget.com/searchsecurity/definition/biometric-verification#:~:text=Biometric%20verification%20is%20any%20means,voice%20prints%20and%20written%20signatures.
[184] *Id.*
[185] *Id.*

- Voter registers cannot be obtained from reliable and trusted population registers.[186]

It should be understood that biometric sensors possess an inherent reliability issue because biometric readings from an individual can vary.[187] This characteristic of biometric readings can result in false negative and false positive identification. According to the Face Recognition Vendor Test by the NIST, when the false positive rate is adjusted to be below 0.00001, the false negative rate is approximately three percent for the more robust biometric verification algorithms when an image is captured in an uncontrolled or wild environment.[188]

Identification Methods

With facial recognition, it is vital to ensure that the individual whose face is being captured is alive and that a still image of the person is not being employed. Methods to determine whether a subject is alive include asking a subject to blink their eyes, rotate their head, move their lips, and raise an eyebrow.[189] Xu *et al.,* showed that a liveliness test could be avoided by employing a virtual reality system that generates three-dimensional representations of faces.[190]

The two other issues with employing facial recognition in an election process are the failure-to-capture rate and the failure-to-enroll rate. The failure-to-capture rate or the failure-to-acquire rate occurs if the "feature extraction (including all preceding operations) was not successful during a recognition attempt."[191]The reasons for a failure-to-capture rate may be an inherent ability to capture the data, insufficient sample quality (i.e., noisy sample data), or an insufficient number of features. The failure-to-capture rate can be altered by increasing or decreasing quality thresholds. In particular, a high-quality threshold does not necessarily result in better recognition performance.[192]Failure to enroll is the "inability to store a new reference template."[193]The main reason for a failure to enroll is a failing feature extraction. Different quality thresholds may be used for enrolment and recognition if enrolment and recognition employ the same data.[194]A higher threshold is typically selected for enrolment since it increases performance during all subsequent recognition attempts. Consequently, a failure-to-enroll rate is often larger than a failure-to-capture rate.

General Issues with Facial Recognition

It should be remembered that biometric authentication is a probabilistic activity where it is not guaranteed to identify an individual correctly. The facial recognition algorithm can be biased on the previously collected training data. For instance, in 2018, it was found that the benchmark datasets Adience and IJB-A overrepresented light-skinned individuals, where the former consisted of 86.2 percent and the latter 79.6 percent of the samples, whereas the PPB dataset had a more balanced representation of lighter-skinned people at 53.6 percent of the samples.[195] The study also tested commercial gender classification systems for Microsoft, Face++, and IBM.[196] For lighter-skinned people, the error rates were 0.7 percent, 4.7 percent, and 3.2 percent, respectively, whereas, for darker-skinned people, the error rates were 12.9 percent, 16.5 percent, and 22.4 percent, respectively.[197]Grother *et al.,* compared over 100 facial recognition algorithms, discovering that many of the algorithms tended to possess a demographic bias in the used data training data sets.[198] Even so, the better identification and verification algorithms did not have a significant demographic bias.

As previously stated, the robust algorithms had a false negative rate of approximately three percent. Facial recognition algorithms are questionably reliable. The implication is that the only appropriate alternative to voter identification is to have a human being verifying the facial recognition results in real time. Suppose the software fails to identify an individual correctly. In that case, a voter could take another picture, where the person is allowed to vote pending facial verification, or the voter is not permitted to vote. The former may give an individual the impression that their vote counted, whereas the latter might prevent a legitimate voter from voting.

Privacy Issues with Facial Recognition

The primary issue with facial recognition in voting is that an individual's personally identifiable information may be at risk.[199]A referenced dataset of previously captured facial images is essential for a facial recognition algorithm to function correctly. An existing government database can be employed when a governmental unit issues IDs that possess a photograph. A third-party commercial service may not provide individuals with the level of comfort they would have if the government collected their facial images.[200] Also, employing a remote collection mechanism such as the camera in a cell phone may not sit well with voters because of the possibility of the data collector gathering identifying background data. The issue is who would possess and own the image collected. Justice Gorsuch in *Carpenter* opined that the cell phone owner should hold title to the facial images, whereas the data collectors are bailees.[201] However, Justice Gorsuch's opinion in *Carpenter* was dissenting and currently does not have the force of law.[202]

