Cybersecurity Ethical Dilemmas:

Aviation Cybersecurity Vulnerability Disclosure

You have discovered what you suspect is a vulnerability in aviation control software for a major aircraft manufacturer. You suspect a passenger using the in-flight wifi could access aircraft controls and potentially cause catastrophic damage. You reported the issue to the manufacturer and received a response saying no such vulnerability exists.. You escalated the report the FAA and received a letter informing you that it is illegal to provide information a terrorist could use to damage the transportation infrastructure. A friend has put you in contact with a national reporter who could help disclose the issue. Should you demonstrate the vulnerability is real yourself by testing it on a flight, continue to pursue disclose paths, or reveal the potential flaw to the reporter?

Security research demonstrates hacking an airplane:
https://www.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html
https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

Legal challenges around disclosure of vulnerabilities
https://www.zdnet.com/article/chilling-effect-lawsuits-threaten-security-research-need-it-most/

Home Camera System Reverse Engineering

You have a security camera that is used to monitor a person in your friend's home that has special needs. You believe you can link the camera to a critical piece of equipment that would help improve the quality of life for the person. In order to implement your change, you need to modify the software on the camera. Do to a flaw in their security system, you can exploit a vulnerability in their system and modify the code. You contacted the company to ask for a modification but the company simply replied that the ULA prohibits any reverse engineering. By exploiting the vulnerability, modifying the code, and posting it online, you can benefit a large number of people in similar situations.

Reverse Engineering Laws:
https://www.internetlawyer-blog.com/reverse-engineering-fair-use-rights/
Reverse Engineering IoT Devices
https://dzone.com/articles/reverse-engineering-of-a-not-so-secure-iot-device

Social Media Privacy

A student in your cybersecurity course showed you how she could hack into a popular social media platform. To prove it works, she sent you a link that provided access to her friend's account. As part of this you inadvertently saw a small part of conversation that raised concerns about the friend's safety (e.g. you saw only the text title or first few lines of a private message). Should you further explore the student's social media to make sure she is safe or not access any of her private data?