

### **Laws and Technology**

1. Provide a brief summary regarding information privacy law or data protection laws in the United States and in the European Union. (3 to 5 sentences)

The US does not have a dedicated federal law to protect privacy and data. Instead, the Federal Trade Commission Act and many other laws enables the FTC to protect consumers from companies that do not follow their privacy statements. [2] In the European Union, there is a General Data Protection Regulation that gives rules that companies must follow when handling users data. [1]

2. Explain what the 1st and 4th Amendments to the US Constitution have to do with your expectation of privacy in the United States. (5 to 8 sentences)

The 1st Amendment relates to privacy because it protects the right of free speech, and stops the government from making laws that violate the freedoms listed in the Amendment. Amendment 4 states that the government cannot take things that belong to a citizen without just cause. If the data stored on our computers is considered out property, then the government should not be allowed to access our data without just cause. This can be expanded upon with the idea that things that we say are considered our property as well. Harper states that "Communications belong to to parties between whom they pass." [3] Meaning the government cannot wiretap phone lines and listen on communication.

3. Explain how the Supreme Court ruling in Carpenter v. United States effects digital privacy in the US. (5 to 8 sentences)

The ruling for Carpenter v United States was that the government needs a warrant to access cell site location information from mobile phones. They leaned this way because cell phones are becoming more of a necessity than a luxury and people are not voluntarily giving out their location, it is needed for the phone to work. Previously the Supreme court has ruled that law enforcement does not need a warrant to access information given to a third party. According to the Supreme Court CSLI data is a different category of information that would give law enforcement accurate movements of a majority of Americans' movements. [4] This would essentially put a GPS tracker on everyone, which was considered a violation of 4th Amendment rights previously. If the location data that is collected by third party companies is protected under the 4th Amendment then other data also collected by third parties could be considered protected as well, like browsing information.

## References

- [1] Data protection in the eu. *European Commission* 19/3/2020, [https://ec.europa.eu/info/law/law-topic/data-protection-eu\\_en](https://ec.europa.eu/info/law/law-topic/data-protection-eu_en).
- [2] Data protection law. *HG.org*, (2020) <https://hg.org/data-protection.html>.
- [3] Jim Harper. Administering the fourth amendment in the digital age. *A Twenty-First Century Framework for Digital Privacy*, National Constitution Center, <https://constitutioncenter.org/digital-privacy/The-Fourth-Amendment-in-the-Digital-Age>.
- [4] Justin Sullivan. The supreme court just greatly strengthened digital privacy. *Wired*, 22/6/2018, <https://wired.com/story/carpenter-v-united-states-supreme-court-digital-privacy/>.