UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	**Hon. Susan D. Wigenton**
	:	**U.S. District Judge**
v.	:	
	:	
ANDREW AUERNHEIMER	:	**Criminal No. 11-470 (SDW)**
a/k/a "Weev"	:	
a/k/a "Weevlos"	:	
a/k/a "Escher"	:	

BRIEF IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

PAUL J. FISHMAN
United States Attorney
970 Broad Street
Newark, New Jersey 07102
(973) 645-2700

On The Brief:
MICHAEL MARTINEZ
Executive Assistant U.S. Attorney
EREZ LIEBERMANN,
ZACH INTRATER
Assistant U.S. Attorneys

TABLE OF CONTENTS

PRELIMINARY STATEMENT

In January 2010, Apple Computer introduced the iPad to the market. Superseding Indictment, Count 1, ¶ 1e. AT&T was then the exclusive provider of 3G wireless network services for iPad users. Id., Count 1, ¶ 1f. AT&T's 3G wireless network allowed iPad users to access the Internet. Id., Count 1, ¶¶ 1f, 1j. To access the Internet using AT&T's 3G wireless network, iPad users had to register with AT&T. Id., Count 1, ¶ 1k. During that registration process, the iPad user had to provide, among other things, an e-mail address, a password, and a billing address. Id., Count 1, ¶ 1l.

At the time of registration, AT&T automatically linked the iPad 3G customer's e-mail address with the Integrated Circuit Card Identifier, or ICC-ID, on the customer's iPad. Superseding Indictment, Count 1, ¶ 1m. The ICC-ID is a 19- to 20-digit number that is unique to the Subcriber Identity Module card in every iPad. Id., Count 1, ¶ 1m. As a result of AT&T automatically linking the iPad 3G customer's e-mail address with the customer's ICC-ID, each time the customer accessed the AT&T website, the customer's ICC-ID was recognized and the customer's e-mail address was automatically displayed. Id., Count 1, ¶ 1n. This automated feature provided the customer with quicker and more user-friendly Internet access. Id., Count 1, ¶ 1o.

In June 2010, the defendant, Andrew Auernheimer, and his coconspirator, Daniel Spitler, both of whom belonged to an association of Internet hackers known as Goatse Security, discovered that each ICC-ID was connected to an iPad 3G customer's e-mail address and wrote a computer program, the "Account Slurper," designed to exploit this automated feature. Superseding Indictment ¶¶ 2-3, 7-8. Specifically, the program "was designed to mimic the behavior of an iPad 3G so that AT&T's servers were fooled into believing that they were communicating with an actual iPad 3G and wrongly granted the Account Slurper access to AT&T's servers." Id., Count 1, ¶ 8a. In essence, the Account Slurper randomly guessed ICC-ID ranges, and correct guesses were rewarded with an ICC-ID/e-mail pairing for a specific iPad 3G user. Id., Count 1, ¶ 8b.

From June 5, 2010 through June 9, 2010, the conspirators' Account Slurper gained unauthorized access to AT&T's servers and stole approximately 120,000 ICC-ID/e-mail address pairings from iPad 3G customers, including thousands of customers in New Jersey. Superseding Indictment ¶¶ 9, 27d. That theft of approximately 120,000 ICC-ID/e-mail address pairings was conducted without the authorization of the individual iPad 3G customers, AT&T, or Apple. Id., Count 1, ¶¶ 9, 10.

Immediately following the theft, on June 9, 2010, the defendant and his conspirators knowingly disclosed the stolen ICC-ID/e-mail address pairings to

Gawker, an Internet magazine, knowing or expecting that Gawker would disseminate that information to the world. Superseding Indictment, Count 1, ¶¶ 11, 12. Gawker published the stolen information, in redacted form, on its website, as well as published an article regarding the privacy breach. Id., Count 1, ¶ 11. Rather than remain silent about his criminal conduct, the defendant boasted about his crime on his weblog and posted a link to the Gawker article. Id., Count 1, ¶ 12. Moreover, the defendant sent e-mails to members of news organizations, such as News Corporation, the San Francisco Chronicle, the Washington Post, and Thomson-Reuters, offering "to describe the method of theft in more detail." Id., Count 1, ¶¶ 24 & n.4, 27c. Finally, the defendant had at least one interview regarding the AT&T iPad data breach with CNET, which was published on June 10, 2010. Id., Count 1, ¶ 13.

On August 16, 2012, a federal grand jury sitting in Newark, New Jersey returned a two-count Superseding Indictment against the defendant. Count One charged that, from June 2, 2010 through June 15, 2010, the defendant conspired to access a computer without authorization (or exceeding authorized access), and thereby obtain information from a protected computer, in furtherance of a criminal act in violation of a New Jersey criminal statute, i.e., N.J.S.A. 2C:20-31(a), contrary to the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), in violation of 18 U.S.C. § 371. Count Two

charged that, from June 2, 2010 through June 15, 2010, the defendant knowingly transferred, possessed, and used, without lawful authority, means of identification of other persons, including New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to 18 U.S.C. § 1030(a)(2)(C), in violation of 18 U.S.C. §§ 1028(a)(7) and 2.

The defendant now moves to dismiss the Superseding Indictment. He raises five arguments in support of his motion to dismiss: (1) that the Superseding Indictment is void for vagueness; (2) that Count One suffers from a merger problem tantamount to double jeopardy; (3) that the District of New Jersey is not a proper venue for either of the two Counts; (4) that Count Two is improperly pled, because the 18 U.S.C. § 1028(a)(7) offense cannot be "in connection with" a past crime; and (5) that Count Two violates the First Amendment.

The defendant's arguments lack merit. First, his void-for-vagueness argument fails because the relevant definitions of unauthorized access are clear and unambiguous, and provide reasonable persons with fair notice that their conduct puts them at risk of punishment. Moreover, the *mens rea* element in the CFAA offense alleviates vagueness concerns. Additionally, the federal courts are in agreement regarding the definition of unauthorized access in cases, like this one, where the defendant accesses computer servers without the permission of the computer account holders.

Second, there is no merger problem tantamount to double jeopardy because not only are the elements of 18 U.S.C. § 1030(a)(2)(C) and N.J.S.A. 2C:20-31(a) different, but the conduct required to prove them is also different.

Third, venue for both Counts is proper in the District of New Jersey. The defendant's knowing disclosure of personal identifying information for thousands of New Jersey victims is a crucial element of Count One, and, as a result, venue is proper in this District. Furthermore, because there is venue in this District for Count Two's predicate offense – i.e., the CFAA offense alleged in Count One – there is also venue in this District for Count Two. Moreover, the disclosures at issue were continuing offenses that affected this District. Finally, the defendant failed to obtain authorization for the taking and disclosing of personal identifying information from residents in this District.

Fourth, Count Two properly pleads a violation of 18 U.S.C. § 1028(a)(7), notwithstanding the defendant's claim that the words "in connection with" in § 1028(a)(7) must be read to criminalize only possession or transfer of means of identification related to present or future criminal activity, as opposed to past criminal activity. The defendant's argument is not supported by either the legislative history or the case law that he cites. Furthermore, contrary to the defendant's argument, a plain reading of "in connection with" is not subject to any temporal restriction. Lastly, even if the defendant were correct in his reading of

the statute, the Superseding Indictment clearly alleges that the defendant's possession of victim ICC-ID/e-mail address pairings took place during the period of unlawful access charged in Count One.

