

1 THOMAS P. O'BRIEN
 United States Attorney
 2 CHRISTINE C. EWELL
 Assistant United States Attorney
 3 Chief, Criminal Division
 MARK C. KRAUSE (SBN 198142)
 4 Assistant United States Attorney
 Deputy Chief, Cyber and Intellectual
 5 Property Crimes Section
 1200 United States Courthouse
 6 312 North Spring Street
 Los Angeles, California 90012
 7 Telephone: (213) 894-3493
 Facsimile: (213) 894-8601
 8 Email: mark.krause@usdoj.gov

9 Attorneys for Plaintiff
 United States of America

11 UNITED STATES DISTRICT COURT
 12 FOR THE CENTRAL DISTRICT OF CALIFORNIA

13	UNITED STATES OF AMERICA,)	CR NO. 08-582-GW
14	Plaintiff,)	<u>GOVERNMENT'S RESPONSE TO</u>
15	v.)	<u>COURT'S SEPTEMBER 23, 2008</u>
16	LORI DREW,)	<u>INQUIRY; EXHIBIT</u>
17	Defendant.)	Hearing Date: October 30, 2008
18)	Hearing Time: 8:30 a.m.
19)	Trial Date: November 18, 2008
20)	Trial Time: 8:00 a.m.
21)	Place: Courtroom of the
22)	Hon. George H. Wu

23 Plaintiff United States of America, by and through its
 24 counsel of record, United States Attorney Thomas P. O'Brien and
 25 Assistant United States Attorney Mark C. Krause, hereby files
 26 this response pursuant to the Court's September 23, 2008 request
 27 for supplemental briefing.

28 \\ \\ \\

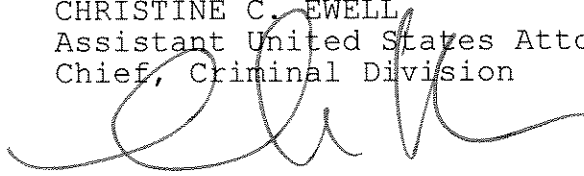
1 This response is based on the attached memorandum of points
2 and authorities, the files and records, in this case, and
3 whatever argument or evidence this Court may consider.

4 Dated: October 6, 2008

5 Respectfully submitted,

6 THOMAS P. O'BRIEN
United States Attorney

7 CHRISTINE C. EWELL
8 Assistant United States Attorney
9 Chief, Criminal Division



10

MARK C. KRAUSE
11 Assistant United States Attorney

12 Attorneys for Plaintiff
13 United States of America
14
15
16
17
18
19
20
21
22
23
24
25
26
27

TABLE OF CONTENTS

Page

1

2 I INTRODUCTION 1

3 II ARGUMENT 3

4

5 A. FEDERALISM DOES NOT BAR THE INSTANT PROSECUTION 3

6 1. The Indictment Adequately Alleges Facts

7 Sufficient to Establish Jurisdiction 4

8 2. The Court Has No Authority to Engage in an

9 Independent Assessment of Federalism Concerns . 6

10 B. THE CONDUCT AT ISSUE FALLS WITHIN THE MEANING OF

11 SECTION 1030(a)(2)(C) BECAUSE THE STATUE PROHIBITS

12 MORE THAN SIMPLE THEFT 13

13 1. The Plain Terms of the Statute, the Legislative

14 History, and Cases Construing Section 1030

15 Demonstrate Section 1030(a)(2)(C) Prohibits More

16 than Theft 14

17 2. The CCIPS Report Cited by the Court Does

18 Not Provide A Basis for Limiting the Statute

19 to Theft 18

20 3. The Conduct at Issue Did Involve Theft 20

21 C. INFORMATION ABOUT M.T.M. THAT WAS OBTAINED THROUGH

22 THE MYSPACE SERVERS IS "INFORMATION" UNDER SECTION

23 1030(a)(2)(C) 21

24 III CONCLUSION 25

25

26

27

28

TABLE OF AUTHORITIES

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

FEDERAL CASES

Page(s)

In re AOL, Inc. Version 5.0 Software Litigation,
168 F. Supp. 2d 1359 (S.D. Fla. 2001) 16

America Online v. National Health Care Discount,
174 F. Supp.2d 890 (N.D. Iowa 2001) 24

Badders v. United States,
240 U.S. 391 (1916) 4

Chevron v. National Resources Defense Counsel,
467 U.S. 837 (1984) 19

Cohens v. Virginia,
19 U.S. (6 Wheat.) 264 (1821) 7

Connecticut National Bank v. Germain,
503 U.S. 249 (1992) 14

Crandon v. United States,
494 U.S. 152 (1990) 19

Credentials Plus v. Calderone,
230 F. Supp. 2d 890 (N.D. Ind. 2002) 24

Dolfi v. Pontesso,
156 F.3d 696 (6th Cir. 1998) 19

In re Doubleclick Privacy Litigation,
154 F. Supp. 197 (S.D.N.Y. 2001) 24

EF Cultural Travel BV v. Zefer Corp.,
318 F.3d 58 (1st Cir. 2003) 23

Gonzalez v. Raich,
545 U.S. 1 (2005) 4

Greyhound Corp. v. Mt. Hood Stages, Inc.,
437 U.S. 322 (1978) 12

Healthcare Advocates v. Harding, Earley, Follmer & Frailey,
497 F. Supp. 2d 627 (E.D. Pa. 2007) 23

Himes v. Thompson,
336 F.3d 848 (9th Cir. 2003) 10

Hines v. Davidowitz,
312 U.S. 52 (1941) 12

TABLE OF AUTHORITIES (cont'd)

Page(s)

