No. 13-1816

IN THE

UNITED STATES COURT OF APPEALS

FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA,
PLAINTIFF-APPELLEE,

v.

ANDREW AUERNHEIMER,
DEFENDANT-APPELLANT.

On Appeal From The United States District Court
For The District of New Jersey
Case No. 2:11-cr-00470-SDW-1
Honorable Susan D. Wigenton, District Judge

BRIEF OF *AMICUS CURIAE* DIGITAL MEDIA LAW PROJECT IN SUPPORT OF DEFENDANT-APPELLANT

Kit Walsh (MA BBO#673509)
cwalsh@cyber.law.harvard.edu
Clinical Instructional Fellow
Cyberlaw Clinic
Berkman Center for Internet and Society
Harvard Law School
23 Everett St., 2nd Floor
Cambridge, MA 02140
Tel: (617) 384-9125
Fax: (617) 495-7641

Counsel for Digital Media Law Project

On the brief:

Jeffrey P. Hermes
Andrew F. Sellars
Digital Media Law Project
Berkman Center for Internet & Society
23 Everett Street, 2nd Floor
Cambridge, MA 02138
Tel: (617) 495-7547
Fax: (617) 495-7641

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST[1]

Amicus Curiae the Digital Media Law Project ("*Amicus*" or "DMLP") provides legal assistance, training, and other resources for online and citizen media. The DMLP has a strong interest in ensuring that online journalists, media organizations, and their sources are allowed to examine and debate network security and data protection vulnerabilities without criminal punishment, in order to inform citizens and lawmakers about networked computer security.

SUMMARY OF ARGUMENT

Had Defendant Andrew Auernheimer simply obtained the email addresses and device identification numbers that AT&T left open to the public on its website, without more, the Department of Justice would have treated this act as a misdemeanor. But because Auernheimer shared this information with the news website Gawker in order to inform the public about AT&T's poor data security, the government escalated his crime to a felony. This was premised upon the alleged violation of the New Jersey computer intrusion statute as a predicate offense to the

[1] The DMLP herby certifies that both parties consented to the filing of this brief. Pursuant to Fed. R. App. P. 29(c)(5), the DMLP certifies that no party's counsel authored the brief in whole or in part, and that no person, including any party or party's counsel, contributed money that was intended to fund preparing or submitting this brief.

Computer Fraud and Abuse Act ("CFAA"). The substantive elements of the statutes are identical apart from the requirement that under the New Jersey law the defendant must also disclose information obtained through the intrusion. The effect of this unprecedented application is a dramatic escalation of punishment based specifically and solely upon Auernheimer's speech. This requires First Amendment scrutiny, and cannot be sustained absent the government demonstrating a state interest of the highest order.

The First Amendment may tolerate punishment of unauthorized access to information, but prior decisions from both this Court and the Supreme Court indicate that the First Amendment bars the escalation of penalties for the publication of true and newsworthy information under any circumstance that does not fall into any existing exception to First Amendment protection. Absent satisfaction of First Amendment scrutiny, the escalation applied in this case is unconstitutional.

The DMLP, on behalf of its constituency of independent and online journalists, respectfully request that this Court apply First Amendment scrutiny in the case at bar in order to protect those who discover vulnerabilities and decide to inform the public. A contrary rule would limit public understanding of data

security, frustrate informed public policy around the proper nature and extent of computer crimes laws, and leave the public ignorant of existing vulnerabilities.

ARGUMENT

I. APPLICATION OF 18 U.S.C. § 1030(c)(2)(B)(ii) TO NEW JERSEY'S COMPUTER INTRUSION LAW ESCALATES PUNISHMENT SOLELY FOR DISSEMINATING INFORMATION, AND THUS MANDATES FIRST AMENDMENT SCRUTINY.

Auernheimer was charged with a violation of 18 U.S.C. § 1030(a)(2)(C), escalated from a misdemeanor to a felony under § 1030(c)(2)(B)(ii) as committed "in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." The superseding indictment alleges that the CFAA violation was committed in furtherance of New Jersey's computer crime law, N.J. Stat. § 2C:20-31(a). Superseding Indictment at ¶ 5. This law is substantively identical to the federal CFAA, save for one distinction: the New Jersey statute applies only when the defendant "knowingly or recklessly discloses or causes to be disclosed any data, data base, computer software, computer programs or personal identifying information" from an unlawfully-accessed computer. *See* Opening Brief of Appellant at 35-36 [hereinafter Appellant's Br.]. Had Auernheimer chosen not to disclose the data he obtained from AT&T's website, he would have faced a maximum of one year in prison for the CFAA

charge, under 18 U.S.C. § 1030(c)(2)(A). His disclosure of the information to a news outlet raised the maximum punishment to five years in prison, escalating punishment from a misdemeanor to a felony based exclusively upon the dissemination of information.

Dissemination of the information obtained from AT&T's website is indisputably an act of free expression. *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001) ("The naked prohibition against disclosures is fairly characterized as a regulation of pure speech."). It is atypical for free speech issues to arise out of generally applicable laws governing access, because access laws do not typically escalate punishment or damages based upon the disclosure of information obtained through unlawful activity. When they do, they must satisfy First Amendment scrutiny. *Bartnicki*, 532 U.S at 526 (analyzing a law that punishes disclosure of unlawfully-intercepted communications under the First Amendment); *see Food Lion, Inc. v. Capital Cities/ABC, Inc.*, 194 F.3d 505, 522 (4th Cir. 1999) (upholding liability for breach of a duty of loyalty, but refusing to escalate damages based on the disclosure of information obtained); *Shulman v. Group W Prods.*, 955 P.2d 469, 497 (Cal. 1998) (analyzing claims of unauthorized intrusion

upon seclusion and disclosure of private facts separately "for constitutional reasons").