Fifth, the defendant's argument that Count Two violates the First Amendment by criminalizing the transmission of public information fails. To start, the ICC-ID/e-mail pairings at issue are confidential, not public, information. And the knowing possession and transfer of stolen means of identification constitutes conduct with "little or no communicative value," not speech.

POINT I

COUNT ONE OF THE INDICTMENT IS NOT VOID FOR VAGUENESS.

The defendant argues that the conspiracy alleged in Count One must be dismissed because the defendant "had no notice under the Fifth Amendment's Due Process Clause that the object of the conspiracy – the alleged unauthorized access – was illegal." DB at 4.[1] Specifically, the defendant argues that "[t]he CFAA provides no definition as to what constitutes unauthorized access to a protected computer, and the courts are conflicted as to what unauthorized access means." DB at 4.

The defendant's argument fails for three reasons. First, by applying the canons of statutory construction, taking guidance from federal circuit courts that have construed the meaning of unauthorized access in the CFAA, and examining the defendant's vagueness challenge in light of the facts of this specific case, the relevant definitions of unauthorized access are clear and unambiguous, and provide reasonable persons with fair notice that their conduct puts them at risk of punishment. Second, § 1030(a)(2)(C)'s *mens rea* requirement alleviates vagueness concerns. Third, federal courts are not conflicted regarding the definition of "without authorization" or "exceeds authorized access" in cases, like this one,

[1] "DB" refers to the "Memorandum of Law in Support of Defendant's Motion to Dismiss."

where the defendant accessed computer servers without the permission of the computer account holders.

An indictment must contain only a "plain, concise, and definite written statement of the essential facts constituting the offense charged." Fed. R. Crim. P. 7(c)(1). An indictment is sufficient so long as it "(1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution." United States v. Kemp, 500 F.3d 257, 280 (3d Cir. 2007) (quotation marks and citation omitted). Further, "no greater specificity than the statutory language is required so long as there is sufficient factual orientation to permit the defendant to prepare his defense and to invoke double jeopardy in the event of a subsequent prosecution." Id. (quotation marks and citation omitted); accord Hamling v. United States, 418 U.S. 87, 117 (1974) (similar standard under Constitutional requirements); United States v. Rankin, 870 F.2d 109, 112 (3d Cir. 1989). "[T]he Federal Rules were designed to eliminate technicalities in criminal pleadings and are to be construed to secure simplicity in procedure. While detailed allegations might well have been required under common-law pleading rules, they surely are not contemplated by [Rule 7(c)(1)]." United States v. Resendiz-Ponce, 549 U.S. 102, 110 (2007) (quotation marks and citations omitted).

Federal Rule of Criminal Procedure 12(b)(3)(B) permits a defendant to move to dismiss an indictment for failure "to state an offense." But only in rare circumstances will an indictment fail adequately to state an offense. For instance, dismissal is appropriate only "if the specific facts alleged in the charging document fall beyond the scope of the relevant criminal statute, as a matter of statutory interpretation," United States v. Panarella, 277 F.3d 678, 685 (3d Cir. 2002), such as where a statute penalizes assaults on a rape victim but the indictment alleges assault only on a male companion of the rape victim, Gov't of Virgin Islands v. Greenidge, 600 F.2d 437, 438-40 (3d Cir. 1979).

When determining the sufficiency of an indictment, a district court must "accept[] as true the factual allegations set forth in the indictment." United States v. Besmajian, 910 F.2d 1153, 1154 (3d Cir. 1990). "The government is entitled to marshal and present its evidence at trial, and have its sufficiency tested by a motion for acquittal pursuant to" Rule 29. United States v. DeLaurentis, 230 F.3d 659, 660-61 (3d Cir. 2000).

A. By applying the canons of statutory construction, taking guidance from the analysis of federal circuit court opinions, and examining the defendant's vagueness challenge in light of the facts of this specific case, the definitions of "without authorization" and "exceed authorized access" are clear and unambiguous.

The definitions of "without authorization" and "exceeds authorized access" in the context of § 1030(a)(2) are clear and unambiguous, and provide reasonable

persons with fair notice that their conduct puts them at risk of punishment. "It is well established that vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in the light of the facts of the case at hand." United States v. Moyer, 674 F.3d 192, 211 (3d Cir. 2012) (quoting United States v. Mazurie, 419 U.S. 544, 550 (1975)). "In criminal cases, because vagueness attacks are based on lack of notice, they may be overcome in any specific case where reasonable persons would know their conduct puts [them] at risk of punishment under the statute." Id. (internal quotation marks and citation omitted) (alteration in original).

Section 1030(a)(2)(C) does not involve First Amendment freedoms. Rather, it subjects to criminal punishment[2] "[w]hoever . . . intentionally accesses a computer *without authorization* or *exceeds authorized access*, and thereby obtains . . . information from any protected computer[3][.]" 18 U.S.C. § 1030(a)(2)(C) (italics added). The CFAA does not define "without authorization," but does define "exceeds authorized access." "A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary,

---

[2] Section 1030 also provides civil remedies for computer fraud and abuse. See 18 U.S.C. § 1030(g) ("[A]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."). As a result of the availability of civil remedies, much of the case law developing Section 1030 has occurred in the civil arena. See United States v. Drew, 259 F.R.D. 449, 456-57 (C.D. Cal. 2009) ("Because of the availability of civil remedies, much of the law as to the meaning and scope of the CFAA has been developed in the context of civil cases.").

[3] The CFAA defines the term, "protected computer," as, among other things, "a computer . . . which is used in or affecting intderstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]" 18 U.S.C. § 1030(e)(2)(B).

contemporary, common meaning." Perrin v. United States, 444 U.S. 37, 42 (1979). This Court, therefore, should take the "ordinary, contemporary, common meaning" of "without authorization." Although the Third Circuit has not addressed the definition of "without authorization" as used in § 1030, at least three other federal circuit courts have done so. In each case, the circuit court sought the term's "ordinary, contemporary, common meaning" by referring to contemporary dictionary definitions and concluded that "without authorization" means "without permission" or "without approval." See, e.g., WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012) (noting that "the Oxford English Dictionary defines 'authorization' as 'formal warrant, or sanction[,]'" and concluding that an individual "accesses a computer 'without authorization' when he gains admission to a computer without approval"); id. at 206 (holding that "without authorization" applies "only when an individual accesses a computer without permission"); Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 658 F.3d 295,304 (6th Cir. 2011) (relying on the Oxford English Dictionary's definition of "authorization" as "[t]he conferment of legality; . . . sanction" and concluding that "a defendant who accesses a computer 'without authorization' does so without sanction or permission") (quoting 1 Oxford English Dictionary 798 (2d ed. 1989)) (alteration in original); LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (observing that "[a]uthorization is defined in the dictionary as

'permission or power granted by an authority'" and concluding, "[b]ased on this definition," that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it").