1

2

3 I.M.S. Inquiry Management System v. Berkshire Inf. System,
307 F. Supp.2d 521 (S.D.N.Y. 2001) 23

4 K & N Engineering, Inc. v. Bulat,
510 F.3d 1079 (9th Cir. 2007) 14

6 Keg Technology Inc. v. Laimer,
436 F. Supp.2d 1364 (N.D. Ga. 2006) 23

7 McCarthy v. Bronson,
8 500 U.S. 136 (1991) 12

9 P.C. Yonkers, Inc. v Celebrations the Party and Seasonal
10 Superstore, LLC,
428 F.3d 504 (3d Cir. 2005) 16

11 Pacific Aerospace & Electronics, Inc. v. Taylor,
295 F. Supp. 2d 1188 (E.D. Wash. 2003) 16

12 Pennsylvania Department of Corrections v. Yeskey,
13 524 U.S. 206 (1998) 16

14 Register.com v. Verio,
126 F. Supp. 2d 238 (S.D.N.Y. 2000) 24

15 Schmuck v. United States,
16 489 U.S. 705 (1989) 6

17 Sedima, S.P.L.R. v. Imrex Co.,
473 U.S. 479 (1985) 16

18 Shurgard Storage Centers v. Safeguard Self Storage,
19 119 F. Supp. 2d 1221 (W.D. Wash. 2000) 22, 24

20 Southwest Airlines v. Farechase, Inc.,
318 F. Supp. 2d 435 (N. D. Tex. 2004) 23

21 Tennessee Valley Authority v. Hill,
22 437 U.S. 153 (1978) 15

23 United States v. Acosta,
421 F.3d 1195 (11th Cir. 2005) 5

24 United States v. Andrino-Carrillo,
25 63 F.3d 922 (9th Cir. 2002) 5

26 United States v. Ballinger,
395 F.3d 1218 (11th Cir. 2005) 14

27

28

TABLE OF AUTHORITIES (cont'd)

Page(s)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States v. Becker,
569 F.2d 951 (5th Cir. 1978) 6

United States v. Bishop,
66 F.3d 569 (3d Cir. 1995) 5

United States v. Corona-Sanchez,
234 F.3d 449 (9th Cir. 2000) 20

United States v. Dickson,
816 F.2d 751 (D.C. Cir. 1987) 7, 8, 10

United States v. Garner,
663 F.2d 834 (9th Cir. 1981) 6

United States v. Hanousek,
176 F.3d 1116 (9th Cir. 1999) 14

United States v. Martinez,
49 F.3d 1398 (9th Cir. 1995) 4, 5

United States v. Middleton,
231 F.3d 1207 (9th Cir. 2000) 16

United States v. Miller,
722 F.2d 562 (9th Cir. 1983) 11

United States v. Mitra,
405 F.3d 492 (7th Cir. 2005) 13

United States v. Patterson,
314 F.2d 491 (7th Cir. 1963) 12

United States v. Pecora,
693 F.2d 421 (5th Cir. 1982) 6

United States v. Robertson,
45 F.3d 1423 (10th Cir. 1995) 11

United States v. Salerno,
481 U.S. 739 (1987) 4

United States v. Sawyer,
85 F.3d 713 (1st Cir. 1996) 7

TABLE OF AUTHORITIES (cont'd)

Page(s)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States v. Serang,
156 F.3d 910 (9th Cir. 1998) 6

United States v. Tocco,
135 F.3d 116 (2d Cir. 1998) 5

United States v. Turkette,
452 U.S. 576 (1981) 6

United States v. Vincent,
758 F.2d 379 (9th Cir. 1985) 6

United States v. Welch,
327 F.3d 1081 (10th Cir. 2003) 7, 19

United States v. Willis,
476 F.3d 1121 (10th Cir. 2007) 24

United States v. Woodward,
149 F.3d 46 (1st Cir. 1998) 7

Whitfield v. United States,
543 U.S. 209 (2005) 15

STATE CASES

Hoovel v. State,
69 S.W.2d 104 (Tex Crim. App. 1934) 20

People v. Miller,
81 Cal. App. 4th 1427 (2000) 20

FEDERAL STATUTES

18 U.S.C. § 1030 1

18 U.S.C. § 1030 (1985) 22

18 U.S.C. 1030(a) 21

TABLE OF AUTHORITIES (cont'd)

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

	Page(s)
15 U.S.C. § 1618	22
18 U.S.C. § 371	1
18 U.S.C. § 641	14
18 U.S.C. § 657	15
18 U.S.C. § 659	15
18 U.S.C. § 665	15
18 U.S.C. § 669	15
18 U.S.C. § 922	5
18 U.S.C. § 1030	passim
18 U.S.C. § 1201	5
18 U.S.C. §§ 1961-1968	6
18 U.S.C. § 2119	5
18 U.S.C. § 2312	5
12 U.S.C. § 3401	22

MEMORANDUM OF POINTS AND AUTHORITIES

I

INTRODUCTION

Defendant Lori Drew has been charged in the four count indictment with: (1) conspiracy to access protected computers without authorization in violation of 18 U.S.C. § 371; and (2) unauthorized access to a protected computer to obtain information to further a tortious act in violation of 18 U.S.C. § 1030. The parties anticipate filing a stipulation proposing continuing the trial until November 18, 2008.

On September 23, 2008, this Court posed three questions to counsel: (1) whether the Court could exercise its discretion to decline to assert jurisdiction over the case based on federalism concerns even if the allegations in the indictment regarding interstate communications were adequately pled and proven, (9/23/08 RT 5); (2) whether Section 1030(a)(2) only prohibits the "theft" of information, (9/23/08 RT 4); and (3) if so, what was the information that was stolen, (9/23/08 RT 21).¹

First, the allegations in the indictment are sufficient to allege an interstate communication and thus to provide an adequate jurisdictional nexus. At the time of the offense, Section 1030(a)(2) required proof of an interstate

¹The Court also asked whether the government was alleging that defendant's conduct was "without authorization" or "in excess of authorization." As the government stated at the hearing, it was both.

1 communication.² Here, the indictment alleges that defendant
2 obtained information and her conduct involved an interstate
3 communication. Accordingly, jurisdiction has been adequately
4 pled. So long as the government can prove the interstate
5 communication, this Court lacks discretion to dismiss based on a
6 conclusion that the case is "local" and not "federal." Indeed,
7 if it were to do so, such a dismissal would raise serious
8 constitutional concerns because it would infringe on the
9 Executive Branch's exclusive authority to make charging
10 decisions.

11 Second, this Court should decline to dismiss the indictment
12 based on the mistaken belief that Section 1030(a)(2) only covers
13 "theft" and that no theft occurred here. The plain terms of
14 Section 1030(a)(2)(c) do not refer to theft. Instead, they
15 explicitly -- and only -- prohibit "obtaining" information under
16 certain circumstances. The legislative history likewise does not
17 suggest that the statute should be limited to "theft" because it
18 envisions other misuses of information. Nor is the memorandum
19 prepared by the Computer Crime and Intellectual Property Section
20 ("CCIPS") and cited by the Court to the contrary. But even if
21 that memorandum did suggest Section 1030(a)(2)(c) was restricted
22 to theft offenses notwithstanding the plain language of the
23 statute, that report is not entitled to deference because it was
24

25
26 ²As explained in greater detail below, on September 26,
27 2008, the Former Vice Presidents Protection Act was passed,
28 which, inter alia, amended Section 1030 to strike the requirement
that the conduct involve an interstate communication.

