
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 *AMICI CURIAE* MOZILLA FOUNDATION, COMPUTER
SCIENTISTS, SECURITY AND PRIVACY EXPERTS IN SUPPORT OF
DEFENDANT-APPELLANT AND REVERSAL**

Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for *Amici Curiae*

TABLE OF CONTENTS

STATEMENT OF INTEREST	1
INTRODUCTION AND SUMMARY OF THE ARGUMENT.....	3
I. Auernheimer Used Commonplace, Legitimate Techniques to Collect Email Addresses from AT&T’s Public Unsecured Website	5
A. People Often and Easily Modify Variables in Website Addresses	5
B. People Often and Easily Change User-Agents	7
C. People Often and Easily Automate HTTP Requests, Including for Valuable Privacy and Security Research.....	9
1. “Brute Force” Is Not Nefarious	9
2. The ICC-ID Is Not a Password.....	10
II. Researchers Commonly Use Techniques Technologically Indistinguishable from Auernheimer’s Conduct in This Case.....	11
A. Research Akin to Conduct in This Case Helps Fight Malicious Software on Android Smartphones.....	12
B. The Wall Street Journal Used Similar Techniques in Its Investigation of Online Price Discrimination	13
III. Researchers Conduct Valuable Independent Experiments on Unsecured Public Websites and Other Publicly Accessible Computers Without Permission	15
IV. Individuals Must Be “Authorized” to Access Open Public Websites, Or Risk Sweeping Security and Privacy Research Under the CFAA’s Broad Prohibitions	18

V. Neither Auernheimer’s Post-Discovery Conduct Nor His Motive Are Grounds for CFAA Liability.....21

 A. Security and Privacy Researchers Commonly Publish Their Findings21

 B. A Researcher’s Attitude and Motivations Are Irrelevant to CFAA Liability22

VI. Criminalizing Computer Security and Privacy Research Would Frustrate Congressional Intent and Policy24

 A. Congress Funds Applied Computer Security and Privacy Research.....24

 B. Sweeping Security and Privacy Research Within CFAA Undermines the Very Purpose of the Statute.....26

CONCLUSION27

TABLE OF AUTHORITIES

Cases

<i>WEC Carolina Energy Solutions v. Miller, LLC</i> , 687 F.3d 199 (4th Cir. 2012)	21
<i>EF Cultural Travel BV v. Zefer Corp.</i> , 318 F.3d 58 (1st Cir. 2003)	19
<i>Int'l Airport Ctrs., LLC v. Citrin</i> , 440 F.3d 418 (7th Cir. 2006).....	20
<i>Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am.</i> , 648 F.3d 295 (6th Cir. 2011)	4
<i>United States v. Nosal</i> , 676 F.3d 854 (9th Cir. 2012).....	20, 22, 27

Statutes

<i>Cyber Security Research & Development Act</i> (2002) 15 U.S.C. § 7401	25
---	----

Other Authorities

Alfred V. Aho, <i>Complexity Theory</i> , in <i>Computer Science: The Hardware, Software and Heart of It</i> 241 (Edward K. Blum & Alfred V. Aho eds., 2011)	9
E. Gabriella Coleman, <i>Phreaks, Hackers, and Trolls: The Politics of Transgression and Spectacle</i> , in <i>The Social Media Reader</i> 191 (Michael Mandiberg ed., 2012)	24
Christine D. Galbraith, <i>Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Websites</i> , 63 Md. L. Rev. 320 (2004)	26
Orin S. Kerr, <i>Cybercrime's Scope</i> , 78 N.Y.U. L. Rev. 1596 (2003).....	27
Bruce Schneier, <i>Applied Cryptography</i> (1st ed. 1996).....	11

Yajin Zhou et al., *Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets*, Proc. 19th Annual Network & Distributed Sys's Symp., Feb. 201212

Oxford Univ. Press, *New Oxford American Dictionary* (3d ed. 2010)11

S. Rep. No. 104-357 (1996)27

S. Rep. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 5, 26

**DISCLOSURE IN COMPLIANCE WITH
FEDERAL RULE OF APPELLATE PROCEDURE 29(c)(5)**

(A) No party's counsel authored this brief in whole or in part.