Moreover, "[i]t is a cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." TRW Inc. v. Andrews, 534 U.S. 19, 31 (2001) (internal quotation marks and citation omitted). Consistent with this principle, the definition of "without authorization" as "without permission" or "without approval" does not render the congressionally defined term, "exceeds authorized access," "superfluous, void, or insignificant." See TRW Inc., 534 U.S. at 31. The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]" 18 U.S.C. § 1030(e)(6). Reading both terms together, an individual accesses a computer "without authorization" when he gains access without permission or approval, whereas an individual "exceeds authorized access" when he has permission or approval to access a computer, but uses his access to obtain or alter information that he is not entitled to access.[4] These clear and unambiguous definitions are

[4] See WEC Carolina Energy Solutions, 687 F.3d at 204 (concluding that an individual "accesses a computer 'without authorization' when he gains admission to a computer without approval" and "'exceeds authorized access' when he has approval to access a computer, but uses his access to obtain or alter information that falls outside the bounds of his approved access"); LVRC Holdings, 581 F.3d at 1133 (holding that "a person who 'intentionally accesses a computer without authorization,' . . . accesses a computer without any permission at all, while a person who 'exceeds authorized access,' . . . has permission to access the computer, but accesses information on the

consistent with Congress's view that their meaning is "self-explanatory." See S. Rep. No. 99-432, at 13, (1986), available at 1986 WL 31918, at *7 (commenting that the term "exceeds authorized access," the definition of which includes "access[ing] a computer with authorization," is "self-explanatory").

In this specific case, "reasonable persons would know their conduct puts [them] at risk of punishment under the statute." Moyer, 674 F.3d at 211 (alteration in original). Here, Count One charges the defendant with conspiracy to access a computer without authorization or to exceed authorized access, and thereby obtain information from AT&T servers, in furtherance of a New Jersey criminal statute, i.e., N.J.S.A. 2C:20-31(a), contrary to 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), in violation of 18 U.S.C. § 371. Superseding Indictment, Count 1, ¶¶ 5, 27. Specifically, the Superseding Indictment alleges that the defendant and his coconspirators employed a computer program to fool AT&T's servers into believing that they were communicating with iPad users who actually had registered with AT&T's 3G network. Id., Count 1, ¶ 8a. The Superseding Indictment alleges that the defendant and his coconspirators gained unauthorized access to those servers and stole approximately 120,000 ICC-ID/e-mail address pairings from iPad 3G customers. Id., Count 1, ¶ 9. The Superseding Indictment

computer that the person is not entitled to access."); Pulte Homes, 648 F.3d at 304 (same).

further alleges that the defendant's theft was committed without the authorization of the individual iPad 3G users, AT&T, or Apple. Id., Count 1, ¶¶ 9-10.

Indeed, the defendant himself described his conduct as a "theft." Superseding Indictment, Count 1, ¶ 24. The defendant explained in an e-mail to a board member of News Corporation that the board member's "iPad[ ] unique network identifier was pulled straight out of AT&T's database," that the defendant and his coconspirators had "collected many such identifiers for members of the media and major tech companies," and that the defendant "would be absolutely happy to describe *the method of theft* in more detail" with "a journalist in [News Corporation's] organization." Id. (emphasis added). It bears noting that the defendant did not limit his offer to describe "the method of theft" to News Corporation, but also emailed similar offers to the San Francisco Chronicle, the Washington Post, and Thomson Reuters. Id., Count 1, ¶ 24 & n.4.

Assuming that the Superseding Indictment's allegations are true – as this Court must, see Besmajian, 910 F.2d at 1154 – "reasonable persons would know their conduct" – i.e., designing and employing a computer program to fool AT&T computer servers into believing that they were communicating with actual, registered AT&T customers, and then harvesting the personal identifiers of more than a hundred thousand AT&T customers without their authorization – "puts

[them] at risk of punishment under the statute." Moyer, 674 F.3d at 211 (internal quotation marks and citation omitted) (alteration in original).

Moyer is instructive here. In Moyer, the defendant, Nestor, argued that the application of 18 U.S.C. § 1519 – which criminalizes knowingly making false entries in any document with the intent to obstruct the investigation or proper administration of any matter within the jurisdiction of any United States department or agency or any title 11 case, "or in relation to or contemplation of any such matter or case" – was constitutionally vague because the "contemplation of" clause "does not specify what a defendant must know to trigger criminal liability." Moyer, 674 F.3d at 212. In rejecting Nestor's vagueness argument, the Third Circuit observed that "even if this element is potentially vague as it relates to hypothetical defendants, it is clearly not vague as it relates to Nestor." Id. The Third Circuit explained that "the government presented sufficient evidence to prove that when Nestor falsified the police reports, he contemplated an investigation into a matter within the jurisdiction of the FBI, intending to impede that investigation." Id. The Third Circuit then "conclude[d] that the statute is not vague 'in light of the facts of the case at hand.'" Id. (quoting Mazurie, 419 U.S. at 550).

Here, even if the "without authorization" element were vague with respect to hypothetical defendants, it is not vague with respect to this defendant, "in light of

the facts of the case at hand." Moyer, 674 F.3d at 212 (quoting Mazurie, 419 U.S. at 550). As alleged in the Superseding Indictment, the defendant admitted that his conduct constituted a "theft," confessing in an email to a victim that he and his co-conspirators had pulled that victim's "iPad[ ] unique network identifier . . . straight out of AT&T's database," that they had "collected many such identifiers for members of the media and major tech companies," and that the defendant "would be absolutely happy to describe the method of theft in more detail." Superseding Indictment, Count 1, ¶ 24. In the defendant's online conversations with his co-conspirator, Spitler, he wrote: "if we get 1 reporters [sic] address with this somehow we instantly have a story . . . the best way to have a leadin [sic] on it . . . HI I STOLE YOUR EMAIL FROM AT&&T [sic] WANT TO KNOW HOW?" Id., Count 1, ¶ 22. In light of the defendant's own admissions, it borders on the absurd to claim that he did not understand that he obtained information from AT&T's servers without AT&T customers' permission or approval. Accordingly, this Court should conclude that the statute is not vague "in the light of the facts at hand." Moyer, 674 at 212 (citation omitted).

B. Section 1030(a)(2)(C)'s *mens rea* alleviates vagueness concerns.

Section 1030(a)(2)(C)'s *mens rea* requirement alleviates vagueness concerns, because it reduces the likelihood that a defendant will be convicted for conduct that he committed through inadvertence. As the Third Circuit explained in

Moyer: "Scienter requirements in criminal statutes 'alleviate vagueness concerns' because a *mens rea* element makes it less likely that a defendant will be convicted for an action committed by mistake." 674 F.3d at 211-12 (quoting Gonzales v. Carhart, 550 U.S. 124, 149 (2007)). The Third Circuit in Moyer reasoned that "[b]ecause a defendant will be convicted for violating § 1519 'only for an act knowingly done with the purpose of doing that which the statute prohibits, the accused cannot be said to suffer from lack of warning or knowledge that the act which he does is a violation of law.'" Id. at 212 (quoting Screws v. United States, 325 U.S. 91, 102 (1945)). Specifically, the Moyer Court found that "by the express language of the statute, no liability will be imposed for knowingly falsifying documents *without* an 'intent to impede, obstruct, or influence a matter.'" Id. (quoting 18 U.S.C. § 1519). (emphasis in original).