This Court "cannot turn a blind eye to the First Amendment implications" of adding up to four years to a prison sentence because the defendant chose to alert the public. *Saxe v. State College Area Sch. Dist.*, 240 F.3d 200, 206 (3d Cir. 2001) (applying scrutiny to anti-harassment policy). First Amendment scrutiny is mandated for more innocuous punishments, such as placing an additional financial burden on speakers based on the disclosure of certain information. *Simon & Schuster, Inc. v. Members of the N.Y. State Crime Victims Bd.*, 502 U.S. 105, 115 (1991). It is critical to apply such scrutiny before increasing criminal punishment based on disclosure of information of public concern. Failing satisfaction of such scrutiny, Auernheimer's felony conviction under Section 1030 must be overturned.[2]

[2] Overturning the felony conviction under 18 U.S.C. § 1030 would also invalidate the felony charge under 18 U.S.C. § 1028(a)(7), as the only possible application of that statute to these facts is through Auernheimer's use of personally identifying information in the course of disclosure to Gawker. Any other "use" would be so general as to be unconstitutionally vague. *See* Appellant's Br. at 42. While the DMLP writes to specifically address the First Amendment concern inherent in the escalation here, the DMLP agrees with the Defendant that a finding of unauthorized access based solely on entering a website URL with a specific browser configuration would constitute a drastic over-reading of both the CFAA

II. UNDER THE FIRST AMENDMENT, DISCLOSURE OF INFORMATION OF PUBLIC IMPORTANCE CANNOT SUBJECT THE DEFENDANT TO ADDITIONAL PUNISHMENT ABSENT A STATE INTEREST OF THE HIGHEST ORDER.

The escalation of Auernheimer's punishment, based solely on the knowing or reckless disclosure of "any data, data base, computer software, computer programs or personal identifying information," N.J. Stat. § 2C:20-31, is a regulation of pure speech. *See Bartnicki,* 532 U.S. at 526; *Sorrell v. IMS Health, Inc.*, 131 S. Ct. 2653, 2667 (2011) ("[T]he creation and dissemination of information are speech within the meaning of the First Amendment."). Under Supreme Court precedent, such punishment is only permissible if it can survive exacting First Amendment scrutiny.[3]

---

and the New Jersey equivalent, Appellant's Brief at 20-21, 36-37; *see Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011), and that use of the federal computer intrusion law's felony escalation provision to an alleged violation of state computer intrusion law frustrates the intent of Congress and serves as an inappropriate "double counting" of an offense tantamount to double jeopardy, Appellant's Br. at 33-35; *see United States v. Cioni*, 649 F.3d 276, 283 (4th Cir. 2011). Even if this Court opts to find unauthorized access and no double jeopardy issue here, the valid application of the CFAA to this conduct would not mitigate the free speech harm raised by the escalation of punishment based on disclosure.

[3] Auernheimer first raised a First Amendment challenge in this case – specifically, to the application of § 1028 – in his motion to dismiss. Memorandum of Law in Support of Motion to Dismiss at 18. In addressing that challenge the prosecution argued, and the District Court agreed, that the case did not present First Amendment issues, citing the Supreme Court cases of *New York v. Ferber*, 458

A. The Information Disclosed by Auernheimer Was Both True and Related to a Matter of Public Concern.

It is critical to the First Amendment analysis in this case that the information Auernheimer disclosed to the press (and by extension, the public) was both true and related to a matter of public concern. "The central commitment of the First Amendment . . . is that 'debate on public issues should be uninhibited, robust, and wide-open.'" *Bond v. Floyd*, 385 U.S. 116, 136 (1966) (quoting *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)). Discussion of public affairs is thus "at

---

U.S. 747 (1982), and *Giboney v. Empire Storage & Ice Co.*, 336 U.S. 490 (1949). *See* Order on Motion to Dismiss at 12. *Giboney*, a case that allowed punishment of picketing activity under anticompetition law, is severely limited in both facts and principle by *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (limiting punishment of speech that induces unlawful conduct only when unlawful activity is imminent and likely, and the speaker directs speech to produce such unlawful action), and *NAACP v. Claiborne Hardware Co.*, 458 U.S. 886, 911-12 (1982) (recognizing the First Amendment protection for non-violent boycotts, and limiting Giboney to its strict antitrust application). Similarly, this Court has recognized the limited application of *New York v. Ferber* to the specific context of child pornography. *United States v. Stevens*, 533 F.3d 218, 225 (3d Cir. 2008), *aff'd* 559 U.S. 460 (2010) ("Without guidance from the Supreme Court, a lower federal court should hesitate before extending the logic of *Ferber* to other types of speech."). Neither case absolves the obligation to engage in First Amendment scrutiny when the government specifically seeks to assign punishment for the disclosure of information, and the district court's conclusion to the contrary need not be afforded any deference. *See Snyder v. Phelps*, 131 S. Ct. 1207, 1216 (2011) (in First Amendment cases "the court is obligated to make an independent examination of the whole record in order to make sure that the judgment does not constitute a forbidden intrusion on the field of free expression" (internal quotations omitted)).

the heart of the First Amendment's protection." *Snyder v. Phelps*, 131 S. Ct. 1207, 1215 (2011) (quoting *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758-59 (1985)). "Speech deals with matters of public concern when it can be fairly considered as related to any matter of political, social or other concern to the community, . . . or when it is a subject of legitimate news interest; that is, a subject of general interest and of value and concern to the public." *Snyder*, 131 S. Ct. at 1216 (internal quotations omitted).