1 not prepared by Congress, but by employees of the Attorney
2 General. Such a construction of Section 1030(a)(2)(c) also would
3 not warrant dismissal because the statute would still cover the
4 conduct at issue: obtaining information from a protected computer
5 through fraud and deception.

6 Finally, the information at issue in the case -- data about
7 victim M.T.M. that would be used to torment and harass her --
8 falls plainly within the meaning of Section 1030. The term
9 "information" is not defined. It should be given its plain
10 meaning and include data of any and all kinds. Such a definition
11 is consistent with the legislative history of Section 1030 and
12 case law construing it.

13 II

14 ARGUMENT

15 A. FEDERALISM DOES NOT BAR THE INSTANT PROSECUTION

16 At the September 23, 2008, hearing, the Court expressed
17 concern whether the instant prosecution could be maintained
18 consistent with principles of federalism. (9/23/08 RT 4). The
19 Court noted that in 1986, during the first round of amendments to
20 Section 1030, Congress cited concerns for federalism in
21 explaining why it declined to draft a broader statute to combat
22 computer crime. (Id.). The Court therefore questioned whether
23 it could exercise jurisdiction over this case consistent with
24 Congress' earlier concerns.³

25
26 ³The Court did not appear to be contemplating a facial
27 challenge to Section 1030(a)(2)(c). "A facial challenge to a
28 legislative Act is, of course, the most difficult challenge to

1 Under settled law, not only may this Court exercise
2 jurisdiction, it must do so. Congress initially sought to
3 balance its desire for a broad statute with a respect for
4 existing state computer crime laws by requiring proof of an
5 interstate communication in order to proceed under Section
6 1030(a)(2)(c). The indictment comports with this jurisdictional
7 requirement by alleging that defendant's conduct involved
8 interstate communications. Assuming the government can prove
9 that jurisdictional allegation, this Court is not free to decline
10 to exercise jurisdictions based on a view that the case is
11 "local" and not "federal." Gonzalez v. Raich, 545 U.S. 1, 23
12 (2005) (when "the class of activities is regulated and the class
13 is within the reach of federal power, the courts have no power to
14 excise, as trivial, individual instances of the class").

15 1. The Indictment Adequately Alleges Facts Sufficient to
16 Establish Jurisdiction

17 Courts have frequently recognized that Congress is
18 authorized under the Commerce Clause to enact legislation
19 regarding conduct affecting interstate or foreign commerce.
20 Const. Art. I, § 8, cl. 3; Raich, 545 U.S. at 16-17; Badders v.
21 United States, 240 U.S. 391, 393 (1916). Congress has repeatedly
22 used its Commerce Clause authority to prohibit criminal

23 _____
24 mount successfully, since the challenger must establish that no
25 set of circumstances exists under which the Act would be valid."
26 United States v. Salerno, 481 U.S. 739, 745 (1987). Such a
27 challenge would fail given the statutory requirement that the
28 government prove an interstate communication. United States v.
Martinez, 49 F.3d 1398 (9th Cir. 1995) (rejecting argument that
car jacking statute was unconstitutional).

1 activities that have an interstate nexus, even if those
2 activities were traditionally a matter of local concern. See,
3 e.g., 18 U.S.C. § 922(g)(1) (felon in possession of firearm that
4 traveled in interstate commerce); 18 U.S.C. § 1201 (federal
5 kidnaping statute); 18 U.S.C. § 2119 (federal car jacking
6 statute); 18 U.S.C. § 2312 (interstate transportation of stolen
7 automobiles). Courts have repeatedly upheld these statutes
8 against constitutional attack. United States v. Tocco, 135 F.3d
9 116 (2d Cir. 1998) (upholding constitutionality of federal arson
10 statute and finding sufficient evidence was adduced to meet
11 jurisdictional requirements); United States v. Martinez, 49 F.3d
12 1398 (9th Cir. 1995) (rejecting argument that federal car jacking
13 statute was unconstitutional); United States v. Bishop, 66 F.3d
14 569 (3d Cir. 1995) (rejecting argument that Section 2119 was
15 unconstitutional).

16 In this case, Section 1030(a)(2) provides, in relevant part:

17 [Whoever] intentionally accesses a computer without
18 authorization or exceeds authorized access, and thereby
19 obtains --

20 . . . (c) information from any protected computer if
21 the conduct involved an interstate or foreign
22 communication . . . shall be [guilty of an offense
23 against the United States].

24 18 U.S.C. § 1030(a)(2)(c). Here, the indictment alleges that
25 defendant's conduct "involved an interstate . . . communication"
26 because defendant's conduct in Missouri involved communications
27 with MySpace servers outside of Missouri, namely, in California.
28 Such allegations are sufficient to ground jurisdiction. United
States v. Acosta, 421 F.3d 1195, 1198 (11th Cir. 2005)

1 (jurisdictional requirement of mailing child pornography
2 satisfied by mailing by Postal Inspector); United States v.
3 Serang, 156 F.3d 910, 914-15 (9th Cir. 1998) ("A mailing is
4 sufficiently closely related to the fraudulent scheme if it is
5 'for the purpose of executing the scheme' or 'incident to an
6 essential part of the scheme'"); United States v. Vincent, 758
7 F.2d 379 (9th Cir. 1985) (evidence sufficient to ground
8 jurisdiction based on single interstate phone call); United
9 States v. Pecora, 693 F.2d 421, 424 (5th Cir. 1982) (rejecting
10 argument that interstate phone call was insufficient); United
11 States v. Garner, 663 F.2d 834, 838 (9th Cir. 1981) (telephone
12 calls sufficient to establish interstate commerce even though not
13 essential part of scheme); United States v. Becker, 569 F.2d
14 951, 964 (5th Cir. 1978) (rejecting argument that use of mails
15 was "too incidental"); see also Schmuck v. United States, 489
16 U.S. 705, 711 (1989) (mailing must be "a step in the plot").