Similarly, by § 1030(a)(2)'s express language, no liability will be imposed for "access[ing] a computer without authorization or exceed[ing] authorized access" unless it was done "intentionally." 18 U.S.C. § 1030(a)(2). Indeed, Congress specifically amended § 1030(a)(2) in 1986 to change the scienter requirement from "knowingly" to "intentionally" because, in part, "intentional acts of unauthorized access – rather than mistaken, inadvertent, or careless ones – [we]re precisely what the Committee intend[ed] to proscribe." S. Rep. No. 99-432, at 3-4 (1986), available at 1986 WL 31918, at *3-*4. Congress expressly

substituted the "intentional" standard "to focus Federal criminal prosecutions on those whose conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." Id. at *6. Accordingly, § 1030(a)(2)'s scienter requirement "makes it less likely that a defendant will be convicted for an action committed by mistake[,]" thereby "alleviat[ing] vagueness concerns." Moyer, 674 F.3d at 211-12 (internal quotation marks and citation omitted).

C. The defendant's reliance on federal court conflict regarding the CFAA is misplaced, as the federal courts are not conflicted regarding the definition of "without authorization" or "exceeds authorized access" in cases where the defendant intentionally accessed a computer without the computer account holder's permission.

The federal courts are not conflicted regarding the definition of "without authorization" or "exceeds authorized access" in cases, like this one, where the defendant accessed computer servers without the permission of the computer account holders. The defendant attempts to support his contention that § 1030(a)(2) is vague by directing this Court to "the federal courts' struggle with its meaning" and the "understandable consternation among the federal courts as they attempt to divine the meaning of what Congress has declined to define." DB at 5. Specifically, the defendant directs this Court to United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc); United States v. Drew, 259 F.R.D. 449, 464 (C.D.

Cal. 2009); and Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964-65 (D. Ariz. 2008).

The defendant's argument lacks merit, as the cases he cites relate to individuals who had approval to access a computer, but arguably made improper use of their authorized access, either by acting in a manner adverse to their employer's interests or by breaching a contract, such as a website's terms of service. See Nosal, 676 F.3d at 862-63 (holding that CFAA "target[s] the unauthorized procurement or alteration of information, not its misuse or misappropriation," and rejecting "the decisions of our sister circuits that interpret the CFAA broadly to cover violations of corporate computer use restrictions or violations of a duty of loyalty") (citing United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); United States v. John, 597 F.3d 263 (5th Cir. 2010); and Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006)); United States v. Drew, 259 F.R.D. 449, 466-67 (C.D. Cal. 2009) (holding that conscious breach of a website's terms of service does not violate section 1030(a)(2)(C)); Shamrock Food Co. v. Gast, 535 F. Supp. 2d 962, 967 (D. Ariz. 2008) (holding that, under CFAA, a "violation for accessing 'without authorization' occurs only where initial access is not permitted[,]" and "a violation for 'exceeding authorized access' occurs where initial access is permitted but the access of certain information is not permitted[,]" and rejecting interpretation that "would sweep broadly within the

criminal statute breaches of contract involving a computer") (citation omitted).[5] Here, however, Count One alleges that the defendant did not have approval to access AT&T's servers. Therefore, the cases on which the defendant relies are inapposite.

Finally, the defendant argues that the rule of lenity requires this Court to limit the scope of § 1030 to cases involving the bypassing of security measures and relies on Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 933 (E.D. Va. 2010) and Koch Indus., Inc. v. Does, 2011 WL 1775765, *8 (D. Utah May 9, 2011) to support his argument. DB at 7-8 ("If the CFAA is to avoid constitutional infirmity, it must be narrowly read to require the bypassing of computer security measures.") This argument also fails. The cases on which the defendant relies do not stand for the proposition that a § 1030 violation always requires the bypassing of security

[5] See generally WEC Carolina Energy Solutions, 687 F.3d at 203 (discussing "two schools of thought": the first, which was promulgated by the Seventh Circuit and advanced by the Fourth Circuit in WEC Carolina Energy Solutions, holding "that when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it"; and the second, which was promulgated by the Ninth Circuit, limiting the terms "without authorization" and "exceeds authorized access" to "situations where an individual accesses a computer or information on a computer without permission"); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-84 (1st Cir. 2001) (holding that defendants "exceeded authorized access" because of ample evidence that they violated "broad confidentiality agreement").

measures.[6] Although bypassing security measures is certainly one means of gaining access without authorization, the plain text of the statute is simply broader and more general than the defendant's unduly confined construction. For instance, the defendant's statutory interpretation would not cover obvious statutory violations, such as a defendant's gaining access to a computer using a stolen password. And it is unrealistic to expect Congress to proscribe conduct using a list of specifically articulated examples. As the Seventh Circuit explained in United States v. Mitra, 405 F.3d 492 (7th Cir. 2005): "[Legislators] do know that complexity is endemic in the modern world and that each passing year sees new developments. That's why they write general statutes rather than enacting a list of particular forbidden acts." Id. at 495 (italics removed).

Lastly, the United States disagrees with the defendant's assertion that "[t]here is no allegation that Mr. Auernheimer acted in any way to bypass any computer security measures." DB at 7. The Superseding Indictment alleges that AT&T linked each iPad 3G user's e-mail address to the iPad's ICC-ID. Superseding Indictment, Count 1, ¶ 1m. The ICC-ID is "a 19 to 20 digit number unique to every iPad[.]" Id. "[E]ach time a user accessed the AT&T website, the user's ICC-ID was recognized and, in turn, the user's e-mail address was

[6] Cvent, Inc. stands for the proposition that, while the CFAA prohibits unauthorized access to a website, it does not prohibit downloading publicly available material. 739 F. Supp. 2d at 932-33. Koch Industries, similarly, stands for the proposition that defendants cannot exceed their authority to access data by using information that the plaintiff made publicly available on the Internet. 2011 WL 1775764, at * 8.

automatically displayed." Id. That 19- to 20-digit number unique to every iPad qualifies as an individualized grant of access. See Cvent, Inc., 739 F. Supp. 2d at 932-33 (denying motion to dismiss § 1030 claim, in part, because Cvent's website was "publicly available on the Internet, without requiring any . . . individualized grant of access"). By comparison, a Social Security number is a mere nine digit number, and the winning Powerball Lottery ticket is only a 12-digit number. The claim that the ICC-ID's unique 19- to 20-digit identifier was not a security measure designed to ensure that only registered customers gained access to AT&T's servers strains credulity.

POINT II

COUNT ONE DOES NOT POSE A MERGER PROBLEM TANTAMOUNT TO A DOUBLE JEOPARDY VIOLATION.

The defendant contends that the alleged conduct of intentionally accessing iPad 3G customer accounts without permission and viewing their email addresses – conduct which would prove the elements of a misdemeanor § 1030(a)(2)(C) charge – is the same conduct that proves the felony-elevating element that the § 1030(a)(2)(C) offense was committed in furtherance of N.J.S.A. 2C:20-31(a). See DB at 8-11. Relying principally on United States v. Cioni, 649 F.3d 276 (4th Cir. 2011), the defendant argues that the same conduct supports both crimes and that the resulting overlap constitutes a "merger problem, tantamount to double jeopardy," Cioni, 649 F.3d at 282 (internal quotation marks and citation omitted). DB at 10.