Disclosures like Aurenheimer's are essential to our collective understanding of Internet data privacy and security. Indeed, all parties seem to agree that the information disclosed here was newsworthy. *See* Trial Tr., Nov. 14, 2012, at 119 (testimony that the defendant and co-conspirator believed that it was newsworthy); *id.* at 124 (in examination, the prosecution states, "[a]nd it was big media news; correct?"); *see also Ostergren, v. Cuccinelli*, 615 F.3d 263, 272 (4th Cir. 2010) (disclosure of Social Security Numbers ("SSNs") addresses a matter of public concern when done as part of criticism over entity's handling of that information).

One need only look to the reaction the publication of this information received to see both its newsworthiness and social utility. The reporting that resulted from Auernheimer's disclosure included:

- Gawker's criticism of AT&T and Apple, Inc. for their lax data security practices. Ryan Tate, *Apple's Worst Security Breach: 114,000 iPad Owners Exposed*, Gawker (June 9, 2010), http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed;
- reporting on the user impact of AT&T's data practices, *see* John Herrman, *Should I Worry About the Apple iPad + AT&T Security Breach? (Probably Not.)*, Gizmodo (June 9, 2010), http://gizmodo.com/5559586/should-i-worry-about-the-apple-ipad-%252B-att-security-breach-probably-not;
- discussion of what companies should do to address comparable oversights in their own systems, *see* Dan Cornell, *4 Lessons from the AT&T/Apple Data Breach for Smartphone App Developers*, Denim Group (June 9, 2010), http://blog.denimgroup.com/denim_group/2010/06/4-lessons-from-the-attapple-data-breach-for-smartphone-app-developers.html; and
- recognition of the importance of Auernheimer's disclosure of this information, such as the popular information technology website TechCrunch's giving a "public service" award to Auernheimer's organization for discovering and disclosing the vulnerability. Michael Arrington, *We're Awarding Goatse Security a Crunchie Award for Public*

Service, TechCrunch (June 14, 2010), http://techcrunch.com/2010/06/14/were-awarding-goatse-security-a-crunchie-award-for-public-service/.

This widespread discussion and debate through the "vast democratic forums of the Internet," *Reno v. ACLU*, 521 U.S. 844, 869 (1997), is a testament to the information's newsworthiness and underscores the importance of this information to our understanding of data security and privacy. *Beyer v. Duncannon Borough*, 428 Fed. App'x 149, 154 (3d Cir. 2011) ("Communicating the message in a public manner through the [I]nternet and news further weighs in favor of the conclusion that the speech here is of public concern."); *see* Section III, *infra*.

The public importance of this information is not altered by Auernheimer's choice to speak by directly disclosing the material obtained from AT&T's website. The disclosure is integral to his message regarding data security, *see Ostergren*, 615 F.3d at 271-72 (disclosure of documents with unredacted SSNs integral to message criticizing entity's handling of SSNs), and is essential to substantiate claims about the nature and extent of the AT&T's data mismanagement. *See* Trial Tr., Nov. 14, 2012, at 92 (testimony noting that Gawker asked for a copy of the data in order to verify the authenticity of the story); *Anderson v. Suiters*, 499 F.3d

1228, 1236 (10th Cir. 2007) (disclosure of primary source material "heightened the report's impact and credibility by demonstrating that the allegations rested on a firm evidentiary foundation and that the reporter had access to reliable information"); *Ross v. Midwest Commc'ns, Inc.*, 870 F.2d 271, 274-75 (5th Cir. 1989) (disclosure of private details related to newsworthy event had "unique importance to the credibility and persuasive force of the story"); Yochai Benkler, The Wealth of Networks 228 (2006) (noting that Internet news reporting is highly effective where the "[t]he first move . . . is to make the raw materials available for all to see").

The social utility of the disclosure here is clear, both as evidence of AT&T's poor security practice and as a description of the technological vulnerability. As one scholar has noted, "[p]ublishing detailed information about a computer program's security vulnerabilities may help security experts figure out how to fix the vulnerabilities, persuade apathetic users that there really is a serious problem, persuade the media and the public that some software manufacturer isn't doing its job, and support calls for legislation requiring manufacturers to do better." Eugene Volokh, *Crime-Facilitating Speech*, 57 Stan. L. Rev. 1095, 1118 (2005). As Internet services and digital communications are increasingly integral to our lives,

the data security practices of intermediaries and service providers are of vital public importance. *See generally* Andrea M. Matwyshyn, *Hidden Engines of Destruction: The Reasonable Expectation of Code Safety and the Duty to Warn in Digital Products*, 62 Fla. L. Rev. 109 (2010) (identifying data security harms and calling for a duty to warn and public disclosure regime to help the public appreciate such dangers).

The government does not refute this, but instead casts doubt upon the motives for Auernheimer's disclosure. Trial Tr., Nov. 15, 2012, at 49-50, 55 (cross-examination of Defendant as to his motive). The motive of the speaker, however, is irrelevant. "In deciding whether an individual may be punished for her speech, it is necessary to focus on what she says and the danger she creates, rather than on her motives. . . . [W]e learned long ago that inquiries into subjective intent and personal motivation are usually fruitless – and often dangerous – in the context of free speech." Geoffrey R. Stone, *Government Secrecy vs. Freedom of the Press*, 1 Harv. L. & Policy Rev. 185, 216 (2007). Indeed, "many things done with motives that are less than admirable are protected by the First Amendment," and a speaker's motive does not change the newsworthiness of the information disclosed. *Hustler Magazine, Inc. v. Falwell*, 485 U.S. 46, 53 (1988). In order to protect the

disclosure of such newsworthy information, whatever the motivation, First Amendment scrutiny is required before assigning Auernheimer additional years in prison for informing the public about AT&T's poor data security practices.