17 2. The Court Has No Authority to Engage in an Independent
18 Assessment of Federalism Concerns

19 So long as the interstate nexus is pled and proven, this
20 Court is without discretion to refuse to exercise jurisdiction
21 even if it differs with the Executive's judgment and believes the
22 case is more appropriately considered "local" in character.
23 United States v. Turkette, 452 U.S. 576 (1981) (where Congress
24 knew that RICO, 18 U.S.C. §§ 1961-1968, would alter federal-state
25 balance in enforcement of criminal law, courts are "without
26 authority to restrict the application of the statute" on
27 federalism grounds); Cohens v. Virginia, 19 U.S. (6 Wheat.) 264,
28

1 404 (1821) ("We have no more right to decline the exercise of
2 jurisdiction which is given, than to usurp that which is not
3 given"); United States v. Dickson, 816 F.2d 751 (D.C. Cir. 1987)
4 (reversing district court's dismissal on federalism grounds);
5 United States v. Welch, 327 F.3d 1081, 1093 (10th Cir. 2003)
6 (rejecting federalism challenge in light of ample allegations in
7 indictment). Accordingly, courts have routinely rejected similar
8 arguments raised by defendants in similar circumstances. See,
9 e.g., United States v. Woodward, 149 F.3d 46 (1st Cir. 1998)
10 (rejecting argument that wirings and mailings were merely "a
11 pretext to manufacture federal jurisdiction over a local
12 offense"; United States v. Sawyer, 85 F.3d 713, 722 (1st Cir.
13 1996).

14 In Dickson, for example, the D.C. Circuit reversed the
15 dismissal of an indictment after concluding the district court
16 was without authority to decline to exercise jurisdiction. 816
17 F.2d at 753. The defendants were charged in a multi-count
18 indictment with violating the federal murder-for-hire statute,
19 conspiracy, and attempted murder. Id. at 752. The indictment
20 alleged that the defendants solicited a supposed "hit man" (who
21 was actually an undercover police officer) to murder a rival of
22 one of the defendants. Id. The indictment also alleged that the
23 defendants triggered a beeper owned by the undercover agent by
24 radio signals on several occasions. Id. "On one such occasion,"
25 the officer was in Virginia and he called one of the defendants
26 in the District of Columbia. Id. Although the district court
27
28

1 "[a]cknowledg[ed] that the beeper transmissions and the
2 triggering of the officer's interstate call 'established the
3 requisite interstate nexus,'" it concluded, after reviewing the
4 statute's legislative history, that Congress did not want the
5 statute employed to address "purely local" cases and dismissed
6 the federal charges. Id. at 752.

7 The Court of Appeals reversed, holding that the district
8 court lacked discretion to decline to exercise jurisdiction over
9 the proceeding because "[t]he statutory language [was] broad,
10 unqualified, and unambiguous." Id. at 754. The Court of Appeals
11 further held:

12 The expressions of congressional concern featured by the
13 district court were more sensibly read as admonitions to
14 federal prosecutors -- guidelines of the exercise of
15 prosecutorial discretion in the application of the murder-
16 for-hire statute. There is no suggestion that Congress
17 intended to grant the courts license to oversee that
18 discretion more actively than in the ordinary case. Absent
19 allegations of prosecutorial misconduct, we hold, courts are
20 not free to turn down federal jurisdiction once the
21 statutory nexus has been established.

22 Id.⁴ This case is indistinguishable from Dickson. Section
23 1030(a)(2)'s jurisdictional requirements are "broad, unqualified,
24
25
26
27

28 ⁴ Likewise, in Perrine v. United States, 444 U.S. 37 (1979),
the Supreme Court rejected the petitioner's claim that broadly
interpreting the meaning of "bribery" in a Travel Act case would
have serious federalism implications. Id. at 49-50. The Court
reasoned that "so long as the requisite interstate nexus is
present, the statute reflects a clear and deliberate intent on
the part of Congress to alter the federal-state balance in order
to reinforce state law enforcement." Id. at 50. The same can be
said about the conduct here, where so long as the jurisdictional
requirement is satisfied, Congress has explicitly provided that
conduct in furtherance of a criminal or tortious act under state
law may subject a defendant to a more serious punishment under
federal law. 18 U.S.C. § 1030(c)(2)(B)(ii).

1 and unambiguous." So long as an interstate communication is
2 proven, this Court lacks the authority to decline to exercise
3 jurisdiction.

4 As this Court has observed, it is true that in 1986 Congress
5 cited federalism concerns in declining to enact an even broader
6 version of Section 1030(a)(2)(c) for fear that it would interfere
7 with state law enforcement efforts. The Senate Report on the
8 legislation, which this Court cited, stated in part:

9 It has been suggested that, because some States lack
10 comprehensive computer crime statutes of their own, the
11 Congress should enact as sweeping a Federal statute as
12 possible so that no computer crime is potentially
13 uncovered. The Committee rejects this approach and
14 prefers instead to limit Federal jurisdiction over
15 computer crime to those cases in which there is a
16 compelling Federal interest, *i.e.*, where computers of
the Federal Government or certain financial
institutions are involved, or where the crime itself is
interstate in nature. The Committee is convinced that
this approach strikes the appropriate balance between
the Federal Government's interest in computer crime and
the interests and abilities of the States to proscribe
and punish such offenses.

17 Senate Report 99-432, 1986 U.S.C.C.A.N. 2479, 2482. Based on
18 this passage, this Court seemed to suggest that it felt obliged
19 to undertake an independent review to determine whether "the
20 crime here [is] interstate in nature." (9/23/08 RT 5).

21 The passage cited by the Court does not render appropriate
22 an independent judicial assessment of federalism concerns as a
23 prerequisite to the exercise of jurisdiction.⁵ This passage

24

25 ⁵A review of crimes not covered by Section 1030(a)(2)(c)
26 demonstrates that this compromise was not insignificant. At the
27 time of the instant offense, for example, Section 1030(a)(2)(c)
did not cover crimes that did not involve an interstate
communication or a "protected computer." Accordingly, a burglar

28

1 merely explains why Congress adopted one of the jurisdictional
2 requirements it placed in the statute, namely, that conduct
3 involve an interstate communication. Once this requirement is
4 pleaded and proved, jurisdiction is established, and a court has
5 no authority to itself weigh federalism concerns in assessing
6 whether it believes the crimes as a whole is sufficiently federal
7 in nature. See Dickson, 816 F.2d 751.⁶

8 The judicial analysis of federalism issues seemingly
9

10 who stole a laptop, an employee who stole trade secrets from a
11 stand alone computer not connected to the Internet, or a
12 hacker/identity thief who accomplished his crime without
13 utilizing an interstate communication all could not be charged
under Section 1030(a)(2)(c), although they might be subject to
liability under some other law.

14 ⁶The Court's focus on Congress' statements in connection
15 with the first 1986 amendment to Section 1030 also risks
overstating Congress' concerns for federalism. Just six years
16 later, Congress greatly expanded the scope of Section 1030 to
cover all computers used in interstate commerce or communication.
17 In doing so, Congress explicitly stated that it sought to
maximize federal law enforcement authority:

18 It is the intent of the legislation to exercise the
19 full extent of the powers of Congress under the
commerce clause of the United States Constitution, art.
20 I, sec. 8, to prohibit forms of computer abuse which
arise in connection with, and have a significant effect
upon, interstate or foreign commerce.