ELECTION INTEGRITY & COUNTING VOTES

According to Deluzio *et al.,* Robert Brehm, the co-executive director of the New York State Board of Elections, said that it is not reasonable to expect state and local election offices to defend independently against hostile nation-state actors.[203] The problem with this statement is that it is loaded with assumptions that must be unpacked. For example, is Brehm speaking only about elections

[186]Peter Wolf, *supra*, note 181.
[187]Sven Heiberg et al., *supra*, note 180.
[188]NIST Staff, *FRVT 1:1 Verification*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Nov. 1, 2022), *available at*https://pages.nist.gov/frvt/html/frvt11.html.
[189] Sven Heiberg et al., *supra*, note 180.
[190]Yi Xu, True Price, Jan-Michael Frahm, & Fabian Monrose, *Virtual U: Defeating Face LivenessDetection by Building Virtual Models from Your Public Photos*, *in*25TH USENIX SECURITY SYMPOSIUM 497 (USENIX Association 2016), *available at* https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xu.2
[191]Manfred Bromba, *Biometric Failure Rates: Intra-CharacteristicConsideration*, BROMBAGMBH (Mar. 7, 2020), *available at*https://www.bromba.com/knowhow/BiometricFailureRates.htm.
[192]*Id.*
[193]*Id.*
[194]*Id.*
[195]Joy Buolamwini, &TimnitGebru, *GenderShades: IntersectionalAccuracyDisparities in Commercial Gender Classification*, *in* CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (2018), *available at*https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.
[196]*Id.*
[197]*Id.*
[198]Patrick Grother, Mei Ngan, &KayeeHanaoka, *Face Recognition Vendor Test (FRVT) Part 3: DemographicEffects*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Dec. 2019), *available at*https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.
[199]Sven Heiberg et al., *supra*, note 180.
[200]*Id.*
[201]Donald L. Buresh, *supra*, note 92.
[202]Id.
[203]Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, &Rachael Dean Wilson, *DefendingElections: FederalFundingNeeds for State Election Security*, BRENNAN CENTER FOR JUSTICE (Jul. 18, 2019), *available at* https://www.brennancenter.org/media/170/download.

where individuals vote using voting machines that count the vote or is Brehm referring to voting where the ballots are counted manually and where no voting machines are employed? If it is the latter, then nation-state actors cannot hack the electron process because the tallying of the votes is not accomplished using electronic equipment. There is almost no possibility that hostile nation-state actors can engage in voter fraud in a manual vote-counting process because human beings at the local level count the paper ballots. In a manual vote-counting process, the only way an antagonistic nation-state can affect a local election is to corrupt an individual or group of vote counters at the precinct or parish (Louisiana) level. Thus, the financial cost to the hostile nation-state is prohibitive and will likely not be conducted. However, with manual vote counting, there is still the possibility of a miscount, where the vote counters, intentionally or negligently, failing to count the votes cast correctly. There is also the possibility that paper ballots can be intentionally "lost," thereby violating the integrity of an election.

Automated Vote Counting without Internet Access

The next possibility that must be addressed is the use of voting machines that are not connected to the Internet during the voting process. In this instance, to change the vote count, the machines must be pre-programmed to change the vote from one candidate to another based on specific pre-specified voting trends. Suppose that a voting machine counts votes for candidates A and B. If the vote count for candidate A reaches a pre-specified percentage, the software within the voting machine can be pre-programmed to change an individual's vote for candidate B. Because there are typically multiple voting machines at a given local voting location, each device could be pre-programmed at a different percentage to change a vote from candidate A to candidate B. In this instance, unless a manual vote count was conducted, it would be improbable that a local election officer would identify the fraud. The reason is that the vast majority of local election officers are not highly computer literate. They would have to rely on the judgment of software experts or companies tasked with certifying voting machines. Even so, if a third-party vendor was employed to certify voting machines, then a hostile nation-state could corrupt the third-party corporate certifier.

There is a way where under these circumstances, the voting counts could be changed. Suppose the local election officials connect all of the machines to the Internet at the end of the voting process, uploading the vote counts offsite, where the votes would be counted. When the voting machines are connected to the Internet, an antagonistic nation-state could change the votes at the offsite vote-counting location. To prevent the hack from ever being discovered, the bad actor could download the new vote counts to the voting machines, thereby preventing the fraud from being found. The local election officials would have no way to determine that this fraud was occurring short of manually counting the votes and comparing the manual tally with the automated total.