B. Application of the New Jersey Statute in This Case Requires Exacting Judicial Scrutiny Because the Prosecution Targets the Publication of Truthful Information of Public Concern.

Given that Auernheimer's speech was on a matter of public concern, the targeting of that speech for punishment requires constitutional scrutiny. Although Auernheimer was convicted for a violation of 18 U.S.C. § 1030(a)(2), his alleged violation of N.J. Stat. § 2C:20-31(a) escalated his punishment from a misdemeanor to a felony. It was the disclosure element of this statute that led to punishment for Auernheimer's speech, and therefore careful examination of this statute is required.

Statutes that are either written or justified on the basis of the content of speech receive strict scrutiny, satisfied only when the law is narrowly tailored to a compelling state interest. *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 642-43, 680 (1994); *Startzell v. City of Philadelphia*, 533 F.3d 183, 193 (3d Cir. 2008); Leslie Kendrick, *Content Discrimination Revisited*, 98 Va. L. Rev. 231, 238 (2012) (a law is "content-based" if it targets content either on its face or in its purpose). The New Jersey statute seeks to limit disclosure specifically as to "any data, data

base, computer software, computer programs, or personal identifying information" obtained through unauthorized access to a computer. N.J. Stat. § 2C:20-31. Targeting specific types of information, drawn from specific sources, strongly suggests that the New Jersey legislature sought to punish dissemination based upon the privacy or proprietary interest that may be harmed if the public is made aware of such information. This targets the speech for its "communicative impact," warranting strict scrutiny. *See Bartnicki v. Vopper*, 200 F.3d 109, 123 (3d Cir. 1999), *aff'd* 532 U.S. 514 (2001); Geoffrey R. Stone, *Content-Neutral Restrictions*, 54 U. Chi. L. Rev. 46, 47 (1987) (using "a ban on the publication of confidential information" as an example of a content-based restriction of speech) [hereinafter Stone, *Content-Neutral Restrictions*]. Should the Court consider this to be a content-based restriction on speech, the statute is "presumptively invalid" and the government bears a heavy burden to rebut that strong presumption. *United States v. Stevens*, 130 S. Ct. 1577, 1584 (2010).

Even if this Court finds that the New Jersey law is a content-neutral restriction of speech, the government may not assign additional punishment based on Auernheimer's dissemination of information absent a state interest of the highest order. In *Bartnicki*, the Supreme Court found that a statute banning the

publication of information gained through unlawful wiretapping was content-neutral, but nevertheless held that: "'[S]tate action to punish the publication of truthful information seldom can satisfy constitutional standards [.] ... [I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information absent a need . . . of the highest order.'" 532 U.S. at 527-28 (quoting *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97 (1979)) (citing *Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829 (1978)); *accord. Bowley v. City of Uniontown Police Dep't*, 404 F.3d 783, 786 (3d Cir. 2005); s*ee Cox Broad. Corp. v. Cohn*, 420 U.S. 469 (1976) (disclosing elements of public record, even if sensitive, cannot be criminalized consistent with the First Amendment). To establish such a need, the government must present evidence "'far stronger than mere speculation about serious harms.'" *Bartnicki*, 532 U.S. at 532 (quoting *United States v. Treasury Employees*, 513 U. S. 454, 475 (1995)).

The prosecution of Auernheimer "implicates the core purposes of the First Amendment because it imposes sanctions on the publication of truthful information of public concern." *Bartnicki*, 532 U.S. at 534-35. The case at bar bears close resemblance to a recent Fourth Circuit case building upon the *Bartnicki*

line of Supreme Court decisions: *Ostergren v. Cuccinelli*, 615 F.3d 263. There, the Fourth Circuit examined a First Amendment challenge to Virginia's Personal Information Privacy Act, as applied to a protester who called attention to Virginia's lax data privacy practices by posting documents obtained from government websites that contained the unredacted Social Security Numbers ("SSNs") of Virginian public officials. *Id.* at 267-69. The court in *Ostergren* rejected the government's argument against First Amendment scrutiny, noting that while disclosure of SSNs may not present First Amendment issues in other contexts, the postings were "integral to [Ostergren's] message. Indeed, they *are* her message." *Id.* at 271 (emphasis in original). The Fourth Circuit thus scrutinized the application of the law to Ostergren's disclosure and found that the First Amendment barred punishment for Ostergren's publication, stating that "[w]e cannot conclude that prohibiting Ostergren from posting public records online would be narrowly tailored to protecting individual privacy . . . ." of information. *Id.* at 286.[4]

[4] The *Ostergren* court declared the Virginia law a content-based restriction of speech, 615 F.3d at 271, but proceeded to apply the lesser scrutiny from the *Daily Mail* line of cases. This is similar to this Court's approach in *Bartnicki v. Vopper*, where this Court noted both content-based and content-neutral justifications for the law, but decided the case along the *Daily Mail* line of cases. 200 F.3d at 123. This

Here, Auernheimer similarly disclosed information initially hosted online by AT&T in order to highlight AT&T's poor data security practices. Appellant's Br. at 11. Such disclosure is integral to the Defendant's message, and although his disclosure bore with it some chance that one could use the disclosed information to cause the harm of which he was warning, the First Amendment protects such disclosure. *See Ostergren*, 615 F.3d at 269 (noting a similar self-fulfilling danger in the speaker's message there, but nevertheless protecting the speech under the First Amendment). And, like the speaker in *Ostergren*, Auernheimer's speech led to the correction of the identified issue, thus further benefiting the public. *See* Trial Tr., Nov. 14, 2012, at 66 (testimony of Defendant's co-conspirator, noting that AT&T changed its practices after disclosure); *Ostergren*, 615 F.3d at 269 n.4