21 S. Rep. 101-544, available at 1990 WL 201793. Moreover, on
22 September 26, 2008, the President signed into law the Former
Vice Presidents Protection Act, which amended Section 1030
23 to strike the requirement that information be obtained
through an interstate communication. See Himes v. Thompson,
24 336 F.3d 848, 860 (9th Cir. 2003) ("Subsequent amendments .
. . . reinforce this point"); United States v. Andrino-
25 Carrillo, 63 F.3d 922 (9th Cir. 2002) ("Although we
26 recognize that subsequent amendments are not necessarily a
reliable indicator of congressional intent, they do confirm
27 the conclusions we already reached after an analysis of the
statutory history.").

1 contemplated by the Court also would raise serious separation of
2 powers concerns. "Charging decisions are primarily a matter of
3 discretion for the prosecution, the representatives of the
4 executive branch of government, who 'are not mere servants of the
5 judiciary.'" United States v. Robertson, 45 F.3d 1423, 1437 (10th
6 Cir. 1995) (citing United States v. Miller, 722 F.2d 562, 564
7 (9th Cir. 1983)). This principle is also established by the
8 Federal Rules of Criminal Procedure. If a trial court were free
9 to dismiss a criminal case over which there was proper
10 jurisdiction based on a conclusion that the case was "too local,"
11 charging authority properly reserved to the Executive Branch
12 would be improperly infringed by the Judiciary.

13 The Court's federalism concerns appear to be rooted in the
14 fact that the government will prove that the purpose of
15 defendant's conduct in this case was to further a tortious act on
16 a victim in the same state as defendant. (9/23/08 RT 4). This
17 proof, however, does not affect the jurisdictional element.⁷
18 That jurisdictional element is unambiguous and requires that
19 defendant's conduct involve an interstate or foreign
20 communication based on Congress' stated determination that such
21 conduct was sufficiently "interstate in nature" to address
22

23
24 ⁷Moreover, the relevant section of the statute providing for
25 increased punishment makes clear that it does not require
26 interstate conduct, instead expansively encompassing "any
27 criminal or tortious act in violation of the . . . laws . . . of
any state. 18 U.S.C. § 1030(c)(2)(B)(ii). Thus, there is no
basis for the Court's suggestion that "the tort itself would have
to concern the interstate or foreign theft of information."
(9/23/08 RT 22).

1 federalism concerns. Greyhound Corp. v. Mt. Hood Stages, Inc.,
2 437 U.S. 322, 330 (1978) (The "starting point in every case
3 involving construction of a statute is the language
4 itself") (internal quotation marks omitted); McCarthy v. Bronson,
5 500 U.S. 136, 139 (1991) ("In ascertaining the plain meaning of a
6 statute, the court must look to the particular statutory language
7 at issue, as well as the language and design of the statute as a
8 whole.") (quotation marks and brackets omitted).

9 In any event, even if this Court were free to go beyond the
10 unambiguous jurisdictional element, the facts of this case
11 demonstrate that it involves precisely the kind of crime that is
12 appropriately addressed by federal law. Although defendant's
13 conduct was undertaken to harass a juvenile victim in her own
14 state, defendant did so by means of interstate communications.
15 United States v. Patterson, 314 F.2d 491, 493-94 (7th Cir. 1963)
16 (interstate transportation of dentures made by unauthorized
17 persons "constitutionally unchallengeable"). Additionally,
18 defendant did so by accessing a computer owned by a corporation
19 in another state without authorization and in excess of
20 authorization. Computer Crimes, American Criminal Law Journal
21 (2007) (noting obstacles to state law enforcement). Finally,
22 defendant's conduct violated rules established to ensure the
23 safety of social networking, an increasingly important method of
24 nationwide communication operated by a business with a
25 substantial effect on interstate and foreign commerce. See,
26 e.g., Hines v. Davidowitz, 312 U.S. 52 (1941) (relying on need
27
28

1 for national uniformity in immigration law). Thus, the instant
2 offense was accomplished through channels of interstate commerce,
3 affected entities in other states, and influenced an industry
4 with a substantial effect on interstate and foreign commerce --
5 all factors demonstrating that the application of federal law is
6 appropriate.⁸

7 B. THE CONDUCT AT ISSUE FALLS WITHIN THE MEANING OF
8 SECTION 1030(a)(2)(c) BECAUSE THE STATUE PROHIBITS MORE THAN
9 SIMPLE THEFT

9 The Court also seemed to question whether the conduct at
10 issue in the case, namely, obtaining information about M.T.M.
11 that would be used to torment her, fell within the scope of
12 Section 1030(a)(2)(c). In doing so, the Court questioned whether
13 Section 1030(a)(2)(c) prohibited only "theft" of information.
14 (9/23/08 RT 4). In fact, Section 1030(a)(2)(c) does more than
15 prohibit theft. But even if it only criminalized "theft," the
16 conduct at issue in this matter involved theft in that it
17 included the misappropriation of information by fraud.

18
19 ⁸To the extent that the Court is concerned that
20 technological developments may result in Section 1030's scope
21 expanding, that trend does not justify cabining the scope of
22 Section 1030. United States v. Mitra, 405 F.3d 492 (7th Cir.
23 2005), is instructive. In that case, the Seventh Circuit
24 rejected a defendant's attempt to limit the scope of Section 1030
25 on policy grounds based on an argument that Section 1030 could
26 not reach his disruption of a municipal computer-based radio
27 system because Congress could not have thought such a system was
28 a "computer" covered by the statute. Id. at 495. In rejecting
29 defendant's argument, the court observed that "Section 1030 is
30 general." Id. It noted that as technology developed, the
31 effective scope of the statute would grow. Id. It nonetheless
32 held that while the expansion of the statute might prompt
33 Congress to amend the statute, technological development "did not
34 authorize the judiciary to give the existing version less
35 coverage than its language portends." Id.

1 Accordingly, a prosecution would be appropriate even under such a
2 confined construction of 1030(a)(2)(c).

3 1. The Plain Terms of the Statute, the Legislative
4 History, and Cases Construing Section 1030 Demonstrate
5 that Section 1030(a)(2)(c) Prohibits More than Theft

6 "Statutory interpretation begins with the plain language of
7 the statute." K & N Engineering, Inc. v. Bulat, 510 F.3d 1079,
8 1081 (9th Cir. 2007); United States v. Hanousek, 176 F.3d 1116,
9 1120 (9th Cir. 1999). The "cardinal canon" of statutory
10 interpretation is "that courts must presume that a legislature
11 says in a statute what it means and means in a statute what it
12 says there." Connecticut Nat'l Bank v. Germain, 503 U.S. 249,
13 253-54 (1992). As a result, courts must construe statutes so
14 that "no clause, sentence, or word shall be superfluous, void or
15 insignificant." United States v. Ballinger, 395 F.3d 1218, 1236
16 (11th Cir. 2005).

