UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CHRISTIAN W. SANDVIG *et al.*,

Plaintiffs,

v.

LORETTA LYNCH, in her official capacity as Attorney General of the United States,

Defendant.

Case No. 1:16-cv-1368 (JDB)

REPLY IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

Plaintiffs assert a preenforcement challenge to a provision of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(2)(C), under the First and Fifth Amendments to the United States Constitution. The challenged provision prohibits individuals from obtaining information by intentionally accessing a protected computer without authorization or in a manner that exceeds authorized access. Plaintiffs are seeking an Order permanently enjoining defendant from enforcing the provision in all instances. *See* Compl. at 47.

In their Opposition to defendant's Motion to Dismiss, plaintiffs fail to establish standing to pursue their claims. Standing to assert a First and Fifth Amendment preenforcement statutory challenge exists where a plaintiff shows that the challenged statutory provision regulates conduct implicating constitutional interests and a credible fear of prosecution exists. With respect to the regulation of constitutionally protected conduct, plaintiffs cite to no authority suggesting that the First Amendment protects an individual's ability to deploy information-gathering software on the websites of non-

consenting private entities or to post false information on corporate websites in violation of the website operator's terms of use. The First Amendment does not prohibit private website operators from placing restrictions on access to or conduct occurring on their websites. Indeed, the Supreme Court has held that the "constitutional guarantee of free expression has no part to play" in a case involving a private actor's abridgment of free expression in a private forum. *Hudgens v. NLRB*, 424 U.S. 507, 513 (1976). Additionally, plaintiffs provide no information in their Opposition that would render credible their purported fear of prosecution. In attempting to state such a fear, plaintiffs rely primarily on an excerpt from a CFAA educational manual last updated in 2010. The manual upon which plaintiffs rely does not state the policy of the Department of Justice; the Department's CFAA policy, which was issued more recently, expressly disfavors the sort of CFAA charge that plaintiffs claim to fear. Thus, because plaintiffs cannot show that the challenged provision regulates constitutionally protected conduct or establish a credible fear of prosecution, they lack standing to assert their preenforcement challenge.

Plaintiffs' Opposition also provides reason for the Court to dismiss their First and Fifth Amendment claims on their merits. With respect to their Free Speech Clause claim, plaintiffs fail to establish that the challenged provision implicates First Amendment interests. The restrictions on expression that plaintiffs identify are imposed by private actors governing conduct on privately owned and operated websites. Supreme Court precedent indicates that the First Amendment does not extend to such restrictions. With respect to their overbreadth claim, plaintiffs admit that limiting constructions of the challenged provision are possible, and they fail to argue credibly that the challenged provision expressly regulates conduct necessarily intertwined with speech, such as

picketing or demonstrating. Plaintiffs also provide no support for their contention that a Petition Clause claim is viable where the challenged statute does not regulate petitions to the government or create sanctions against individuals who submit a petition.

With respect to their Fifth Amendment claims, plaintiffs contend that the existence of a circuit split with respect to the proper interpretation of the challenged provision is evidence that the provision is unconstitutionally vague. Courts have categorically rejected similar arguments. Moreover, plaintiffs fail to recognize that the challenged provision contains a *mens rea* requirement, which the Supreme Court has held alleviates vagueness concerns. Finally, there is no merit to plaintiffs' contention that the challenged provision contains the type of broad delegation of legislative and executive power that the Supreme Court rejected in its Depression era non-delegation jurisprudence.

Accordingly, because plaintiffs cannot identify an injury sufficient to confer standing to sue and because plaintiffs fail to state a claim upon which relief can be granted, defendant respectfully requests the Court dismiss the complaint pursuant to Rule 12(b)(1) or 12(b)(6).

ARGUMENT

I. Plaintiffs Lack Standing to Sue.

A. Analogies to Real Property or Traditional Notions of Trespass may be Useful in Considering the Proper Interpretation of the CFAA.

In their Opposition, plaintiffs first argue that, in interpreting the CFAA and in considering the legal issues presented in the parties' briefing, the Court should eschew any invitation to analogize issues relating to the CFAA to scenarios involving real property or to traditional notions of trespass. *See* Opp'n at 9-10. Plaintiffs contend that,

because the basic nature of the internet is "open to all," any "analogy to property is . . . inaccurate" and "flawed." *Id.* at 9 (citing Orin S. Kerr, *Norms of Computer Trespass*, 166 Colum. L. Rev. 1143, 1162 (2016)).

Yet analogies to real property and traditional trespass may be particularly fitting in analyzing the CFAA given that Congress drafted the CFAA as an analogue to physical trespass law. Indeed, Professor Kerr, upon whom plaintiffs rely, has noted that the legislative history of the CFAA demonstrates that Congress intended for it to do "for computers what trespass and burglary laws did for real property." *See, e.g.*, Orin S. Kerr, *Cybercrimes' Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1617 (2003). In crafting the CFAA, Congress was specifically responding to what it considered to be a "recent flurry of electronic trespassing incidents." *See* H.R. Rep. No. 98–894, at 6, 9-10 (1984), *reprinted in* U.S.C.C.A.N. 1984, pp. 3689, 3691. After the statute's original enactment, Congress continued to rely on analogies to real property and to the legal framework of trespass in discussing the need for amendments to the statutory language. *See, e.g.*, H.R. Rep. No. 99-612, at 5-6 (1986) (equating computer hackers to "trespassers, just . . . as if they broke a window and crawled into a home while the occupants were away"); S. Rep. No. 99–432, at 7 (1986) (equating "unauthorized access" with "a simple trespass offense"). Indeed, in the very essay upon which plaintiffs rely, Professor Kerr argues that "[t]respass provides an appropriate framework" for considering restrictions on computer misuse. Kerr, *Norms of Computer Trespass*, 166 Colum. L. Rev. at 1159.[1]

[1] Contrary to plaintiffs' assertion, Professor Kerr does not broadly suggest that all websites on the internet are "open to all." Rather, he avers that the default protocol used in website publishing provides for general public access to websites, but he notes that

Moreover, federal courts considering the proper interpretation of the CFAA have frequently recognized the utility of analogies to more traditional fields of law, and those fields have varied depending on the relevant facts at issue. Thus, where the facts at issue concern employee misconduct, some courts have analogized to traditional theories of agency law. *See, e.g.*, *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). Where the facts at issue show a contractual relationship between the parties, some courts have analogized to traditional theories of contract law. *See, e.g.*, *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001). And where the facts at issue concern an individual's authorization to access information, some courts have analogized to traditional theories of trespass law. *See, e.g.*, *Theofel v. Farey–Jones*, 359 F.3d 1066, 1072–75, 1078 (9th Cir. 2004).