The defendant's argument lacks merit. Not only are the elements of § 1030(a)(2)(C) and N.J.S.A. 2C:20-31(a) different, but the conduct required to prove them is also different. Count One charges the defendant with conspiracy to access a computer without authorization or to exceed authorized access, and thereby obtain information from AT&T's servers, in furtherance of a New Jersey criminal statute, i.e., N.J.S.A. 2C:20-31(a), contrary to 18 U.S.C. §§ 1030(a)(2)(C) and 1030(c)(2)(B)(ii), in violation of 18 U.S.C. § 371. Superseding Indictment, Count 1, ¶¶ 5, 27. A § 371 conspiracy has three elements: (1) "an agreement to

commit an offense proscribed by federal law;" (2) "the defendants intentionally joining in the agreement;" and (3) "one of the conspirators committing an overt act . . . in furtherance of the conspiracy." United States v. Wright, 665 F.3d 560, 568 (3d Cir. 2012). If the offense that is the object of the conspiracy is a felony, then the maximum term of imprisonment is five years. 18 U.S.C. § 371. On the other hand, if the offense that is the object of the conspiracy is a misdemeanor, then the maximum punishment is the same as it is for that misdemeanor. Id.

Section 1030(a)(2)(C) has two elements: (1) the defendant intentionally accessed a computer without authorization or exceeding authorized access; and (2) the defendant obtained information thereby from a protected computer. Eighth Circuit Model Criminal Jury Instructions, 6.18.1030B (2011). The phrase "obtained information" in § 1030(a)(2) "includes merely reading the information." S. Rep. No. 104-357, at 7 (1996), available at 1996 WL 492169, at *7. "There is no requirement that the information be copied or transported." Id.; S. Rep. No. 99-432, at 6-7 (1986), available at 1986 WL 31918, at *6-*7 ("The Department of Justice has expressed concerns that the term 'obtains information' in 18 U.S.C. 1030(a)(2) makes that subsection more than an unauthorized access offense, i.e., that it might require the prosecution to prove asportation of the data in question. Because the premise of this subsection is privacy protection, the Committee wishes to make clear that 'obtaining information' in this context includes mere

observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.") (footnote omitted).

Without more, § 1030(a)(2)(C) is punishable as a misdemeanor. 18 U.S.C. § 1030(c)(2)(A). But if "the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," then it is punishable as felony. 18 U.S.C. § 1030(c)(2)(B)(ii). Here, the Superseding Indictment alleges that the §1030(a)(2)(C) offense was committed in furtherance of a New Jersey felony criminal statute, N.J.S.A. 2C:20-31(a). Accordingly, the § 1030(a)(2)(C) offense is elevated to a felony, pursuant to 18 U.S.C. § 1030(c)(2)(B)(ii). And, because the § 1030(a)(2)(C) offense is elevated to a felony, the § 371 charge is also punishable as a felony. See 18 U.S.C. § 371.

Turning to N.J.S.A. 2C:20-31(a), it has three elements: (1) the defendant accessed data knowingly; (2) the defendant accessed data without authorization; and (3) the defendant "knowingly or recklessly disclosed or caused to be disclosed any data . . . or personal identifying information." N.J.S.A. 2C:20-31(a); see State v. Riley, 988 A.2d 1252, 1254 (N.J. Super. 2009). A comparison of § 1030(a)(2)(C) and N.J.S.A. 2C:20-31(a) reveals that § 1030(a)(2)(C)'s two elements are similar to the first two elements of N.J.S.A. 2C:20-31(a) and require substantially similar proof of conduct. N.J.S.A. 2C:20-31(a)'s additional third

element, however, is distinct from §1030(a)(2)(C): it requires proof that the defendant "knowingly or recklessly discloses or causes to be disclosed any data, . . . or personal identifying information." N.J.S.A. 2C:20-31(a). Here, the Superseding Indictment alleges that the defendant and his co-conspirators "knowingly disclosed approximately 120,000 stolen ICC-ID/e-mail address pairings for iPad 3G customers – including thousands of customers who resided in New Jersey – to the internet magazine Gawker." Superseding Indictment, Count 1, ¶ 27d. In view of the additional and different conduct required to prove N.J.S.A. 2C:20-31(a), the defendant's argument that the same conduct supports both crimes fails. For the same reason, the defendant's related arguments that Congress did not intend to elevate a misdemeanor charge into a felony without proof of an additional illegal act, DB at 9, and that the Superseding Indictment failed to allege an additional act "in furtherance" of a distinct violation of New Jersey law, DB at 11, also lack merit.[7]

[7] The defendant also argues that object of conspiracy cannot be a felony aggravator. That argument is mistaken as a matter of law. For a § 371 conspiracy to be punished as a felony, it must have a felony, as opposed to a misdemeanor, as the object of the conspiracy. And § 1030(a)(2)(C) is punishable as a felony only if one of the felony aggravators identified in § 1030(c)(2)(B) is satisfied. Accordingly, the felony aggravator must be included as part of the offense that is the object of the conspiracy.

POINT III

VENUE PROPERLY LIES IN THE DISTRICT OF NEW JERSEY FOR BOTH COUNTS OF THE SUPERSEDING INDICTMENT.

The defendant argues that the indictment should be dismissed for lack of venue. DB at 13. In particular, the defendant contends that "[t]he Indictment does no more than cite the threadbare and conclusory allegation that the acts described 'occurred in the District of New Jersey and elsewhere.'" DB at 13 (citing Superseding Indictment, Count 1, ¶ 5). The defendant's argument fails for several reasons. First, the defendant's knowing disclosure of the personal identifying information for thousands of New Jersey victims is a crucial element of Count One, and thus, venue is proper in the District of New Jersey. Second, because there is venue in the District of New Jersey for Count Two's predicate offense – i.e., the CFAA offense alleged in Count One – there is also venue in the District of New Jersey for Count Two. Third, the disclosures in question were continuing offenses that affected this District. Fourth, the defendant failed to obtain authorization for the taking and disclosing of personal identifying information from the residents of this District.

Article III of the United States Constitution provides that "[t]he Trial of all Crimes . . . shall be held in the State where said Crimes shall have been committed." Art. III, § 2, cl. 3. "Its command is reinforced by the Sixth Amendment's requirement that '[i]n all criminal prosecutions, the accused shall

enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed,' and is echoed by Rule 18 of the Federal Rules of Criminal Procedure ('prosecution shall be had in a district in which the offense was committed')." United States v. Rodriguez-Moreno, 526 U.S. 275, 278 (1999).

"Congress has the power to lay out the elements of a crime to permit prosecution in one or any of the districts in which the crucial elements are performed." United States v. Perez, 280 F.3d 318, 328-29 (3d Cir. 2002); accord United States v. Pendleton, 658 F.3d 299, 3030 (3d Cir. 2010). To that end, 18 U.S.C. § 3237(a), in pertinent part, provides: "[A]ny offense against the United States begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." Section 3237(a) further provides that any "offense involving . . . transportation in interstate . . . commerce . . . is a continuing offense and, except as otherwise expressly provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such commerce . . . moves."