Another way to ensure that the fraud would not be discovered is to count the votes at a site not part of the United States site. The reason is that companies in a neutral country might be paid to count the votes, where the cost of counting votes would be minimized. However, it should be remembered that the United States court and law enforcement may have no jurisdiction in the vote-counting country, thereby ensuring that the fraud would go undetected by local and state election officials. The only way to snag the scam is to conduct a manual vote count and then compare the two totals to establish discrepancies.

Automated Vote Counting with Internet Access

In this instance, the voting machines are connected to the Internet throughout the voting process. From the perspective of voter fraud, this is the most fraught with danger. A hostile nation-state could dynamically alter votes as the votes are being cast to ensure that one party wins an election. Again, this kind of fraud would probably go unobserved unless local election officials were computer savvy. The only way fraud could be discovered is if there was a manual recount of the votes to validate or invalidate the vote count.

Based on what was said above, it can be presumed that Brehm referred to the use of vote-counting machines, not manual vote-counting. Brehm's statement may be correct given the processes discussed above regarding automated voting machines and the lack of computer expertise of local and state election officials.[204] The fraud highlighted exploits the computer ignorance of local and state election officials. The only way to prevent a hostile nation-state from hacking into an election is to conduct manual vote counting at the local and state levels and ensure the vote counters are individuals of integrity. Even a manual vote-counting process is subject to fraud if the vote counters are unscrupulous. The fraud can be minimized if the vote counters have allegiance to different political parties, where the vote counters are watching each other count the votes.

Federal Election Oversight

There is a feeling that many things should be left to the federal government to oversee and regulate. The problem with the federal government scrutinizing the vote-counting processes, there is always the admonishment from Lord Acton, which he stated,"Power tends to corrupt and absolute power corrupts absolutely. Great men are almost always bad men, even when they exercise influence and not authority; still more when you superadd the tendency of the certainty of corruption by authority."[205]One of the advantages of insisting that local election officials count votes is that the potential for fraud is minimized with adequate safeguards. Decentralized vote counting prevents the concentration of the power in counting ballots at the federal level. The fewer people responsible for maintaining the integrity of the vote-counting process, the higher the probability that corruption will occur; at least, that is Lord Acton's observation.[206]

Brehm's statement implies that the only way to count votes is to use voting machines, recognizing that local election officials are ill-equipped to discover electronic voting fraud. Another implication is that only the federal government has sufficient Information Technology (IT) sophistication to minimize voter fraud. The statement seemingly ignores that manual vote counting is still a viable alternative where the risks are well-known and can be effectively mitigated. Unfortunately, Brehm's statement failed to discuss the manual vote-counting alternative.

CONCLUSIONS

Based on the information presented in the previous sections, facial recognition technology is not necessarily a foolproof method in achieving reliable election results. Biometric technology possesses not only technical issues that prevent a significant minority of individuals from being uniquely identified when they go to vote, but there are also substantial privacy issues that are present when

[204]Id.
[205]Lord Acton, Lord Action Quote Archives, ACTON INSTITUTE (n.d.), *available at*https://www.acton.org/research/lord-acton-quote-archive.
[206]Id.

people vote for the candidates of their choice. If facial recognition technology is employed in the voting process, it is evident that human intervention is necessary to avoid false negatives and false positives.

Facial recognition algorithms are strictly dependent on the dataset of faces that have been collected to teach the software how to identify an individual. A significant issue is that facial recognition algorithms have high failure rates when it comes to identifying people of color. Also, in the age of Covid-19 where individuals wear protective masks to shield them from the virus, facial recognition software is hard-pressed to identify a person with only half a face of information. The blind reliance on technology to ensure election integrity is maintained and enhanced does not appear viable. There are also numerous issues with electronic voting machines that can be hacked, particularly when they can access the Internet via hard writing or a Wireless Fidelity (Wi-Fi) connection. However primitive it may seem, there are distinct advantages to manually counting votes or using voting machines that are not software dependent. When the balance of power is strictly dependent on who is elected to political office, there is a temptation not to count votes accurately or precisely. For some people, winning at all costs is seemingly preferable to ensure that one person only casts one vote.There is no royal road here. Voting mechanisms and vote counting are fraught with the potential for fraud.

There is no getting around it. Individuals of integrity are required to manage elections so that the will of the People is honored no matter what the outcome. Facial recognition technology is not a substitute for individuals of integrity whose function is to manage an election properly. Nothing less will suffice.