Accordingly, although trespass or other crimes against real property are governed by separate statues that have their own specific terms, given the CFAA's history and purpose, nothing prevents the Court from analogizing the facts at issue here to traditional notions of real property or to the legal framework governing trespass.

B. Plaintiffs Fail to Establish that the Challenged Provision of the CFAA Chills Conduct Protected Under the First Amendment.

To establish standing to assert a preenforcement First Amendment constitutional challenge to a statute, a plaintiff must show that "First Amendment rights are arguably chilled," and that "there is a credible threat of prosecution." *Chamber of Commerce of*

website operators often attempt to alter that default by "plac[ing] limits and restrictions on access to information." *Id.* at 1163. Those limits and restrictions can include terms of use restrictions, code-based access barriers, or other authentication requirements. *Id.* at 1157 (noting that "[c]ompanies often hire counsel to write detailed terms of use that purport to say when access is permitted").

U.S. v. Fed. Election Comm'n, 69 F.3d 600, 603 (D.C. Cir. 1995). In their Opposition, plaintiffs argue that the challenged provision of the CFAA impedes their ability to engage in three types of conduct: the gathering of information from the websites of private corporations through the use of data-scraping computer programs; the posting of fictional information on certain corporate websites and deploying computer software to collect and analyze responses to those postings; and the future publication of articles relating to the results of their information-gathering activity. *See* Opp'n at 10-18.[2] The Supreme Court has made clear, however, that First Amendment rights are not implicated where the expressive conduct at issue is limited by a private actor in a private forum. *See e.g.*, *Hudgens v. NLRB*, 424 U.S. 507, 513 (1976) ("[W]hile statutory or common law may in some situations extend protection or provide redress against a private corporation or person who seeks to abridge the free expression of others, *no such protection or redress is provided by the Constitution itself*.") (emphasis added). Thus, because the First Amendment does not protect the deployment of computer software on the websites of non-consenting private corporations, guarantee individuals the right to post information

[2] Plaintiffs also briefly analogize the conduct in which they intend to engage to the use of testers in the housing market who help uncover potential violations of the Fair Housing Act (FHA). *See* Opp'n at 14-15. To the extent plaintiffs are attempting to assert standing under the theory they are housing testers, the Court should reject such an argument as inapposite and unrelated to the claims asserted in this case. The Supreme Court has held that housing testers have standing to sue for FHA violations because, when a housing provider makes misrepresentations or discriminatory statements to a housing tester, the tester has suffered a statutory injury that satisfies traditional Article III standing principles. *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982). But plaintiffs here are not asserting FHA claims; they do not seek FHA damages, nor do they allege that any of their FHA rights have been violated. Thus, *Havens Realty Corp.* does not offer plaintiffs standing to preemptively strike a provision of a federal criminal statue.

on private websites in violation of restrictions set by the website operators, or prohibit private website operators from attempting to restrict publication of information available on a private website, plaintiffs are incapable of showing that their "First Amendment rights are arguably chilled." *Chamber of Commerce of U.S.*, 69 F.3d at 603.

Plaintiffs first allege that the First Amendment protects their ability to deploy on the websites of non-consenting private corporations bot-creating computer software designed to gather information about the business practices of those corporations. Although the challenged provision of the CFAA restricts certain types of access to protected computers, plaintiffs encourage the Court to not to rely on First Amendment jurisprudence addressing restrictions on access to information. *See* Opp'n at 13-14. Rather, plaintiffs contend that their proposed activity is protected by a First Amendment "right to record . . . information that is made available to them." *Id.* at 14. But the cases upon which plaintiffs rely to support the existence of such a right concern the recording of information of public importance in a public forum, such as street protests or police activity occurring in a public place. None of the cases suggests the existence of a First Amendment right to record corporate information from a website operated by a private entity through means that the website operator explicitly prohibits.

In support of their purported "right to record information made available to them" on the internet, plaintiffs rely on a series of decisions involving the recording of public activity occurring in a public forum, such as police actions and public protests. *Id.* (citing, *inter alia*, *ACLU of Ill. v. Alvarez*, 679 F.3d 583, 586 (7th Cir. 2012) (concerning the enforcement of an "eavesdropping statute against people who openly record police officers performing their official duties in public"); *Fordyce v. City of Seattle*, 55 F.3d

436, 438 (9th Cir. 1995) (concerning interference by police officers with an individual's attempt to videotape a public protest march); *Demarest v. Athol/Orange Cmty. Television, Inc.*, 188 F. Supp. 2d 82, 85 (D. Mass. 2002) (concerning the recording of a conversation with a public official on a public sidewalk).

These cases are readily distinguishable from the facts at issue here in that they concern government-imposed restrictions on the recording of activity of public importance occurring in a public forum, not privately-created restrictions on the retrieval and recording of information controlled by a private entity on a corporate website. Indeed, several of the cases explicitly caution that their analysis and holding rests on the public nature of the forum involved, and that a change in that forum would result in a change in the holding. The *Demarest* court, for example, found that the right to record matters of public interest "was not unlimited," and that the plaintiffs in that case "could not have invaded private homes, no matter how newsworthy the subject," and "plaintiffs did not have an unlimited right to publicize private facts." 188 F. Supp. 2d at 94–95.

The vitality of plaintiffs' argument that they have a "right to record information made available to them" appears to rest on the presumption that the internet in general, and certain corporate websites in particular, are the equivalent of the public fora at issue in the cases cited above. Plaintiffs, however, provide no legal support for that presumption. The Supreme Court has held that privately owned property can be considered as the equivalent of a public forum subject to constitutional obligations only in a scenario where the private property has taken on "all the characteristics" of public property, such as in a company-owned town. *See Marsh v. Alabama*, 326 U.S. 501, 502-03 (1946) (finding that the privately-owned town contained residential buildings, streets,

a system of sewers, a sewage disposal plant, security officers and other public attributes). Courts addressing whether a corporate website can be considered the equivalent of the company-owned town at issue in *Marsh* have rejected such a conclusion. *See, e.g.*, *Cyber Promotions, Inc. v. Am. Online, Inc.*, 948 F. Supp. 436, 442-45 (E.D. Pa. 1996) (rejecting the argument that a corporation's decision to open its website "to the public, free of charge to any user where public discourse, conversations and commercial transactions can and do take place" was sufficient to render the website a public forum).