When the criminal statute does not contain an express venue provision, as is the case with the statutes charged in both counts of the Superseding Indictment, then this Court determines venue "from the nature of the crime alleged and the

location of the act or acts constituting it." Rodriguez-Moreno, 526 U.S. at 279; Pendleton, 658 F.3d at 303. "In performing this inquiry, a court must initially identify the conduct constituting the offense (the nature of the crime) and then discern the location of the commission of the criminal acts." Rodriguez-Moreno, 526 U.S. at 279. "When the crime consists of distinct acts occurring in different places, venue is proper where any part of the crime occurs." Pendleton, 658 F.3d at 303; Rodriguez-Moreno, 526 U.S. at 281 ("where a crime consists of distinct parts which have different localities the whole may be tried where any part can be proved to have been done") (citation omitted).

To "identify the conduct constituting the offense," courts identify the elements of the offense. See Rodriguez-Moreno, 526 U.S. at 279-80; Pendleton, 658 F.3d at 303-04. Count One is a § 371 conspiracy charge. The offense, the commission of which is the object of the conspiracy, requires, among other elements, that the defendant committed the § 1030(a)(2)(C) offense in furtherance of a New Jersey criminal statute prohibiting the knowing or reckless disclosure of personal identifying information that the defendant knowingly accessed without authorization. See 18 U.S.C. § 1030(c)(2)(B)(ii); N.J.S.A. 2C:20-31(a). "The premise of [§ 1030(a)(2)] is privacy protection[.]" S. Rep. No. 99-432, at 6 (1986), available at 1986 WL 31918, at *6. Here, as alleged in the Superseding Indictment, AT&T kept the ICC-ID/e-mail pairings of iPad 3G users confidential.

Superseding Indictment, Count 1, ¶ 1o. The defendant violated the privacy of thousands of New Jersey residents by knowingly disclosing their personal identifying information – i.e., ICC-ID/e-mail pairings – to Gawker. Id., Count 1, ¶ 27d. The defendant's knowing disclosure of the personal identifying information for thousands of New Jersey victims is a "crucial element" of Count One. See Perez, 280 F.3d at 329. Count One, therefore, has proper venue in the District of New Jersey.

United States v. Powers, No. 8:09CR361, 2010 WL 1418172 (D. Neb. March 4, 2010), is instructive. In Powers, the defendant was charged with intentionally exceeding authorized access to a computer, and thereby obtaining information from a protected computer, in violation of 18 U.S.C. § 1030(a)(2)(C). Powers, 2010 WL 1418127, at *1. "The alleged offense was committed in furtherance of a tortious act in violation of the laws of the State of Nebraska, specifically, invasion of privacy and intentional infliction of emotional distress." Id. The victim, who resided in Nebraska at the time of the offense, had an AOL email account. Id. She had given the defendant her password to gain access to her email account. Id. The victim's account had past e-mail messages, including images of her partially nude and in provocative poses. Id. Exceeding the purpose for which the password was given, the defendant e-mailed compromising images of the victim to individuals in the victim's e-mail account address book. Id. at *1-

*2. The images attached to those e-mails were not located on the victim's hard drive, but on a computer server where AOL email accounts resided. Id. at *2.

The defendant argued that venue was improper in the District of Nebraska, contending that "he was never physically in Nebraska, and the computer he allegedly used was in Phoenix, Arizona." Powers, 2010 WL 1418127, at *2. The District Court rejected the defendant's venue argument. The Court explained: "Although Powers may not have been physically present in Nebraska, and the computer used to facilitate the violation was located in Arizona, venue would be proper in any district in which the offense began in one district, and was completed or committed in any other district." Id. (citing 18 U.S.C. § 3237). The Court continued:

> Powers' violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(2)(C), began in Arizona when he intentionally exceeded authorized access to [the victim's] e-mail account and sent e-mail messages containing compromising images of [the victim]. However, Powers' violation of 18 U.S.C. § 1030(a)(2)(C) was completed in Nebraska. [The victim] resided in and was injured in Nebraska when Powers violated the CFAA. Powers committed the violation in furtherance of tortious acts, specifically violations of Nebraska law under invasion of privacy and intentional infliction of emotional distress.

Id. The Court concluded: "Venue would not only be proper in the District of Arizona where the crime began, but also in the District of Nebraska where the

crime was completed. Hence, Powers may be prosecuted in any district where such crime began, continued, or completed." Id.

The same reasoning applies here. Although the defendant may not have been physically present in New Jersey, and the computer used to facilitate the violation was not located in New Jersey, the defendant's CFAA offense was completed in New Jersey. The victims – in this case the thousands of New Jerseyans who had their confidential ICC-ID/e-mail pairings disclosed to Gawker – resided in New Jersey when the defendant violated the § 1030(a)(2)(C) offense in furtherance of criminal acts, specifically, violations of a New Jersey criminal statute prohibiting the knowing or reckless disclosure of personal identifying information that was knowingly obtained without authorization. As the Powers Court concluded, the defendant "may be prosecuted in any district where such crime began, continued, or completed." Id. Accordingly, venue is proper in the District of New Jersey.

Venue for Count Two is also proper in the District of New Jersey. Count Two charges the defendant with "knowingly transfer[ring], possess[ing], and us[ing], without lawful authority, means of identification of other persons, including means of identification of New Jersey residents, in connection with unlawful activity, specifically, the unlawful accessing of AT&T's servers contrary to Title 18, United States Code, Section 1030(a)(2)(C), [i]n violation of Title 18,

United States Code, Sections 1028(a)(7) and Section 2." Superseding Indictment, Count 2, ¶ 2. Venue for a § 1028(a)(7) is proper in any district in which venue is proper for the predicate violation of federal law. Cf. United States v. Magassouba, 619 F.3d 202, 206 (2d Cir. 2010) ("[W]e have no trouble concluding that venue properly lies with respect to an aggravated identity theft offense in any district in which venue lies for the predicate[.]"). Section 1028(a)(7) prohibits certain conduct "in connection with, any unlawful activity that constitutes a violation of Federal law[.]" 18 U.S.C. § 1028(a)(7). Here, that conduct was "in connection with" the 18 U.S.C. § 1030(a)(2)(C) offense alleged in the Superseding Indictment. Because the § 1030(a)(2)(C) constitutes an essential element of the § 1028(a)(7) offense, venue properly lies wherever that crime was begun, continued, or completed. See 18 U.S.C. § 3237(a). For substantially the same reasons that the § 1030(a)(2)(C) offense, which is the object of Count One's § 371 conspiracy, is properly brought in the District of New Jersey, venue for the § 1028(a)(7) charge is also properly brought here. Cf. Magassouba, 619 F.3d at 206-07 (holding that § 1028A's predicate felony offense, for which there was proper venue, constitutes an essential element of the § 1028A charge, and therefore the venue for the § 1028A charge was proper as well).

Venue is also proper on both Counts in this District because they charge "continuing" offenses under 18 U.S.C. § 3237(a). An essential element of both

offenses, as charged, requires the United States to prove that the conduct involved obtaining information from a "protected computer." That term, in turn, means, as charged here, a computer "which is used in or affecting interstate or foreign commerce or communication . . . ." 18 U.S.C. § 1030(e)(2)(B). Because "interstate commerce" is an element of the charged offenses, they "may be inquired of and prosecuted in any district from, through, or into which such commerce . . . moves." 18 U.S.C. § 3237(a). Here, information that the defendant provided to Gawker is to this day accessible by computer connected to the Internet within New Jersey. See http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed?skyline=true&s=I. Accordingly, the defendant's offense are continuing and may be prosecuted in this District. Cf. United States v. Grenoble 413 F.3d 569, 573-74 (6th Cir. 2005).