DONALD L. BURESH BIOGRAPHY

Donald L. Buresh earned his Ph.D. in engineering and technology management from North central University. His dissertation assessed customer satisfaction for both agile-driven and plan-driven software development projects. Dr. Buresh earned a J.D. from The John Marshall Law School in Chicago, Illinois, focusing on cyber law and intellectual property. He also earned an LL.M in intellectual property from the University of Illinois Chicago Law School (formerly, The John Marshall Law School). Dr. Buresh received an M.P.S. in cybersecurity policy and an M.S. in cybersecurity, concentrating in cyber intelligence, both from Utica College. He has an M.B.A. from the University of Massachusetts Lowell, focusing on operations management, an M.A. in economics from Boston College, and a B.S. from the University of Illinois-Chicago, majoring in mathematics and philosophy. Dr. Buresh is a member of Delta Mu Delta, Sigma Iota Epsilon, Epsilon Pi Tau, Phi Delta Phi, Phi Alpha Delta, and Phi Theta Kappa. He has over 25 years of paid professional experience in Information Technology and has taught economics, project management, and negotiation at several universities. Dr. Buresh is an avid Chicago White Sox fan and keeps active by fencing épée at a local fencing club. Dr. Buresh is a member of the Florida Bar.

LIST OF ABBREVIATIONS

Abbreviation	Description
ACLU	American Civil Liberties Union
APT	Advanced Persistent Threat
AI	Artificial Intelligence
BEC	Business Email Compromise
DDoS	Distributed Denial of Service
EFF	Electronic Frontier Foundation
EU	European Union
IS	Information Systems
IT	Information Technology
NIST	National Institute and Standards Technology
NSA	National Security Agency
NTH	Nothing to Hide
Wi-Fi	Wireless Fidelity
XSS	Cross-Site Scripting

MISCELLANEOUS CONSIDERATIONS

Author Contributions: The author has read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The author declares no conflict of interest.

Acknowledgments: Not applicable.

REFERENCES

FEDERAL AND STATE COURT CASES

Aiken Mills v. United States, D.C.S.C., 144 F.2d 23 (4th Cir. 1944), available at https://law.justia.com/cases/federal/appellate-courts/F2/144/23/1547763/.

Arkwright Corporation v. United States, D.C. Mass., 53 F.Supp. 359, 361 (D.C. Mass. 1943), available at https://casetext.com/case/arkwright-corporation-v-united-states.

Gallopin v. Continental Casualty Co., 290 Ill. App. 8, 7 N.E.2d 771, 774 (1937), available at https://casetext.com/case/gallopin-v-continental-casualty-co.

In the Matter of Everalbum, Inc., UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE COMMISSION (May 7, 2021), available at https://www.ftc.gov/system/files/documents/cases/1923172_-_everalbum_complaint.

In the Matter of TaxSlayer, LLC, Complaint Docket No. C-2646 (n.d.), available at https://www.ftc.gov/system/files/documents/cases/1623063_c4626_taxslayer_complaint.pdf.

Katz v. United States, 386 U.S. 954 (1967) (see Justice Harlan's concurrence), available at https://supreme.justia.com/cases/federal/us/389/347/.

Lyons v. Otter Tail Power Co., 70 N.D. 681, 297 N.W. 691, 693 (1941), available athttps://cite.case.law/nd/70/681/.

Nichols v. Ocean Accident & Guarantee Corporation, 70 Ga.App. 169, 27 S.E.2d 764, 766 (1943), available at https://casetext.com/case/nichols-v-ocean-accident-c-corporation/.

FEDERAL RULES, REGULATIONS, STANDARDS, AND STATUTES

DOF Staff, Identity Theft, UNITED STATES DEPARTMENT OF JUSTICE (n.d.), available at https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud.

NIST Staff, Federal Information Security Modernization Act (FISMA) Background, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Updated September 28, 2021), available at https://csrc.nist.gov/projects/risk-management/fisma-background.

NIST Staff, NIST Launches Studies into Masks' Effect on Face Recognition Software, NATIONAL INSTITUTE OF STANDARDS AND

TECHNOLOGY (July 27, 2020), available at https://www.nist.gov/news-events/news/2020/07/nist-launches-studies-masks-effect-face-recognition-software.

Patrick Grother, Mei Ngan, & Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Dec. 2019), available at https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8280.pdf.

U.S. Const, amends. XV, XIX, XXIV, & XXVI.

