Compelled Testimony? A U.S. Legal and Ethical Review of Compelled Biometric Data and Encryption

Dominique Dove[1] and Kenneth Chamberland Jr.[2]
[1]The George Washington University School of Law, Washington, D.C., USA
[2]Capella University, Minneapolis, Minnesota, USA

Dominique.dove.esq@gmail.com
Ken.chamberland@gmail.com

Abstract: Biological data has increasingly become interconnected and digitized, leading to the emergence of the field of biocybersecurity to address cyber threats within bioinformatic systems. Encryption provides significant social benefits by safeguarding sensitive information, but it also presents challenges to public safety. The increase of cell phone use and the rise of internet-connected devices have resulted in a greater volume of digital data for law enforcement agencies to investigate. These trends have created a demand for advanced encryption methods, including access controls relying on facial recognition or other kinds of biometric data. While policy debates regarding backdoor access to aid law enforcement in combating crime continue, courts increasingly confront important Fifth Amendment questions in criminal investigations relying on digital evidence. In these cases, courts must frequently assess whether compelling the disclosure or use of biometric identifiers infringes upon protections against compelled testimonial evidence. The balancing of national security and privacy concerns are crucial in determining whether we are willing to sacrifice privacy and civil liberties for safety. This paper examines the intersection of encryption, law enforcement access, and the legal and ethical considerations raised by compelled disclosure or use of biometric data from a U.S. perspective.

Keywords: Biometric data, Back door access, 5th amendment, Sensitive information, Compelled testimony

1. Introduction

As life sciences and digital technology become increasingly interconnected, the need to protect biological systems and data has never been more critical. Biocybersecurity (BCS) addresses the risks that arise with this intersection, focusing on how biological systems can be exploited through cyber assets. With the digitization of healthcare, genomics, and agriculture, BCS plays a vital role in safeguarding these essential resources. It applies cybersecurity principles to biosecurity challenges, countering threats like data breaches, ransomware, and unauthorized access. Tools such as techno-surveillance networks help detect and neutralize vulnerabilities like backdoors and privilege escalation attacks, ensuring the resilience and integrity of sensitive systems (Potter & Palmer, 2023). A key component of biocybersecurity is data encryption, which protects sensitive biological information from being accessed or tampered with. Encryption transforms data into a secure, unreadable format that only authorized users can decode, ensuring the confidentiality of genomic databases, patient records, and research data. This protection is especially important in bioinformatics and healthcare, where digitized data is a valuable target for cyberattacks. By safeguarding patient privacy, intellectual property, and biometric data, encryption serves as a critical defense against breaches and malicious tampering (Stine & Dang, 2011).

However, the growing challenge of securing sensitive data has brought the issue of backdoor access into focus. While backdoors are often promoted as a necessary tool for law enforcement to combat cybercrime and terrorism, they also raise significant concerns about privacy, security, and potential misuse. Genomic databases are already prime targets for cyberattacks, and the existence of backdoors could amplify these risks if exploited. Beyond the technical dangers, many individuals lack an understanding of their digital rights, leaving them vulnerable to intimidation or misuse of backdoor mechanisms. Striking a balance between public safety and personal freedoms requires clear public education on digital rights and robust protections against abuse. Trust in law enforcement and digital systems depends on addressing these challenges thoughtfully (Abelson et al., 2015). This paper examines biocybersecurity and the need to protect bioinformatic data versus legal and ethical concerns with backdoor access and using bioinformatic data for law enforcement purposes.

2. Biocybersecurity Overview

Bioinformatics and genomic data storage systems face significant vulnerabilities due to the sensitive and highly valuable data they contain. Genomic information, which serves as an individual's biological blueprint, is a prime target for cyberattacks with potential violations ranging from identity theft and insurance discrimination to unauthorized research and the development of biological weapons. The interconnected nature of these systems exposes them to threats such as ransomware, backdoors, and privileged escalation. Lack of strong security measures often prioritize access for researchers over strict protections such as encryption and access controls.

These vulnerabilities not only threaten individual privacy but also risks undermining public confidence. These issues highlight the urgent need for strong cyber security measures (Pulivarti et al., 2023). The digitization of biological data has introduced significant threats, particularly, the misuse of genomic information. Genomic data, which contains the unique biological identifiers of individuals, is vulnerable to exploitation for harmful purposes, such as creating targeted bioweapons or enabling discriminatory practices. Bioterrorism represents a particularly alarming threat, as genomic information combined with predictive modeling could enable the engineering of pathogens tailored to specific genetic vulnerabilities within populations (Pulivarti et al., 2023).