Because the facts at issue in this case do not involve government-imposed restrictions on the recording of public activity occurring in a public forum, the appropriate issues to consider regarding plaintiffs' information-gathering activity are whether the First Amendment guarantees plaintiffs a right to gather information in the manner they desire, and whether the First Amendment requires website operators to provide that information without restriction. The Supreme Court's holdings in *Zemel v. Rusk*, 381 U.S. 1, 16-17 (1965), and *Houchins v. KQED, Inc.*, 438 U.S. 1, 10–11 (1978) address those issues. *Zemel* made clear that the First Amendment "right to speak and publish does not carry with it the unrestrained right to gather information." 381 U.S. at 16-17. And *Houchins* made clear that there is "no basis for the claim that the First Amendment compels others—private persons or governments—to supply information." 438 U.S at 11. Under that precedent, the Court should reject plaintiffs' contention that the First Amendment guarantees them the right to deploy software on the websites of a non-consenting corporations for the purpose of eliciting and recording corporate data despite website terms of use that prohibit such conduct.

For similar reasons, plaintiffs' alleged intent to post false information on certain corporate websites in violation of the terms of use of those websites and to deploy without the consent of the website operator software that collects and analyzes responses to those false postings is also not conduct that the First Amendment protects. In support of their position that the First Amendment guarantees individuals the right to post false information on a corporate website, plaintiffs rely on a series of cases in which the government placed direct, content-based restrictions on untruthful speech. *See e.g.*, Opp'n at 14-17 (citing, *inter alia*, *United States v. Alvarez*, 132 S. Ct. 2537, 2546 (2012) (rejecting the constitutionality of a statute that created criminal penalties for making false statements regarding the receipt of a military award); *281 Care Comm. v. Arneson*, 766 F.3d 774, 795 (8th Cir. 2014) (rejecting the constitutionality of a statute providing criminal penalties for making false statements regarding ballot questions); *Animal Legal Def. Fund v. Otter*, 118 F. Supp. 3d 1195, 1202 (D. Idaho 2015) (appeal pending) (rejecting the constitutionality of a statute providing criminal penalties for "speech critical of animal agricultural practices").

These cases stand for the proposition that the untruthful content of certain speech does not necessarily alleviate First Amendment concerns with the government's ability to enact content-based restrictions on that speech. They do not, however, address facially neutral statutes of general applicability, such as the CFAA, nor do they stand for the proposition that individuals have a First Amendment right to access a private forum and engage in speech in that forum in a manor prohibited by a private actor who controls the forum. Indeed, courts have routinely rejected the claim that First Amendment rights are implicated where limitations on speech are created by a private actor in a forum

controlled by a private individual or corporation. *See Pacific Gas & Elec. Co. v. Pub. Util. Comm'n of Cal.*, 475 U.S. 1, 28 (1986) ("[The] First Amendment does not itself grant a right of access to private forums"); *Wilson v. Layne*, 526 U.S. 603, 613 (1999) (there is no First Amendment right to record photographs of the execution of a search warrant in a private home without the consent of the homeowner).

The Supreme Court's holding in *Hudgens v. NLRB*, 424 U.S. 507, 519-21 (1976), may be most analogous to the facts at issue here. *Hudgens* involved picketing at a large, privately-owned shopping mall that was generally open to the public. The shopping mall owner prohibited picketing on the grounds of the shopping center and threatened picketers who disobeyed the prohibition with arrest for trespass. The Court held that, because the restriction on picketing was created by a private actor an applied to a privately-controlled forum, the "constitutional guarantee of free expression has no part to play in a case such as this." *Id.* at 521. The Court noted that the First Amendment would apply to similar restrictions only in a situation in which the privately-owned property served as *de facto* municipality, such as in a company-owned town. *Id.* at 519.

Like *Hudgens*, the restrictions on expression that plaintiffs complain of here result from terms of use created by private entities, and those terms apply to privately-owned websites. Although those websites, like the shopping mall in *Hudgens*, can be visited by members of the public, the websites do not provide government functions and municipal services similar to those provided in a company town. *See Cyber Promotions, Inc.*, 948 F. Supp. at 442-45. Accordingly, the First Amendment "has no part to play" in reviewing of the terms of use restrictions of which plaintiffs complain.

Plaintiffs' final allegation—that a website operator theoretically could attempt to issue a term of use that purports to prohibit the future publication of information accessed through a corporate website— fails to implicate a First Amendment guarantee for the same reason articulated in *Hudgens, i.e.*, such a restriction would be created by a private actor in a private forum. Moreover, plaintiffs cannot state preenforcement claims based on hypothetical concerns or imaginary situations. *See Wash. State Grange v. Wash. State Republican Party*, 552 U.S. 442, 449-50 (2008) ("In determining whether a law is facially invalid, we must be careful not to go beyond the statute's facial requirements and speculate about 'hypothetical' or 'imaginary' cases."). The Complaint contains no allegation that any website on which plaintiffs intend to conduct their activity contains such a restriction, Compl. ¶¶ 72-74, and plaintiffs lack standing to assert claims based on hypothetical circumstances. *See, e.g.*, *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992) (to satisfy Article III standing, a plaintiff must establish, *iner alia*, an "injury in fact," which is "concrete and particularized . . . not conjectural or hypothetical"); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007) ("[A] plaintiff's obligation to provide the grounds of his entitlement to relief requires more than labels and conclusions" and "[f]actual allegations must be enough to raise a right to relief above the speculative level.") (internal quotation marks and citations omitted).

C. Plaintiffs Are Unable to Allege A Credible Threat of Prosecution

Plaintiffs lack standing for the independent reason that they have not alleged "a credible threat of prosecution." *Chamber of Commerce*, 69 F.3d at 603–04. Plaintiffs fail to meet *any* of the factors that courts consider in determining whether a credible threat of prosecution exists. *See Johnson v. D.C.*, 71 F. Supp. 3d 155, 160 (D.D.C. 2014).

Specifically, plaintiffs make no allegation that the government has threatened them with CFAA enforcement; they cite no instances in which the government has enforced the challenged provision for harmless terms of service violations; and the Department of Justice (DOJ) has expressly stated that it has no intention of prosecuting harmless terms of service violations that are not in furtherance of other criminal activity or tortious conduct. As plaintiffs are incapable of stating a credible threat of prosecution under the CFAA, they lack standing to assert their preenforcement challenge.

