**The Development and Amendments of the Electronic**

**Communications Privacy Act of 1986**

Corbin Osman

American Public University System

ITMG281 – Law, Privacy and Digital Data

Dr. Christopher Weppler

02/25/2024

**Introduction**

With technology growing at a rapid rate around the world, newer methods of digital communication are being created. In the last several decades advances in digital technology have allowed for faster and simpler communication between individuals and parties across a multitude of different devices. With the potential to communicate with someone from practically anywhere in the world in a matter of seconds, some are concerned about the type of content that is being shared and transmitted. Others are concerned about the privacy of their personal and professional communications, and who may potentially be listening in. Countries around the world strive to establish laws and regulations that govern who can perform surveillance on electronic communications and how they are permitted to do so, but are these laws effective in offering a balance between privacy and authorized surveillance of communications?

This study will review one such law, The Electronic Communications Privacy Act of 1986, and assess its effectiveness in governing and regulating the permitted surveillance of electronic communications. The background of the law will be explored, and analysis of both the adequacies and inadequacies of the law will be performed. Additionally, proposed changes to the law and existing attempts at reform to the act will be reviewed. The stance here taken is in favor of the law and supporting the protection and confidentiality of certain electronic communications between individuals and parties while not protecting other communications as determined by the laws and regulations surrounding the subject.

**Background and General Provisions**

The Electronic Communications Privacy Act (ECPA) was enacted by the United States Congress in 1986 to further protect the electronic communications of individuals and parties. The ECPA prohibits attempting to intercept or access communications while they are in transit or being stored on devices such as computers, with exceptions to this being when the practice is authorized or the methods of communications are not covered by the ECPA (Regan, 2014). While the law is fairly effective at governing this, it can be improved by allowing law enforcement and government agencies more access to electronic communications while still offering greater levels of privacy to national citizens.

The ECPA has three provisions which cover areas of electronic communications. The first, Title I, is the Wiretap Act which prohibits the interception of oral, wire, and electronic communications except for those authorized by law to do so. The second, Title II, is known as the Stored Communications Act (SCA), which protects files, information, and records of clients stored by service providers. The third, Title III, governs the permissible use of pen registers and trap-and-trace devices. Collectively these provisions make up the Electronic Communications Privacy Act, and while they cover many areas of electronic communications there are still improvements to consider that could increase the effectiveness of the law.

**Adequacies**

There are many things that the Electronic Communications Privacy Act does right to provide privacy and confidentiality to individuals and parties who communicate electronically. The 18 U.S. Code Chapter 119 thoroughly outlines when interception and confiscation of electronic communications is prohibited, when it can be authorized, who is responsible for authorizing such permissions, and the procedure to be followed when intercepting communications (Legal Information Institute). In order for a party to intercept or capture communications they must receive authorization to do so through a subpoena, search warrant, or special court order (Bureau of Justice Assistance). Receiving such authorization requires evidence of legally punishable offenses that have been committed, such as fraud, counterfeiting, money laundering, trafficking, and assault. These communications may provide evidence that aids in a criminal investigation. The ECPA exceeds at offering privacy of electronic communications while still giving those who need to intercept or access such communications the permission to do so.

The ECPA covers many types of electronic communications, but what is specifically covered under its purview? There is no clearly outlined list of electronic communications that are and are not covered by the ECPA, but general communications such as email communications, phone calls, text messages, video calls, and social networking are often protected. This manner of outlining what communications are protected is ideal as it protects these forms of communication even if the devices on which they are performed evolve and change over time. Some communications might still be accessible and monitorable by others even without obtaining special authorization, such as a business reviewing an employee’s work communications or a service provider monitoring a client’s online interactions. While these parties may have unrestricted access to the communications and their information, those with law enforcement and government agencies may still need special permissions to intercept or confiscate electronic communications.

Electronic communications that are stored also fall under the coverage of the ECPA. Title II, the Stored Communications Act, governs what stored communications and information are protected and what is required to access them. This information is permissibly accessible by the entity providing an electronic communications service, such as a service provider, or the user of the service to which the information pertains (Possino, 2023). Those who attempt to access electronic communications from storages or facilities without proper authorization can face punishments of both fines and imprisonment. This provision is helpful for those who want their stored electronic communications to be private and accessible to few.

