CRJS475 Unit 4 Discussion Board - Intercepting Electronic Communications

Terms

- 18 U.S.C. § 2510 – Definitions: click here
- 18 U.S.C. Ch. 119 – Wire and Electronic Communications Interception and Interception of Oral Communications – click here
- 18 U.S.C. § 3121 – General Prohibition on Pen Register and Trap and Trace Device Use; exceptions – click here
- 18 U.S.C. Ch. 206 – Pen Registers and Trap and Trace Devices – click here
- Review of Fourth Amendment Digital Protections in Unit 3 – click here

History of Electronic Searches

In the 19th and 20th Centuries, it took special equipment for the government to capture incoming and outgoing phone numbers. For example:

- **Pen Register** (*for outgoing calls*): It is a surveillance device that captures outgoing phone numbers that were dialed.
- **Trap and Trace Device** (*for incoming calls*): It is a surveillance device that captures incoming phone numbers. (18 U.S.C. Ch. 206)

The above old terms are still listed in the United States Code (U.S.C.), but 21st Century technology far exceeds the original capabilities of pen registers and trap and trace devices. Today, digital technology has the ability to monitor the internet, email communications and ISP addresses (18 U.S.C. § 3127).

Legal Evolution of Electronic Searches & Seizures

- 1928 – The U.S. Supreme Court initially ruled that electronic eavesdropping is not a search or seizure under the Fourth Amendment, as long as the government intercepts conversations without actually entering a person's home (Olmstead v. U.S, 1928).
- 1967 – The Court later held that the Fourth Amendment "protects any place where an individual maintains a reasonable expectation of privacy" (Katz v. U.S, 1967).
- 2010 – An email subscriber has a reasonable expectation of privacy in the content and storage of emails that are sent through an internet service provider – and the government must have a search warrant before it can compel a commercial provider to turn over the contents of emails (United States v. Warshak, 2010).

It is a federal crime to wiretap or to capture the communications of others without court approval, unless one of the parties has given prior consent. It is also a federal crime to disclose any information that was acquired through illegal electronic eavesdropping (Stevens, 2012). The Electronic

Communications Privacy Act (ECPA) places legal restrictions on the government for wiretapping phone calls and for monitoring electronic data on a computer or on the internet (18 U.S.C. § 2510).

Warrantless Seizures of Evidence in Plain View

Officers may make several different kinds of warrantless seizures of evidence when it is in plain, depending on the circumstances. Three legal conditions must be satisfied for the government to make plain view seizures (Grantham, 2010, Horton v. California, 1990):

1. The evidence must be in plain view of the officer.
2. The officer must be lawfully in the place where he discovers the evidence.
3. The incriminating nature of the evidence must be obvious or immediately apparent.

Plain view seizures may happen in several different types of circumstances. For example:

- **Traffic stop:** If an officer makes a lawful traffic stop – and then while interviewing the driver, the officer sees pictures of child porn in plain view on the passenger seat – then the officer may make a warrantless seizure of it.
- **Public location:** If an officer smells marijuana and then sees a person smoking it in a public park (in the days when marijuana was illegal), then the officer may seize it without a warrant because it is in plain view – and the officer is lawfully allowed to be in the park.

A public location where plain view seizures may occur includes public sidewalks, public squares, public libraries and other public spaces where a person does not have a reasonable expectation of privacy. For example, while surfing the internet, you can expect privacy in your home, but you cannot necessarily expect privacy in a library while using a free computer with free internet access where the screen is viewable to anyone who walks by.

Warrantless Digital Exceptions under the Plain View Doctrine

In the ordinary course of business, an interception of private information must have occurred for a legitimate business purpose (Stevens, 2012). For example, if a librarian is responsible for monitoring computers that provide free internet access to the public, then the librarian's job task may include looking at the computer screens of unattended workstations, to ensure that they are ready for the next patron. The librarian has a legitimate business purpose and right to see texts and images that are still up on a computer screen at an unattended computer workstation that is designed for public use. Subsequently, if a librarian sees something that appears to be illegal, such as images of child porn, that were accidently left up on a screen in an open email account, then it is not an illegal search because it is in plain view – and the librarian discovered it during the ordinary course of business duties. The librarian may notify law enforcement, who will also have a warrantless access to any images or texts that remain up on the screen in plain view. However, if officers want to see other unseen emails that might have more illegal images or texts, then they must apply for a subpoena or a warrant to do so – because the rest of the electronic account is not in plain view (United States v. Warshak, 2010). They may use the

plain view images or texts as probable cause to apply for a warrant to search the entire email account – and to search other electronic devices of the holder of the account.

References

Grantham, P. M. (2010). *Plain view* [Legal Analysis]. National Center for Justice and the Rule of Law. https://olemiss.edu/depts/ncjrl/pdf/Law%20Enforcement%20Materials/Plain%20View%20Doctrine.pdf

Stevens, G. (2012). *Privacy: An overview of the Electronic Communications Privacy Act* [Legal Analysis]. U.S. Congressional Research Service. https://fas.org/sgp/crs/misc/R41733.pdf