---

was followed by the Supreme Court's own analysis when affirming *Bartnicki*, which purported to apply content-neutral scrutiny, but nevertheless applied something higher than the standard content-neutral scrutiny of *United States v. O'Brien*, 319 U.S. 367 (1968). *See, e.g.*, *Bartnicki*, 532 U.S. at 544 (Rehnquist, C.J., dissenting) (noting the "tacit application of strict scrutiny"); Kendrick, *supra*, at 279 (same); Wilson Huhn, *The Emerging Constitutional Calculus*, 79 Ind. L.J. 801, 831, 846 (2004) (noting the Court's application of a "higher level of judicial review than intermediate scrutiny" in part because the case "clearly turned upon the content of the speech being restricted"). This stronger scrutiny than the *O'Brien* test is consistent with the entire *Daily Mail* line of cases, and appropriate, given the closer nexus between the speech and punishment sought by the government and the unlikelihood that the government seeks to punish anything other than the communicative impact of the speech in question.

(noting an instance where Ostergren's publication led a county to reform its data practices). Accordingly, this Court must consider whether the government has satisfied its First Amendment burden in punishing Auernheimer's disclosures.

C. The Jury's Verdict that Auernheimer Accessed the Information at Issue Illegally Does Not Satisfy First Amendment Scrutiny for Punishing the Disclosure of that Information.

The court in *Ostergren*, as well as the Supreme Court and other courts considering the *Daily Mail* line of cases, leave unsettled the question of whether the government may punish one who unlawfully acquires information by punishing the information's subsequent disclosure. *Florida Star*, 491 U.S. at 535 n.8. At the same time, this Court has never declined to apply First Amendment considerations to a statute that punishes disclosure of unlawfully obtained information. The Supreme Court's decision in *Bartnicki* indicates that information does not lose First Amendment value or become categorically off-limits for discussion merely because it was unlawfully acquired. 532 U.S. at 535. Moreover, the Supreme Court has only tolerated punishment of speech to deter underlying unlawful conduct in the special case of child pornography, where the value of the speech is extremely low and the interests of the government are especially strong. *See* discussion at n.3, *supra*.

Courts that have addressed crimes and torts that punish both access and disclosure – as the prosecution does here by taking a misdemeanor access law and elevating it to a felony based on disclosure – have applied separate First Amendment scrutiny when considering the validity of the disclosure element. *See Bowley*, 404 F.3d at 787 n.5 (noting that it is appropriate to separately consider questions of unlawful access and disclosure); *see also First Amend. Coalition v. Judicial Inquiry Review Bd.*, 784 F.2d 467, 472 (3d Cir. 1986) (noting, in the context of access to court proceedings, that "the right of publication is . . . broader [than access], and in most instances, publication may not be constitutionally prohibited even though access to the particular information may properly be denied").

In describing the CFAA, Congress often likens the law to a "trespass" statute for electronic information. S. Rep. No. 99-432, at 7-10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484-88. This analogy is instructive to the First Amendment analysis as well. Although it is an oft-cited principle that newsgatherers are not exempt from generally applicable civil laws, *see Cohen v. Cowles Media Co.*, 501

U.S. 663, 669-70 (1991),[5] courts have carefully separated damages attributable to illegal access from those caused by disclosure, and only punished the latter when penalties for disclosure survived First Amendment scrutiny. *See* Nathan Siegel, *Publication Damages in Newsgathering Cases*, 19 Comm. Law. 11, 14 (2001) ("No court has ever finally approved a verdict for publication damages [in newsgathering tort cases.]"). For example, in *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, a case involving claims that reporters engaged in trespassing to acquire information for broadcast, the Fourth Circuit allowed trespass and breach of duty claims to survive First Amendment scrutiny but barred recovery of damages for reputational harm based on subsequent disclosure. 194 F.3d at 522. Like AT&T in this case, *see* Appellant's Br. at 14, plaintiff Food Lion claimed that the reputational damage caused by the defendants' disclosure of unlawfully gathered information compounded the harm from the trespass. However, the Fourth Circuit cited *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964), and *Hustler*, 485 U.S. 46, for the principle that even generally applicable laws are subject to First Amendment scrutiny when they target the publication of

[5] Notably, the Court in *Cohen* limited this principle to cases involving "compensatory damages," and distinguished a situation involving "criminal sanctions" for newsgathering activity. *Cohen*, 501 U.S. at 670.

information, rejecting the application of *Cohen*. 194 F.3d at 523-24; *see also Bartnicki*, 200 F.3d at 119 (distinguishing *Cohen*); *Desnick v. ABC, Inc.*, 44 F.3d 1345 (7th Cir. 1995) (separately considering the claims related to the "production of the broadcast" and the "content of the broadcast," and applying *Cohen* only to the production elements). Because Food Lion sought damages for dissemination of information without evidence of actual malice, its claim failed the scrutiny of *Sullivan* and *Hustler*. 194 F.3d at 522.[6]

The Supreme Court of California reached a similar conclusion in *Shulman*. 955 P.2d 469. In assessing intrusion upon seclusion and public disclosure of private facts claims of accident victims who were recorded during rescue, the Supreme Court of California carefully distinguished between the two torts "for

