**Analyzing Criminal and Civil Law: Encryption as Protected Free Speech**

Student's Name

Institutional Affiliation

Professor

Course

Date

**Analyzing Criminal and Civil Law: Encryption as Protected Free Speech**

The security and confidentiality of individuals' messages is one of the most essential communication factors today. As the world continues to advance technologically, cases of cyber-attacks have also been rising at an alarming rate calling for appropriate measures to protect digital content and communication (Kim et al., 2021). Among a wide range of communication protection tools that can be applied, encryption serves as the most effective and reliable practice. This practice involves converting information into a code, restricting the access of the data embedded without a proper decryption key. Although encryption is crucial in safeguarding digital privacy, security, and personal confidentiality, it has led to several concerns relating to criminal and civil law.

According to Koomen (2019), encryption has become a human rights issue that must be examined based on criminal and civil law. This issue can be supported by *the Apple Inc. v. FBI* (2016) case, which concerns the aftermath of the San Bernardino terrorist attack 2015. It was found that one of the shooters used an iPhone that had encrypted messages concerning the attack. This case ignited a great concern about balancing national security and personal privacy rights. Can encryption be protected as free speech? The key issue presented by encryption practices today is how it can be protected as free speech (Pang, 2023). Perhaps most people ask themselves whether their privacy and free speech depend on encryption. This study explains how encryption can be protected as free speech and highlights the significant differences between criminal and civil law in examining free speech issues.

**Examining Encryption as Free Speech**

While many people acknowledge the privacy role of adopting encryption in the communication context, there arises a question of whether this practice can be considered or equipped with free speech and if the practice can enjoy the same constitutional protection. According to the First Amendment of the U.S. Constitution, every individual is usually guaranteed the right to freedom of speech (Balkin, 2023; Balkin, 2015). This law could be used to mean encryption is a human right and must be protected under U.S. law. The protection covers both verbal and written communications. Using Lakier’s (2020) perspectives, encryption must be considered free speech as it conveys an individual's thoughts, ideas, and information in a coded language. In the same way, encoding a message in poetry or any art is protected under the First Amendment, as shown in Tushnet (2011); encryption must also be included. Since poetry and art are all forms of communication, just as encryption, there is no valid reason it could not be made as an extension of the same principle. This explanation explains how encryption can be protected as free speech. One of the significant ways encryption can be protected as free speech include when the message or communication shows expressive conduct,

According to the findings of the U.S. courts, an action can only be considered free speech and protected under the law if it is expressive conduct (Minow, 2021; Lind & Rankin, 2012). Balkin (2023) and Lakier (2020) also show that communication can only qualify for First Amendment free speech protection if they convey a particularized message or intent. Since encryption is only applied to protect digital communication from unauthorized users but conveys the message of an individual's desire for security, it qualifies protection as free speech. Conveying intended information to the target members shows that it is an act of expression. By framing this practice as an act of expression, there is no denial of encryptions qualification as protected free speech under the First Amendment. Therefore, encryption can be protected as free speech expressing a particular message—the concept of how encryption can be confirmed by determining clear distinctions between criminal vs. Civil Law.

**Analysis of the Free Speech Issue Using the Criminal vs. Civil Law Concepts**

The significant differences between civil and criminal laws serve as one of the best aspects to help shape people's understanding of how encryption can be protected as free speech. Cryer et al. (2019) highlight that criminal laws focus on offenses against society and use the state as the prosecuting party. The law uses the criminal justice system to maintain order, deter unlawful behavior or even punish the offenders. This concept explains how encryption can be protected as free speech by looking into clarity and presentation of danger. As evidenced in the case of *Schenck v. United States* (1919), speech can be restricted only if it presents a clear and immediate danger to public safety. Therefore, if a person employs encrypted communication to plan evil or endanger lives, the state might argue that encryption loses its protection as free speech protection. However, if the encrypted information does not present or intend any harm or danger, it remains protected under the U.S. Constitution. Therefore, encryption can be protected as free speech provided it does not have evidence of the intent of danger to the public.

Conversely, civil law concerns disputes revolving around private parties and awarding remedies to the injured party. In this context, free speech is linked to the issues of defamation, privacy, and intellectual property rights (Minow (2021). Encryption can be protected as free speech if it intends to protect individuals' trade secrets, confidential data, or privacy. Trade issues such as export controls on encryption technology can be protected as free speech under an individual's right to privacy and secured communication. As evidenced in cases such as Bernstein v. U.S. Department of State (1999), encryption software on trade matters must be protected. Although the Bernstein v. U.S. Department of State (1999) case did not explicitly determine encryption as free speech, it considered the issue as a code of expression that must be protected as free speech. Therefore, encryption can be protected as free speech if it intends to protect an individual's trade secrets and shows a conduct of expression. However, the question of whether the encryption, in this case, is seen as an expression of an individual's desire to protect their personal information or whether this application compromises the rights of other parties. This concern calls for a significant balance of the Act to help realize a consensus.