Therefore, significant improvements should be made to protect bioinformatic and genomic data. When faced with protecting biosecurity, the most essential tool is data encryption. With the growing reliance on genomic databases and advanced technologies in healthcare and research, the sensitive data they hold has become a prime target for cyberattacks. Encryption keeps this data safe by turning it into unreadable code that only authorized people can access. Without strong encryption, these systems would be vulnerable to breaches that could erode trust in healthcare, science, and more (Fayayola et al., 2024).

3. The U.S. Constitution

The Fourth Amendment prohibits unreasonable searches and seizures. In general, a law enforcement officer is required to obtain a warrant before conducting a search. Warrantless searches are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions. In general, the warrant requirement applies to searches of cell phones because of the broad array of private information contained in modern cell phones. *People v. Ramirez*, 98 Cal. App. 5th 175, 316 Cal. Rptr. 3d 520 (2023). A search occurs when an expectation of privacy that society is prepared to consider reasonable is infringed. Invasions of the body, including nonconsensual extractions of an incarcerated felon's blood for DNA profiling, are searches entitled to the protections of the Fourth Amendment. As the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is reasonableness. Reasonableness is measured in objective terms by examining the totality of the circumstances, and whether a particular search meets the reasonableness standard is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests. *People v. Ramirez*, 98 Cal. App. 5th 175, 316 Cal. Rptr. 3d 520 (2023).

The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The proper inquiry is whether an act would require the compulsion of a testimonial communication that is incriminating. *See Fisher v. United States,* 425 U.S. 391, 409, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). The challenge facing the courts is that technology is outpacing the law. In recognition of this reality, the United States Supreme Court recently instructed courts to adopt rules that "`take account of more sophisticated systems that are already in use or in development.'" *Carpenter v. United States,* 138 S.Ct. at 2218-19 (quoting *Kyllo v. United States,* 533 U.S. 27, 36, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)). Courts have an obligation to safeguard constitutional rights and cannot permit those rights to be diminished merely due to the advancement of technology. *See Carpenter,* 138 S.Ct. at 2214 (quoting *Kyllo v. United States,* 533 U.S. at 34, 121 S.Ct. 2038).

3.1 Compelled Testimony and Biometric Data in the U.S. Legal System

U.S. courts have held that producing a fingerprint to unlock a cell phone is not testimonial and therefore, does not implicate the privilege of self-incrimination. In *People v. Ramirez*, a Court of Appeal's case, the defendant was convicted of multiple lewd offenses against four children. 98 Cal. App. 5th 175, 316 Cal. Rptr. 3d 520 (2023). The defendant argued on appeal that the compelled use of his fingerprint to unlock his phone constituted an unreasonable search under the fourth amendment and the compelled use of his fingerprint to unlock his phone violated his privilege against self-incrimination under the Fifth Amendment. in the state of California, the court held the compelled use of the defendant's fingerprint to unlock his phone did not violate his Fourth Amendment rights nor was the act of producing his fingerprint considered to be testimonial evidence and thus the privilege of self-incrimination was not implicated. *People v. Ramirez*, 98 Cal. App. 5th 175, 316 Cal. Rptr. 3d 520 (2023).

The United States Supreme Court has held that communications are testimonial under the Fifth Amendment when they "explicitly or implicitly relate to a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201. Due to advances in encryption, attorneys have presented good arguments in front of the courts on whether the use of a suspect's biometric feature to potentially unlock an electronic device is testimonial under the Fifth Amendment. Courts have already determined that a passcode cannot be compelled because it is testimonial. *In Matter of Residence in Oakland, California,* the government was investigating two individuals

suspected of extortion. They allegedly, used Facebook Messenger to threaten to distribute an embarrassing video if the victim did not give them monetary compensation. The government submitted a search and seizure warrant to compel any individual present at the time of the search to press a finger or to use other biometric features to unlock the digital devices to perform a search of its contents. However, the court denied the Government's request for a search warrant because it stated, the government "may not compel or otherwise utilize fingers, thumbs, facial recognition, optical/iris, or any other biometric feature to unlock electronic devices and that utilizing a biometric feature to unlock an electronic device is not akin to submitting to fingerprinting or a DNA swab." 354 F.Supp.3d 1010 (2019).

