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

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, Plaintiff, vs. LORI DREW Defendant.	Case No. CR-08-0582-GW REPLY TO GOVERNMENT'S RESPONSE TO PRE-TRIAL CONFERENCE ORDER

Comes now counsel for defendant Lori Drew, and replies to the response filed by the government to the Court's pre-trial conference order.

Dated: Oct. 20, 2008

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

Other Authorities

A. The Indictment Must Be Dismissed Because the Conduct Alleged Does Not Violate 18 U.S.C. § 1030(a)(2)(C).

The Government's Response to the Court's September 23 Inquiry focuses on several matters that are not in dispute. First, the government argues that 18 U.S.C. § 1030 is within the commerce clause power. Second, the government argues that courts cannot exercise discretion to dismiss indictments simply because judges feel a case is "too local." We agree with both of these positions. At the same time, we understand the Court was interested in a different question: Whether the indictment is sufficient as a matter of law given the statute *as it exists*.

The difference is essential. While courts lack the power to dismiss an indictment because a case "feels" too local, an indictment must be dismissed if it fails to allege facts that would constitute the crime charged. That is just as true when the indictment fails to allege facts that satisfy a necessary jurisdictional requirement such as an interstate commerce requirement. *See e, g., United States v. Havelock*, 560 F. Supp.2d 828, 834 (D. Ariz. 2008) (dismissing indictment for intrastate gun charge); *United States v. LaFleur*, 669 F. Supp. 1029, 1035 (D. Nev. 1987) (dismissing interstate racketeering count). *See also United States v. Oxendine*, 531 F.2d 957, 959 (9th Cir. 1976) (per curiam) (overturning conviction for failure to establish requirement of interstate communication).

The allegations in the indictment do not satisfy the statute as a matter of law. Under *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), the government must do more than simply allege that some Terms of Service were violated over an interstate network.

"Not all deceit vitiates consent." *Id.* at 1073. Instead, the indictment must allege that MySpace.com was actually tricked as to "the essential character of the act" that the MySpace computers had consented to when the computers allowed the defendant and others to use its services. *Id.* at 1073. If the allegations in the indictment merely suggest that MySpace.com was induced into providing access by misrepresentation as to "some collateral matter which merely operates as an inducement," such misrepresentation cannot make the access unauthorized and the indictment is insufficient as a matter of law. *See id*.

Put another way, the government must prove that the victim was tricked as to *what* it was consenting to rather than *why* it was consenting. *See Boro v. Superior Court*, 163 Cal. App.3d 1224, 1228-31 (Cal. App. 1 Dist. 1985) (fraud that induces victim to act does not make act without consent so long as victim knew the nature of the act); Rollins M. Perkins & Ronald N. Boyce, Criminal Law 1075-84 (3d ed. 1982) (distinguishing consent obtained by "fraud in the factum," which vitiates consent, from consent obtained by "fraud in the inducement," which does not).

The fatal flaw in the government's case is that MySpace knew perfectly well at all times exactly what it was doing. MySpace knew that it was providing an account to users who might or might not comply with the Terms of Service. Most users violate Terms of Service frequently, as MySpace is surely aware. As a result, MySpace was never tricked into thinking that it was providing access to a user that would comply strictly with all of MySpace's Terms of Service.

Assuming the government can prove the facts alleged in the indictment, those facts amount to a breach of contract. MySpace was induced to provide an account to the defendant or others based on a false representation that they would comply with the Terms of Service, breaching the Terms of the service contract. This is at most a misrepresentation that induced reliance, however, not a misrepresentation as to what service was being provided.

As a result, the access was not "without authorization" or in "excess of authorization" under Ninth Circuit precedent. *See Theofel*, 359 F.3d at 1073.

What occurred was a breach of contract with minimal damages, not an interstate theft that constitutes a federal crime. *See SecureInfo Corp. v. Telos Corp.*, 387 F. Supp.2d 593, 609 (E.D. Va. 2005) (holding that access to a computer in violation of license agreement does not make access without authorization or in excess of authorization). It was an intended use, and therefore not criminal. *See United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (noting that courts "typically analyze[] the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use").

B. The Legislative History of the Recent Amendment to 18 U.S.C . § 1030(a)(2)(C) Offers Additional Evidence that the Statute Does Not Apply When the Defendant and the Victim Are in the Same State.

