Southern New Hampshire University

CYB 320 Module Two Activity Worksheet
Privacy and Communication Laws

This worksheet has two parts that you must complete. For **Part I**, complete the table by filling in the two blank columns for each law. For **Part II**, select either the *United States v. Simons* case study or the *Steve Jackson Games, Inc. v. United States Secret Service* case study from the Module Two Reading and Resources section, then respond to the questions in the table.

Part I: Laws

Law	Briefly describe the law (3–4 sentences)	Describe the law's effect on digital investigations (3–4 sentences)
First Amendment	The First Amendment to the U.S. Constitution protects several fundamental freedoms in the United States, including freedom of religion, freedom of speech, freedom of the press, and the right to assemble peacefully. It prevents Congress from making laws that regulate the establishment of religion or prohibit the free exercise of religion, infringe on the freedom of speech and the freedom of the press, or limit the right to assemble or to petition the government for a redress of grievances.	The First Amendment can impact digital investigations by safeguarding the right to free speech, including various digital expression forms. This can complicate online investigations involving hate speech or radicalization, as investigators must distinguish between illegal activities and protected speech. It also challenges enforcing laws on digital platforms without infringing on freedom of speech and the press.
Fourth Amendment	The U.S. Constitution's Fourth Amendment protects against arbitrary searches and seizures. requiring any search or seizure to be carried out under a warrant issued upon probable cause. This amendment guarantees the privacy and security of persons and property from arbitrary interference by the government.	The Fourth Amendment requires law enforcement to obtain a warrant before accessing private digital records in digital investigations. Such as emails, digital documents, and online personal data. Safeguarding individuals' privacy can also delay or limit investigators' access to potentially crucial digital evidence unless there is a clear justification for a search.

Law	Briefly describe the law (3–4 sentences)	Describe the law's effect on digital investigations (3–4 sentences)
Electronic Communications Privacy Act	The Electronic Communications Privacy Act of 1986 is a U.S. federal law that extends government restrictions on wiretaps from telephone calls to include electronic data transmissions by computer, adding protections against unauthorized government access to private electronic communications.	The ECPA protects against the unlawful interception and disclosure of electronic communications. However, it also provides provisions under which law enforcement can obtain access to electronic communications. Transactional records are made through specific procedures, such as warrants or subpoenas, which affect the scope and approach of digital investigations.
Privacy Act of 1974	The Privacy Act of 1974 regulates federal agencies' collection, maintenance, use, and dissemination of personal information. It establishes a code of fair information practices that demand transparency and accountability in handling personal records. The act also grants individuals the right to access and amend their records.	This act imposes strict limitations on how personal data obtained during digital investigations can be shared and used, often requiring individual consent or legal necessity. Compliance with this act is crucial to avoid legal challenges and potential civil rights violations. It impacts how federal agencies handle data, ensuring that investigations respect the privacy and rights of individuals.
USA Patriot Act	The USA Patriot Act strengthened domestic security and widened law enforcement agencies' powers to prevent and respond to terrorism. It enables more accessible access to communications and other records through less restrictive standards than traditional criminal investigations. The act includes measures that expand surveillance capabilities, including roving wiretaps and business record searches.	The Patriot Act allows investigators to use tools such as delayed notification search warrants, enabling access to stored electronic information without immediate disclosure. Doing so facilitates quicker responses in national security cases and raises concerns about privacy and civil liberties. The act simplifies obtaining communication intercepts and transactional records, accelerating the pace of digital investigations.

Law	Briefly describe the law (3–4 sentences)	Describe the law's effect on digital investigations (3–4 sentences)
Regulation (EU, Euratom) No 883/2013 of the European Parliament	This EU regulation empowers the European Anti-Fraud Office (OLAF) to conduct investigations related to fraud, corruption, and activities affecting the EU's financial interests. It outlines procedural rules for cooperation among EU members and third countries. The regulation aims to enhance transparency and efficiency in combating fraud and corruption.	It facilitates cross-border digital investigations within the EU by standardizing investigative procedures and promoting cooperation among member states. The regulation mandates that digital investigations uphold fundamental rights and adhere to legal processes. It enhances OLAF's capabilities to access necessary data while ensuring that the investigations adhere to strict data protection and procedural norms.

Part II: Case Study

Explain which laws apply to the case study.	The Fourth Amendment and the Electronic Communications Privacy Act (ECPA) apply to the case study involving Steve Jackson Games and the US Secret Service. The Fourth Amendment protects people from unreasonable searches of their property by the government, which means the government needs a valid reason and usually a warrant to search someone's property. The Fourth Amendment would determine if the Secret Service had the right to take computers and other electronic items from Steve Jackson Games. The ECPA deals with the privacy of electronic communications, such as emails, and sets rules on how others, including the government, can access and handle these. This law was critical in deciding whether the actions of the Secret Service in handling the company's emails and other electronic communications were lawful.
How does knowledge of these laws affect your understanding of organizational policy creation when it comes to policies such as acceptable use, email, data storage, backup, data retention, or bring-your-own-device (BYOD)?	Knowing about the Fourth Amendment and the ECPA helps make company policies on properly using company systems, handling emails, storing essential data, and managing devices that employees bring to work, like smartphones and laptops. For example, email use policies must protect the privacy of employees' emails by the ECPA. Data storage and backup policies should secure company data and ensure only authorized people can access it, keeping in line with the protection against unreasonable searches stated in the Fourth Amendment. Policies should specify how long it takes to retain data or records to comply with the ECPA. Finally, BYOD policies should ensure that personal devices do not jeopardize company data and are also by these laws. Creating these policies while understanding these laws helps the company protect itself from legal issues and ensures everyone's privacy and rights are respected.