Military courts in the United States also struggle to stay up to date with the advancement of technology and whether encrypted data should be viewed differently than unencrypted data. *United States v. Secord*, a pending United States Court of Appeals for the Armed Forces case (CAAF), illustrates the need for courts to determine how encrypted data should be viewed. (*Unites States. V. Secord*, No. 24-0217/AR 2025). In this case, a soldier was suspected of selling and using cocaine. Special Agents (SAs) from the U.S. Army Criminal Investigation Division investigated appellant's cocaine use and distribution. SAs lawfully seized appellant's cell phone pursuant to a search and seizure authorization. However, the Criminal Investigation Division (CID) could not extract any data from appellant's cell phone because it was passcode protected and the CID's extraction software was incompatible with the cell phone. In this case, the government argued that data is separate from the physical object (the phone) and that the phone itself was not "evidence" because, without the PIN, it was nothing more than an inert physical object that could provide no information to either side. Therefore, the government only had possession of the phone and not the data because the government could not access the data. However, the defense argued that once the government seized the phone, they took possession of both the phone and the data. Cases like *United States. v. Secord* exemplifies that technology is rapidly changing and that courts cannot continue to view data and encrypted data the same way it has been viewed previously.

Recently, the U.S. Army Court of Appeals held that compelled facial recognition is testimonial. in this case, the appellee was charged with a variety of offenses stemming from his attempts to sexually exploit a fourteen-year-old whom he had previously known from school. During the investigation, special agents lawfully seized appellee's cell phone. The appellee was later advised of, and waived, his rights under Article 31, UCMJ[1], and submitted to questioning. During this initial interview, agents asked the appellee for the passcode. After none of the provided passcodes unlocked the phone, CID successfully asked appellee to unlock the phone using facial recognition. With the phone unlocked, agents conducted a manual review of the phone which revealed suspected child sexual abuse material on multiple cell phone applications, including an application called "Mega," described as an online cloud-based storage drive. (*United States v. Gilkey*, 2025 CCA LEXIS 86).

Here, the government argued that the use of appellant's face to unlock his phone is non-testimonial. However, the court stated, "a servicemember' s protection against compulsory self-incrimination is unparalleled in the civilian sector' because '[t]his fundamental right is protected by both the Fifth Amendment *and* Article 31, UCMJ."' *United States v. Nelson,* 82 M.J. 251, 255 (C.A.A.F. 2022) (quoting *United States v. Mapes,* 59 M.J. 60, 65 (C.A.A.F. 2003) (alterations and emphasis in original). The court said Article 31, UCMJ, protections are "broader" than those afforded under the Fifth Amendment because they are required before questioning anyone suspected of an offense, not just those in custody, and provide a statutory restriction against admissibility of unwarned statements at courts-martial. *United States v. Swift,* 53 M.J. 439, 445 (C.A.A.F. 2000) (stating the statute reflects Congress' decision "that the unique circumstances of military service required specific statutory protections or members of the armed forces"). In looking at the facts and circumstances of this case, the court held the "line between testimonial and nontestimonial is crossed when the contents of an individual's mind are used against him." (*United States v. Gilkey*, 2025 CCA LEXIS 86 at 13).

The Army Court of Appeals heavily relied on a recent D.C. Circuit Court of Appeals case, *United States v. Brown,* 125 F.4th 1186, 2025 U.S. App. LEXIS 1219 (D.C. Cir. 2025). In this case, after the appellant was arrested, the FBI seized his phone and asked him for the passcode to unlock it. After several failed attempts, the agents were able to unlock his phone using his thumbprint. On appeal, the issue before the D.C. Circuit was whether the act of

[1] Article 31 (b) states that "no person subject to this chapter may interrogate, or request any statement from, an accused or a person suspected of an offense without first informing him of the nature of the accusation and advising him that he does not have to make any statement regarding the offense of which he is accused or suspected and that any statement made by him may be used as evidence against him in a trial by court-martial"

unlocking the phone was testimonial and therefore protected by the Fifth Amendment. *Id.* at *23. The court, under the circumstances of that case, determined that it was. *Id.*

Currently, there is a consensus of U.S. courts is that providing a password to unlock an encrypted phone is considered a testimonial act for the purposes of the Fifth amendment. However, there is not a consensus on whether using a fingerprint or facial recognition to unlock an encrypted phone is testimonial.