(B) No party or party's counsel contributed money to counsel for *Amici Curiae* or to any *Amicus* that was intended to fund preparing or submitting this brief,

(C) No person—other than the *Amicus Curiae*, its members, or its counsel—contributed money that was intended to fund preparing or submitting this brief.

CONSENT OF PARTIES TO FILING

All parties have consented to the filing of this brief, via attorney Tor Ekeland on behalf of Defendant-Appellant Andrew Auernheimer and Mark Coyne, Chief, Appeals Division United States Attorney's Office for the District of New Jersey on behalf of Plaintiff-Appellee United States of America.

STATEMENT OF INTEREST

The parties listed in Exhibit A submit this brief as *Amici Curiae*. *Amici* are an illustrious group of computer scientists, computer science professors, software developers, privacy researchers, professional and freelance computer security researchers, and academics with diverse expertise on the science and practice of network and data security. *Amici* include the Mozilla Foundation, maker of the popular Firefox web browser, Princeton University Professor of Computer Science and Public Affairs and former Federal Trade Commission Chief Technologist Edward Felten, University of Pennsylvania Associate Professor of Computer and Information Science Matt Blaze, and David L. Dill, Professor of Computer Science and, by courtesy, Electrical Engineering at Stanford University. Among other activities, *Amici* build, study, and test software, computers, and computer networks, including websites, medical devices, voting machines, and smartphones. *Amici* also report and publish papers on security and privacy deficiencies that they discover, as well as aid in repairing defects.

Many *Amici* routinely scrutinize websites, software interfaces, electronic devices, and other computer systems for security and privacy shortcomings, and use information derived from such testing in their work. Researchers commonly test public, unsecured websites to discover how they collect, store, and use consumer information. These tests may include sending websites a series of similar

information requests, changing a variable each time to see how the website will respond. As Defendant-Appellant Andrew Auernheimer did, researchers usually use software programs, or “scripts” to automate these changes and thereby quickly collect more data.

The work of *Amici* and other security and privacy researchers immensely benefits public health, safety, and welfare. Researchers’ tests have revealed dangerous software distributed for Android smartphones, price discrimination by online retailers, techniques some websites deploy to defeat consumer efforts to protect their online privacy, illegal practices involving Social Security numbers and other private personal data, as well as other important discoveries.

Because of the striking similarities between the important research tools and techniques used by *Amici* and others, which broadly benefit privacy and security, and the conduct that led to Auernheimer’s conviction in this case, *Amici* have a vital interest in presenting to this Court the following arguments why individuals must be deemed “authorized” under the Computer Fraud and Abuse Act when they access unsecured data on public websites. Auernheimer’s conviction under 18 U.S.C. § 1030(a)(2)(C) should therefore be reversed.

INTRODUCTION AND SUMMARY OF THE ARGUMENT

Computer security and privacy are important national priorities. “Strong consumer data privacy protections are essential to maintaining consumers’ trust in the technologies and companies that drive the digital economy.” Exec. Office of the President, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy* 1 (2012), available at <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>.

Amici have diverse and deep technological expertise in computer security and privacy from both an academic and practical perspective. Their work — and that of numerous other researchers and security and privacy professionals — is critical to helping protect security and privacy on the computer networks that are key for our nation and economy.

This legitimate, highly valuable research commonly employs techniques that are essentially identical to what Defendant-Appellant did in this case. Most importantly, like Auernheimer, researchers cannot always conduct testing with the approval of a computer system’s owner. Such *independent* research is of great value to academics, government regulators and the public even when — often especially when — conducted without permission and contrary to the website owner’s subjective wishes.

