

**Internet Law
Spring 2018
Midterm Examination**

This examination consists of **one question** and **three pages**, including this cover page. Your answer has a limit of 1,500 words, which will be strictly enforced. Submit your answer by email to Christina Ko by the deadline of **5:00 PM on March 19**. Please make sure that your answer contains **no identifying information**.

This is an **open-book** examination. You should not need to consult anything beyond the coursepack and your notes, but you can if you wish. You are free to discuss the general legal principles we covered this semester with anyone, including each other. But **you may not discuss the examination questions** with anyone else until after the examination period. Your work on this examination is subject to the Cornell Code of Academic Integrity, the Law School Code of Academic Integrity, and the Campus Code of Conduct.

The question puts you in a role, but the genre for your answer should be "**law school examination**." Use **simple citations** (e.g. "*see Zeran*") where appropriate. I include **spelling, grammar, clarity, and organization** in my grading. I appreciate the use of headings to organize your answer, but they're not required. If you find the question **ambiguous** or need to **assume additional facts**, state your assumptions explain how they affect your answer. No reasonable resolution of an ambiguity will be penalized.

To help ensure uniformity in my grading, please use the following **formatting**: 13-point Palatino, 1-inch margins, double-spaced, bold for any major headings and italics for any minor headings.

The problem is set in the fictional American state of Roosevelt. Assume for purposes of the examination that present-day law has been fully in effect at all relevant times.

Unless otherwise noted, all names are fictitious. Please disregard any resemblance to actual persons, places, or institutions—living, dead, or nonexistent.

Flash Boys

You have been approached by the public defender appointed to represent P.J. Fishburne, a Ugandan national who was recently arrested in the United States and charged with aggravated assault. The case raises Internet issues beyond your colleague's usual expertise, and she would like your strategic advice.

The backstory is that Fishburne was a regular user (with the username "ScumbagSteve") of a website called LOLCOW, where he was an active participant on the Danker Than Thou discussion board. He got into an extended argument over a period of several weeks with another user, Alex Nyan, who resides in the United States. The two of them traded insults on the Danker Than Thou board and repeatedly egged each other on to more brazen attempts to annoy the other. Previously, Fishburne had temporarily locked Nyan out of her LOLCOW account by triggering the password-reset feature, and Nyan had responded by flooding Fishburne's LOLCOW account with tens of thousands of spammed messages. According to the indictment, in mid-2017, Fishburne posted several images featuring rapid strobe flashes in an attempt to induce a seizure in Nyan, who is epileptic.

The FBI opened a file on the case. The investigation began by serving an order under § 2703(d) of the Stored Communications Act to LOLCOW, which provided the IP address from which ScumbagSteve had connected. The FBI, with the assistance of Ugandan authorities in a procedure that complied with Ugandan law, was able to use the IP address to request appropriate subscriber records from Uganda Telecom, which turned over Fishburne's name.

The FBI took no further action at the time, but Fishburne's name triggered an alert in their systems when he applied for a six-month tourist visa to the United States. The FBI applied for and obtained warrants for his arrest and to search "any electronic devices in his possession," then arrested him when he arrived in the United States. He was carrying an Android phone, and while it was secured with a passcode lock, the FBI forensic technician observed a pattern of fingerprint smudges on the glass that she correctly guessed corresponded to the numeric passcode. Once she had unlocked the phone, the technician tapped on the "Archive" folder in

his email app, which caused the app to connect Gmail and download the emails to the phone. Those included emails in which he allegedly bragged to others about successfully inducing seizures with flashing images.

Your colleague is considering raising the following arguments as part of her defense of Fishburne:

1. His actions took place in cyberspace rather than the United States, so his actions should be judged by the norms of cyberspace.
2. A 2016 decision by the Supreme Court of Uganda held that similar conduct is not a crime under Ugandan law, so he should be not be prosecuted in the United States for actions that were legal where he lives and acted.
3. His actions are protected by the First Amendment.
4. The § 2703(d) order to LOLCOW violated the Stored Communications Act.
5. The search of his phone violated the Fourth Amendment.
6. The search of his phone violated the Fifth Amendment.
7. The search of his phone violated the Wiretap Act.
8. The search of his phone violated the Stored Communications Act.

Write a short memorandum to your colleague assessing the strength of each of these arguments. What is Fishburne's best legal strategy, and do you have any other advice?