Internet Law
Spring 2018
Midterm Sample Answer

To: Waldorf T. Flywheel

From: Pseuedonymous Bosch

Re: *United States v. Fishburne*

Your best arguments have to do with the way the FBI obtained the contents of Fishburne's emails from Gmail, which likely violated the Fourth Amendment and Stored Communications Act. The rest of the arguments you have suggested to me are weak.

In the following, I will assume for the sake of argument that the facts of the case are as stated by the government in the indictment.

1. Fishburne's Actions Did Not Take Place in "Cyberspace"

There is no such thing as "cyberspace." He is a real person who caused harm to another real person. Yes, he used computers and the Internet, but governments have never treated online conduct as occurring somewhere they can't

regulate. When their citizens are harmed by online activity, they are willing to apply their laws against people who would have been liable if they had done the same thing in the physical world. *Target*. This is not a good case for applying Orin Kerr's internal perspective, because the flashing images were intended to harm Nyan in person, rather than just her online presence on LOLCOW.

2. Ugandan Law Is Not Determinative

If Fishburne had targeted and harmed another Ugandan resident, it would be inappropriate to apply United States criminal law against Fishburne. But since he targeted and harmed a resident of the United States, the United States has enough of an interest in the case that its courts will allow the prosecution to proceed. This case is like *Gutnick*, in which the Australian courts allowed a defamation suit against an American publisher to proceed, because the defamation harmed an Australian in Australia. The fact that United States free speech law would have protected the publisher there was not a defense; the Australian court required the publisher to defend itself in Australia under Australian law.

Fishburne might be able to argue that he did not know he was targeting an American and therefore could not expect American law to apply to him. But I

expect that the government will respond, and the court will agree, that Fishburne voluntarily took the risk that he was targeting an American rather than a Ugandan.

3. The First Amendment Will Not Protect Fishburne

It is true that the flashing images were communicated online rather than in the physical world. It is also true that the courts have sometimes treated computer code as "speech," as in *Bernstein*. And it is true that the images may have had other meaningful elements besides just flashing. But none of this is likely to convince a court to treat the images as protected "speech" rather than unprotected "conduct."

Fishburne is not being prosecuted here because of a "particularized message" that was a "understood by those who viewed it," *Texas v. Johnson*. He is being prosecuted for causing Nyan physical injury by activating her brain at a neural level, rather than by showing her an understandable message. That makes this case like *Petrovic*: any "speech" in the images was incidental to the harm they directly inflicted on her.

All that said, the image was probably not a "true threat." It was not intended to cause Nyan to fear future harm: it was intended to inflict harm directly. It was not speech at all, rather than being threatening speech.

4. The § 2703(d) Order Was Allowable Under the Stored Communications Act

First, the § 2703(d) order was legitimately obtained. The government had "specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought, are relevant and material to an ongoing criminal investigation." The investigation was into the strobe-image attack on Nyan, and the identity of the person who posted them is clearly relevant in a potential prosecution of that person.

Second, the government obtained records covered by a (d) order. Under § 2703(c)(1)(B) and (2)(E) a (d) order can be used to obtain a user's "instrument number or other subscriber number or identity, including any temporarily assigned network address," which includes ScumbagSteve's IP address, the only thing divulged by LOLCOW.

And third, although you did not specifically ask, this application of the SCA is not likely to be problematic under the Fourth Amendment. *Warshak* ap-

plied to the *contents* of electronic communications, but this case involves only metadata, which the courts so far have not held to be covered by the Fourth Amendment.

5. The Search of Fishburne's Phone and Gmail Account Raises Serious Fourth Amendment Concerns

The government had probable cause to obtain a warrant to search Fishburne's phone. It had evidence of a crime (deliberately exposing Nyan to seizure-inducing images) and evidence that Fishburne was the most likely suspect (the combination of LOLCOW's and Uganda Telecom's records). The warrant also "particularly describ[ed] the place to be searched, and the persons or things to be seized." That is sufficient.

The search of the *phone* complied with this warrant. But when the FBI technician downloaded emails from Fishburne's Gmail account, she arguably exceeded the scope of the warrant. The warrant did not mention the Gmail account or Google's servers; it provided no authorization to search them. It's not enough that they were accessed through the phone, the search of which was authorized:

otherwise, the FBI could use a search warrant for a computer to use that computer to hack into any other computer in the world.

Instead, the government will need to argue that some other Fourth Amendment exception applies. One such argument might be plain view: that Fishburne's Gmail account was in "plain view" from the phone the FBI had a right to search. But in *Riley*, the government conceded that the "search incident to arrest exception may not be stretched to cover a search of files accessed remotely," and a similar principle would seem to apply to a search in excess of a warrant. Indeed, the fact that the government easily could get a search warrant for Fishburne's emails from Gmail strongly suggests it should not be able to circumvent the warrant requirement by using his phone. *Riley* itself rejects the use of search incident to arrest even for a search of the phone (let alone connected cloud accounts), and it is hard to argue that Fishburne consented to any of these searches. So the Gmail portion search looks like a Fourth Amendment violation.

6. The Search of Fishburne's Phone Did Not Violate the Fifth Amendment

The Fifth Amendment protects only against communications that are compelled, incriminating, and testimonial. In this case, there was no compelled

communication because the FBI technician only observed the consequences of Fishburne's past conduct: the finger smudges. At no point was he required to tell the government anything. Indeed, it's arguable that there was not even a "communication" because the smudges were just the physical record of his unlocking the phone rather than an attempt on his part to convey a message to anyone.

7. The Search of Fishburne's Phone Did Not Violate the Wiretap Act

The Wiretap Act applies only to *contemporaneous* interceptions of communications. *O'Brien v. O'Brien*. But here the FBI acquired Fishburne's emails well after they were sent and received, from the archive on his Gmail.

8. The Search of Fishburne's Phone May Have Violated the SCA

When the FBI technician opened the email app on Fishburne's phone and tapped on the "Archive" folder, she caused the app to "access" Gmail's servers by downloading his stored email. 18 U.S.C. § 2701(a)(1). Since those servers are a "facility through which an electronic communication service is provided" and

the emails are "electronic communications," *id.*, this might be a violation of the SCA.[1]

The government may respond that the technician did not "intentionally" access the server if she did not realize she would be triggering a download. But this depends on her state of mind, and if you can show that she expected something like this might happen, then you will be able to establish that this was an intentional access. The government might also argue that this access was "authorized" by Fishburne, but given that the phone was seized from him and unlocked without his permission, I think this argument is untenable.

[1] [JG: The Stored Communications Act doesn't have a statutory suppression remedy, so this claim is not much use in defending against a prosecution. But we didn't discuss this in class, so I didn't expect you to know this.]