The CFAA draws a line between lawful “authorized” access and illegal “unauthorized” access to computers. The concept of “authorization” is different and distinct from a computer owner’s expressed or implicit desires. *See Pulte Homes, Inc. v. Laborers’ Int’l Union of N. Am.*, 648 F.3d 295, 304 (6th Cir. 2011) (Union members flooded plaintiff with unwanted calls and emails but did not violate CFAA because “like an unprotected website, [the] phone and e-mail systems ‘[were] open to the public, so [LIUNA] was authorized to use [them].” (citations omitted). Businesses often have substantial economic, legal, and reputational interests in keeping their security flaws, privacy missteps, and other product or service shortcomings quiet. But these private, commercial desires are frequently at odds with the public interest and should not receive the force of criminal law. To hold otherwise threatens to sweep security and privacy research under the harsh prohibitions of the CFAA. Such an application of the CFAA would greatly harm privacy and security and give private parties enormous power to enforce their parochial concerns against the public’s interest.

Rather, this Court should hold that an individual who accesses unsecured data published on a public website is “authorized” under the CFAA, regardless of the website owners’ subjective wishes. Such a holding would reduce the chill that the risk of CFAA criminal liability places on the important work of privacy and security researchers. Such a holding also would accord with congressional intent to

protect security and privacy, and Congress' recognition that technological security measures, and not overreaching criminal law, are the most effective means of obtaining that protection. *See* S. Rep. No. 99-432, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 (“[The] most effective means of preventing and deterring computer crime is ‘more comprehensive and effective self-protection by private business’ and that the primary responsibility for controlling the incidence of computer crime falls upon private industry and individual users, rather than on the Federal, State, or local governments.” (citation omitted)).

I. Auernheimer Used Commonplace, Legitimate Techniques to Collect Email Addresses from AT&T’s Public Unsecured Website

Auernheimer accessed the AT&T website using commonplace techniques familiar to and frequently employed by both computer scientists and regular Internet users.

A. People Often and Easily Modify Variables in Website Addresses

The World Wide Web (“web”) consists of computer systems that “speak” a shared language, the Hypertext Transfer Protocol (HTTP). A website is information stored on a computer connected to the web, where a user can access information or services. Websites are programmed to accept HTTP requests from users and return responses.

People access websites by running their own “user agent” software that speaks HTTP. That software is commonly a web browser application, like Mozilla

Firefox on a desktop computer, or Apple Safari on an iPad. When the user agent contacts a website, it initiates communication with an HTTP request. For example, if a user chose to visit the homepage for this Court, her browser would begin by issuing an HTTP request to the Third Circuit’s website. That HTTP request incorporates several components, including the homepage’s address (“http://www.ca3.uscourts.gov”).

In the case at bar, when an iPad user visited the AT&T website, she would automatically be directed to a webpage with the following address, where “X” stands for the identification number of the iPad’s cellular card (called the “ICC-ID”): “https://dcp2.att.com/OEPCClient/openPage?ICCID=X&IMEI=0”. App2. 726.¹ iPads registered with AT&T would visit the page associated with that address automatically. App2. 255-56. However, AT&T configured its website so that it would share an email address with anyone—not just the account holder—who entered a webpage address with a correct ICC-ID. App2. 409, 412-13.

Thus, Auernheimer, or any member of the public, could visit the AT&T website, and—by changing the value of X in the address above—view a webpage that included an email address.

Changing the value of X in the AT&T webpage address is trivial to do. For example, to visit this Court’s homepage, one might type the address

¹ “App2.” refers to Volume 2 of the Appendix filed with this Court on July 1, 2012 in connection with Defendant-Appellant’s opening brief.