In their Opposition, plaintiffs allege that a credible threat of prosecution exists under the CFAA for harmless terms of use violations because a manual published in 2010 by the Office of Legal Education (OLE) in DOJ's Executive Office for U.S. Attorneys suggests that prosecutors might rely on terms of use violations in proving the unauthorized access element of a CFAA violation. *See* Opp'n at 24-25. Plaintiffs contend that their fear of prosecution remains credible because the government has failed to suggest that the manual "is out of date," nor does the government "mention plans to alter the DOJ Manual to discourage prosecutions except in certain narrow instances identified in [defendant's opening] brief." *Id.* at 24.

The OLE manual was designed as an educational tool; it expressly cautions that it does not and has never created binding prosecutorial guidelines for U.S. Attorneys. *See* OLE, *Prosecuting Computer Crimes*, at v[3] ("This manual is intended as assistance, not authority. The research, analysis, and conclusions herein . . . do not represent the official position of the Department of Justice or any other agency. This manual has no regulatory effect, confers no rights or remedies, and does not have the force of law or a U.S.

[3] The manual is available at https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (last visited Oct. 24, 2016).

Department of Justice directive."). Accordingly, any fear plaintiffs assert arising from the presumption that the manual governs federal prosecutions is not credible.

Actual DOJ policy is not announced in OLE manuals but through directives from DOJ leadership. In 2014, the Attorney General issued a memorandum to relevant DOJ officials setting forth intake and charging policies for CFAA prosecutions. *See* Mem. from the Att'y Gen. to U.S. Att'ys and Assistant Att'ys Gen. for the Criminal and Nat'l Sec. Divs. (Sept. 11, 2014) (attached hereto as Ex. 1). That binding guidance makes clear that CFAA prosecutions should only be pursued when a "substantial federal interest would be served by prosecution[.]" The memorandum sets forth a number of factors that prosecutors must consider in determining whether to seek charges against potential defendants for violations of the CFAA. Consistent with the position articulated in defendant's opening brief and with the statements that Department officials have made publically to Congress, those factors include, *inter alia*, whether the access in question "threatened national or economic interests, was in furtherance of a larger criminal endeavor, or posed a risk of bodily harm or threat to national security[.]" *Id.* at 4. The memorandum also cautions that "if the defendant exceeded authorized access solely by violating an access restriction contained in a . . . term of service with . . . [a] website, federal prosecution may not be warranted." *Id.* at 5. Moreover, to ensure consistency in charging decisions across the country, the Attorney General has required government attorneys to consult with a central office in the Criminal Division of DOJ prior to making a charging decision under the CFAA. *Id.* at 6. The guidelines contained in the 2014 Memorandum render plaintiffs' purported fear of prosecution even more implausible.

Additionally, in their Opposition, plaintiffs do not dispute that the only CFAA cases they previously identified as examples of "terms of use violation prosecutions" actually involved code-based access violations (not mere terms of use violations), or conduct committed in furtherance of other crimes or torts that resulted in substantial harm. *See United States v. Drew*, 259 F.R.D. 449, 452 (C.D. Cal. 2009) (defendant charged under the felony portion of the CFAA for violating a website's terms of use for the purposes of committing the tort of intentional infliction of emotional distress in a case involving cyber bullying that resulted in the suicide death of a thirteen year-old girl); *United States v. Lowson*, Crim. No. 10-114 KSH, 2010 WL 9552416, at *1 (D.N.J. Oct. 12, 2010) (unreported) (defendants charged with using *code-based access breaches* to gather information in furtherance of a fraudulent scheme that resulted in more than $25 million dollars in illegitimate profit).

Plaintiffs have not been threatened with CFAA enforcement, they identify no instances in which DOJ has enforced the CFAA for harmless terms of use violations, and DOJ has denied any intention of prosecuting harmless terms of use violations that are not in furtherance of other crimes or torts. Accordingly, plaintiffs cannot assert a credible threat of prosecution, and their preenforcement challenge should be dismissed. *See Johnson*, 71 F. Supp. 3d at 160; *see also Firearms Imp./Exp. Roundtable Trade Grp. v. Jones*, 854 F. Supp. 2d 1, 19–20 (D.D.C. 2012), *aff'd sub nom. Firearms Imp./Exp. Roundtable Trade Grp. v. ATFE*, 498 F. App'x 50 (D.C. Cir. 2013) (no standing to assert a Fifth Amendment vagueness claim where there is "no evidence of even an intent to investigate plaintiffs" and the asserted injury consists of a fear of "possible criminal prosecution" and a claim that they "cannot determine what is illegal and what is legal").

II. Plaintiffs Fail to State a Claim Upon Which Relief Can Be Granted.

A. Plaintiffs Fail to State a Free Speech Claim.

In addressing a First Amendment claim, Courts first determine whether the allegedly restricted conduct is protected speech activity, "for, if it is not, [the court] need go no further." *Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, 473 U.S. 788, 797 (1985). The First Amendment's protections are "a restraint on government action, not that of private persons," thus, in stating a First Amendment claim, a plaintiff must establish a nexus to state action. *Columbia Broad. Sys., Inc. v. Democratic Nat. Comm.*, 412 U.S. 94, 114 (1973). As discussed in more detail above, the First Amendment "has no part to play in a case" involving a private actor's restriction on speech in a forum controlled by a private entity, and a plaintiff cannot rely on the government's enforcement of a criminal statute arising from violations of private rights to satisfy the state action requirement. *Hudgens*, 424 U.S. at 521; *NB ex rel. Peacock v. D.C.*, 794 F.3d 31, 43 (D.C. Cir. 2015) (state action exists where "there is such a close nexus between the State and the challenged action that seemingly private behavior may be fairly treated as that of the State itself," such as "when a private party acts as an agent of the government") (internal citations omitted).

Plaintiffs ostensibly attempt to show a nexus between state action and the terms of use restrictions contained on private websites by asserting that the government may one day regulate terms of service violations pursuant to the authority contained in the CFAA. But, absent a scenario involving a company-owned town, Courts have refused to extend First Amendment protections to restrictions on expression imposed by private actors in private fora where the only nexus to state action is the possibility that the government

might enforce content neutral crimes of general applicability, such as effectuating an arrest for trespass on property. In *Cape Cod Nursing Home Council v. Rambling Rose Rest Home*, 667 F.2d 238, 239 (1st Cir. 1981), the First Circuit, relying on *Hudgens*, held that that a legal services organization failed to show a sufficient nexus to state action to establish a First Amendment right to access a privately-owned nursing home, despite the fact that representatives of the legal organization were "arrested and charged with criminal trespass" for attempting access. The court reasoned that "[s]ince plaintiffs had no right to be on the property, the police action in removing them could not in itself create such a right where none existed before." *Id.* at 243. The Court thus rejected plaintiff's attempt "to create a first amendment right of access simply from the police involvement in arresting them[;] . . . [t]his bootstrap argument would turn any arrest in support of private rights into state action, thereby eviscerating" the state action requirement. *Id.*; *see also Loren v. Sasser*, 309 F.3d 1296, 1303 (11th Cir. 2002) (homeowners' association's denial of permission to post a "for sale" sign on plaintiffs' yard was not state action merely based on the potential judicial enforcement of a deed restriction barring the display of signs); *King v. Friends of Kelly Ayotte*, 860 F. Supp. 2d 118, 125 (D.N.H. 2012), *aff'd* (Apr. 5, 2013) ("Defendants' use of municipal police officials to enforce their rights does not convert their private actions into state conduct.").