ACADEMIC JOURNALS AND BOOKS

Clare Garvis, & Laura M. Moy, America under Watch: Face Surveillance in the United States, GEORGETOWN L. CTR. FOR PRIV. AND TECH. (May 16, 2019), available at https://www.americaunderwatch.com/.

Daniel J. Solove, "I've Got Nothing to Hide" and Other Misunderstandings of Privacy, 44 SAN DIEGO L. REV. 745, 747 (February 7, 2007), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565.

Donald L. Buresh, A Comparison Between the European and American Approaches to Privacy, 6 INDONESIAN J. OF INTL AND COMP. L. 2, 253-281 (2019), available at https://heinonline.org/HOL/LandingPage?handle=hein.journals/indjicl6&div=16&id=&page=.

Donald L. Buresh, Should Personal Information and Biometric Data Be Protected under a Comprehensive Federal Privacy Statute that Uses the California Consumer Privacy Act and the Illinois Biometric Information Privacy Act as Model Laws?, 38 SANTA CLARA UNIV.: HIGH TECH L. J., available at https://digitalcommons.law.scu.edu/chtlj/vol38/iss1/2/.

Donald L. Buresh, The Meaning of Justice Gorsuch's Dissent in Carpenter v. United States, 43 AMERICAN JOURNAL OF TRIAL ADVOCACY 1 55-103 (2019), available at https://heinonline.org/HOL/LandingPage?handle=.

Eileen Guo, & Hikmat Noori, This Is the Real Story of the Afghan Biometric Databases Abandoned to the Taliban, MIT TECH. REV. (August 30, 2021), available at https://www.technologyreview.com/2021/08/30/1033941/afghanistan-biometric-databases-us-military-40-data-points/.

IT GOVERNANCE PRIVACY TEAM,EU GENERAL DATA PROTECTION REGULATION (GDPR): AN IMPLEMENTATION AND COMPLIANCE GUIDE 11, 11 (2nd ed. 2017).

Jeff Kosseff, Defining Cybersecurity Law, 103 IOWA L. REV. 985 (2018), available at https://ilr.law.uiowa.edu/print/volume-103-issue-3/defining-cybersecurity-law/.

Joy Buolamwini, & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, in CONFERENCE ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY (2018), available at https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

PETER F. DRUCKER, MANAGEMENT: TASKS, RESPONSIBILITIES, PRACTICES (HarperBusiness 1993).

PETER WOLF, INTRODUCING BIOMETRIC TECHNOLOGY IN ELECTIONS, (International Institute for Democracy and Electoral Assistance 2017), available athttps://www.idea.int/sites/default/files/publications/introducing-biometric-technology-in-elections-reissue.pdf.

Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARVARD L. REV. 193 (1890) available at https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

OTHER AUTHORITIES

Abigail Abrams, Here's What We Know So Far About Russia's 2016 Meddling, TIME (April 18, 2019), available at https://time.com/5565991/russia-influence-2016-election/.

ACLU Staff, Facial Recognition Technology, AMERICAN CIVIL LIBERTIES UNION (n.d.), available athttps://www.aclu.org/issues/privacy-technology/surveillance-technologies/face-recognition-technology.

Anthony K. Haynes, Global Privacy Regimes, CSDP 501 – CYBERSECURITY PUBLIC POLICY SEMINAR (2021), available at https://albanylaw.instructure.com/courses/1828/files/145476/download?download_frd=1. PowerPoint Presentation.

Bill Allison et al., Trump Team's Conflicts and Scandals: An Interactive Guide, BLOOMBERG (March 14, 2019), available at https://www.bloomberg.com/graphics/trump-administration-conflicts/?leadSource=uverify%20wall.

California Privacy Rights Act: An Overview, PRIVACY RIGHTS CLEARINGHOUSE (December 10, 2020), https://privacyrights.org/resources/california-privacy-rights-act-overview#:~:text=The%20California%20Privacy%20Rights%20Act%20clarifies%20that%20people%20can%20opt,personal%20information%20to%20third%20parties.&text=The%20California%20Privacy%20Rights%20Act%20expands%20this%20to%20cover%20data,includes%20a%20username%20and%20password.

CCC Staff, Introduction to the Cyber Threat Environment, CANADIAN CENTRE FOR CYBERSECURITY (June 29, 2021), available at https://cyber.gc.ca/en/guidance/cyber-threat-and-cyber-threat-actors.