[6] The Ninth Circuit, seventeen years before *Hustler*, allowed a plaintiff to obtain enhanced damages for intrusion upon seclusion based upon subsequent disclosure of the information obtained. *Dietemann v. Time, Inc.*, 449 F.2d 245 (9th Cir. 1971). Courts outside of the Ninth Circuit have found that the analysis of *Food Lion* and *Hustler* supersedes that of *Dietemann*. *See, e.g., Hornberger v. ABC, Inc.*, 799 A.2d 566, 598 (N.J. Super. App. Div. 2002) ("*Dietemann* pre-dates *Hustler* and *Food Lion*; these later cases control."); *Smithfield Foods, Inc. v. United Food & Commercial Workers Int'l*, 585 F. Supp. 2d 815, 818-23 (E.D. Va. 2008); Siegel, *supra*, at 16 (doubting that *Dietemann* "supports the proposition for which it is often cited"). The Ninth Circuit itself has narrowed the merits of *Dietemann* to intrusions upon the home itself, suggesting a form of newsworthiness analysis that would allow punishment for publication of private facts even after First Amendment scrutiny. *Medical Laboratory Mgmt. Consultants v. ABC, Inc.*, 306 F.3d 806, 818 n.6 (9th Cir. 2002); *see* Section II.D, *infra*.

constitutional reasons." *Id.* at 497. The court held that triable issues prevented summary judgment for the media defendants as to intrusion. *Id.* at 490-91. But as a matter of law, the court held that the newsworthiness of the information gathered through the intrusion was fatal to the public disclosure of private facts claim. *Id.* at 488-89. The court noted its differing treatment of the two, stating that "the intrusion tort, unlike that for publication of private facts, does not subject the press to liability for the contents of its publications." *Id.* at 496. This case necessitates similar scrutiny; the government cannot let unauthorized access taint the subsequent disclosure of information without engaging in a First Amendment analysis. And because the information was both true and newsworthy, *see* Section II.A, *supra*, Auernheimer's conviction cannot stand absent the prosecution's satisfaction of that scrutiny.

D. Application of First Amendment Scrutiny Does Not Invalidate Punishment for Disclosures Which Would Violate an Existing Duty Not to Disclose, Disclosure of Purely Private Information, or Disclosures that Violate Copyright or Trade Secret Laws.

Applying First Amendment scrutiny to protect Auernheimer's disclosure in this irregular case does not disrupt application of computer intrusion laws to pure access crimes. Nor does it affect application of such laws to disclosure crimes where the disclosure is a paradigmatic example of the harms that computer crimes

seek to address (including violation of a preexisting duty to keep the information confidential, disclosure of purely of private information, or disclosures that can be punished as falling within an unprotected category of speech). *See Ostergren*, 615 F.3d at 272 (protecting disclosure of SSNs, but noting that the court did not "foreclose the possibility that communicating [SSNs] might be found unprotected in other situations").

In enacting its computer crime law, the New Jersey legislature was especially concerned with disclosure of information in violation of a preexisting duty to use the information only for certain purposes. Legislators cited an incident where a Connecticut auxiliary police officer was suspected of accessing a police computer to gain information on his full-time employer (and presumably disclosed that information to others, given the context of the lawmakers' statements). *See* N.J. Senate, 201st Legislature, Sponsor's Statement for S. No. 1807, at 7 (May 14, 1984); N.J. Assembly Judiciary Committee, 201st Legislature, Statement to Assembly Committee Substitute for Assembly No. 1301 at 1 (Mar. 26, 1984). Applying First Amendment scrutiny would not generally prevent punishment of such behavior. Courts have consistently held that violation of a preexisting duty not to disclose information can be punished, even when the information is true and

newsworthy. *See, e.g., United States v. Aguilar*, 515 U.S. 593, 605-06 (1995) (federal judge's disclosure of information could be punished in part because the information was obtained through his role in a sensitive confidential position); *compare Boehner v. McDermott*, 484 F.3d 573, 579 (D.C. Cir. 2007) (en banc) (disclosure of information obtained through another's unlawful interception can be punished when information was provided to defendant in his role as member of House Ethics Committee), *with Jean v. Mass. State Police*, 492 F.3d 24, 32 (1st Cir. 2007) (protecting similar disclosure against punishment, and noting that the court in *Boehner* would have protected disclosure "if McDermott had been a private citizen, like Jean").

Similarly, the New Jersey statute's punishment of the disclosure of "any data, data base, computer software, computer programs or personal identifying information," N.J. Stat. § 2C:20-31, might properly be invoked to protect purely private information, subject to the constitutional constraint that the information is not newsworthy. *See Jenkins v. Dell Publ'g Co.*, 251 F.2d 447, 450 (3d Cir. 1958) (allowing liability for publication of non-newsworthy private information, balancing "the embarrassment, humiliation or other injury which may result from public disclosure concerning his personality or experiences" with "the interest of

the public in the free dissemination of the truth and unimpeded access to news"); *see also Time, Inc. v. Hill*, 385 U.S. 374, 383 n.7 (1967) (citing many cases where a state right of privacy "was held to give way to the right of the press to publish matters of public interest"); *Shulman*, 955 P.2d at 479 ("Although we speak of the lack of newsworthiness as an element of the private facts tort, newsworthiness is at the same time a constitutional defense to, or privilege against, liability for publication of truthful information."). On a closely related matter, the Court has previously held that disclosures that defraud the public, such as "phishing" scams conducted with email addresses, can be punished consistent with the First Amendment. *Nat'l Taxpayers Union v. U.S. Soc. Sec. Admin.*, 302 Fed. App'x 115, 118 (3d Cir. 2008). Protecting Auernheimer's disclosure would not disrupt that holding.