The United States also argues that 18 U.S.C. § 1030(a)(2)(C) does not require that an interstate communication must be obtained. According to the government, an *intra*state communication is sufficient so long as some aspect of the defendant's conduct

involves some kind of interstate communication. *See* Govt's Response at 21, n.11. The Government cites a very recent amendment to § 1030 as evidence. The Vice President's Protection Act was passed into law on September 26, 2008, and it eliminated the requirement that the government must prove that an interstate communication was obtained. *See* Govt's Response at 2 n.2, 10 n.6. According to the Government, Congress's amendment to § 1030 establishes that the interstate requirement in the statute is minimal. By amending the statute, the Government suggests, Congress simply reaffirmed that it never intended to require the government to prove that an interstate communication was obtained. *See* Govt's Response at 10 n.6.

This interpretation would come as quite a surprise to the members of the United States Congress who pushed for the recent amendment with the support of the U.S. Department of Justice. Congress pressed for the elimination of the interstate commerce requirement because influential members decided to change the law: Congress's express goal was to change the law so § 1030(a)(2)(C) could be used in cases, like this one, where a defendant and the victim were in the same state. Because the government has properly charged the defendant under the earlier version of the statute, before the recent changes, the statute as charged must be construed as applying only to thefts from a victim in one state to a defendant in another.

The changes to § 1030 that passed on September 26 began life as the *Identity Theft Enforcement and Restitution Act*, S. 2168, introduced in the Senate by Vermont Senator Patrick Leahy on October 16, 2007. Section 4 of the original bill eliminated the

interstate requirement for 18 U.S.C. § 1030(a)(2)(C) offenses.[1] When Senator Leahy introduced the Act in the Senate, he explained that the purpose of the elimination of the interstate requirement in §1030(a)(2)(C) was precisely to allow prosecutions when the defendant and the victim are located in the same state, which was then not covered by the statute. *See Leahy, Specter Introduce Bill To Add And Toughen Penalties For Identity Theft And Fraud*, October 16, 2007, available at http://leahy.senate.gov/press/200710/101607b.html (emphasis added). According to Senator Leahy, eliminating the interstate requirement in §1030(a)(2)(C) would:

> Eliminate the prosecutorial requirement that sensitive identity information must have been stolen through an interstate or foreign communication and instead focuses on whether the victim's computer is used in interstate or foreign commerce, *allowing for the prosecutions of cases in which both the identify thief's computer and the victim's computer are located in the same state[.]*

Id. (emphasis added).

This amendment passed the Senate in November 2007 but stalled in the House of Representatives. In July 2008, Senator Leahy

---

[1] The text of the original bill is available at http://www.govtrack.us/congress/bill.xpd?bill=s110-2168. Section 4 was titled "ENSURING JURISDICTION OVER THE THEFT OF SENSITIVE IDENTITY INFORMATION," and it states: "Section 1030(a)(2)(C) of title 18, United States Code, is amended by striking 'if the conduct involved an interstate or foreign communication'."

"attached provisions of the anti-cyber crime bill to a House-passed bill to extend Secret Service protection to former Vice Presidents." *Leahy-Authored Anti-Cyber Crime Provisions Set To Become Law*, Sept 15, 2008, *available at* http://leahy.senate.gov/press/200809/091508b.html. The cybercrime amendments became Title II of the Former Vice Presidents Protection Act, H.R. 5938, and that Act passed into law on September 26, 2008. The removal of the interstate commerce requirement of § 1030(a)(2)(C) became § 203 of the law, titled "ENSURING JURISDICTION OVER THE THEFT OF SENSITIVE IDENTITY INFORMATION."

The legislative history directly contradicts the Government's interpretation. Although the Government imagines that Congress amended § 1030(a)(2)(C) to reaffirm that the statute was always meant to be read broadly, Senator Leahy pushed this legislation precisely to permit the kind of prosecution found in this case: the goal was to "allow[] for the prosecutions of cases in which both the identify thief's computer and the victim's computer are located in the same state[.]" As Senator Leahy's statement reflects, such prosecutions were not permitted under the version of § 1030 in place in the period covered by the indictment.

Indeed, even the Justice Department's own guidance to its prosecutors on the meaning of § 1030(a)(2)(C) contradicts the broad claims made by the Government in this case. The Justice Department's manual on computer crimes explains:

> Note that a violation of this subsection must involve an actual interstate or foreign communication and not merely the use of an interstate communication mechanism, as other parts

> of the CFAA allow. The intent of this subsection is to protect against the interstate or foreign theft of information by computer, not to give federal jurisdiction over all circumstances in which someone unlawfully obtains information via a computer. *See* S. Rep. No 104-357. Therefore, using the Internet or connecting by telephone to a network may not be sufficient to charge a violation of this subsection where there is no evidence that the victim computer was accessed using some type of interstate or foreign communication.