**Inadequacies**

While the ECPA offers privacy and privileges to those it covers, there are notable inadequacies with the law. One such area is that the restrictions set are primarily focused on government access to information and greatly restrict their ability to listen in to and surveil electronic communications. With cybercrime and technology growing and advancing, electronic communications are optimal methods of communication for criminals. By restricting federal agencies and law enforcement’s surveillance and interception of communications, they may lose out on finding critical evidence to aid in combating crime. Reform has been made for the law through newer acts such as the Communications Assistance for Law Enforcement Act (CALEA), but the limits still restricting law enforcement and other agencies may be detrimental to investigations of criminal activity.

Another consideration is how newer practices of communication monitoring are being performed. In recent years there has been an increase in the number of individuals working from home, and employers have made efforts to monitor employee actions and communications from afar. The ECPA lacks coverage of employee confidentiality in this practice, and employees’ information and electronic communications may not be protected by federal regulations. Some companies already ensure that their employees know when they are covered, but without an official law in place that requires companies to inform employees that their communications and actions may be or are being monitored and recorded, many court cases involving electronic communications are being resolved on a case-by-case basis throughout the U.S. (Possino, 2023).

**Proposed Changes to the ECPA**

In order for the ECPA to be effective and fulfill its purpose, there needs to be a strong balance between protecting electronic communications and allowing its surveillance. To further aid government agencies and law enforcement in combatting criminal activity, it may be beneficial to increase the scope of acceptable reasons to obtain interception permissions. For example, instead of strictly requiring evidence for authorization to intercept electronic communications, a change could be made to give this authorization if there is reasonable suspicion of a crime that has been or may be committed. This would give law enforcement and government agencies more time to potentially stop crime before it occurs.

To further protect individuals whose personal communications may be vulnerable, an amendment could be made that requires service providers and companies to clearly inform their clients and employees that their communications may be monitored. Many companies monitor and record all of their employee’s communications and interactions, which would require them to inform their employees that all of their interactions performed on work devices, whether personal or professional, are monitored and may be stored. Many service providers and companies already practice this, but implementing it in the ECPA would further ensure that employee and client electronic communications are protected and kept private.

Another change that would aid in future proofing the act would be not covering communications right away as they evolve over time. With the evolution of technology and newer practices, individuals and parties with malicious intent may attempt to use these means of communication if they are automatically protected by an act such as the ECPA. Until they are understood and enough time has passed, the law should not protect these newer electronic communications. The period of time this will last depends on the judgment of those passing the law, but a reasonable time could be between two to five years. This would hopefully prevent those with malicious intentions from abusing newer technologies and means of communication.

**Conclusion**

In summary and in making a final analysis of the Electronic Communications Privacy Act, there are many positives in maintaining such a law for the future of the country. As technology continues to advance and newer methods of electronic communication are developed, it will be increasingly important to protect the privacy of clients, employees, and individuals. Having the rights to personal privacy can be reasonably assumed, but the law does not always offer it in every circumstance. The proposed changes offered should be implemented in some form to further protect electronic communications. Employers and service providers will be required to inform their employees and clients about the ways their information and communications will be monitored, and government agencies and law enforcement will still have access to the information and potential evidence they search for.

These proposed changes will most likely be successful by making amendments to the ECPA and passing a new act. This act should establish similar provisions as found in the ECPA and include the aforementioned changes. By future-proofing the act and the protection of electronic communications, the government is able to offer privacy to its citizens while still permitting appropriate interception and surveillance of communications.

References

*18 U.S. Code Chapter 119 - WIRE AND ELECTRONIC COMMUNICATIONS INTERCEPTION AND INTERCEPTION OF ORAL COMMUNICATIONS*. (n.d.). LII / Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/part-I/chapter-119

*Electronic Communications Privacy Act of 1986* (ECPA) (n.d.). Bureau of Justice Assistance. https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285

Possino, I. (2023). Employee Monitoring: As Technology Advances Yet the Electronic Communications Privacy Act Stays in the Past. *SMU Science and Technology Law Review, 26*(1), 135-. https://doi.org/10.25172/smustlr.26.1.9

Regan, L. (2014). Electronic Communications Surveillance. *Monthly Review (New York. 1949), 66*(3), 32–42. https://doi.org/10.14452/MR-066-03-2014-07\_2