H. Dean Steward SBN 85317
107 Avenida Miramar, Ste. C
San Clemente, CA 92672
949-481-4900
Fax: (949) 496-6753
deansteward@fea.net

Orin S. Kerr
Dist. of Columbia BN 980287
2000 H. Street NW
Washington, DC 20052
202-994-4775
Fax 202-994-5654
okerr@gwu.edu

Attorneys for Defendant
Lori Drew

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

| | |
|---|---|
| UNITED STATES,<br><br>Plaintiff,<br><br>vs.<br><br>LORI DREW<br><br>Defendant. | Case No. CR-08-00582-GW<br><br>REPLY TO GOVERNMENT RESPONSE TO DEFENSE RULE 29 |

COMES NOW defendant Lori Drew, together with counsel, and responds to the government's reply to the defense Rule 29 motion.

Dated: 1-2-09 s./ H. Dean Steward

H. Dean Steward
Orin Kerr
Counsel for Defendant Drew

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. Introduction

Although counsel earlier had assumed that a reply to the Government's Response on the Rule 29 motion would not assist the Court, upon reading it counsel has come to believe that a reply would greatly help the Court in understanding the issues raised in this case. In particular, a reply can help the Court understand why the civil authorities the Government relies on cannot be adopted in a criminal setting, and why the one criminal case the government cites provides no support for its position. With that end in mind, the undersigned counsel respectfully submits this reply.

II. Civil Tort Cases Adopting a Contractual View of 18 U.S.C. § 1030 Cannot Be Applied To A Criminal Prosecution.

The government's response rests almost entirely on civil tort cases. In the context of civil business-to-business litigation, brought under 18 U.S.C. § 1030(g), a few courts have indeed adopted an extremely broad view of 18 U.S.C. § 1030. Those courts have construed § 1030 as a commercial statute that provides federal court jurisdiction for business contract disputes. Under these cases, breach of a contract renders access unauthorized. Almost all of the cases that the government cites as authority arose in that setting. See Govt's Response to Defendant's Supplement to Rule 29 Motion at 5-10.

The Government cannot properly rely on those broad civil cases in this criminal prosecution. Although the Government does not

acknowledge it, the lower courts are sharply divided even in the civil setting on whether those broad civil interpretations of § 1030 are correct. Two competing lines of cases have emerged. One line of cases has adopted the broad contractual reading that the Government relies on here. Another line of cases has recognized that 18 U.S.C. § 1030 is also a criminal statute, and it has rejected that expansive reading as overly broad for a statute with criminal remedies. See, e.g., Condux Intern., Inc. v. Haugum, 2008 WL 5244818 (D. Minn. Dec. 15, 2008) (discussing the two lines of cases).

What makes the government's prosecution of Lori Drew so novel is that it takes the line of broad civil precedents and tries to carry them over to the criminal setting for the very first time. As a result, the government's prosecution is based almost entirely on broad civil cases that have never been cited before in a criminal case. The government makes no argument for why the broad civil § 1030 cases arising in business-to-business litigation should also apply in a criminal prosecution, or why the narrower cases interpreting § 1030 are incorrect. Instead, the Government simply assumes that the broad civil cases should also apply, jot-for-jot, when a defendant's liberty is at stake.

This assumption is false. Civil precedents can only make the jump to the criminal side of the docket if the resulting interpretation would satisfy the three related "fair warning" canons for interpreting criminal statutes: vagueness, the rule of lenity, and overbreadth. See United States v. Lainier, 520 U.S. 259, 266-67 (1997). These three doctrines ensure that no criminal

case can proceed unless it is "reasonably clear at the relevant time that the defendant's conduct was criminal." Id. Civil interpretations of statutes that violate these doctrines cannot make the jump from the civil realm to the criminal realm. See, e.g., Screws v. United States, 325 U.S. 91 (1945) (adopting a narrow reading of criminal civil rights law to save its constitutionality when applied in a criminal setting).

As several courts have already noted, in the course of rejecting the very same civil cases that the government cites, the broad contractual interpretation of § 1030 cannot survive the "fair warning" canons that apply to the construction of criminal statutes. Only a narrow construction of 18 U.S.C. § 1030 can be lawfully applied in a criminal setting. See, e.g., Condux Intern., Inc. v. Haugum, 2008 WL 5244818 (D. Minn. Dec. 15, 2008) ("The CFAA has both civil and criminal applications and given the two proposed readings of the statute . . . the rule of lenity requires the Court to favor the narrower interpretation."); Black & Decker (US), Inc. v. Smith, 568 F.Supp.2d 929, 933 (W.D. Tenn. 2008) (relying on the rule of lenity to reject the broad line of § 1030 civil cases); Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7(M.D. Fla. Aug. 1, 2006) ("To the extent 'without authorization' or 'exceeds authorized access' can be considered ambiguous terms, the rule of lenity, a rule of statutory construction for criminal statutes, requires a restrained, narrow interpretation.").