3.2 Encryption Backdoors and Privacy

The use of bioinformatic data is an advancing technology where more individuals are using their fingerprints and facial features to encrypt their cellphone devices. The San Bernardino attack continues to illustrate the importance of the debate between individual privacy concerns and national security. This attack resulted in the deaths of 14 individuals, however, the Federal Bureau of Investigations (FBI) was unable to unlock the phone of one of the attackers. The FBI attempted several times to unlock the phone and in doing so, accidentally reset the passcode which resulted in data no longer being transmitted to the cloud (Anand and Kumar, 2021). The FBI was unable to unlock the phone due to Apple's strong encryption. Therefore, the FBI sought an order requiring Apple to create a new firmware that would remove the passcode lock out on the seized phone (Anand and Kumar, 2021). The FBI argued for backdoor access through Apple, and they refused. Apple argued that establishing a new code would risk the security of iPhone users worldwide. Eventually, the Justice Department purchased a third-party tool to gain access to the contents of the phone.

The Justice Department argued, "It remains a priority for the government to ensure that law enforcement can obtain crucial digital information to protect national security and public safety, either with cooperation from relevant parties or through the court system when cooperation fails," DOJ's Newman said. "We will continue to pursue all available options for this mission, including seeking the cooperation of manufacturers and relying upon the creativity of both the public and private sectors." (Selyyukh, 2016).

4. Law Enforcement and the "Backdoor" Debate

Technology professionals argue against backdoor access not only for privacy concerns but also due to a potential increase for hackers (Endeley, 2019). However, law enforcement agencies argue for the development of backdoor access for public safety. According to the U.S. Senate in 2015, law enforcement agencies are concerned that they lack the technical means to search for evidence of a crime even after obtaining a warrant as they are reporting that there is a decrease in their ability to intercept real-time communications (U.S. Department of Homeland Security, 2015). Additionally, they voice concerns about accessing encrypted phones pursuant to valid search warrants. There has been a long-simmering struggle between privacy rights and national security (Dolph, 2016). The Patriot Act, a landmark law, was implemented to improve national security relating to foreign terrorism (Dolph, 2016). In 2013, the National Security Agency whistleblower, Edward Snowden, released classified documents, bringing the debate between privacy and national security into the forefront (Dolph, 2016). His actions highlight the ongoing necessity of the Patriot Act versus an individual's right to privacy.

The U.S. Department of Justice has noted that they often lack the tactical ability to carry out their obligations due to the advancements in technology. (Mitchell, et al, 2017). Advancements in technology also present challenges for law enforcement and forensic experts. Encryption and the use of other obfuscation techniques create a serious threat to national security. (Mitchell, et al, 2017). However, the use of backdoor access is not widely accepted.

Counterterrorism officials are increasingly concerned about terrorists using encryption as a means of communicating. (Graham, 2016). Recent events illustrate that counterterrorism is intertwined with encryption (Tang, 2016). As encryption advances, terrorists are exploiting the technology and avoiding incrimination by "going dark" creating the need for law enforcement agencies to desire "backdoor" access to data encryption. (Graham, 2016). The implementation of law enforcement "backdoor" access to encryption has been a debate for the last decade, weighing out legitimate safety concerns with security and privacy concerns.

4.1 Commercial Spyware

"Spyware appears to be a new and rapidly growing practice that poses a risk of serious harm to consumers." (Sipior, et al, 2005). Spyware includes "[a]ny software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes." (Sipior, et al, 2005). There are various types of spyware such as adware cookies, adware, trojan horses, and system monitors. U.S. agencies, such as the U.S. Department of State are working with other countries to endorse a multilateral commitment to counter the proliferation and misuse of commercial spyware. To date, 23 countries have joined this effort and

have agreed to implement strict domestic and international controls on the proliferation and use of commercial spyware. (Sipior, et al, 2005).