Finally, venue lies for both Counts in this District because the United States must prove that the defendant's access to AT&T's computers was "without authorization." Thus, the United States must show that neither AT&T nor AT&T's iPad 3G customers authorized the defendant's conduct. Where an offense requires the United States to prove the failure to do or obtain something, that offense may be prosecuted in the District where the failure occurs. For example, prosecutions for willful failure to pay child support may lie in any venue where the child or children entitled to the support payments reside. See, e.g., United States v.

Muench, 153 F.3d 1298, 1300-04 (11th Cir. 1998); United States v. Murphy, 117 F.3d 137, 139-41 (4th Cir. 1997). Here, as alleged in the Superseding Indictment, neither AT&T nor victims of the defendant in New Jersey authorized the data breach here. Superseding Indictment, Count 1, ¶¶ 9-10.

POINT IV

COUNT TWO PROPERLY PLEADS A VIOLATION OF 18 U.S.C. § 1028(a)(7).

The defendant next seeks dismissal of Count Two of the Superseding Indictment, claiming that the words "in connection with" in § 1028(a)(7) must somehow be read to criminalize only possession or transfer of means of identification related to "present or future criminal activity, and not past criminal activity." DB at 16. The facts alleged in Count Two of the Superseding Indictment, which must be accepted as true, Besmajian, 910 F.2d at 1154, clearly establish a violation of § 1028(a)(7), and so the defendant's argument fails, for four different reasons.

First, it is not supported by the legislative history the defendant cites. Rather, that legislative history makes clear that § 1028(a)(7) was amended to expand liability under § 1028(a)(7) and was changed in part to deal precisely with the kinds of crimes committed by the defendant. Second, it is not supported by the case law the defendant cites – indeed, the central case to which he refers was decided under a prior version of § 1028(a)(7), a version which did not even include the "in connection with" language. Third, a plain reading of "in connection with" is not subject to any temporal restriction. The statute simply criminalizes possessing means of identification of other people, which possession is connected to some other crime – here, the crime of unauthorized computer access. Fourth,

even if the defendant were correct in his cramped reading of § 1028(a)(7) – which he is not – the Superseding Indictment in this case clearly alleges that the defendant's possession of victims' e-mail addresses and ICC-IDs took place during the period of unlawful access charged in Count One, and therefore his motion to dismiss Count Two must fail.

The defendant asserts that the "legislative intent" of § 1028(a)(7) was to limit the possession of means of identification in connection with "present and future crimes." DB at 17. This is simply not the case. The legislative history of § 1028(a)(7) does not include any temporal limitation, or any kind of "if, then" restriction, which the defendant seeks to read into the statute.

Prior to 2004, § 1028(a)(7) prohibited "knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law . . . ." 18 U.S.C. § 1028(a)(7) (2000) (amended 2004). In 2004, concerned with "the growing problem of identity theft," Congress amended the language of § 1028(a)(7). H.R. Rep. No. 108-528, at 1 (2004), available at 2004 WL 1260964, at *1 (the "2004 Amendment"). The 2004 Amendment added the term "in connection with" after "aid or abet," and added the word "possesses" after "transfers."

By selectively quoting the legislative history, the defendant claims that with the 2004 Amendment, Congress somehow sought to restrict the application of § 1028(a)(7), cabining its application to cases where a defendant "intended" to commit another crime after unlawfully obtaining means of identification. See Def. Mot. at 17-18. But examination of the entire legislative history shows that, in fact, the opposite is true. The House report states plainly why Congress added "in connection with" to the language of § 1028(a)(7): to expand, not contract, the number and types of activities that could be prosecuted under the statute.

> The addition of the words "in connection with" would broaden the reach of section 1028(a)(7) in two important ways. First, it will make possible the prosecution of persons who knowingly facilitate the operations of an identity-theft ring by stealing, hacking, or otherwise gathering in an unauthorized way other people's means of identification, but who may deny that they had the specific intent to engage in a particular fraud scheme. Second, it will provide greater flexibility for the prosecution of section 1028(a)(7) offenses. With this proposed change, prosecutors would have the option of proving that the defendants either had the requisite specific intent to commit a particular unlawful activity or engaged in the prohibited use, transfer, or possession of others' means of identification in connection with that unlawful activity.

H.R. Rep. No. 108-528, at 10, available at 2004 WL1260964, at *10. The House report explains the purposes of the 2004 Amendment, and nowhere in this explanation does Congress state that conduct giving rise to a § 1028(a)(7) violation must precede the "other" crime to which it is connected. The legislative history instead makes clear that precisely because of the added language – "in connection

with" – prosecutors would have the option of proving either intent to commit another specific crime, or simply that the unlawful possession of means of identification was connected to that other crime.

The legislative history of the 2004 Amendment thus strongly supports the viability of Count Two. The Superseding Indictment charges that the defendant participated in the theft of e-mail addresses and ICC-IDs – means of identification – from over 100,000 AT&T customers. See Superseding Indictment, Count One, ¶ 9. This is the "stealing, hacking, or otherwise gathering in an unauthorized way" of means of identification referred to in the House report. H.R. Rep. No. 108-528, at 10, available at 2004 WL1260964, at *10. Indeed, the defendant himself characterized his actions as a "theft." Further, in his motion to dismiss, the defendant "den[ies] that [he] had the specific intent to engage in" the unauthorized computer access. The Superseding Indictment has charged that the defendant did have such specific intent. Because this is a well-pled allegation, it easily surpasses the standard for a motion to dismiss. But, importantly, just as Congress intended with the 2004 Amendment, a conviction on Count Two is possible even if the jury somehow buys the defendant's argument that he did not specifically intend to participate in unauthorized computer access. Whether or not the defendant had the specific intent to participate in the theft of victims' data, the 2004 Amendment makes it possible for him to be convicted on Count Two if the United States can

prove that his possession and transfer of that data was connected to the theft. The Superseding Indictment alleges just that, and therefore, pursuant to Fed. R. Crim. P. 12(b)(3)(B), the defendant can find no solace in the legislative history of the 2004 Amendment.

Nor do the cases the defendant cites provide him any support. The defendant cites two cases in his motion to dismiss, which he uses to claim that "[a]lmost universally, the courts read the 'in connection with' language . . . to refer to present and future crimes." DB at 17. The first case is United States v. Sutcliffe, 505 F.3d 944 (9th Cir. 2007), where the defendant, a former Global Crossing employee, obtained and posted personal information about other Global Crossing employees on a website he created. The Court set forth the issue as follows: "Defendant was convicted of violating § 1028(a)(7), which at the time of his trial prohibited 'knowingly transfer[ring] or us[ing], without lawful authority, a means of identification of another person . . . .'" Id. at 959.

"[A]t the time of his trial" is important, for Sutcliffe was tried before the 2004 Amendment. Therefore, the Ninth Circuit performed its analysis of § 1028(a)(7) pursuant to the pre-2004 Amendment language – which did not include the critical phrase "in connection with." Accordingly, Sutcliffe cannot help the defendant here.