CDC Staff, Health Insurance Portability and Accountability Act of 1996 (HIPAA), CENTERS FOR DISEASE CONTROL AND PREVENTION (September 18, 2018), available at https://www.cdc.gov/phlp/publications/topic/hipaa.html.

Charles Kim, Pelosi: Leaving Military Equipment Behind Is 'What Happens' in Withdrawal, NEWSMAX, (August 18, 2021), available at https://www.newsmax.com/politics/pelosi-democrats-biden-war/2021/08/18/id/1032933/.

Christopher R. Deluzio, Liz Howard, Paul Rosenzweig, David Salvo, & Rachael Dean Wilson, Defending Elections: Federal Funding Needs for State Election Security, BRENNAN CENTER FOR JUSTICE (July 18, 2019), available at https://www.brennancenter.org/media/170/download.

Cisco Staff, What Is IT Security?, CISCO SYSTEMS, INC. (n.d.), available at https://www.cisco.com/c/en/us/products/security/what-is-it-security.html.

Customer, BLACK'S LAW DICTIONARY 462 (4th ed. 1968), available athttps://heimatundrecht.de/sites/default/files/dokumente/Black'sLaw4th.pdf.

EFF Staff, Street-Level Surveillance, ELECTRONIC FRONTIER FOUNDATION (October 24, 2017), available at https://www.eff.org/pages/face-recognition.

Espionage, ENCYCLOPEDIA BRITANNICA (n.d.), available at https://www.britannica.com/topic/espionage.

Espionage, MERRIAM-WEBSTER DICTIONARY (n.d.), available at https://www.merriam-webster.com/dictionary/espionage.

Face First Staff, 21 Amazing Uses for Face Recognition, FACE FIRST (n.d.), available at https://www.facefirst.com/blog/amazing-uses-for-face-recognition-facial-recognition-use-cases/.

Gary Kranz, Gramm-Leach-Bliley Act (GLBA), TECH TARGET (Jun. 2021), available at https://searchcio.techtarget.com/definition/Gramm-Leach-Bliley-Act.

Gordon Adams, From Vietnam to Afghanistan, all US governments Lie, THE CONVERSATION, (August 31, 2019), available at https://theconversation.com/from-vietnam-to-afghanistan-all-us-governments-lie-128695.

Hegel's Dialectics, STANFORD ENCYCLOPEDIA OF PHILOSOPHY, (October 02, 2020), available at https://plato.stanford.edu/entries/hegel-dialectics/.

Ian Sample, What is Facial Recognition - And How Sinister Is It?, THE GUARDIAN (July 29, 2019), available at https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it.

Information, MERRIAM-WEBSTER'S DICTIONARY, (n.d.), available at https://www.merriam-webster.com/dictionary/information.

Ivy Wigmore, Threat Actor, TECH TARGET (Jan. 2016), available at https://www.techtarget.com/whatis/definition/threat-actor.

Jake Frankenfield, revised by Amy Drury, General Data Protection Regulation (GDPR), INVESTOPEDIA, (November 11, 2020), https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp.

Juliana De Groot, What is Cyber Security? Definition, Best Practices & More, DATA INSIDER (October 5, 2020), available at https://digitalguardian.com/blog/what-cyber-security.

Kaspersky Labs Staff, What is Facial Recognition – Definition and Explanation, KASPERSKY LABS (n.d.), available at https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition.

Laura Jakes, How Many People in Afghanistan Need to be Rescued? The Number Remains Elusive., THE NEW YORK TIMES, (August 24, 2021), available athttps://www.nytimes.com/2021/08/24/us/politics/afghanistan-evacuations-kabul-airport.html.

Lee Cataluna, Honesty vs. Transparency: Which Is Key to Successful Government? (Opinion), GOVERNMENT TECHNOLOGY, (November 09, 2016), available at https://www.govtech.com/opinion/honesty-vs-transparency-which-is-key-to-successful-government-opinion.html.

Lord Acton, Lord Action Quote Archives, ACTON INSTITUTE (n.d.), available at https://www.acton.org/research/lord-acton-quote-archive.

Manfred Bromba, Biometric Failure Rates: Intra-Characteristic Consideration, BROMBA GMBH (March 7, 2020), available at https://www.bromba.com/knowhow/BiometricFailureRates.htm.

Misdirection, MERRIAM-WEBSTER DICTIONARY, (n.d.), available athttps://www.merriam-webster.com/dictionary/misdirection.