Nor would applying First Amendment scrutiny here invalidate prohibitions for copyright infringement or theft of trade secrets. Putting aside Congress's disfavor of state regulation of copyright-related issues, *see* 17 U.S.C. § 301, disclosures that constitute a valid claim of copyright infringement could be pursued consistent with the First Amendment. *Eldred v. Ashcroft*, 537 U.S. 186, 219-21 (2003). Similarly, most trade secret cases can be justified based upon a preexisting

duty or obligation not to disclose information. *See* Robert G. Bone, *A New Look at Trade Secret Law: A Doctrine in Search of a Justification*, 86 Cal. L. Rev. 241, 244 (1998).

Thus, a rule that applied First Amendment scrutiny here would not disrupt the established body of caselaw that allowing sanctions for disclosure based on preexisting duties, disclosure of purely private information, or disclosures that constitute copyright infringement or theft of trade secrets. By contrast, where a disclosure like the one here does not fit within one of these excepted areas, or any other categorical exception to First Amendment scrutiny, *see Stevens*, 130 S. Ct. at 1584, punishment for dissemination of information is not constitutionally permissible.

III. ALLOWING ADDITIONAL PUNISHMENT OF THE DEFENDANT HERE WOULD CHILL REPORTING ON DATA SECURITY VULNERABILITIES AND HARM THE PUBLIC'S UNDERSTANDING OF DATA PRIVACY ISSUES.

The DMLP and its constituency of independent online journalists share in the public's concern over the use of personal, online information by corporations, governments, and unscrupulous individuals. It is vitally important that persons who discover technological vulnerabilities do not suffer additional punishment when they bring information about such vulnerabilities to the public's attention.

"Freedom of discussion, if it would fulfill its historic function in this nation, must embrace all issues about which information is needed or appropriate to enable the members of society to cope with the exigencies of their period." *Thornhill v. Alabama*, 310 U.S. 88, 102 (1940). With the rapid development and expansion of networked technology, data security is one of today's critical issues. *See* Lieberman Research Group, *Unisys Security Index: US*, Unisys (Apr. 18, 2013), http://www.unisyssecurityindex.com/system/reports/uploads/288/original/Unisys%20Security%20Index_United%20States_May%202013.pdf?1370347491 (a March 2013 survey found that 82.1% of Americans were at least somewhat concerned about data breaches). Prosecution of Auernheimer for a felony threatens to chill analysis of the nature and scope of discovered network vulnerabilities, which the public must understand in order to make informed decisions about whom to trust with personal information. *See* Stone, *Content-Neutral Restrictions*, *supra*, at 55 (noting that one of the risks in content-based laws is that they "mutilate[] the thinking process of the community'" (quoting Alexander Meiklejohn, Political Freedom 27 (1960)).

Data vulnerabilities are often discovered by researchers operating independent of the vulnerable company, in circumstances where the vendor may

not wish to report their own bad practices to the public out of fear of embarrassment or litigation. Ethan Peterson & John Lofton, *Computer Security Publications: Information Economics, Shifting Liability, and the First Amendment*, 24 Whittier L. Rev. 71, 77, 137-38 (2002). For example, the company Skype took over a year to fix a known data vulnerability, and only addressed the problem after the researcher who found the vulnerability told the press. *See* Joel Schectman, *Skype Knew of Security Flaw Since November 2010, Researchers Say*, Wall St. J. (May 1, 2012), http://blogs.wsj.com/cio/2012/05/01/skype-knew-of-security-flaw-since-november-2010-researchers-say/. Sony similarly waited several months to fix a known vulnerability disclosed to it by an independent researcher, leaving users of its Playstation 3 console vulnerable in the interim. *See* Eduard Kovacs, *Experts Find Code Execution Flaw in PS3, Password Reset Bug in Sony Entertainment Network*, Softpedia (May 29, 2013), http://news.softpedia.com/news/Experts-Find-Code-Execution-Flaw-in-PS3-Password-Reset-Bug-in-Sony-Entertainment-Network-356623.shtml.

In this case, AT&T was clearly embarrassed. *See* Appellant's Br. at 14 (noting that AT&T cited their "reputation" as the harm suffered). Several witnesses in this case testified as to the bad data management practices of AT&T, and how

that company should not have set up a system whereby any individual entering a series of specific Internet addresses in a browser could obtain a the emails of over a hundred thousand AT&T customers. *See generally* Appellant's Br. at 7-9; Trial Tr., Nov. 19, 2013, at 39, 41, 57 (testimony of AT&T's security officer, who called the system a "poorly crafted design feature," stated that the company "did something we probably should not have done," and that "we had no security in place"). Testimony shows that AT&T changed their practices only after this breach was discovered and disclosed to the public. *See* Trial Tr., Nov. 15, 2012, at 72 (from AT&T's Chief Security Officer, "we very quickly shut down that feature the day we found out what was going on"); *see generally* Peter P. Swire, *A Model for When Disclosure Helps Security: What Is Different About Computer and Network Security?*, 3 J. Telecomm. & High Tech. L. 163 (2004) (exploring circumstances when disclosure of a security vulnerability improves overall security). It is impossible to know whether AT&T would ever have informed its customers about their vulnerability without Auernheimer's disclosure.[7]

[7] This fear of corporate secrecy and misdirection around public data vulnerabilities is why most states mandate corporate disclosure of data breaches. *See State Security Breach Notification Laws*, National Conference of State Legislatures, http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