“http://www.ca3.uscourts.gov/” into the address bar of the browser window. The browser sends an HTTP request to the Court website, which will respond with this Court’s homepage. Changing the “3” to “4” by typing in the browser window address bar returns the Court of Appeals for the Fourth Circuit’s homepage. Changing the “3” to a “12” returns an error message.²

Many individual users modify web requests by typing new values in the browser address bar. Changing these values is useful when navigating through online photo albums or reading through comment threads for online forums. Doing so is technologically identical to what Auernheimer and his co-defendant did when they changed the value of X in the public website location above, and thereby received different responses from AT&T’s server.

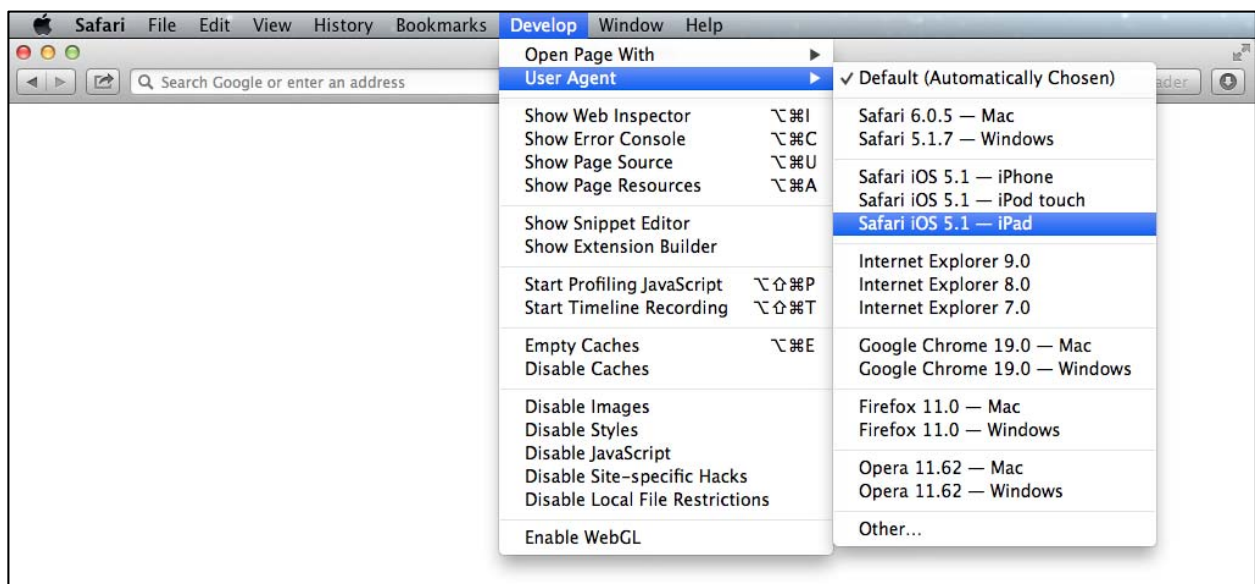
B. People Often and Easily Change User-Agents

Another component of an HTTP request is the “user agent,” which identifies the software that the user is running.³ The government may argue that Auernheimer and his co-defendant did something wrong because they set their software’s user-agent to appear as an iPad. App2. 264, 610. But the user-agent

² Publicly available software makes it easy for anyone to automate modified HTTP requests. See e.g. Kai Liu, URL Flipper, <https://addons.mozilla.org/en-US/firefox/addon/url-flipper/>. (Last visited July 8, 2013). The software “quickly and easily increment[s] and decrement[s] numbers and strings in URLs for navigating through URL sequences.” Id.

³ To clarify, a “user agent” is software that a user runs. A “user-agent” is text included in an HTTP request that identifies the user agent.

setting is nothing more than an optional, voluntary field that suggests to a website what kind of software is making an HTTP request to improve the user experience. App2. 510. People change user-agents for many reasons, including improving compatibility with older websites. Changing the user-agent is trivial. In Apple's Safari web browser, for example, a user can simply select a different user-agent from a menu.



