Discussion Cyber Law:

Question

Part a) Getting to Know You Again and Part b) Former FBI Director Jim Comey

a) If you had to delete all the apps on your phone except for 3, which apps would you keep and why?

b) Review Lawfare Podcast Episode # 96 below discussion former FBI Director Jim Comey's comments on "Going Dark" and questions from the audience.

https://www.lawfareblog.com/lawfare-podcast-episode-96-james-comey-going-dark

Then use what you have learned to:

1. Identify in your initial post a point(s) or general assertion(s) by former FBI Director Comey that surprised you, challenged you or led you to agree or disagree with him, and explain why. In so doing use this podcast as a platform to address the legal, policy, and technical challenges posed by encryption. In your posts, you may also consider what the rest of the world is doing in responding to the challenges of encryption.

2. Provide one informed, thoughtful response to a classmate's initial post.

Response

Part A:

If I could only keep 3 apps, I would choose iMessages for my constant communications with friends, family, and boyfriend, Email since it is essential to my schoolwork and personal accounts and find my iPhone...My dog chases butterflies and often gets lost.

Part B:

Jim Comey discussed the growing challenges encryption creates for law enforcement. He explained that as encrypted devices and networks become the norm, investigators are finding it increasingly difficult to access digital evidence, something that affects both criminal prosecutions and counterterrorism efforts. While encryption plays a crucial role in protecting personal privacy, he pointed out that law enforcement and legal systems have not kept up with rapid technological changes.

What stood out to me most was how something meant to safeguard privacy can also hinder investigations. Encryption protects innocent users from unnecessary intrusion, but it also makes it harder to pursue real criminals. It is a tough balance between protecting citizens' rights and maintaining public safety, and I think both sides need to work together to find a fair middle ground.

Discussion Cyber Law:

Question

Part a) Getting to Know You More and Part b) WikiLeaks

a) What is the figurative "hill you would die on" - meaning what belief or issue would you defend no matter the cost?

b) In this course we consider the value of both gathering and protecting information, as well as sharing it. In the digital world, relative ease with which we may access information and vast troves of data raise significant questions that impact the individual and society, and even our national security. Freedom, trustworthiness of sources and methods, national security concerns, and privacy interests also come into play. With these and other considerations in mind, watch the video below (yes, it is dated, but the issues survive) and answer the following related questions

in an informed manner. It will help to review Module 4 and other credible and relevant sources. Cite any outside sources.

Question 1: What are some important reasons for a) support or b) oppose Julian Assange's position in defending the work and mission of Wikileaks?

Question 2: In your opinion, is Assange a hero, a criminal or both, or neither? Why?

Your contributions are worth up to 8 points. As always, earlier initial contributions are encouraged. Do not forget to provide one thoughtful, informed response to another classmate's post for full credit.

https://www.youtube.com/watch?v=HNOnvp5t7Do

Answer

Part A: Getting to know you better.

What is the figurative "hill you would die on" meaning what belief or issue would you defend no matter the cost?

The figurative hill I would die on is that Chihuahua's are scarier/more aggressive than labeled "dangerous" dogs (Pitbulls, Cane Corso's, Malinois, and Staffordshire's).

Part B:

Question 1:

What are some important reasons for a) support or b) oppose Julian Assange's position in defending the work and mission of Wikileaks?

There are more than a few arguments to support or oppose Julian's work, as he has worked in the figurative moral grey areas.

Support:

Transparency and accountability:

Supporters argue that WikiLeaks promotes transparency by publishing classified documents, exposing government and corporate wrongdoing, and holding powerful entities accountable for their actions. They believe in the public's right to access information that impacts their lives and the need for government transparency.

Freedom of the press: Assange's defenders argue that his prosecution sets a dangerous precedent for press freedom. They believe that WikiLeaks is a journalistic organization that engages in investigative reporting, and prosecuting Assange could have chilling effects on journalists and their ability to report on sensitive issues.

Oppose:

National security concerns:

Opponents argue that WikiLeaks' indiscriminate release of classified information may endanger national security by exposing sensitive intelligence, military strategies, or confidential diplomatic communications. They believe that some information should remain classified to protect the interests and safety of a nation.

