

1 H. Dean Steward SBN 85317  
2 107 Avenida Miramar, Ste. C  
3 San Clemente, CA 92672  
4 949-481-4900  
5 Fax: (949) 496-6753  
6 [deansteward@fea.net](mailto:deansteward@fea.net)

7 Orin S. Kerr  
8 Dist. of Columbia BN 980287  
9 2000 H. Street NW  
10 Washington, DC 20052  
11 202-994-4775  
12 Fax 202-994-5654  
13 okerr@gwu.edu

14 Attorneys for Defendant  
15 Lori Drew

16 UNITED STATES DISTRICT COURT  
17 CENTRAL DISTRICT OF CALIFORNIA

18 UNITED STATES,

19 Plaintiff,

20 vs.

21 LORI DREW

22 Defendant.

Case No. CR-08-00582-GW

REPLY TO GOVERNMENT RESPONSE TO  
DEFENSE RULE 29

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

25 Dated: 1-2-09

s./ H. Dean Steward

26 H. Dean Steward  
27 Orin Kerr  
28 Counsel for Defendant Drew

1	TABLE OF CONTENTS	
2	I. Introduction	4
3	II. Civil Tort Cases Adopting a Contractual View	
4	Of 18 USC §1030 Cannot Be Applied to a Criminal	
5	Prosecution	4
6	III. The Only Criminal case the Government	
7	Relies on Does Not Support its Position	10
8	IV. Conclusion	14
9	Proof of Service	15
10		
11		
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		

1 TABLE OF AUTHORITIES

2 Cohen v. Cowles Media Co. 501 U.S. 663 (1991) 7

3 Reno v. ACLU 521 U.S. 844 (1997) 7

4 Screws v. U.S. 325 U.S. 91 (1945) 6

5 U.S. v. Lanier 520 U.S. 259 (1997) 5

6 U.S. v. O'Brien 391 U.S. 367 (1968) 8,9

7 U.S. v. Williams 128 S. Ct. 1830 (2008) 7,9

8 Black & Decker, Inc. v. Smith 568 F. Supp. 2d 929

9 (W.D. Tenn. 2008) 6

10 Condux Intern. Inc. v. Haugum 2008 WL 5244818 5,6

11 (D. Minn. 12-15-08)

12 Layshock v. Hermitage School Dist. 496 F. Supp. 2d 8

13 587 (W.D. PA 2007)

14 Lockheed Martin Corp. v. Speed 2006 WL 2683058 6

15 (M.D. Fla 8-1-06)

16 U.S. v. Phillips 477 F.3d 215 (5<sup>th</sup> Cir. 2007) 10,12,13,14

17 U.S. v. Popa 187 F.3d 672 (DC Cir. 1999) 8,9

---

18

19 18 USC §1030 et. al. 4,5,8,9

20 47 USC §223 8

21 Rule 29, Federal Rules of Criminal Procedure 14

22

23

24

25

26

27

28

1 I. Introduction

2 Although counsel earlier had assumed that a reply to the  
3 Government's Response on the Rule 29 motion would not assist the  
4 Court, upon reading it counsel has come to believe that a reply  
5 would greatly help the Court in understanding the issues raised in  
6 this case. In particular, a reply can help the Court understand  
7 why the civil authorities the Government relies on cannot be  
8 adopted in a criminal setting, and why the one criminal case the  
9 government cites provides no support for its position. With that  
10 end in mind, the undersigned counsel respectfully submits this  
11 reply.  
12

13 II. Civil Tort Cases Adopting a Contractual View of 18 U.S.C. §  
14 1030 Cannot Be Applied To A Criminal Prosecution.

15  
16 The government's response rests almost entirely on civil tort  
17 cases. In the context of civil business-to-business litigation,  
18 brought under 18 U.S.C. § 1030(g), a few courts have indeed adopted  
19 an extremely broad view of 18 U.S.C. § 1030. Those courts have  
20 construed § 1030 as a commercial statute that provides federal  
21 court jurisdiction for business contract disputes. Under these  
22 cases, breach of a contract renders access unauthorized. Almost  
23 all of the cases that the government cites as authority arose in  
24 that setting. See Govt's Response to Defendant's Supplement to  
25 Rule 29 Motion at 5-10.

26 The Government cannot properly rely on those broad civil cases  
27 in this criminal prosecution. Although the Government does not  
28

1 acknowledge it, the lower courts are sharply divided even in the  
2 civil setting on whether those broad civil interpretations of §  
3 1030 are correct. Two competing lines of cases have emerged. One  
4 line of cases has adopted the broad contractual reading that the  
5 Government relies on here. Another line of cases has recognized  
6 that 18 U.S.C. § 1030 is also a criminal statute, and it has  
7 rejected that expansive reading as overly broad for a statute with  
8 criminal remedies. See, e.g., Condux Intern., Inc. v. Haugum, 2008  
9 WL 5244818 (D. Minn. Dec. 15, 2008) (discussing the two lines of  
10 cases).