17 Here, the statute provides in its relevant part that whoever
18 "intentionally accesses a computer without authorization or
19 exceeds authorized access, and thereby obtains . . . information
20 from any protected computer if the conduct involved an interstate
21 or foreign communication" shall be guilty of a federal crime.
22 18 U.S.C. § 1030(a)(2). The statute does not use the word
23 "theft" nor does it require that information be "stolen."
24 Rather, it proscribes "obtain[ing] . . . information" through
25 unauthorized access and in excess of authorization. Had Congress
26 opted to prohibit only theft or stealing, it could have done so
27 explicitly as it has throughout Title 18. See, e.g., 18 U.S.C.

1 § 641 ("Whoever embezzles, steals, purloins, or knowingly
2 converts to his use any . . . thing of value of the United
3 States"); 18 U.S.C. § 668 (prohibiting "steal[ing]" from a museum
4 any object of cultural heritage); 18 U.S.C. § 659 (prohibiting
5 "embezzl[ing], steal[ing], or unlawfully tak[ing]" goods or
6 chattels from certain carriers); 18 U.S.C. § 657 (prohibiting
7 "embezzl[ing], abstract[ing], and purloin[ing]" funds of credit
8 institutions) ; 18 U.S.C. § 669 (prohibiting "embezzl[ing],
9 steal[ing] . . . or convert[ing]" funds belonging to a health
10 care benefit program); 18 U.S.C. § 665 (prohibiting
11 "embezzl[ement], . . . misappli[cation], steal[ing], or
12 obtain[ing] by fraud" money from a Job Training program).
13 Congress' decision not to use language of this type makes clear
14 its intent to reach conduct beyond "theft" or "stealing."

15 The legislative history further suggests that the statute
16 was not intended only to prohibit theft.⁹ As explained in the
17 government's prior filings, the legislative history demonstrates
18 Congress' intent that Section 1030 be available to be used in a
19 fluid fashion to address new computer crimes as they emerged.
20 Consistent with this intent, as time has gone on, Congress has

21

22
23 ⁹ As explained in the government's prior filings, the Court
24 need not look to the legislative history given the lack of
25 ambiguity in the statutory language. See Whitfield v. United
26 States, 543 U.S. 209, 215 (2005) ("Because the meaning of [the
27 statute's] text is plain and unambiguous, we need not accept
petitioners' invitation to consider the legislative history.");
Tennessee Valley Authority v. Hill, 437 U.S. 153, 184 n.29 (1978)
("When confronted with a statute which is plain and unambiguous
on its face, [courts] ordinarily do not look to legislative
history as a guide to its meaning").

28

1 continually broadened the scope and coverage of the section.
2 See Pacific Aerospace & Electronics, Inc. v. Taylor, 295 F.
3 Supp.2d 1188, 1195 (E.D. Wash. 2003) ("Congress has . . .
4 continuously broadened the scope and coverage of the CFAA since
5 its original enactment in 1984. And no doubt as new forms of
6 computer crimes emerge, the CFAA will continue its evolution as
7 courts construe and apply particular provisions of the
8 statute."); In re AOL, Inc. Version 5.0 Software Litig., 168 F.
9 Supp.2d 1359, 1374 (S.D. Fla. 2001) (noting that "the CFAA has
10 been increasingly broadened by Congress"); United States v.
11 Middleton, 231 F.3d 1207, 1212 (9th Cir. 2000) (relying on the
12 statute's "purpose and legislative history" to conclude it
13 covered more than what definition of loss provided for); P.C.
14 Yonkers, Inc. v Celebrations the Party and Seasonal Superstore,
15 LLC, 428 F.3d 504, 510 (3d Cir. 2005) (acknowledging that while
16 the majority of CFAA cases still involve "classic" hacking
17 activities, the scope of the CFAA's reach "has been expanded over
18 the last two decades").¹⁰

19 Rather than focus only on theft, Congress emphasized the
20 privacy protection aspects of Section 1030(a)(2)(c). S. Rep 99-

21
22
23 ¹⁰As a result, the fact that the application of the statute
24 in this case was not contemplated ten years of ago is of no
25 moment. As previously noted in other pleadings, "the fact that a
26 statute can be applied in situations not expressly anticipated by
27 Congress does not demonstrate ambiguity. It demonstrates
28 breadth." Pennsylvania Dept. of Corrections v. Yeskey, 524 U.S.
206, 212 (1998) (quoting Sedima, S.P.L.R. v. Imrex Co., 473 U.S.
479, 499 (1985)). The statute's evolution and application were
inevitable given the development of technology and the evolution
of cyber crime.

1 432, 1986 U.S.C.C.A.N. 2479, 2485 ("Because the premise of this
2 subsection is privacy protection, the Committee wishes to make
3 clear that 'obtaining information' in this context includes mere
4 observation of the data"). Congress has also emphasized the need
5 to maintain the confidentiality and integrity of computer
6 systems. H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3707
7 (observing that statute did not "extend to normal and customary
8 business procedures and information usage" but imposed sanctions
9 on hackers and others who "access[ed] computers without
10 authorization"); S. Rep. 99-432, 1986 U.S.C.C.A.N. 2479, 2481
11 (describing how technological advancement has "created a new type
12 of criminal -- one who uses computers to steal, to defraud, and
13 to abuse the property of others"). In connection with the 1996
14 amendments to Section 1030, Congress stated that a goal of
15 Section 1030(a)(2)(c) was to protect against theft. S. Rep. 104-
16 357, available at 1996 WL 492169 at *7-8 ("The proposed
17 subsection 1030(a)(2)(c) is intended to protect against the
18 interstate or foreign theft of information by computer.") Almost
19 immediately thereafter, however, Congress stated that the "crux"
20 of the offense was "the abuse of a computer to obtain the
21 information," and went on to suggest that it sought to protect
22 against harms other than simple theft. Id. ("The seriousness of
23 a breach in confidentiality depends, in considerable part, on the
24 value of the information taken, or on what is planned for the
25 information after it is obtained.").