United States Department of Justice, Prosecuting Computer Crimes Manual, Ch.1, Part C.6, *available at* http://www.cybercrime.gov/ccmanual/01ccma.html#tocC.6.

The interpretation of § 1030(a)(2)(C) that the Government has offered in this case is contrary to what the Justice Department has said and contrary to what Congress has long thought the statute meant. It should be rejected.

C. Prosecutions Under 18 U.S.C. § 1030(a)(2)(C) Require Proof of A Theft, and There Was No Theft In This Case.

The government argues also that 18 U.S.C. § 1030(a)(2) does not require proof of a theft. According to the government, any Term of Service violation plus any sort of information receipt – such as what any Internet user would receive when surfing the Internet – is sufficient. The Government's vision of the statute reveals a remarkable misunderstanding of the basic purpose and

scope of 18 U.S.C. § 1030(a)(2). To see the government's basic error, and to see why the indictment must be dismissed for failure to assert a theft, a review of the history of unauthorized access law and the structure of § 1030 is necessary.

18 U.S.C. § 1030 was enacted by Congress because Congress recognized the difficulties of prosecuting computer crimes using statutes designed for traditional property crimes. With traditional physical property, it was easy to identify when property was stolen, damaged, or destroyed. Property was stolen when it was taken away from its owner; property was damaged when it was physically altered; and property was destroyed when it was physically altered so much that it could not be used. This wasn't true with computer crimes, however. As a result, prosecutors and judges struggled to fit the new computer crimes into the traditional property crime statutes. *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L. Rev. 1596, 1607-1616 (2003) (discussing cases).

Specifically, the fit was a poor one because the physicality requirements of traditional criminal laws no longer made sense with data crimes. An Internet thief would break into a network and take data away without depriving the owner of the original copy. Although the data was "stolen" in the sense of taken from the owner, the owner was not actually deprived of the original when a copy was made. To use the common law term, there was no "asportation" of the original data. Similarly, an Internet vandal would alter valuable files but not alter the physical computer itself. Congress realized that it needed new statutes to apply

the traditional concepts of theft and damage in a virtual environment. *See id.*

The statute that Congress enacted, 18 U.S.C. § 1030, features seven distinct crimes found in §§ 1030(a)(1)-(7). Each of these seven crimes mirrors traditional offenses in the United States Code that predate Section 1030 and apply to the physical crimes committed with physical property. Section 1030(a)(1) punishes theft of classified information by computer; Section 1030(a)(2) punishes theft of interstate information; Section 1030(a)(3) prohibits trespass into a U.S. Government computer; Section 1030(a)(4) prohibits theft of information that furthers a fraud scheme; Section 1030(a)(5) prohibits damaging computer data; Section 1030(a)(6) prohibits computer password trafficking; and Section 1030(a)(7) prohibits extortionate threats to damage computers. Each statute has a physical-world cousin upon which the computer version is based.[2]

Section 1030(a)(2)(C) is the interstate theft prohibition in the statute. It prohibits breaking into a computer and taking information across state lines. Of course, given the then-existing conceptual problems with identifying when copied information is "property" that is "stolen," *see* Kerr, *supra*, at 1609-13, Congress studiously avoided using the words such as "theft" or "stolen" to describe the prohibited act. Instead,

---

[2] *See, e.g.,* 18 U.S.C. § 793 (theft of classified information, analogous to §1030(a)(1)); 18 U.S.C. § 641, § 2314 (theft of and transportation of property, analogous to § 1030(a)(2)); 18 U.S.C. § 1832 (trespass on to U.S. military property, analogous to § 1030(a)(3)); 18 U.S.C. § 1343 (wire fraud, analogous to § 1030(a)(4); 18 U.S.C. § 1361 (damage to property, analogous to § 1030(a)(5)); 18 U.S.C. § 1029 (password trafficking, analogous to §

Congress expressed the notion of interstate theft by requiring an intentional breaking in – that is, unauthorized access – followed by obtaining information.

The idea behind § 1030(a)(2)(C) was that a person who intentionally broke into a computer and retrieved interstate data had committed an interstate theft by breaking in to the other person's machine and taking (unlawfully obtaining) their confidential data. *See* S. Rep. 104-357, *available at* 1996 WL 492169 at *7-*8 ("The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information.") There was no requirement that the original data be actually removed from the original storage site, which was the conceptual difficulty with using traditional physical property theft laws. *See id.* (noting that "actual asportation" need not be proved). But the goal was for the new statute to be a theft statute, otherwise mirroring theft statutes in the physical world. As a result, the new § 1030(a)(2) would "ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected." S. Rep. No. 104-357, at *7, *available at* 1996 WL 492169.