Plaintiffs here are similarly attempting to create a First Amendment right to access and gather information from the websites of private companies by asserting a nexus to state action arising from the potential that the government might one day be involved in enforcing the CFAA. But just as the government's enforcement of a trespass statute in *Cape Cod* was insufficient to create a First Amendment right to enter a nursing

home where one did not previously exist, the government's potential enforcement of the CFAA does not create a First Amendment right to access and gather information from private corporations where those corporations otherwise prohibit such conduct. Thus, because the First Amendment "has no part to play" in this case, *Hudgens*, 424 U.S. at 521, the Court "need go no further." *Cornelius*, 473 U.S. at 797.

B. Plaintiffs Fail to State an Overbreadth Claim.

Even if the challenged provision implicated First Amendment interests (which is does not), Plaintiffs provide no authority in their Opposition that would allow their preenforcement overbreadth challenge to survive. Plaintiffs admit that a limiting construction can be placed on the challenged provision that would alleviate their overbreadth concerns. That admission is sufficient to extinguish their preenforcement overbreadth challenge. Plaintiffs also fail to point to any authority indicating that the challenged provision is so substantially overbroad that it will "significantly compromise recognized First Amendment protections of parties not before the Court." *New York State Club Ass'n, Inc.*, 487 U.S. at 11 (1988). And although they attempt to distinguish *Virginia v. Hicks*, 539 U.S. 113, 124 (2003), they cannot reasonably assert that the challenged provision is "specifically addressed to speech or to conduct necessarily associated with speech (such as picketing or demonstrating)." Considering the Supreme Court has admonished that the overbreadth doctrine is "strong medicine" that should be administered "only as a last resort," the Court should reject plaintiffs' attempt to invalidate the challenged provision on overbreadth grounds. *L.A. Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32, 39 (1999).

The Supreme Court has cautioned that "[f]acial overbreadth has not been invoked when a limiting construction has been or could be placed on the challenged statute." *Broadrick v. Oklahoma*, 413 U.S. 601, 613 (1973) (gathering cases). Plaintiffs admit in their Opposition that their overbreadth concerns would "be addressed were the statute to be construed not to reach terms-of-use violations alone[.]" Opp'n at 35. Several courts have adopted such a construction. *See, e.g.*, *United States v. Nosal*, 676 F.3d 854, 863-64 (9th Cir. 2012). Accordingly, because "a limiting construction has been or could be placed on the challenged statute," plaintiffs' preenforcement overbreadth challenge must fail. *Broadrick*, 413 U.S. at 613.

Plaintiffs also fail to demonstrate in their Opposition that the challenged provision is so substantially overbroad that it will "significantly compromise recognized First Amendment protections of parties not before the Court." *N.Y. State Club Ass'n, Inc.*, 487 U.S. at 11 (1988). The Supreme Court recognized in *Hicks* that such an overbreadth challenge "[r]arely, if ever, will . . . succeed against a law or regulation that is not specifically addressed to speech or to conduct necessarily associated with speech (such as picketing or demonstrating)." 539 U.S. at 124. Plaintiffs argue that the phrase "exceeds authorized access" as it appears in the challenged provision specifically addresses recognized speech activity equivalent to picketing or demonstrating. Opp'n at 35. But plaintiffs point to no authority equating "exceeding authorized access to a computer" with recognized First Amendment activity. Given the Supreme Court's caution that overbreadth doctrine should be invoked "only as a last resort," this Court should decline to expand the doctrine to activity not previously recognized as protected.

C. Plaintiffs Fail to State a Petition Clause Claim.

The challenged provision does not create a general prohibition on certain forms of government advocacy, nor does it impose sanctions for the expression of particular views that the government opposes. Accordingly, plaintiffs fail to state a claim that the challenged provision violates the Petition Clause. *See Smith v. Ark. State Highway Emps., Local 1315*, 441 U.S. 463, 464 (1979) (*per curiam*).

In their Opposition, plaintiffs present a theory of a Petition Clause violation that is unsupported by law or facts. Plaintiffs' theory rests on the assertion that a hypothetical private website's terms of use could theoretically include a non-disparagement provision that would purport to restrict the subsequent publication of information gathered from the website, which in turn might inhibit plaintiffs' ability to one day petition the government. *See* Opp'n at 43. Plaintiffs provide no legal support for the contention that a Petition Clause claim can be asserted under such an attenuated theory, and, as mentioned above, the Supreme Court has expressly cautioned that facial challenges to federal statutes that rely on speculation or hypothetical situations cannot be sustained. *See Wash. State Grange*, 552 U.S. at 449-50. Moreover, contrary to plaintiffs' theory, courts have routinely rejected Petition Clause claims that fail to identify specific and direct prohibitions on government advocacy. *See, e.g., United States v. Harriss*, 347 U.S. 612, 625 (1954) (statute requiring lobbyists to register with Congress and to make specific disclosures did not violate the plaintiff's First Amendment petition rights); *Nat'l Ass'n for the Advancement of MultiJurisdiction Practice v. Roberts*, Civ. Action No. 13-01963-NMG, 2015 WL 10459071, at *11 (D.D.C. Dec. 31, 2015) (rejecting a Petition Clause claim where the regulation at issue did not facially "restrict [an individual's] ability . . . to

file petitions"); *Ryan, LLC v. Lew*, 934 F. Supp. 2d 159, 173 (D.D.C. 2013) (rejecting Petition Clause claim where the agency directive did not categorically prohibit the pursuit of claims with the agency).

Additionally, as discussed above, in asserting any First Amendment claim, a plaintiff must identify a sufficient nexus between state action and a restriction on constitutionally protected conduct. *See Columbia Broad. Sys., Inc.*, 412 U.S. at 114. A theoretical restriction imposed by a private actor regarding information gathered from the website of a private company lacks a nexus to state action sufficient to create a First Amendment right. And such a right—under the Petition Clause or any other clause—does not spring into being simply because the state might have the authority to enforce laws of general applicability that relate to private rights. *See King*, 860 F. Supp. 2d at 125 ("Defendants' use of municipal police officials to enforce their rights does not convert their private actions into state conduct.").