4.2 Ethical and Legal Considerations

Using backdoor access has sparked arguments concerning the erosion of civil liberties from an ethical standpoint. It is imperative to analyze when would it be appropriate to implement backdoor access, who would make the decision to use the technology, and the safeguards implemented to prevent misuse. Backdoor access could lead to the United States losing their credibility relating to privacy concerns with other countries since it has adamantly opposed other country's invasion of privacy of their citizens (Tang, 2016). Privacy is a one of the main concerns with commercial spyware as is surreptitious data collection. In the U.S., the Federal Trade Commission has the legal authority to protect its citizens against spyware.

5. The Role of Encryption in Biocybersecurity

The integration of biometrics causes emerging security risks that needs protection (Ney, 2019). Encryption is fundamental in ensuring the confidentiality and integrity of biological data, making it a cornerstone of modern biosafety. In today's world, understanding security is crucial to understanding technology as technology is rapidly evolving (Tang, 2016). By converting sensitive information into unreadable code, encryption ensures that only authorized users with the appropriate decryption keys can access the data. This process protects the confidentiality of genome sequences, patient health records, and research information, even if the data is intercepted during transmission or accessed through legitimate means.

5.1 The Necessity of Encryption

According to the National Institute of Standards and Technology (NIST), encryption is essential for providing information security, including confidentiality and data integrity (Stine & Dang, 2011). In addition to maintaining confidentiality, encryption safeguards the integrity of biological data by preventing unauthorized alterations. Techniques such as cryptographic hashing generate unique digital signatures for the information. If any modification occurs, the hash value changes, signaling potential tampering. This mechanism ensures the accuracy and reliability of sensitive information, which is critical for patient care, research outcomes, and maintaining trust in scientific processes. As highlighted in the article "Ensuring privacy and security of genomic data and functionalities," the sensitive nature of genomic data necessitates robust security measures to protect against unauthorized access and modifications (Yakuba and Chen, 2019).

However, implementing encryption at scale for massive datasets presents challenges, particularly in bioinformatics, where large volumes of genomic data are processed. The computational demands of encrypting and decrypting extensive datasets can be significant, potentially leading to delays in data access or analysis. Moreover, encrypted data often requires more storage space than unencrypted formats, straining resources in systems handling vast amounts of biological information. Managing encryption keys at scale adds complexity, as keys must be securely stored and accessible only to authorized parties, while maintaining the ability to recover lost keys. There are various strategies to ensure the security and integrity of sensitive information in connected environments, including robust data management practices (Srivastav et al., 2024).

5.2 Education Concerning Encryption

Educating individuals about their rights concerning data security is also crucial. Many people are unaware of how their biological data is protected or may hesitate to inquire about encryption and access controls. Providing clear, straightforward information empowers individuals to make informed decisions and hold organizations accountable for safeguarding their sensitive information. In a data-driven world, transparency and education are as important as the technologies used to protect information. Murdoch, 2021 highlights the ethical implications surrounding the convergence of biotechnology and digital technologies, discussing concerns such as privacy, data ownership, and consent. Managing encryption keys adds another layer of complexity in the legal field, and it also creates competing priorities of individual privacy while ensuring effective law enforcement.

6. The Way Forward

As technology continues to evolve, U.S. courts should update their laws concerning data and compelled testimony and include compelled biometrics as a violation of the Fifth Amendment. The U.S. should also continue to inform its citizens about the dangers of spyware and implement legislation to protect its citizens. Additionally, The U.S. and other countries should continue to support each other in strict controls of commercial

spyware to counter misuse by preventing the export of technology to users who will likely use them for malicious cyber activity.

7. Conclusion

This paper has illustrated some key issues with the advancement of technology and the evolution of the legal system. As technology continues to advance, the need for legal interpretations concerning BCS should advance. The intersection of BCS and law enforcement will face even more challenges in the upcoming years, however, it is vital for lawmakers, policy writers, and technology developers to work together. While policy debates regarding backdoor access to aid law enforcement in combating crime will continue and courts will increasingly confront important Fifth Amendment questions in criminal investigations relying on digital evidence, courts should frequently assess whether compelling the disclosure or use of biometric identifiers infringes upon protections against compelled testimonial evidence. The balancing of national security and privacy concerns are crucial in determining whether we are willing to sacrifice privacy and civil liberties for safety.

8. Acknowledgements

The authors would like to thank Allen Walker, Xavier Polymer, and Lucas Potter for their encouragement and assistance with data collection. Without their support, this paper would have never been written.