There is nothing nefarious or tricky about changing a user-agent. We agree with Auernheimer that if changing a user-agent is a federal crime, millions of Americans may be criminals for the way they routinely browse the web. *See* Appellant's Opening Br. 31.

C. People Often and Easily Automate HTTP Requests, Including for Valuable Privacy and Security Research

The government may also argue that the co-defendants did something wrong by writing a computer program to automate HTTP requests to AT&T's website. Specifically, the record shows that Auernheimer's co-defendant used a computer program that he called the "account slurper" to automatically change the value of X—representing different ICC-ID numbers—in the HTTP requests he sent to the AT&T website. App2. 259-61, 726-27. This technique is no more remarkable than writing a software program to change the "3" in this Court's website to a "4" in order to get different public information.

1. "Brute Force" Is Not Nefarious

The government may refer to the "account slurper" as a "brute force" technique. That term has a particular and innocuous meaning: an approach to a problem that "evaluat[es] all possible solutions." Alfred V. Aho, *Complexity Theory*, in *Computer Science: The Hardware, Software and Heart of It* 241, 257 (Edward K. Blum & Alfred V. Aho eds., 2011). Despite the thuggish name, there is nothing nefarious about using a "brute force" technique to solve a problem.

Here, the co-defendant did not "force" his way into anything. The AT&T website displayed an email address to anyone who sent an HTTP request containing a valid ICC-ID number. AT&T used sequential ICC-ID numbers. All the "account slurper" did was add one and recalculate the ICC-ID number, then

send it to the AT&T website. The defendants did not avoid any password requirement, decrypt any encrypted data, access any private accounts, or cause the AT&T website to malfunction.

2. The ICC-ID is not a Password

The government may argue that AT&T used the ICC-IDs as passwords to secure iPad owner email addresses and that by guessing the ICC-IDs, the co-defendants bypassed a security measure. This assertion is wrong for many reasons. First, this after-the-fact justification is contradicted by AT&T's website itself, which explicitly requested a password in addition to the ICC-ID. *See* Appellant's Opening Br. 8 n.5.

Second, unlike a password, ICC-IDs are not secret. The numbers are frequently printed on the outside of phone packaging. *See, e.g.,* AT&T, Activate Your Phone, <https://www.wireless.att.com/GoPhoneWeb/goPhoneLanding.do?method=activatePayGo> (last visited July 6, 2013) (“If you have the package your phone came in, you can find the SIM Card number on the outside of the package on a white label with bar codes. Look for the letters 'ICCID' and then a long number.”).

Also, the ICC-ID format is defined by a public specification document ISO/IEC7812. The number is partially comprised of numbers representing the service type, Country Code and Mobile Network Code. These numbers are

identical for every U.S. iPad on the AT&T network. Only the subscriber number and one check digit are unique. The check digit is easily calculated from the subscriber number using a well-known mathematical formula (Luhn).

No one need guess the subscriber numbers, however, because AT&T assigns ICC-IDs *sequentially*. Thus, if you know any iPad number, you know every iPad number (though you may not know the beginning or the end number of the range). ICC-IDs are not a secret.

In contrast, a password—both in computer science and common terminology—must be secret. See, e.g., Bruce Schneier, *Applied Cryptography* 53 (1st ed. 1996) (referring to a password as a “secret piece of knowledge”); Oxford Univ. Press, *New Oxford American Dictionary* (3d ed. 2010) (defining password as “a secret word or phrase that must be used to gain admission to something”).

In sum, as computer experts we believe that modifications to webpage addresses, changing user-agent settings, and automation—alone or in combination—are legitimate means of accessing the public web. We see no technical distinction between these aspects of Auernheimer’s conduct and commonplace online activities.

II. Researchers Commonly Use Techniques Technologically Indistinguishable from Auernheimer’s Conduct in This Case

Security and privacy researchers frequently modify webpage addresses, user-agents, and other components of HTTP requests, and use automation to

conduct valuable testing that promotes security and privacy. This Court cannot uphold Auernheimer's CFAA conviction on the basis of these activities without also interfering with this important work.