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

22 This assumption is false. Civil precedents can only make the  
23 jump to the criminal side of the docket if the resulting  
24 interpretation would satisfy the three related "fair warning"  
25 canons for interpreting criminal statutes: vagueness, the rule of  
26 lenity, and overbreadth. See United States v. Lainier, 520 U.S.  
27 259, 266-67 (1997). These three doctrines ensure that no criminal  
28

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

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

26       Under the rule of lenity, reliance on the broad civil cases  
27 the Government cites must be rejected. No criminal case has ever  
28

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

10 Such an interpretation would also be constitutionally  
11 overbroad. According to the First Amendment's overbreadth doctrine,  
12 "a statute is facially invalid if it prohibits a substantial amount  
13 of protected speech." United States v. Williams, 128 S.Ct. 1830,  
14 1838 (2008). The Government's cases have arisen in the context of  
15 business-to-business contract disputes, where First Amendment  
16 concerns are absent. See Cohen v. Cowles Media Co., 501 U.S. 663  
17 (1991). Applying the line of broad civil cases in the criminal  
18 setting would trigger the First Amendment, however, and it would  
19 prohibit an extraordinary amount of protected speech.

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

---

25  
26 <sup>1</sup> One option would be to not read Terms of Service, on the  
27 theory that this would keep any violations from being intentional.  
28 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.

1 expression on a social networking site like MySpace.com is  
2 protected by the First Amendment just like any other speech. See  
3 Layshock v. Hermitage School Dist., 496 F. Supp.2d 587 (W.D.Pa.  
4 2007) (ruling that First Amendment protects a vulgar and offensive  
5 parody of a high school principal posted by a student on  
6 MySpace.com). By using civil § 1030 cases to prosecute  
7 cyberharassment, the Government seeks to avoid the First Amendment  
8 limitations that would apply if it actually tried to prosecute  
9 cyberharassment under the cyberharassment statutes.

10 To appreciate this point, consider the First Amendment  
11 difficulties that the government would have faced if it had tried  
12 to prosecute the defendant using the federal communications  
13 harassment statute, 47 U.S.C. § 223. A cyberharassment prosecution  
14 brought under § 223 would be unable to proceed unless it first  
15 satisfied the First Amendment. For example, in United States v.  
16 Popa, 187 F.3d 672 (D.C. Cir. 1999), the defendant repeatedly  
17 telephoned the office of Eric Holder, then the U.S. Attorney for  
18 the District of Columbia and now the nominee for Attorney General,  
19 and unleashed a string of racist insults. Popa called Holder "a  
20 criminal, a negro," a "whore, born by a negro whore," and stated  
21 that Holder had "violat[ed] the rights in court of the white  
22 people." Id. at 412-13. Popa was charged under 47 U.S.C. §  
23 223(a) (1) (C), a statute since extended to the Internet that  
24 prohibits sending communications with "intent to annoy, abuse,  
25 threaten, or harass any person." The D.C. Circuit vacated the  
26 conviction, ruling that the statute could not apply to Popa's case  
27 under United States v. O'Brien, 391 U.S. 367 (1968).



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

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

16 The overbreadth doctrine forbids this interpretation of §  
17 1030. Under the overbreadth doctrine, "a statute is facially  
18 invalid if it prohibits a substantial amount of protected speech."  
19 Williams, 128 S.Ct. at 1838. To avoid this constitutional  
20 infirmity, the statute must be construed in a limited way so that a  
21 substantial amount of protected speech is no longer covered by the  
22 statute. Popa, 187 F.3d at 678. The broad civil cases that the  
23 government cites as authority simply cannot be squared with this  
24 doctrine. There is no way to apply them in a criminal setting  
25 without encompassing a great deal of protected speech. As a  
26 result, the civil cases that the Government cites cannot make the

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

3  
4 III. The Only Criminal Case the Government Relies on Does Not  
5 Support Its Position.

6  
7       Amidst the sea of civil authority cited in the Government's  
8 Response, the Government relies on only one criminal decision:  
9 United States v. Philips, 477 F.3d 215 (5th Cir. 2007). The  
10 government's description of the Philips case leaves the distinct  
11 impression that the Fifth Circuit affirmed the conviction merely  
12 because Philips had violated the "acceptable use" computer policy  
13 that he had signed as a University of Texas student. See Govt's  
14 Response at 8. Such an impression is completely false. Philips  
15 was a notorious hacker, and his conduct was criminal because he had  
16 hacked into a sensitive university database using a brute-force  
17 attack to steal others' personal information.