References

Abelson, H., Anderson, R., Bellovin, M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Neumann, P.G. and Landau, S., 2015. Keys under doormats: Mandating insecurity by requiring government access to all data and communications. july 6, 2015. *Google Scholar Google Scholar Digital Library Digital Library*.

Anand, A. and Kumar, R., 2021. Apple Inc. vs FBI A Jurisprudential Approach to the case of San Bernardino.

Basics, E., Stine, K. and Dang, Q., Encryption Basics.

Carpenter v. United States, 138 S.Ct. 2206.

Doe v. United States, 487 U.S. 201.

Dolph, A., 2016. Terrorism Versus the Right to Privacy: Apple Takes on the DOJ.

Endeley, R.E., 2019. *End-to-end Encryption, Backdoors, and Privacy*. Capitol Technology University.

Farayola, O.A., Olorunfemi, O.L. and Shoetan, P.O., 2024. Data privacy and security in it: a review of techniques and challenges. *Computer Science & IT Research Journal*, *5*(3), pp.606-615

Fisher v. United States, 425 U.S. 391

FTC (2004b). Prepared statement of the Federal Trade Commission before the Committee on Energy and Commerce, Subcommittee on Commerce, Trade, and Consumer Protection, United States House of Representatives.

Graham, R., 2016. How terrorists use encryption. *CTC Sentinel*, *9*(6), p.20.

GUIDE, I.J.P., 2015. US Department OF Homeland Security.

Hartel, P. and van Wegberg, R., 2023. Going dark? Analysing the impact of end-to-end encryption on the outcome of Dutch criminal court cases. *Crime Science*, *12*(1), p.5.

Kyllo v. United States, 533 U.S. 27.

Mitchell, B., Kaul, K., McNamara, G.S., Tucker, M., Hicks, J., Bliss, C., Ober, R., Castro, D., Wells, A., Reguerin, C. and Green-Ortiz, C., 2017. Going dark: impact to intelligence and law enforcement and threat mitigation.

Mohammed Yakubu, A. and Chen, Y.P.P., 2020. Ensuring privacy and security of genomic data and functionalities. *Briefings in bioinformatics*, *21*(2), pp.511-526.

Murdoch, B., 2021. Privacy and artificial intelligence: challenges for protecting health information in a new era. *BMC Medical Ethics*, *22*, pp.1-5.

Ney, P.M., 2019. *Securing the future of biotechnology: A study of emerging bio-cyber security threats to dna-information systems* (Doctoral dissertation).

People v. Ramirez, 98 Cal. App. 5th 175, 316 Cal. Rptr. 3d 520 (2023).

Potter, L. and Palmer, X.L., 2023. Mission-aware differences in cyberbiosecurity and biocybersecurity policies: Prevention, detection, and elimination. In *Cyberbiosecurity: A new field to deal with emerging threats* (pp. 37-69). Cham: Springer International Publishing.

Pulivarti, R., Pulivarti, R., Martin, N., Byers, F.R., Wagner, J., Zook, J., Maragh, S., McDaniel, J., Wilson, K., Wojtyniak, M. and Kreider, B., 2023. *Cybersecurity of Genomic Data*. US Department of Commerce, National Institute of Standards and Technology.

Sipior, J.C., Ward, B.ZT., Roselli, G.R., 2005. A United States Perspective on the Ethical and Legal Issues of Spyware.

Selyukh, A., 2016. The FBI has successfully unlocked the iPhone without Apple's help.

Srivastav, A.K., Das, P. and Srivastava, A.K., 2024. Data Management, Security, and Ethical Considerations. In *Biotech and IoT: An Introduction Using Cloud-Driven Labs* (pp. 133-149). Berkeley, CA: Apress.

State v. Diamond, 905 N.W.2d 870 (Minn. 2018).

Tang, O., 2016. Apple and the FBI: The Hazard of an International Precedent. *Brown Political Review*.

United States v. Brown, 125 F.4th 1186, 2025 U.S. App. LEXIS 1219 (D.C. Cir. 2025).

United States v. Gilkey, 2025 CCA LEXIS 86
United States v. Secord. 2025. *Scheduled hearings for January 2025*. Available at: https://www.armfor.uscourts.gov/newcaaf/calendar/202501.htm (Accessed: 18 February 2025).