A. Research Akin to Conduct in this Case Helps Fight Malicious Software on Android Smartphones

There are many malicious software applications ("malware") offered for free download from Google's Play store and other Android marketplaces. *See, e.g.,* Juniper Networks, *Third Annual Mobile Threats Report* (2013), available at <https://www.juniper.net/us/en/local/pdf/additional-resources/jnpr-2012-mobile-threats-report.pdf> (describing over 250,000 instances of malware for Android). Unwitting users may install this malware on their Android smartphones. If they do, the programs will push annoying pop-up ads, steal phone users' personal information, and/or secretly charge money for unwanted services. Learning which Android applications are dangerous benefits user privacy and safety online.

To investigate this malware problem, security researchers download a huge number of free applications and analyze each application for harmful properties. *E.g.,* Yajin Zhou et al., *Hey, You, Get Off of My Market: Detecting Malicious Apps in Official and Alternative Android Markets*, Proc. 19th Annual Network & Distributed Sys's Symp., Feb. 2012, at 5 ("We crawled five representative marketplaces . . . in total, we collected 204,040 free apps.").

To collect these applications, researchers do what Auernheimer did. They set their software's user-agent to look like Android and crawl through the Android store's application inventory by automatically modifying HTTP requests. *See, e.g.,* Android Marketplace Crawler, <https://code.google.com/p/android-marketplace-crawler/> (last visited July 5); Thomas Cannon, *Downloading APKs from Android Market*, thomascannon.net (June 13, 2011), <http://thomascannon.net/blog/2011/06/downloading-apks-from-android-market/>. The research techniques essential for helping Android researchers discover harmful malware are technologically indistinguishable from Auernheimer's interactions with the AT&T website. If Auernheimer's activity is illegal, the ruling endangers Android malware research.

B. The Wall Street Used Similar Techniques in Its Journal Investigation of Online Price Discrimination

A recent inquiry into price discrimination is another example of researchers use of automated website address modification. Jennifer Valentino-Devries et al., *Websites Vary Prices, Deals Based on Users' Information*, *Wall St. J.*, Dec. 24, 2012. In order to determine whether online retailers engaged in price discrimination, the Wall Street Journal's investigative team built custom software that enabled its test computer to simulate website visits from different computers. To do this, among other things, researchers altered the user-agent "so that the simulated visit appeared to be coming from different Web browsers, including the

default browsers on the iPhone and other common smartphones.” Jeremy Singer-Vine et al., *How the Journal Tested Prices and Deals Online*, Wall. St. J. Digits Blog (Dec. 23, 2012), <http://blogs.wsj.com/digits/2012/12/23/how-the-journal-tested-prices-and-deals-online/>. After discovering that Staples appeared to perform geographic price discrimination, “the Journal simulated visits to the Staples.com website from all of the more than 42,000 U.S. ZIP Codes.” To do this, the Journal automated transmission of modified HTTP requests. *Id.* As part of its What They Know series, The Wall Street Journal published an article on the practice, which, though legal, is highly unpopular with customers. *Id.*

As with the Android security research and with the “account slurper,” the Wall Street Journal used both automated website address manipulation and user agent modification to conduct its investigation. Again, if this Court holds that any of these activities, alone or in combination, meet the statutory definition of “without authorization” or “exceeding authorized access” under the CFAA, the ruling endangers common means of accessing the Internet by researchers and the public alike.

These are but two examples of many valuable privacy and security enhancing research that is technologically indistinguishable from the conduct at issue in this case. Changing user-agents and automating modified HTTP requests should not create CFAA liability.

III. Researchers Conduct Valuable Independent Experiments on Unsecured Public Websites and Other Publicly Accessible Computers Without Permission

Researchers routinely scrutinize websites, software interfaces, electronic devices, and other computer systems for security and privacy shortcomings. Much of this research is independent, conducted without permission from the owners, operators, and licensors of those computer systems. Indeed, independent research sometimes is – and is supposed to be -- adverse to the computer owners' economic, legal, or reputational interests.