D. Plaintiffs Fail to State a Vagueness Claim.

In their Opposition, plaintiffs concede that the challenged provision of the CFAA is amenable to a limiting construction that mitigates their constitutional concerns. *See* Opp'n at 35, 38. That concession renders their facial vagueness claim subject to dismissal. Plaintiffs' Opposition also fails to address Supreme Court precedent indicating that the presence of a *mens rea* requirement in a criminal statute alleviates vagueness concerns, particularly with respect to a statute that does not explicitly regulate constitutionally protected conduct. *See City of Chicago v. Morales*, 527 U.S. 41, 55 (1999). The challenged provision is subject to a *mens rea* requirement, and it does not

explicitly regulate constitutionally protected conduct. Accordingly, the Court should decline to consider plaintiffs' facial vagueness claim.

Facial vagueness challenges to federal statutes are not favored, particularly with respect to statutes that do not explicitly inhibit First Amendment freedoms. *Wash. State Grange*, 552 U.S. at 450 (facial vagueness challenges are "disfavored for several reasons," including because such claims often "rest on speculation"). For statutes that do not explicitly inhibit First Amendment freedoms, vagueness challenges "must be examined in the light of the facts of the case at hand." *United States v. Mazurie*, 419 U.S. 544, 550 (1975). And the Supreme Court has recently reaffirmed that, "before striking a federal statute as impermissibly vague," courts must consider "whether the prescription is amenable to a limiting construction." *Welch v. United States*, 136 S. Ct. 1257, 1268 (2016) (citing *Skilling v. United States*, 561 U.S. 358, 405 (2010)).

Plaintiffs admit in their Opposition that a limiting construction of the challenged provision is possible, and that multiple courts have overcome vagueness challenges to the CFAA by interpreting the statute in a limited manner in light of the as-applied facts at hand. *See, e.g.*, *Nosal*, 676 F.3d at 859-63. Plaintiffs contend, however, that their vagueness challenge can survive because the existence of a circuit split regarding the scope of the challenged provision renders the provision vague. *See* Opp'n at 37-38. Courts have consistently rejected that style of argument. *See, e.g., United States v. Morris*, 821 F.3d 877, 880 (7th Cir. 2016) ("[A] circuit split is insufficient to show that a statute is unconstitutionally vague."); *United States v. Morrison*, 686 F.3d 94, 104 (2d Cir. 2012) (same); *United States v. Kernell*, 667 F.3d 746, 754 (6th Cir. 2012) ("[T]he fact that different courts have interpreted a statute differently does not make the statute

vague—if that were true, a circuit split over the interpretation of a criminal statute would by definition render the statute unconstitutional."). Thus, because the challenged provision is "amenable to a limiting construction" that alleviates plaintiffs' constitutional concerns, a preenforcement facial vagueness challenge seeking to enjoin enforcement of the provision in all instances cannot survive. *See Skilling*, 561 U.S. at 405.

Moreover, the Supreme Court has held that facial vagueness challenges are appropriate where "a criminal law . . . contains no *mens rea* requirement . . . and infringes on constitutionally protected rights." *City of Chicago v. Morales*, 527 U.S. 41, 55 (1999). As explained above, the challenged provision does not infringe on constitutionally protected rights. *See infra* Part I.B. And, in any event, the provision is subject to the *mens rea* requirement of intentionality. *See* 18 U.S.C. § 1030(a)(2). The existence of that requirement, which plaintiffs ignore in their Opposition, provides further support for the dismissal of plaintiffs' facial vagueness challenge. *See, e.g.*, *Gonzales*, 550 U.S. at 149 ("[S]cienter requirements alleviate vagueness concerns."); *Colautti v. Franklin*, 439 U.S. 379, 395 (1979) ("This Court has long recognized that the constitutionality of a vague statutory standard is closely related to whether that standard incorporates a requirement of *mens rea*.").

E. Plaintiffs Fail to State a Non-Delegation Claim.

In their Opposition, plaintiffs contend that the challenged provision of the CFAA contains an unconstitutional delegation of legislative power to a private party akin to the delegation the Supreme Court rejected in *Carter v. Carter Coal Co.*, 298 U.S. 238 (1936). It does not. The *Carter Coal* delegation differed dramatically in form and substance from the general prohibition against unauthorized computer access contained in the challenged

provision. Plaintiffs also contend that the challenged provision can be distinguished from the dozens of other generally applicable criminal statutes the enforcement of which depends on authorization from a private entity. Plaintiffs, however, fail to identify any reason for distinguishing the challenged provision. Because a generally applicable statute does not violate the non-delegation doctrine simply because its application depends on the actions of private citizens, plaintiffs' non-delegation claim fails.

Plaintiffs' contention that the challenged provision constitutes a delegation of authority akin to the facts of *Carter Coal* lacks merit. *Carter Coal* did not involve a general statutory prohibition on conduct. It involved a statute that expressly provided a private commission with the authority to set maximum working hours and minimum wages for the entire nation's bituminous coal mining industry. *Carter Coal*, 298 U.S. at 310-11. The statute also explicitly authorized the private commission to enforce those hour and wage rules against dissenting coal producers by subjecting them to severe penalties. *Id.* The Supreme Court rejected the delegation because the power conferred on the commission was "in effect, the power to regulate the affairs of an unwilling minority." *Id.* Unlike *Carter Coal*, the CFAA does not contain any explicit delegation whatsoever, and it cannot be seriously argued that the CFAA expressly empowers private website operates with the ability to issue broad regulations that are binding on an entire national industry, to adjudicate liability for failure to comply with such regulations, or to exercise executive authority to enforce those regulations against third parties. Put simply, the Supreme Court's private non-delegation jurisprudence is inapplicable here.