1 2. The CCIPS Report Cited by the Court Does Not Provide A
2 Basis for Limiting the Statute to Theft

3 At the September 23, 2008, hearing, the Court cited a report
4 by CCIPS and suggested that that document demonstrated that
5 Section 1030(a)(2)(c) prohibited only "theft." (9/23/08 RT 3).
6 The government respectfully disagrees.

7 The Court's focus on a statement in the CCIPS report
8 regarding the design of Section 1030(a)(2)(c) to protect against
9 theft takes the passage out of context. Read as a whole, the
10 report correctly recognizes that Section 1030 was designed to
11 ensure the confidentiality and integrity of data. (Report at 3;
12 see also id. ("In most cases, a single point of reference -- The
13 Computer Fraud and Abuse Act, 18 U.S.C. § 1030 is provided for
14 investigators, prosecutors, and legislators as they attempt to
15 determine whether a particular abuse of new technology is covered
16 under federal criminal law.") Indeed, the report explicitly
17 states at the beginning of its analysis of Section 1030(a)(2):

18 Section (a)(2) is, in the truest sense, a provision designed
19 to protect the confidentiality of computer data.

20 Report at 4 (emphasis added). Moreover, the examples cited in
21 the report show Congress' intent under Section 1030(a)(2)(c) was
22 something broader than simply prosecuting theft. Report at 5-6
23 (citing examples of misusing computers to obtain criminal history
24 information, logistics information, and tax returns). In
25 particular, the report explained that obtaining publically
26 available information can constitute a violation of Section
27 1030(a)(2)(c), a legally impossible situation if the statute only

1 prohibited the "theft" of information. Id. ("to the extent that
2 the information obtained is or should be available, it should be
3 obtained through legal means (e.g., public sources or FOIA)").
4 Likewise, after the passage cited by the Court, the report makes
5 explicit reference to the misuse -- rather than the theft -- of
6 information. Report at 6 (misuse by insiders). Accordingly, the
7 report should not be read as suggesting Section 1030(a)(2)(c)
8 prohibits "theft" only.

9 Even if the CCIPS report were properly read as suggesting
10 that Section 1030(a)(2)(c) prohibits only "theft," that statement
11 of opinion would not be entitled to deference in interpreting the
12 statute. Crandon v. United States, 494 U.S. 152, 177 (1990)
13 (Scalia, J. concurring) (members of the Supreme Court "have never
14 thought that the interpretation of those charged with prosecuting
15 criminal statutes is entitled to deference"). This is not a
16 circumstance where an agency construction of its own regulations
17 is entitled to deference. Chevron v. National Resources Defense
18 Counsel, 467 U.S. 837 (1984). Courts have recognized that even
19 formal opinion memoranda by an attorney general are not binding
20 on the courts. See Welch, 327 F.3d at 1093 (citing Norman J.
21 Singer, Sutherland Statutory Construction § 5A:11 at 498-99 (6th
22 ed. 2002) (noting that "courts have quite uniformly held that the
23 judiciary is not bound by an attorney general's opinion"); United
24 States v. Pievinazi, 23 F.3d 670, 683 (2d Cir. 1994)
25 ("[E]xecutive branch policy judgments about the desirability
26 certain types of prosecutions . . . are not guided solely by the
27
28

1 language of the statute). The CCIPS report cited by the Court
2 does not equate to a formal attorney general opinion, but even if
3 it did, it could not be relied on as a basis for limiting the
4 statute in a way inconsistent with both its language and
5 legislative history, both of which indicate that Section 1030 is
6 not limited only to theft of information.

7 3. The Conduct at Issue Did Involve Theft

8 Even if the Court were to conclude that
9 Section 1030(a)(2)(c) prohibits only "theft" of information, such
10 a construction would cover the instant prosecution. "Theft"
11 includes obtaining something by deception or false pretext.
12 United States v. Corona-Sanchez, 234 F.3d 449, 454-55 (9th Cir.
13 2000) (defining "theft offense" and including notion of theft by
14 deception); People v. Miller, 81 Cal. App. 4th 1427, 1445-47
15 (2000) (false pretext of romance for fraud); Hoovel v. State, 69
16 S.W.2d 104, 107 (Tex Crim. App. 1934) (theft by false pretext).
17 The government expects the evidence at trial will show that
18 defendant and her co-conspirators were only able to obtain
19 information from the MySpace servers through fraud -- both on
20 MySpace and the minor. As laid out in the indictment, defendant
21 and her co-conspirators used both a false identity and false
22 promises to obtain access to the MySpace servers. Moreover, the
23 scheme itself was predicated on the idea that only by posing as a
24 boy on MySpace would defendant and her co-conspirators be able to
25 obtain information about victim M.T.M. over the MySpace servers.
26 During the scheme, defendant and her co-conspirators flirted with

1 victim M.T.M. so that they could obtain information about her
2 that they would use to harass and abuse her. The government
3 expects the evidence at trial will show that but for the fraud
4 and deceit, defendant and her co-schemers would not have obtained
5 access to M.T.M.'s personal page or been able to communicate with
6 her. At the very least, the question whether the conduct at
7 issue constituted "theft" is properly a jury question.

8 C. INFORMATION ABOUT M.T.M. THAT WAS OBTAINED THROUGH THE
9 MYSPACE SERVERS IS "INFORMATION" UNDER SECTION 1030(a)(2)(C)

10 Finally, the Court appeared to express concern whether the
11 data about victim M.T.M. at issue in the case was "information"
12 within the meaning of Section 1030(a)(2)(C). (9/23/08 RT 21)
13 ("what is the information that is interstate").¹¹ As explained
14 previously, the government expects the evidence will show that
15 defendant obtained data from M.T.M.'s page and through MySpace
16 communication services regarding M.T.M.'s feelings, hopes, and
17 desires. This information falls squarely within Section 1030 and
18 the plain meaning of "information."

19 The statutory language suggests that Congress did not seek a
20 limitation on the type of "information" that may be improperly
21 obtained under 18 U.S.C. § 1030(a)(2)(C). Elsewhere, Congress

22 ¹¹As a preliminary matter, the statute requires only that the
23 defendant access a computer and thereby obtain information and
24 that the conduct, that is the access, "involve" an interstate
25 communication. See, e.g., Ninth Circuit Model Jury Instruction
26 No. 8.79. Section 1030(a)(2)(C) does not require that the
27 information be obtained through an interstate communication
28 although the government expects that the evidence will show that
information obtained itself somehow must have an interstate
component.