Misrepresentation, INVESTOPEDIA, (n.d.), available at https://www.investopedia.com/terms/m/misrepresentation.asp.

NIST Staff, FRVT 1:1 Verification, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (November 1, 2022), available athttps://pages.nist.gov/frvt/html/frvt11.html.

Panda Security Staff, Types of Cybercrime, PANDA SECURITY (n.d.), available at https://www.pandasecurity.com/en/mediacenter/panda-security/types-of-cybercrime/.

Rebecca Hawk, 5 Benefits of More Transparency in Your Workplace, THE CENTER FOR ASSOCIATION LEADERSHIP, (n.d.), available at https://www.asaecenter.org/associationcareerhq/career/articles/talent-management/5-benefits-of-more-transparency-in-your-workplace.

Robby Brod, These Republicans Did a Deep Dive into 2020 Election Lawsuits, Including in Pa. Here's Why Most of Them Failed, WITF (September 1, 2022), available at https://www.witf.org/2022/09/01/these-republicans-did-a-deep-dive-into-2020-election-lawsuits-including-in-pa-heres-why-most-of-them-failed/.

Sarah Rippy, Colorado Privacy Act Becomes Law, THE PRIVACY ADVISER (July 8, 2021), https://iapp.org/news/a/colorado-privacy-act-becomes-law/.

Sarah Rippy, Virginia Passes the Consumer Data Protection Act, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, (March 3, 2021), https://iapp.org/news/a/virginia-passes-the-consumer-data-protection-act/.

Scott Ridder, The Biden Administration's Incompetence Has Created the Conditions for a Modern Dien Bin Phu in Kabul, RT, (August 19, 2021), available athttps://www.rt.com/op-ed/532533-us-troops-remain-afghanistan-hkia/.

Sentinel One, Threat Actor Basics: The 5 Main Threat Types, SENTINEL ONE BLOG (September 9, 2019), available at https://www.sentinelone.com/blog/threat-actor-basics-understanding-5-main-threat-types/.

Shannon Vallor, & William J. Rewak, Introduction to Cybersecurity Ethics, SANTA CLARA UNIV. (n.d.), available at https://pdf4pro.com/download/an-introduction-to-cybersecurity-ethics-module-author-668084.html.

Sharon Shea, Alexander S. Gillis, & Casey Clark, What is Cybersecurity?, TECHTARGET (n.d.), available at https://searchsecurity.techtarget.com/definition/cybersecurity.

Sven Heiberg, Kristjan Krips, Jan Willemson, & Priit Vinkel, Facial Recognition for Remote Electronic Voting Missing Piece of the Puzzle or Yet Another Liability?, inEMERGING TECHNOLOGIES FOR AUTHORIZATION AND AUTHENTICATION, 13136. (Springer, Cham. A. Saracino, & P. Mori eds.), available at https://doi.org/10.1007/978-3-030-93747-8_6.

Tech Target Contributor, Biometric Verification, TECH TARGET (Jul. 2021), available at https://www.techtarget.com/searchsecurity/definition/biometric-verification#:~:text=Biometric%20verification%20is%20any%20means,voice%20prints%20and%20written%20signatures.

Technopedia Staff, Facial Recognition, TECHNOPEDIA (August 24, 2021), available at https://www.techopedia.com/definition/32071/facial-recognition.

Techopedia Staff, Cyberlaw, TECHOPEDIA (n.d.), available at https://www.techopedia.com/definition/25600/cyberlaw.

Terry Treadwell, What Is the Cost of Truth?, WOUND CARE LEARNING NETWORK, (n.d.), available at https://www.hmpgloballearningnetwork.com/site/wounds/editorial/what-cost-truth.

What is Accessibility, BLACK'S LAW ONLINE DICTIONARY, (2016), available at http://alegaldictionary.com/accessibility/.

What is Transparency, BLACK'S LAW ONLINE DICTIONARY, (2016), available at http://alegaldictionary.com/transparency/.

WIPO Staff, Trade Secrets: What Is a Trade Secret?, WORLD INTELLECTUAL PROPERTY ORGANIZATION (n.d.), available at https://www.wipo.int/tradesecrets/en/.

Yi Xu, True Price, Jan-Michael Frahm, & Fabian Monrose, Virtual U: Defeating Face Liveness Detection by Building Virtual Models from Your Public Photos, in25TH USENIX SECURITY SYMPOSIUM 497 (USENIX Association 2016), available athttps://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xu.

****