Moreover, were the Court to adopt plaintiffs' theory of non-delegation, every statue that depends in part on the authorization of private citizens for enforcement would

be rendered unconstitutional. Plaintiffs attempt to distinguish similar statutes, such as trespass, copyright, or trade secret laws, by arguing that the owner of a property, copyright, or trade secret "has the right to control *only use* of the particular property in question." Opp'n at 42 (emphasis added). But plaintiffs fail to cite authority for that proposition, and they fail to distinguish why the same logic is inapplicable to website operators. A person who owns a copyright, for example, can restrict not just the use of the copyrighted material, but also the ability of others to record the material, to reproduce the material, or to create derivative works based on the material, among other things. *See* 17 U.S.C. § 106. Moreover, plaintiffs identify no authority suggesting that an individual who creates a website lacks the right to control the website; indeed, website operators can and do control content of and access to their sites. By analogy, if a homeowner determines that she wants a guest in her home to refrain from engaging in certain speech, Congress has not unconstitutionally delegated legislative authority to her simply because a trespass statute might authorize the government to remove a guest who offends her rules and refuses to leave. The fact that authorization from a private party may be a factor in determining the applicability of a federal statute does not render the statute unconstitutional, and plaintiffs identify no authority indicating otherwise.

CONCLUSION

For the foregoing reasons, defendant respectfully request that the Court dismiss the Complaint pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure.

October 24, 2016

Respectfully Submitted,

BENJAMIN C. MIZER
Principal Deputy Assistant Attorney General

JOHN R. TYLER
Assistant Branch Director

/s/ Stephen J. Buckingham
STEPHEN J. BUCKINGHAM (MD Bar)
Special Counsel
U.S. Department of Justice, Civil Division
Tel: (202) 514-3330
Fax: (202) 616-8470
Email: stephen.buckingham@usdoj.gov
P.O. Box 883 Ben Franklin Station
Washington, DC 20530

Attorneys for Defendant

CERTIFICATE OF SERVICE

I certify that on October 24, 2016, I caused a copy of this Reply in Support of Defendant's Motion to Dismiss to be filed electronically and that this documents is available for viewing and downloading from the ECF system. Participants in the case who are registered CM/ECF users will be served by the CM/ECF system.

/s/ Stephen J. Buckingham
STEPHEN J. BUCKINGHAM

Office of the Attorney General

Washington, D.C. 20530

September 11, 2014

MEMORANDUM TO THE UNITED STATES ATTORNEYS AND ASSISTANT ATTORNEY GENERALS FOR THE CRIMINAL AND NATIONAL SECURITY DIVISIONS

FROM: EA THE ATTORNEY GENERAL

SUBJECT: Intake and Charging Policy for Computer Crime Matters

Cyber-based crimes are one of the fastest growing threats our nation faces. Although laws addressing the misuse of computers have not kept pace uniformly with developments in technology and criminal schemes, the Computer Fraud and Abuse Act ("CFAA"), codified at Title 18, United States Code, Section 1030, remains an important law for prosecutors to address cyber-based crimes. As technology and criminal behavior continue to evolve, however, it also remains important that the CFAA be applied consistently by attorneys for the government and that the public better understand how the Department applies the law.

To accomplish these goals, I recently asked the Criminal Division to work with the National Security Division, the Executive Office of United States Attorneys, and the Attorney General's Advisory Committee to develop a policy to guide attorneys for the government in the appropriate considerations for prosecutors contemplating charges under the CFAA. The resulting policy is effective immediately.

A. *Policy.* In addition to the considerations set forth in USAM 9-27.230, which are incorporated herein by reference, an attorney for the Department of Justice should consider the following additional factors in determining whether prosecution of a violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, should be pursued because a substantial federal interest would be served by prosecution in a case in which the admissible evidence is expected to be sufficient to sustain a conviction. It is recognized that the significance of any cyber event for a District can vary depending on facts and circumstances specific to the District. Factors to be considered include:

1. The sensitivity of the affected computer system or the information transmitted by or stored on it and the likelihood and extent of harm associated with damage or unauthorized access to the computer system or related disclosure and use of information;

2. The degree to which damage or access to the computer system or the information transmitted by or stored on it raises concerns pertaining to national security, critical infrastructure, public health and safety, market integrity, international relations, or other considerations having a broad or significant impact on national or economic interests;
3. The extent to which the activity was in furtherance of a larger criminal endeavor or posed a risk of bodily harm or a threat to national security;
4. The impact of the crime and prosecution on the victim or other third parties;
5. Whether the criminal conduct is based upon exceeding authorized access consistent with the policy set forth at page 4 below;
6. The deterrent value of an investigation or prosecution, including whether the need for deterrence is increased because the activity involves a new or expanding area of criminal activity, a recidivist defendant, use of a novel or sophisticated technique, or abuse of a position of trust or otherwise sensitive level of access, or because the conduct is particularly egregious or malicious;
7. The nature of the impact that the criminal conduct has on a particular District or community; and,
8. Whether any other jurisdiction is likely to prosecute the criminal conduct effectively, if the matter is declined for federal prosecution.

B. *Comment.* This policy lists factors that may be relevant in determining whether prosecution of violations of the CFAA should be pursued because a substantial federal interest would be served by prosecution in a case in which the person is believed to have committed an offense under the Act and the admissible evidence is expected to be sufficient to sustain a conviction. The list of relevant considerations and examples of criminal conduct illustrating those factors are not intended to be all-inclusive. Not all of the factors will be applicable to every case, and in any particular case one factor may deserve more weight than it might in another case. The principles set forth here, and internal office procedures adopted pursuant to this memorandum, are intended solely for the guidance of attorneys for the government. They are not intended to, do not, and may not be relied upon to create a right or benefit, substantive or procedural, enforceable at law by a party to litigation with the United States.

1. **Sensitivity of Affected Computer System or Information.** In determining whether to bring a charge for violation of 18 U.S.C. § 1030 in a case involving obtaining information from a protected computer, consideration should be given to the sensitivity and value of the information involved and the potential for harm associated with its disclosure or use. Examples of the types of information that should be given a high priority for federal prosecution when illegally accessed include sensitive personal information such as intimate photographs or correspondence, medical,

educational or financial records, Social Security numbers, biometric information, and other personal identification information, and passwords and access devices; trade secrets, valuable intellectual property, and other confidential business information; and classified or other sensitive government information. To be clear, federal prosecution may be warranted even where the offender did not actually obtain any such information; in other words, in certain aggravated circumstances, mere access to a computer system that stores these types of sensitive information may weigh in favor of prosecution. Further, federal prosecution may be warranted for conduct that involves accessing a computer system without authorization or in excess of authorization for the purpose of selling or trafficking in sensitive information or the public distribution of private information. Conversely, federal prosecution may not be warranted if the information obtained is otherwise publicly available or has little value.