With this understanding in place, it becomes clear that the authorities cited by the government support the view that some sort of theft is necessary to violate 18 U.S.C. § 1030(a)(2)(C). As the government notes, "Section (a)(2) is, in the truest sense, a provision designed to protect the confidentiality of computer data." *See* Govt's Response at 18. That is correct: A person who

---

1030(a)(6)); 18 U.S.C. § 875(d) (threat to damage property, analogous to § 1030(a)(7)).

steals data has breached the confidentiality of the data. Indeed, breaching confidentiality is what it means to "steal" in the case of electronic data. Theft of data brings the data into the possession of the thief who is not authorized to possess the data, breaching its confidentiality even though the original is not taken away. *See, e.g.,* 18 U.S.C. § 1832(a) (equating the theft of information with the unauthorized duplication of information in a statute that prohibits the theft of trade secrets).

Similarly, the government cites the passage of legislative history in which Congress stated that "[t]he seriousness of a breach of confidentiality depends in considerable part, on the value of the information taken, or on what is planned for the information after it is obtained." S. Rep. 104-357, available at 1996 WL 492169 at *7-*8. The Government claims that this shows that Congress "sought to protect against harm other than simple theft." Govt. Response at 17. But that is incorrect: This legislative history demonstrates that Congress sought to limit the statute to property that was "taken" – that is, stolen – and that Congress understood that the requirement the information must be "obtained" is the same as saying that it was "taken." *See also* § 203 of the Former Vice Presidents Protection Act, H.R. 5938 (enacted September 26, 2008) (titling an amendment to the jurisdictional scope of § 1030(a)(2)(C) as "ENSURING JURISDICTION OVER THE THEFT OF SENSITIVE IDENTITY INFORMATION.").

To be sure, the requirement that the Government must prove a theft has never before been a serious issue in § 1030(a)(2) prosecutions. That is because in the 24 years that § 1030 has existed, the Government has never before taken the position that

violations of Terms of Service can make an access "unauthorized" or "in excess of authorization." In the 1990s, the notion of such a prosecution was simply inconceivable to Congress or the Justice Department. At the time it was passed, §1030 was supposed to deal with hackers and employees who stole data from their employers. Congress added two levels of authorization to deal with the two problems. When outsider hackers broke in, they accessed the computers "without authorization." In contrast, when insider employees stole data from their employers, they "exceeded authorized access." *See United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) (discussing legislative history and the insider/outsider distinction).

In either case, the information "obtained" would *necessarily* be stolen under the traditional understanding of access without authorization and exceeding authorized access. By obtaining the data after breaking in, the information obtained would be a stolen copy. *See United States v. Farraj*, 142 F. Supp.2d 484 (S.D.N.Y. 2001) (unauthorized copy of trial plan for litigation treated as "stolen property"). The government is forced to argue that the statute does not require theft because its novel theory of authorization expands the statute so far that it could apply to many cases – such as this one – where no theft occurred. Any person who uses the Internet in any way that violates any Terms of Service will necessarily obtain data in *some* way. Surfing the web necessarily involves the receipt of data from the webserver

queried. 18 U.S.C. § 1030(a)(2) was never intended to cover anything remotely like that, however.[3]

There was no theft in this case. The information that was obtained about M.T.M. was freely offered by her. To the extent M.T.M. offered the information in reliance on false representations, the information is still not "stolen" because any false representation only related to the inducement for revealing the information, not the essential fact that the information was revealed. *See Theofel*, 359 F.3d at 1072-73. *See also Boro v. Superior Court*, 163 Cal. App.3d 1224, 1228-31 (Cal. App. 1st Dist. 1985) (fraud that induces victim to act does not make act without consent so long as victim knew the nature of the act). Because there was no theft, as required by the statute, the indictment must be dismissed.