1 identified specialized information, namely, (1) classified
2 information, see 18 U.S.C. 1030(a); and (2) information from a
3 financial record, see 18 U.S.C. § 1030(a)(2)(A). Congress
4 therefore demonstrated its ability to define a limited subset of
5 information when it intended to do so. By implication, Congress
6 did not intend to limit Section 1030(a)(2)(C) to some particular
7 types of information. See Shurgard Storage Centers v. Safeguard
8 Self Storage, 119 F. Supp.2d 1121, 1125 (W.D. Wash. 2000)
9 ("Nowhere in the language of 1030(a)(2)(C) is the scope limited
10 to entities with broad privacy repercussions. . . . This
11 language is unambiguous.")¹²

12 Nor does the legislative history suggest a limited scope for
13 "information" under Section 1030(a)(2)(C). Congress has
14 recognized that the "information" obtained can have no value and
15 can be "misused" in a variety of ways:

16 The seriousness of a breach in confidentiality depends,
17 in considerable part, on the value of the information taken,
18 or on what is planned or the information after it is
19 obtained. Thus, the statutory penalties are structured to
20 provide that obtaining information of minimal value is only
21 a misdemeanor, but obtaining valuable information, or
22 misusing information in other more serious ways, is a
23 felony.

22 ¹²Likewise, the original version of the statute only
23 protected certain types of information, namely, (1) information
24 protected by the Right to Financial Right to Privacy Act,
25 12 U.S.C. § 3401 or the Fair Credit Reporting Act, 15 U.S.C.
26 § 1618; and (2) information on government computers. 18 U.S.C.
27 § 1030 (1985). Because Congress could have restricted the scope
of "information" under Section 1030(a)(2)(C) as it did in the
original version of the statute, its decision not to limit the
scope of "information" under Section 1030(a)(2)(C) suggests that
any and all types of information may be obtained in violation of
the statute.

1 The sentencing scheme for Section 1030(a)(2) is part of
2 a broader effort to ensure that sentences for section 1030
3 violations adequately reflect the nature of the offense.
4 Thus, under the bill, the harshest penalties are reserved
5 for those who obtain classified information that could be
6 used to injure the United States or assist a foreign state.
7 Those who improperly use computers to obtain other types of
8 information - such as financial records, non-classified
9 Government information, and information of nominal value
10 from private individuals or companies - face only
11 misdemeanor penalties, unless the information is used for
12 commercial advantage, private financial gain or to commit
13 any criminal or tortious act.

14 S. Rep. 104-357, 1996 WL 492169 at *8. This recognition that
15 there are numerous non-commercial types of information that can
16 be abused in numerous ways -- including tortious ones --
17 underscores that the information at issue in this case was
18 covered by Section 1030(a)(2)(C).

19 Finally, courts have construed "information" broadly and
20 held that a variety of things can constitute information under
21 the Computer Fraud and Abuse Act. See EF Cultural Travel BV v.
22 Zefer Corp., 318 F.3d 58 (1st Cir. 2003) (publically available
23 pricing information from a website obtained using a "scraper");
24 Healthcare Advocates v. Harding, Earley, Follmer & Frailey, 497
25 F. Supp. 2d 627 (E.D. Pa. 2007) ("Viewing material on a computer
26 screen constitutes 'obtaining' information under the CFAA."); Keq
27 Tech. Inc. v. Laimer, 436 F. Supp. 2d 1364 (N.D. Ga. 2006) (files
28 "containing KEG's customer lists, financial information, design
drawings, product orders, profit margins, pricing information,
and catalogue production elements and layout."); Southwest
Airlines v. Farechase, Inc., 318 F. Supp. 2d 435 (N. D. Tex.
2004) (plaintiff could state a claim based on scheduling and fare

1 information available on website); I.M.S. Inquiry Management Sys.
2 v. Berkshire Inf. Sys., 307 F. Supp. 2d 521 (S.D.N.Y. 2001)
3 (plaintiff could state claim based on competitors accessing of
4 information available on website for plaintiff's customers);
5 Credentials Plus v. Calderone, 230 F. Supp. 2d 890 (N.D. Ind.
6 2002) (obtaining information from unauthorized client emails
7 sufficient to state a claim); America Online v. National Health
8 Care Discount, 174 F. Supp. 2d 890 (N.D. Iowa 2001) (mass mailers
9 sent "information"); In re Doubleclick Privacy Litigation, 154 F.
10 Supp. 2d 497 (S.D.N.Y. 2001) (assuming, but not deciding that
11 demographic information collected by cookies is "information");
12 Register.com v. Verio, 126 F. Supp. 2d 238 (S.D.N.Y. 2000)
13 ("scraping" publically available information); Shurgard Storage
14 Centers, 119 F. Supp.2d at 1125 ("Nowhere in language of
15 1030(a)(2)(C) is the scope limited to entities with broad privacy
16 repercussions. The statute simply prohibits the obtaining of
17 information from any protected computer if the conduct involved
18 an interstate or foreign communication. . . . This language is
19 unambiguous. There is no reasonable implication in any of these
20 terms that suggests only the computers of certain industries are
21 protected. Therefore, the defendant's argument on this issue is
22 unpersuasive."). Courts have also explicitly recognized that the
23 information obtained need not have any value at all. See United
24 States v. Willis, 476 F.3d 1121, 1126 (10th Cir. 2007) ("The
25 defendant need not know that the value of the information
26 obtained has a particular value, or any value, for that
27
28

1 matter.").

2 Accordingly, although the government acknowledges that in
3 most instances, cases under Section 1030(a)(2) will involve
4 information having commercial value, this is not a statutory
5 requirement, and the information need not have such value. Data
6 obtained about victim M.T.M., both from her personal page and
7 through other communications over the MySpace communication
8 services, falls within the broad scope of "information" that may
9 be obtained through an unauthorized access within the meaning of
10 Section 1030(a)(2)(C).

11 III

12 CONCLUSION

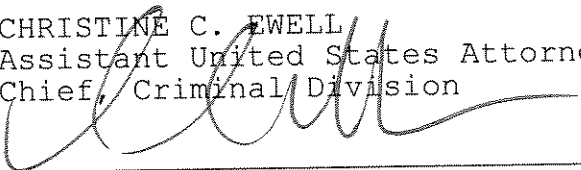
13 For the foregoing reasons, defendant's motion to dismiss for
14 vagueness should be denied.

15 Dated: October 6, 2008

16 Respectfully submitted,

17 THOMAS P. O'BRIEN
United States Attorney

18 CHRISTINE C. EWELL
19 Assistant United States Attorney
Chief, Criminal Division

20 
21 MARK C. KRAUSE
Assistant United States Attorney

22 Attorneys for Plaintiff
23 United States of America