Consumer privacy and security online benefits from unapproved research involving public facing websites. In the Android malware example above, Google Play, the company's Android store, publishes terms of use that may prohibit researchers from using automated means to access the site.⁴ Google Play Terms of Service, Section 3, *available at* <https://www.google.com/intl/%25locale%25/mobile/android/market-tos.html> (last visited July 5, 2013) (“You specifically agree not to access (or attempt to access) Google Play through any automated means (including use of scripts, crawlers, or similar technologies) . . .”). Nor did the Wall Street Journal ask Staples for the company's permission to conduct a price discrimination investigation. Indeed, the company would likely have said no, since customers generally dislike price

⁴ AT&T had no such written limitation.

discrimination. Valentino-Devries et al., *Websites Vary Prices*, *supra* (“Some 76% of American adults have said it would bother them to find out that other people paid a lower price for the same product, according to the Annenberg Public Policy Center at the University of Pennsylvania.”)

In another example, many websites track Internet users as they browse the web by installing small pieces of code called “cookies” on the users’ machines. With rising concern over behavioral advertising, Congress and federal regulators are considering new rules to address online consumer privacy. A key focus is users’ ability to avoid tracking by deleting cookies used for targeted advertising and other potentially unwanted purposes.

In 2009, independent researchers at the University of California at Berkeley discovered that many popular websites were using a new methodology, dubbed “flash cookies,” to track users across the web. These “flash cookie” trackers, unlike traditional cookies, cannot be easily deleted and, in fact “respawned” even after the researchers tried to get rid of them. Ashkan Soltani et al., *Flash Cookies and Privacy* (2009), available at <http://ssrn.com/abstract=1446862>. Needless to say, no one asked the websites deploying flash cookies for permission to test their sites, and if asked, the websites surely would have said “no.”

Similarly, in May of this year, reporters covering data privacy at Scripps News discovered over 170,000 sensitive consumer records were freely available

online. Isaac Wolf, *Data Breach Puts Lifeline Phone Applicants' Privacy at Risk*, Scripps Howard News Service (May 20, 2013), <http://shns.com/privacy-on-the-line>. The files were records of applicants for the Federal Communications Commission's (FCC) Lifeline subsidized cell phone program for low-income consumers. The data was highly personal, and included Social Security numbers, birth dates, home addresses, and sensitive details about family finances. Though the data was supposed to be destroyed once the consumer was approved for the subsidy, two telecom providers unlawfully retained the information and stored it in an open, unsecured file-sharing area.

When Scripps News called the telecom companies to report this serious privacy breach, the business' lawyer accused the reporters of violating the CFAA. Specifically, the lawyer said the reporters' conduct crossed the line into criminality when they, like Auernheimer, used a computer script to send automated requests for the data. Letter from Jonathan D. Lee, Counsel, TerraCom and YourTel America, to William Appleton, General Counsel, E.W. Scripps Co. (Apr. 30, 2013), *available at* <https://www.documentcloud.org/documents/701519-response-from-jonathan-lee.html>. Bravely, the reporters revealed the problem despite the companies' legal threats. As a result of this reporting, at least three state attorneys general launched investigations into the companies' privacy misconduct. Isaac Wolf, *Illinois AG to Investigate Phone Companies After Privacy Breach*, Scripps

Howard News Service (May 20, 2013), *available at* <http://shns.com/privacy-on-the-line>. Those officials rightly recognized that the privacy breach was the phone companies fault, and not that of the reporters who discovered, investigated, and reported it.