18       To be sure, Philips had initially attracted the suspicion of  
19 the university when he used port scans of computers outside the  
20 University of Texas ("UT") network in violation of UT's acceptable  
21 computer use policy. See id. at 217. The port scans enabled  
22 Philips to "succeed[] in infiltrating hundreds of computers,  
23 including machines belonging to other UT students, private  
24 businesses, U.S. Government agencies, and the British Armed  
25 Services webserver." Id. However, Philips was charged and convicted  
26 of different conduct that occurred after his port scans. As the  
27  
28

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

3  
4 Phillips designed a computer program expressly for the  
5 purpose of hacking into the UT system via a portal known as  
6 the "TXClass Learning Central: A Complete Training Resource  
7 for UT Faculty and Staff." TXClass was a "secure" server  
8 operated by UT and used by faculty and staff as a resource for  
9 enrollment in professional education courses. Authorized users  
10 gained access to their TXClass accounts by typing their Social  
11 Security numbers in a field on the TXClass website's log-on  
12 page. Phillips exploited the vulnerability inherent in this  
13 log-on protocol by transmitting a "brute-force attack"  
14 program, which automatically transmitted to the website as  
15 many as six Social Security numbers per second, at least some  
16 of which would correspond to those of authorized TXClass  
17 users.

18 Initially, Phillips selected ranges of Social Security  
19 numbers for individuals born in Texas, but he refined the  
20 brute-force attack to include only numbers assigned to the ten  
21 most populous Texas counties. When the program hit a valid  
22 Social Security number and obtained access to TXClass, it  
23 automatically extracted personal information corresponding to  
24 that number from the TXClass database and, in effect, provided  
25 Phillips a "back door" into UT's main server and unified  
26 database. Over a fourteen-month period, Phillips thus gained  
27  
28

1 access to a mother lode of data about more than 45,000 current  
2 and prospective students, donors, and alumni.

3 Phillips's actions hurt the UT computer system. The  
4 brute-force attack program proved so invasive-increasing the  
5 usual monthly number of unique requests received by TXClass  
6 from approximately 20,000 to as many as 1,200,000-that it  
7 caused the UT computer system to crash several times in early  
8 2003. Hundreds of UT web applications became temporarily  
9 inaccessible, including the university's online library,  
10 payroll, accounting, admissions, and medical records. UT spent  
11 over \$122,000 to assess the damage and \$60,000 to notify  
12 victims that their personal information and Social Security  
13 numbers had been illicitly obtained.

14  
15 Id. at 218.

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

1  
2 Phillips's brute-force attack program was not an intended use  
3 of the UT network within the understanding of any reasonable  
4 computer user and constitutes a method of obtaining  
5 unauthorized access to computerized data that he was not  
6 permitted to view or use. During cross-examination, Phillips  
7 admitted that TXClass's normal hourly hit volume did not  
8 exceed a few hundred requests, but that his brute-force attack  
9 created as many as 40,000. He also monitored the UT system  
10 during the multiple crashes his program caused, and backed up  
11 the numerical ranges of the Social Security numbers after the  
12 crashes so as not to omit any potential matches. Phillips  
13 intentionally and meticulously executed both his intrusion  
14 into TXClass and the extraction of a sizable quantity of  
15 confidential personal data. There was no lack of evidence to  
16 find him guilty of intentional unauthorized access.

17  
18 Id. at 220. The part of Phillips that the Government relies on was  
19 an afterthought to this analysis, in which the court entertained  
20 Philips' frivolous argument that he was "authorized" to hack into  
21 TXClass because the password gate to the service was accessible on  
22 the Internet. The Fifth Circuit understandably disagreed. While  
23 any person could visit the log-in page, the court noted, not just  
24 anyone could bypass the password gate by entering in their Social  
25 Security number:

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

6  
7 Id. at 221. Contrary to the Government's suggestion, this passage  
8 does not suggest that Philips was guilty because he violated UT's  
9 acceptable computer use policy. Rather, it makes the common-sense  
10 point that a computer hacker who hacks into a sensitive university  
11 database to steal the personal information of others is not  
12 "authorized" simply because he has access to the Internet or has  
13 other rights elsewhere on the network.

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

17 IV. Conclusion

18  
19 For the above reasons, the remaining three misdemeanor counts  
20 must be dismissed pursuant to rule 29, FRCP.

21 Dated: 1-2-09

s./ H. Dean Steward

H. Dean Steward

Orin Kerr

Counsel for Defendant Drew

1 **CERTIFICATE OF SERVICE**

2  
3  
4 IT IS HEREBY CERTIFIED THAT:

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

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

10 **REPLY TO GOVT RESPONSE- RULE 29**

11 On the following parties electronically by filing the foregoing  
12 with the Clerk of the District Court using its ECF system, which  
13 electronically notifies counsel for that party.  
14

15 **AUSA MARK KRAUSE- LA**

16  
17 I declare under penalty of perjury that the foregoing is true and  
18 correct.

19 Executed on JAN. 2, 2009

20 H. Dean Steward

21 H. Dean Steward  
22  
23  
24  
25  
26  
27  
28