2. **Potential for Broad or Significant Impact on National or Economic Interests.** Many types of offenses under the CFAA can have an impact far beyond the particular computer that is directly affected by the actions of the offender. Unauthorized access to a computer containing classified information, for example, can harm national security. Shutting down a computer that controls a portion of the electrical grid can harm business activities and put public safety at risk. Unauthorized access to stock market computers can undercut investors' faith in the fairness of the market. And the actions of terrorist organizations and foreign governments can cause significant harms to the safety and prosperity of Americans. Similarly, many types of malicious software can affect thousands of computers or more across the country and have the potential to invade the privacy and harm the financial security of those computers' users. Where criminal activity risks these broad harms or has a substantial effect in several parts of the country, federal prosecution may be warranted. In other circumstances, if the effect of a violation is geographically focused and limited, deference to state or local authorities may be warranted, where they have the legal tools and resources to act.

3. **Connection to Other Criminal Activity or Risk of Bodily Harm.** Offenses under the CFAA often occur in concert with, and in furtherance of, other criminal activity, including that which poses a threat to national security. Depending on the nature of the predicate criminal activity, such circumstances may weigh in favor of federal prosecution. Organized criminal enterprises, for example, access banking and financial computers to steal information in furtherance of fraud and extortion schemes. Individual hackers may gain access to the private information of others in order to stalk or harass, to encourage others to harass or endanger public officials and

other victims, or to profit from its sale. Disrupting a hospital computer can place patients' lives in danger.

4. **Impact of the Crime and Prosecution on Victim or Other Third-Parties.** An attorney for the government may consider whether investigation and prosecution might result in further negative impacts on victims or third-parties that cannot otherwise be avoided. Thus, prosecutors should take into account the impact of the crime on the victim, as detailed in USAM 9-27.230.

5. **Exceeding Authorized Access**. Several portions of the CFAA prohibit obtaining information by accessing a protected computer either (1) without authorization, or (2) in a manner that "exceeds authorized access." Some exceeds-authorized-access violations may occur where the actor had authorization to access the computer for one purpose but accessed the computer for a prohibited purpose. For example, in several circuits, violation of the statute under the exceeds-authorized-access theory might occur where an employee accesses sensitive corporate information in violation of the company's access policy, or where a law enforcement officer accesses the National Crime Information Center ("NCIC") computers to obtain information in order to stalk a former romantic partner, which would violate NCIC's access restrictions.

   When prosecuting an exceeds-authorized-access violation, the attorney for the government must be prepared to prove that the defendant knowingly violated restrictions on his authority to obtain or alter information stored on a computer, and not merely that the defendant subsequently misused information or services that he was authorized to obtain from the computer at the time he obtained it. As part of proving that the defendant acted knowingly or intentionally, the attorney for the government must be prepared to prove that the defendant was aware of such access restrictions.

   The extent of the federal interest in exceeds-authorized-access prosecutions under section 1030(a)(2) varies based upon both the nature of the conduct and the nature of the information obtained during the offense. As with situations presenting an increased need for deterrence, one factor that supports prosecutions under the exceeds-authorized-access provision is the abuse of a position of trust. Examples would include situations in which a system administrator invaded the privacy of email accounts in violation of company policy and for personal gain, or in which a government official accessed information stored on government computers in contravention of clear rules prohibiting such access. Likewise, if the criminal conduct threatened national or economic interests, was in furtherance of a larger criminal endeavor, or posed a risk of bodily harm or threat to national security, those

factors would weigh in favor of prosecution. On the other hand, if the defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website, federal prosecution may not be warranted.

6. **Increased Need for Deterrence.** As technology advances, criminals discover novel ways to exploit it. For example, as mobile devices become increasingly powerful and flexible, they have also increasingly become a target for computer criminals. An individual may also abuse a trusted position to commit a computer crime, or may exhibit particularly malicious motivation or egregious behavior. These considerations may, in combination with other factors, weigh in favor of federal prosecution.

7. **Extent of Harm to One District or Community.** In deciding whether to bring a CFAA prosecution in a particular District, the attorney for the government should consider how much harm the criminal activity caused within the relevant District or community. Where an offense causes particularly significant harm to a single District or community, federal prosecution may be warranted.

8. **Possibility of Effective Prosecution in Another Jurisdiction.** In determining whether prosecution should be pursued even though the person is subject to effective prosecution in another jurisdiction, the attorney for the government should weigh the considerations discussed in USAM 9-27.240.

C. *Consultation.*

1. **Introduction**

Cases under the CFAA are often complex, and analysis of whether a particular investigation or prosecution is warranted often requires a nuanced understanding of technology, the sensitivity of information involved, tools for lawful evidence gathering, national and international coordination issues, and victim concerns, among other factors. USAM 9-50.000 sets forth general requirements for cyber prosecutions, including coordination with and notification of the Computer Crime and Intellectual Property Section ("CCIPS") of the Criminal Division in certain cases. These provisions are still in effect.

2. **Investigative Consultation**

In addition, at important stages of an investigation, because it is the best practice, the attorney for the government should consult with a Computer Hacking and Intellectual

Property Coordinator ("CHIP") within the District in which the case would be brought. Because electronic evidence is often subject to deletion after very short retention periods, the need to preserve or obtain evidence critical to the investigation may require taking preliminary investigative steps before undertaking the consultation above. In such cases, the consultations, as required, should take place as soon as possible.

3. **Charging Consultation**

With respect to charging decisions, the attorney for the government shall consult with CCIPS, which often has knowledge of similar cases in other Districts or how the case may fit into national priorities. Attorneys for the government are encouraged to have a District CHIP participate in this consultation. The consultation should be substantive in nature. It is meant to both assist the prosecutor and promote consistency in the Department in a quickly evolving area of practice. The depth of the consultation and degree of information required to accomplish these goals will vary according to the facts, complexity, and sensitivity of a particular investigation or matter. These types of consultations are already a hallmark of the CHIP program, and the strong working relationships are a key reason for the program's collaborative successes.

4. **Consultation for Cases Involving National Security Issues**

For CFAA cases involving international terrorism or domestic terrorism, or affecting, involving, or relating to the national security, USAM §§ 9-2.136, 9-2.137, 9-90.020, and/or 9-90.800 set forth additional National Security Division notification, consultation, and approval requirements. In such cases, the attorney for the government can, if he or she chooses, satisfy the initial CCIPS and NSD notification requirements with one contact. NSD or CCIPS will then be responsible for facilitating any additional required notifications, consultations, or approvals, including, to the extent requested by the attorney for the government, with the other component. If there is any question about whether a matter involves international terrorism, domestic terrorism or otherwise affects, involves, or relates to the national security, the attorney for the government should consult with the National Security Cyber Specialist (NSCS) within his or her district for further guidance.