Personal behavior and allegations: Assange has faced criticism for his personal behavior and allegations of sexual assault. Some argue that his personal conduct undermines his credibility, and casts doubt on his motivations and ethics.

Question 2:

In your opinion, is Assange a hero, a criminal or both, or neither? Why?

Personally, Julian is both. Throughout his work and publicity, he has given so many reasons why he is not just one or the other. Based on the video, I would say that he is more of a hero;

however, after further research into WikiLeaks, it has changed my opinion that he cannot be labeled as one or the other. To me, he rides along the grey area where his actions feel wrong and right at the same time.

Legally speaking, he broke the law. He was legally declared a criminal for his actions. However, there are times when one does not label something wrong if it is for the better good of the people.

References:

BBC News. (2024, February 13). US Senate passes foreign aid bill despite opposition from Trump. BBC News. https://www.bbc.com/news/world-us-canada-68282613Links to an external site.

TED. (2010, July 19). Julian Assange: Why does the world needs WikiLeaks.https://www.youtube.com/watch?v=HNOnvp5t7Do

Discussion Cyber Law:

Question

Review the article below by Orin Kerr, an important, scholarly voice in so many Fourth Amendment debates, and preferably other sources to help form your opinions about the legal, policy and technical challenges posed by encryption.

https://reason.com/volokh/2016/10/14/the-law-of-encryption-workarou/

The impact of encryption on legitimate law enforcement and national security investigations is no small thing, and it will not go away any time soon. No matter where you stand, there are consequences to the choices we, as a nation and people, make. It is another "wicked" problem -

not a simple one - and we need to be willing to think through our choices, in good faith, and rely on the best available facts and what we believe will best promote security, freedom, and privacy. Be open-minded. If you think there are easy answers to the challenges of encryption in a free yet secure society, think twice.

Then use what you have learned to:

1. Identify in your initial post a point(s) or general assertion(s) by Orin Kerr that surprised you, challenged you or led you to agree or disagree with him, and explain why. In so doing use this article (and others' articles) as a platform to address the legal, policy, and technical challenges posed by encryption. In your posts, you may also consider what the rest of the world is doing in responding to the challenges of encryption.

2. Provide one informed, thoughtful response to a classmate's initial post.

Answer

What stood out most to me in Orin Kerr's "The Law of Encryption Workarounds" is how he refrains from the encryption debate. Instead of asking whether the government should have a universal "backdoor," he argues for a legal framework to evaluate specific investigative workarounds, such as lawful hacking, compelling suspects to reveal passwords, or accessing data from unlocked devices. His approach recognizes that strong encryption is here to stay, and that courts need clear standards to guide law enforcement when they encounter this barrier.

Like the Former FBI Director mentioned in the last discussion, Kerr acknowledges that encryption is a growing obstacle for investigators. Still, he argues this issue is not simply "backdoor or no backdoor." These workarounds are complex, messy, and time-consuming, but they are sometimes the only way to obtain crucial evidence. However, when used without proper

oversight, they risk crossing constitutional lines, as seen in cases like Playpen, which questioned the legality of government hacking warrants.

Each workaround also raises different legal concerns: compelling passwords implies the Fifth Amendment; Apple v. FBI highlights the limits of government power over tech companies, and government hacking brings up Fourth Amendment issues. Kerr's case-by-case approach makes sense; it balances security needs with constitutional rights.

Australia's Telecommunications and Other Legislation Amendment (TOLA) show what can happen when governments mandate decryption assistance. While it helps law enforcement, it also creates serious security and trust risks. The better path is targeted, court-supervised workarounds that let investigators gather evidence without weakening global cybersecurity or public confidence.

References:

"Revisiting Australia's Encryption Landscape | Strategic Technologies Blog | CSIS." Csis.org, 2024, www.csis.org/blogs/strategic-technologies-blog/revisiting-australias-encryption-landscapeLinks to an external site..

Kerr, Orin. "The Law of Encryption Workarounds." Reason.com, 14 Oct. 2016, reason.com/Volokh/2016/10/14/the-law-of-encryption-workarou/.