Under the rule of lenity, reliance on the broad civil cases the Government cites must be rejected. No criminal case has ever

been brought that relied on the civil authorities the Government cites here. Given the two lines of cases, the court must adopt the narrower one in a criminal prosecution. Not only do most computer users violate Terms of Service every day, but venue can be almost anywhere, meaning that any U.S. Attorney's Office in any district through which any Internet communication passed can bring a prosecution. A rule that every intentional breach of every Term of Service is a crime would leave individuals with no realistic way to ensure that their online conduct is lawful.[1]

Such an interpretation would also be constitutionally overbroad. According to the First Amendment's overbreadth doctrine, "a statute is facially invalid if it prohibits a substantial amount of protected speech." United States v. Williams, 128 S.Ct. 1830, 1838 (2008). The Government's cases have arisen in the context of business-to-business contract disputes, where First Amendment concerns are absent. See Cohen v. Cowles Media Co., 501 U.S. 663 (1991). Applying the line of broad civil cases in the criminal setting would trigger the First Amendment, however, and it would prohibit an extraordinary amount of protected speech.

The First Amendment does not permit such a reading of 18 U.S.C. § 1030. The Supreme Court has recognized that "the content on the Internet is as diverse as human thought," and that this content is subject to full First Amendment protection. Reno v. American Civil Liberties Union, 521 U.S. 844, 871 (1997). Personal

---

[1] One option would be to not read Terms of Service, on the theory that this would keep any violations from being intentional. However, this is not much of a choice given the Government's position that a defendant need not actually read Terms of Service to intentionally violate them.

expression on a social networking site like MySpace.com is protected by the First Amendment just like any other speech. See Layshock v. Hermitage School Dist., 496 F. Supp.2d 587 (W.D.Pa. 2007) (ruling that First Amendment protects a vulgar and offensive parody of a high school principal posted by a student on MySpace.com). By using civil § 1030 cases to prosecute cyberharassment, the Government seeks to avoid the First Amendment limitations that would apply if it actually tried to prosecute cyberharassment under the cyberharassment statutes.

To appreciate this point, consider the First Amendment difficulties that the government would have faced if it had tried to prosecute the defendant using the federal communications harassment statute, 47 U.S.C. § 223. A cyberharassment prosecution brought under § 223 would be unable to proceed unless it first satisfied the First Amendment. For example, in United States v. Popa, 187 F.3d 672 (D.C. Cir. 1999), the defendant repeatedly telephoned the office of Eric Holder, then the U.S. Attorney for the District of Columbia and now the nominee for Attorney General, and unleashed a string of racist insults. Popa called Holder "a criminal, a negro," a "whore, born by a negro whore," and stated that Holder had "violat[ed] the rights in court of the white people." Id. at 412-13. Popa was charged under 47 U.S.C. § 223(a)(1)(C), a statute since extended to the Internet that prohibits sending communications with "intent to annoy, abuse, threaten, or harass any person." The D.C. Circuit vacated the conviction, ruling that the statute could not apply to Popa's case under United States v. O'Brien, 391 U.S. 367 (1968).

Criminalizing insulting phone calls such as Popa's did not satisfy O'Brien's intermediate scrutiny standard under the First Amendment, so the statute could not be constitutionally applied to his conduct even though Popa violated the literal language of the statute. Popa, 187 F.3d at 678.

The government's theory would transform Popa's constitutionally protected speech into a criminal violation of 18 U.S.C. § 1030. So long as a Term of Service prohibits offensive speech – which most Terms of Service do – Popa's "access" to the government's telephone or computer network would become "unauthorized" and therefore criminal. The intermediate scrutiny required by the First Amendment in criminal harassment prosecutions would be replaced by no scrutiny at all. Under the broad civil cases that the Government cites, that pesky First Amendment would magically disappear.

The overbreadth doctrine forbids this interpretation of § 1030. Under the overbreadth doctrine, "a statute is facially invalid if it prohibits a substantial amount of protected speech." Williams, 128 S.Ct. at 1838. To avoid this constitutional infirmity, the statute must be construed in a limited way so that a substantial amount of protected speech is no longer covered by the statute. Popa, 187 F.3d at 678. The broad civil cases that the government cites as authority simply cannot be squared with this doctrine. There is no way to apply them in a criminal setting without encompassing a great deal of protected speech. As a result, the civil cases that the Government cites cannot make the

jump from the civil side of the docket to the criminal side of the docket.

III. The Only Criminal Case the Government Relies on Does Not Support Its Position.

Amidst the sea of civil authority cited in the Government's Response, the Government relies on only one criminal decision: United States v. Philips, 477 F.3d 215 (5th Cir. 2007). The government's description of the Philips case leaves the distinct impression that the Fifth Circuit affirmed the conviction merely because Philips had violated the "acceptable use" computer policy that he had signed as a University of Texas student. See Govt's Response at 8. Such an impression is completely false. Philips was a notorious hacker, and his conduct was criminal because he had hacked into a sensitive university database using a brute-force attack to steal others' personal information.