**Balancing Act**

As thisdebate on encryption as protection helps to shed light on the issue of communication under the law, it also raises concerns on how to strike a balance between protecting encryption as free speech and compromising critical concerns such as national security, public safety, and individual's rights (Minow (2021). Although encryption is considered one of the most crucial tools that can be adopted to enhance the security of people's communication, it can also be exploited by evil-minded individuals to hide and plan harm, as seen in Apple Inc. v. FBI (2016) case. For this reason, courts usually apply the principle of proportionality to balance the possible damage linked to the encrypted information against its value to the public (Pang, 2023). Several factors, such as the nature of encrypted content and its intent, can be used to weigh this practice's potential harm or benefits. The results from the examination of encryption may lead to informed decisions that can disqualify encryption protection. Therefore, encryption can only be protected as free speech based on the message's nature, intent, and potential impact. For instance, encryption cannot be protected as free speech if it presents evidence of imminent threats.

Following the complex nature of this debate, it becomes challenging to determine whether encryption can achieve complete protection as free speech or not, as its legality is based on different circumstances. In the Bernstein v. U.S. Department of Justice (1999) case, Daniel J. Bernstein challenged the U.S. export regulation that classified encryption software as munitions that required special licensing by stating that they violated his First Amendment rights. The Court ruled in Berstein’s favor claiming that the encryption source code was protected speech under the First Amendment. Comparing Apple Inc. v. FBI (2016) and Bernstein v. U.S. Department of Justice (1999) case, it can be argued that encryption of messages or communication should always be examined for its intent and potential impact on the public before its consideration as protected speech under the U.S. Constitution (Pang, 2023). Using the differences between criminal and civil law, examining how encryption can be protected as free speech becomes easy.

**Conclusion**

An explanation of how encryption can be protected as free speech presents a need to classify its practices based on the civil and criminal law concepts and the First Amendment Act. This debate also requires a comprehensive dissection of modern digital technology, constitutional rights, and legal compliances. As scholars research the possible implications of encryption for individual liberty and public safety, it is also essential to determine its application to criminal and civil law. There must be a significant balance that respects the principles of free expression and acknowledges the legitimate concerns compromising personal and public safety in this digital communication platform. Overall, encryption can be protected as free speech if it presents expressive conduct, intends to protect users' trade secrets, and does not show any imminent danger to public safety.

**References**

Balkin, J. M. (2015). Information fiduciaries and the first amendment. *UCDL Rev.*, p. *49*, 1183

Balkin, J. M. (2023). Free Speech Versus the First Amendment. *UCLA Law Review, Forthcoming*. Available at SSRN: <https://ssrn.com/abstract=4413721>

*Bernstein v. U.S. Dept. of Justice*, 176 F.3d 1132 (9th Cir. 1999).

Cryer, R., Robinson, D., & Vasiliev, S. (2019). *An introduction to international criminal law and procedure*. Cambridge University Press.

*In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

Kim, K., Alfouzan, F. A., & Kim, H. (2021). Cyber-attack scoring model based on the offensive cybersecurity framework. *Applied Sciences*, *11*(16), 7738. <https://doi.org/10.3390/app11167738>

Koomen, M. (2019). The encryption debate in the European Union. *Carnegie Endowment for International Peace*.

Lakier, G. (2020). The Non-First Amendment Law of Freedom of Speech. *Harv. L. Rev.*, pp. *134*, 2299. https://heinonline.org/hol-cgi-bin/get\_pdf.cgi?handle=hein.journals/hlr134&section=112

Lind, N. S., & Rankin, E. T. (2012). *First Amendment Rights: An Encyclopedia [2 volumes]: An Encyclopedia*. ABC-CLIO.

Minow, M. (2021). *Saving the news: Why the constitution calls for government action to preserve freedom of speech*. Oxford University Press.

Pang, J. (2023). Joint civil society briefing on encryption for Online Safety Bill for the House of Lords: Second Rea. https://policycommons.net/artifacts/4546512/joint-civil-society-briefing-on-encryption-for-online-safety-bill-for-the-house-of-lords/5370035/ on 11 Aug 2023. CID: 20.500.12592/gwbqwp.

*Schenck v. United States*, 249 U.S. 47, 39 S. Ct. 247, 63 L. Ed. 470 (1919).

Tushnet, M. (2011). Art and the First Amendment. *Colum. J.L. & Arts*, pp. *35*, 169.