Overreaching CFAA claims based on disclosure of corporate data practices present very real journalistic harms. As journalism increasingly focuses on public data security, journalists themselves have been subject to readings of the CFAA that chill technological reporting. In May of this year, reporters at the Scripps Howard News Service discovered and broadcast that two companies that manage the federal Lifeline phone service program for low-income Americans had published the names and parts of Social Security Numbers of enrollees online. *See* Scripps Howard News Service, *Privacy on the Line: Scripps Uncovered Security Risks for Some Lifeline Phone Customers*, KJRH-TV (May 18, 2013), http://www.kjrh.com/dpp/news/local_news/special_reports/Privacy-on-the-Line-Scripps-uncovered-security-risks-for-some-Lifeline-phone-customers. Under the government's theory in this case, not only would the accessing those websites constitute unauthorized access for CFAA purposes, the disclosure could escalate the violation to a felony, punishable by up to five years in prison. The companies that were responsible for publishing the confidential Lifeline information appear to welcome the prosecution's argument, as they have threatened Scripps with punishment under the CFAA for exposing their bad data practices. *See* Sarah

---

(last updated Aug. 20, 2012) (providing links to 46 different state data breach disclosure laws).

Laskow, *Reporting, Or Illegal Hacking*, Columbia Journ. Review (June 13, 2013), http://www.cjr.org/cloud_control/scripps_hackers.php.

Preventing punishment in this case absent satisfaction of First Amendment scrutiny also ensures that the government does not have too great a hand in interfering with the ethics and norms of the data security community, who are currently engaged in a robust debate over when it is appropriate to tell a company first about bad data practices, and when it is better to inform the public directly. *See* Trial Tr., Nov. 19, 2012, at 105 (testimony of the Defendant's expert witness, noting the "complex dispute" within the data security community over the proper means of disclosure); Andrea M. Matwyshyn, *Hacking Speech: Informational Speech and the First Amendment*, 107 Nw. U. L. Rev. 795, 825 n.154 (2013) (noting the ongoing debate between "full disclosure" and "coordinated vulnerability disclosure" in the information security community). Prosecutors and lawmakers should not use heavy-handed and chilling applications of law to set the ethical norms around this delicate and complicated space. *See Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 256 (1974) ("[P]ress responsibility . . . cannot be legislated."); *Ostergen*, 615 F.3d at 271 n.8 ("[T]he First Amendment protects [speaker's] freedom to decide how her message should be communicated."

(citing cases)); *Shulman*, 955 P.2d at 485 (formulating a test for newsworthiness in the privacy context that "incorporates considerable deference to reporters and editors, avoiding the likelihood of unconstitutional interference with the freedom of the press").

In sum, the additional punishment sought by the government for disclosure of newsworthy information presents profound danger to the public, data security policymakers, and journalists reporting on technology. Any attempt to punish disclosure of a network vulnerability must first satisfy First Amendment scrutiny. Absent such satisfaction, the felony punishment in this case must be overturned.

Respectfully submitted,

DIGITAL MEDIA LAW PROJECT

By its counsel,[8]

Dated: July 8, 2013

/s/Kit Walsh

Kit Walsh (MA BBO#673509)
cwalsh@cyber.law.harvard.edu
Clinical Instructional Fellow
Cyberlaw Clinic
Berkman Center for Internet and Society
Harvard Law School
23 Everett St., 2nd Floor
Cambridge, MA 02140
Tel: (617) 384-9125
Fax: (617) 495-7641

On the brief:

Jeffrey P. Hermes
Andrew F. Sellars
Digital Media Law Project
Berkman Center for Internet & Society
23 Everett Street, 2nd Floor
Cambridge, MA 02138
Tel: (617) 495-7547
Fax: (617) 495-7641

[8] The DMLP wishes to thank Harvard Law School Cyberlaw Clinic summer interns David Collado and Kerry Sheehan, and DMLP summer intern Kristin Bergman, for their invaluable contributions to the preparation of this brief.

CERTIFICATE OF COMPLIANCE

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6757 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii) and Local App. R. 29.1(b).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it is in 14-point Times New Roman font.

3. The text of the PDF version of this brief and the hard copies are identical.

4. A virus check was performed on the PDF version of this brief using Microsoft Security Essentials Version 4.0.1526.0.

5. I have applied for admission to the bar of this Court pursuant to Local App. R. 46.1.

Dated: July 8, 2013

/s/Kit Walsh

Kit Walsh (MA BBO#673509)
cwalsh@cyber.law.harvard.edu
Clinical Instructional Fellow
Cyberlaw Clinic
Berkman Center for Internet and Society
Harvard Law School
23 Everett St., 2nd Floor
Cambridge, MA 02140
Tel: (617) 384-9125
Fax: (617) 495-7641

CERTIFICATE OF SERVICE

I certify that on this 8th day of July, 2013, the BRIEF OF AMICUS CURIAE DIGITAL MEDIA LAW PROJECT IN SUPPORT OF DEFENDANT-APPELLANT was served on all parties via electronic filing with the Court, that counsel for both parties have consented to electronic service via the Court's ECF system, and that, pursuant to Local App. R. 25.1, ten (10) paper copies will be delivered to a third party commercial carrier for delivery to the Clerk of the Court within three calendar days.

Dated: July 8, 2013

/s/Kit Walsh

Kit Walsh (MA BBO#673509)
cwalsh@cyber.law.harvard.edu
Clinical Instructional Fellow
Cyberlaw Clinic
Berkman Center for Internet and Society
Harvard Law School
23 Everett St., 2nd Floor
Cambridge, MA 02140
Tel: (617) 384-9125
Fax: (617) 495-7641