To be sure, Philips had initially attracted the suspicion of the university when he used port scans of computers outside the University of Texas ("UT") network in violation of UT's acceptable computer use policy. See id. at 217. The port scans enabled Philips to "succeed[] in infiltrating hundreds of computers, including machines belonging to other UT students, private businesses, U.S. Government agencies, and the British Armed Services webserver." Id. However, Philips was charged and convicted of different conduct that occurred after his port scans. As the

Fifth Circuit explained, Philips eventually set his sights on the UT computer network and a sensitive database known as TXClass:

> Phillips designed a computer program expressly for the purpose of hacking into the UT system via a portal known as the "TXClass Learning Central: A Complete Training Resource for UT Faculty and Staff." TXClass was a "secure" server operated by UT and used by faculty and staff as a resource for enrollment in professional education courses. Authorized users gained access to their TXClass accounts by typing their Social Security numbers in a field on the TXClass website's log-on page. Phillips exploited the vulnerability inherent in this log-on protocol by transmitting a "brute-force attack" program, which automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized TXClass users.
>
> Initially, Phillips selected ranges of Social Security numbers for individuals born in Texas, but he refined the brute-force attack to include only numbers assigned to the ten most populous Texas counties. When the program hit a valid Social Security number and obtained access to TXClass, it automatically extracted personal information corresponding to that number from the TXClass database and, in effect, provided Phillips a "back door" into UT's main server and unified database. Over a fourteen-month period, Phillips thus gained

> access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni.
>
> Phillips's actions hurt the UT computer system. The brute-force attack program proved so invasive-increasing the usual monthly number of unique requests received by TXClass from approximately 20,000 to as many as 1,200,000-that it caused the UT computer system to crash several times in early 2003. Hundreds of UT web applications became temporarily inaccessible, including the university's online library, payroll, accounting, admissions, and medical records. UT spent over $122,000 to assess the damage and $60,000 to notify victims that their personal information and Social Security numbers had been illicitly obtained.

Id. at 218.

The Government suggests that the Fifth Circuit allowed Philips' conviction he had violated the "acceptable use" computer policy. This is untrue. Because Philips' lawyer had failed to preserve the issue below, the Fifth Circuit reviewed Philips' conviction under the Fifth Circuit's deferential "manifest miscarriage of justice" standard, according to which a criminal conviction must be upheld unless "the evidence is so tenuous that a conviction is shocking." Id. at 219. In an opinion by Judge Edith Jones, the Fifth Circuit ruled that Philips' conviction was not a shocking miscarriage of justice. Philips, 477 F.3d at 220. The Fifth Circuit's explanation of why does not even mention the computer policy:

> Phillips's brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computerized data that he was not permitted to view or use. During cross-examination, Phillips admitted that TXClass's normal hourly hit volume did not exceed a few hundred requests, but that his brute-force attack created as many as 40,000. He also monitored the UT system during the multiple crashes his program caused, and backed up the numerical ranges of the Social Security numbers after the crashes so as not to omit any potential matches. Phillips intentionally and meticulously executed both his intrusion into TXClass and the extraction of a sizable quantity of confidential personal data. There was no lack of evidence to find him guilty of intentional unauthorized access.

Id. at 220. The part of Phillips that the Government relies on was an afterthought to this analysis, in which the court entertained Philips' frivolous argument that he was "authorized" to hack into TXClass because the password gate to the service was accessible on the Internet. The Fifth Circuit understandably disagreed. While any person could visit the log-in page, the court noted, not just anyone could bypass the password gate by entering in their Social Security number:

> While Phillips was authorized to use his UT email account and engage in other activities defined by UT's acceptable computer use policy, he was never authorized to access TXClass. The method of access he used makes this fact even more plain.

Id. at 221. Contrary to the Government's suggestion, this passage does not suggest that Philips was guilty because he violated UT's acceptable computer use policy. Rather, it makes the common-sense point that a computer hacker who hacks into a sensitive university database to steal the personal information of others is not "authorized" simply because he has access to the Internet or has other rights elsewhere on the network.

This proper reading of Philips, combined with its highly deferential standard of review, makes clear that the Fifth Circuit's opinion offers no support for the Government's case.

## IV. Conclusion

For the above reasons, the remaining three misdemeanor counts must be dismissed pursuant to rule 29, FRCP.

Dated: 1-2-09

s./ H. Dean Steward
H. Dean Steward
Orin Kerr
Counsel for Defendant Drew

**CERTIFICATE OF SERVICE**

IT IS HEREBY CERTIFIED THAT:

I, H. Dean Steward, am a citizen of the United States, and am at least 18 years of age. My business address is 107 Avenida Miramar, Ste. C, San Clemente, CA 92672.

I am not a party to the above entitled action. I have caused, on Jan. 2, 2009, service of the defendant's:

**REPLY TO GOVT RESPONSE- RULE 29**

On the following parties electronically by filing the foregoing with the Clerk of the District Court using its ECF system, which electronically notifies counsel for that party.

**AUSA MARK KRAUSE- LA**

I declare under penalty of perjury that the foregoing is true and correct.

Executed on JAN. 2, 2009

H. Dean Steward

H. Dean Steward