D. The Computer Fraud and Abuse Act Does Not Punish Everything Bad on the Internet.

---

[3] It is true that some courts have taken a remarkably expansive interpretation of "without authorization" in the civil setting, a context far removed from that of criminal law. For example, in *Register.com v. Verio*, 126 F. Supp.2d 238 (S.D.N.Y. 2000), the mere fact that the plaintiff decided to bring a civil suit was considered enough to make the defendant's conduct without authorization. But these civil precedents have roamed far from the limited statute Congress intended, and they have been harshly and soundly criticized. *See, e.g., Lockheed Martin Corp. v. Speed*, 2006 WL 2683058 at *5-7 (M.D. Fla. 2006) (criticizing broad interpretation of the CFAA in civil cases). Further, the rule of lenity that applies in the criminal context counsels strongly against such a broad interpretation here. *See United States v.*

Finally, it is essential to correct the Government's broad misunderstanding of the Computer Fraud and Abuse Act. The Government treats this law as if it punishes everything bad that happens on the Internet. According to the Government, § 1030 is "available to be used in a fluid fashion to address new computer crimes as they emerge[]." Govt's Response at 15. It claims that "the fact that the application of the statute was not contemplated" in the past "is of no moment." *Id.* at 16 n.10. As "technology and the evolution of cyber crime" continue, the Government asserts, the statute must undergo "evolution." *Id*.

If the statute is to evolve, however, it is Congress that must direct the evolution. In our system of separated powers, the legislature determines the scope of criminal laws. Courts may not expand the scope of criminal statutes by judicial construction beyond what the legislature intended. As the Supreme Court stated in *United States v. Lanier*, 520 U.S. 259, 266 (1997), "due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." The Supreme Court explained the point in *Bouie v. City of Columbia*, 378 U.S. 347 (1964):

> [A]n unforeseeable judicial enlargement of a criminal statute, applied retroactively, operates precisely like an ex post facto law, such as Art. I, § 10, of the Constitution forbids. An ex post facto law has been defined by this Court as one

---

Lanier, 520 U.S. 259, 266 (1997) (noting the canon of strict construction of criminal statutes).

> 'that makes an action done before the passing of the law, and which was innocent when done, criminal; and punishes such action,' or 'that aggravates a crime, or makes it greater than it was, when committed.' Calder v. Bull, 3 Dall. 386, 390, 1 L.Ed. 648. If a . . .legislature is barred by the Ex Post Facto Clause from passing such a law, it must follow that a . . . Court is barred by the Due Process Clause from achieving precisely the same result by judicial construction. The fundamental principle that 'the required criminal law must have existed when the conduct in issue occurred,' Hall, General Principles of Criminal Law (2d ed. 1960), at 58-59, must apply to bar retroactive criminal prohibitions emanating from courts as well as from legislatures.

Id. at 353-54. For this reason, the Supreme Court has stressed that ambiguous criminal statutes must be construed *against* the government. *See United States v. Bass*, 404 U.S. 336, 347 (1971) (noting that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity").

Terms of Service have existed for many years. However, there is not one shred of evidence that Congress intended to make violations of Terms of Service a federal crime under 18 U.S.C. § 1030. The statute prohibits theft, not breach of a service contract. Despite many opportunities to do so in sympathetic cases, the Justice Department has never before tried to argue that violating Terms of Service amounts to a § 1030 offense. There was no way a citizen of the United States could know that the Justice Department might get creative, change course after 24 years, and

try such a theory. The Government proclaims that this is "of no moment" because the law is a "fluid" tool that it can "evolve" to punish what it believes is blameworthy. But the rule of lenity requires a narrow construction that gives fair notice to the public, not a broad construction that gives the government the power to punish whoever it likes.[4] *Bass*, 404 U.S. at 347-48.

If the Department of Justice wants to prosecute people for violating Terms of Service, its representatives should go to Congress and persuade Congress to pass such a law. Or at least they should try: It is hard to imagine Congress would agree to such a law given that everyone who uses the Internet routinely violates Terms of Service (members of Congress included). But the recent passage of the Former Vice Presidents Protection Act shows that Congress is eager to legislate in the area of computer crimes. Congress's door is wide open. If violations of Terms of Service are to become federal crimes, it should be Congress that makes the decision to criminalize them.

/

/

/

/

/

---

[4] The government relies on *United States v. Mitra*, 405 F.3d 492 (7th Cir. 2005), for the view that §1030 was intended to broaden as technology advances. But *Mitra* simply makes the obvious point that as society relies more on computers, the number of computers will grow and §1030 will become more significant. *Id*. at 495. That is true, but it has no relevance to this case. The government's theory of the case is expansive not because technology has advanced, but because the Government decided to prosecute an individual for conduct that has existed for many years and has never before been considered a federal crime.

E. Conclusion

For the above reasons, the defense continues to request dismissal of the instant indictment.

Dated: Oct. 20, 2008 s./ H. Dean Steward

H. Dean Steward
Orin Kerr
Counsel for Defendant
Lori 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 Oct. 20, 2008, 2008, service of the defendant's:

Reply to Govt. Response to Pre-Trial Conf Order

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

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

Executed on Oct. 20, 2008

H. Dean Steward

H. Dean Steward