In any event, the actual holding of Sutcliffe has nothing to do with whether the transfer of personal information occurred before or after another crime. Instead, Sutcliffe holds that no other crime must be completed for a § 1028(a)(7) conviction to stand: "We therefore hold that the government must only prove that the defendant committed the unlawful act with the requisite criminal intent, not that the defendant's crime actually caused another crime to be committed. . . . [W]e conclude that a § 1028(a)(7) conviction requires no evidence of an underlying crime . . . ." Id. at 960.

The only other case cited by the defendant, United States v. Villanueva-Sotelo, 515 F.3d 1234 (D.C. Cir. 2008), is similarly unhelpful to him. The defendant seizes on the Court's statement that "Congress amended section 1028(a)(7) to ease the prosecution of identity thieves who intend to use 'another person's means of identification' . . . to commit a felony, but have not yet actually done so." Id. at 1245. Nothing in this sentence, however, indicates that Congress's only intent was to enable the prosecution of those who could, at some point in the future, use means of identification to commit another crime. Rather, just two sentences later, the Court cites the legislative history of the 2004 Amendment, which demonstrates that the 2004 Amendment was directed at individuals similar to the defendant, and then states: "Congress intended to single out and punish those who knowingly steal others' identities." Id. at 1246. The

Superseding Indictment alleges that the defendant possessed and transferred means of identification for over 100,000 individuals – information that he received in connection with an unauthorized access of AT&T's servers. Again, because the allegations in Count Two are well pled according to the standard of Fed. R. Crim. P. 7, the defendant's motion to dismiss Count Two should be denied. The defendant's attempt to read into the statutory language a restriction that is not there is also belied by the plain meaning of the words themselves. The Merriam-Webster Dictionary defines "connection" as a "causal or logical relation or sequence" or as a "relationship in fact." Merriam-Webster Dictionary, available at http://www.merriam-webster.com/ dictionary/connection (last visited Oct. 3, 2012). Black's Law Dictionary defines "connection" as "[t]he state of being connected or joined; union by junction, by an intervening substance or medium, by dependence or relation, or by order in a series." Black's Law Dictionary 302 (6th ed. 1990). Accordingly, by its terms, the phrase "in connection with" means somehow related to – but not necessarily in any particular order. As the Supreme Court has held over and over again, Congress is assumed to know the definitions of the words it uses in Federal laws; if Congress had intended to restrict the application of § 1028(a)(7), it could easily have written "prior to" or "preceding," rather than "in connection with." "[A]s the Supreme Court has often stated, 'courts must presume that a legislature says in a statute what it means and means in a

statute what it says there.'" Hanif v. Attorney General, — F.3d —, 2012 WL 4044727, at *4 (3d Cir. Sept. 14, 2012) (quoting Conn. Nat'l Bank v. Germain, 503 U.S. 249, 253–54 (1992)).

The preceding discussion shows that the defendant's reading of the statutory language is incorrect. Assuming arguendo, however, that he is right about the statute's meaning, his request to dismiss Count Two still fails, because the Superseding Indictment does allege that the defendant's possession and transfer of means of identification was, in part, during the unauthorized computer access.

The Superseding Indictment charges, in Count One, that the conspiracy to access AT&T's servers without authorization lasted from on or about June 2, 2010 to on or about June 15, 2010. See Superseding Indictment, Count One, ¶ 5. The Superseding Indictment further charges, in Count Two, that the defendant transferred, possessed, and used means of identification of other people, during the exact same time as charged in Count One – that is, from on or about June 2, 2010 to on or about June 15, 2010. Thus, contrary to the defendant's motion, the Superseding Indictment does not "allege[] that the unauthorized access was over before the disclosure of data to Gawker began," DB at 16 – the violations are alleged to be contemporaneous.

Perhaps more importantly, even if the unauthorized access did conclude before the disclosure to Gawker – the transfer of data – began, Count Two also

charges the defendant with possession of means of identification. The Superseding Indictment is eminently clear that the defendant possessed means of identification of at least some victims during the period of unauthorized access, before AT&T was able to stop the conspirators' unauthorized computer access and theft of victims' data. Count Two of the Superseding Indictment incorporates paragraph 23 of Count One of the Superseding Indictment. See Superseding Indictment, Count Two, ¶ 1. In turn, paragraph 23 of Count One alleges that on or about June 6, 2010, while the unauthorized access of AT&T's severs was still ongoing, "Spitler then proceeded to provide defendant AUERNHEIMER with an ICC-ID and e-mail address" for a victim. See id., Count One, ¶ 23. As noted above, these allegations must be taken as true, see Besmajian, 910 F.2d at 1154, and therefore, even if the defendant's reading of § 1028(a)(7) is correct, his argument fails in light of the allegations made in the Superseding Indictment itself: the Superseding Indictment alleges that the defendant possessed means of identification during the period of unauthorized computer access, contrary to § 1030(a)(2)(C), in violation of § 1028(a)(7).

For these reasons, the defendant's motion to dismiss Count Two of the Superseding Indictment should be denied.

POINT V

COUNT TWO DOES NOT VIOLATE THE FIRST AMENDMENT.

Without citing a shred of authority, and without accepting as true the allegations in the Superseding Indictment, the defendant contends that his disclosure to Gawker of approximately 120,000 stolen ICC-ID/e-mail pairings qualifies as First Amendment protected speech. DB at 18. Specifically, he contends that the disclosure of that personal identifying information to Gawker "served the public by exposing AT&T's non-existent security and cavalier disregard of its customer's information." Id. He then concludes that "Count Two must be struck down on First Amendment grounds," because "[t]he First Amendment forbids criminalizing the transmission of public information of public concern to the press." Id.

The defendant's First Amendment challenge is without merit. First, as a factual matter, the ICC-ID/e-mail pairings were not "public" information, but information that AT&T kept confidential. Superseding Indictment, Count 2, ¶ 1 (incorporating Paragraphs 1 through 4 and 7 through 27 of Count 1), Count 1, ¶¶ 1o ("The ICC-IDs and iPad user e-mail addresses were not available to the public and were kept confidential by AT&T"). Second, the knowing possession and transfer of stolen means of identification constitutes conduct with "little or no communicative value," not speech. See U.S. v. Chappell, 691 F.3d 388, 395 (4th

Cir. 2012) (holding that Virginia's police impersonation statute does not compromise First Amendment protections, finding that the "statute prohibits a species of identity theft in which there is little or no communicative value," and observing that "[t]his class of identity theft plays no essential part of any exposition of ideas"); see generally New York v. Ferber, 458 U.S. 747, 761-62 (1982) ("'It rarely has been suggested that the constitutional freedom for speech . . . extends its immunity to speech or writing used as an integral part of conduct in violation of a valid criminal statute.'") (quoting Giboney v. Empire Storage & Ice Co., 336 U.S. 490, 498 (1949)).

For the foregoing reasons, the defendant's motion to dismiss should be denied in its entirety.

Respectfully submitted,
PAUL J. FISHMAN
United States Attorney

By: /s/ Michael Martinez
MICHAEL MARTINEZ
Executive Assistant U.S. Attorney

By: /s/ Erez Liebermann
EREZ LIEBERMANN
Assistant U.S. Attorney

Newark, New Jersey
Date: October 5, 2012