None of this important work was done in accordance with any website owner's subjective wishes. Very often, a website owner's interests are antithetical to user security and privacy. If this conviction stands, future investigators who discover egregious security or privacy practices by sending common HTTP requests to public websites may reasonably be too afraid to report the breach to the offending company or to the public so that they may protect themselves. Make no mistake: the Bad Guys already will have found the sensitive information and used it for identity fraud; it is the Good Guys who are chilled by overbroad interpretations of the CFAA.

IV. Individuals Must Be “Authorized” to Access Open Public Websites, Or Risk of Sweeping Security and Privacy Research Under The CFAA’s Broad Prohibitions

Neither Staples, flash cookie purveyors, nor telecoms breaking privacy laws approved of the tests above that researchers conducted. This Court should not hold that the CFAA prohibits such testing as “without authorization”⁵. The CFAA does

⁵ 18 U.S.C. § 1030(a)(2)(C) prohibits accessing a computer “without authorization” or “exceeding authorized access”. At trial, the government did not

not and should not impose upon the public any kind of duty to use an open and unsecured site in accordance with a website operator's subjective wishes.

The CFAA does not require members of the public to ignore unsecured data stored on a public website based on the intuition that the website owner would like them to do so. At trial, the government asserted that Auernheimer's access was "unauthorized" since AT&T clearly did not welcome the kinds of queries the co-defendants sent to their webserver. "[I]f the defendant had called up AT&T ... [t]here's no way that they would have provided that information to the defendant." App2. 608. Yet, the First Circuit has rejected CFAA liability for disregarding a website owner's "reasonable expectations" in *EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003). There, a company used a script to collect pricing data available on a competitor's website in order to use that information to undercut that competitor's prices. *Id.* at 60. Obviously, that defendant "[could] have been in no doubt that [the website operator] would dislike the use of the scraper to construct [such] a database." *Id.* at 63. Yet, the First Circuit rejected CFAA liability in part because the website owner "did not purport to exclude competitors from looking at its website and any such limitation would raise serious public policy concerns." *Id.*

identify which prohibition was the basis for its prosecution. See Defendant's Brief at p. 24 f. 11.

Courts have disagreed on the question of whether violations of employment agreements and terms of service could be the basis for CFAA liability. *See United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (imposing liability for such transgressions “allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law.”); *See Int’l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418, 420–21 (7th Cir. 2006) (employee who accesses a computer to further interests adverse to his employer violates his duty of loyalty, terminates his agency relationship, and loses any “authorization” to access the computer.) Yet, like any independent researcher, Auernheimer had no relationship whatsoever with AT&T.⁶ To force the public to conform to some duty of loyalty to website owners goes beyond the broadest readings of the CFAA. That rule risks arbitrary enforcement of law in the interest of private concerns that may not be in the public interest.

Website owners can choose to secure their sites or the data stored on them via password protection, encryption, or other means. But where, as here, the computer is a public webserver, and an individual does not misuse a password, access private accounts, cause the website to malfunction, or even violate the website terms of use, she cannot violate the CFAA.

⁶ Nor was there any terms of use statement on the AT&T website.

V. Neither Auernheimer's Post-Discovery Conduct Nor His Motive Are Grounds for CFAA Liability

A. Security and Privacy Researchers Commonly Publish Their Findings

Researchers find great value in publicly reporting their findings. Publication is essential to academic research and scientific progress. This truism is unsurprising. But publication has special benefits in the field of computer security. A researcher that finds a flaw in one system can help repair that system. A researcher that publishes that vulnerability can contribute to its repair across the Internet. As the examples above show, publication can be a critical step in improving security and privacy. Auernheimer's decision to go to the press with his discovery is neither surprising nor improper.

Nor does it violate the CFAA. In the Fourth Circuit case of *WEC Carolina*, an employee accessed his employers' proprietary computer system to obtain information for use in soliciting business on behalf of a competitor company. *WEC Carolina Energy Solutions v. Miller, LLC*, 687 F.3d 199 (4th Cir. 2012). The Fourth Circuit held that the plain language of CFAA covered improper *access* to information, and not information *misuse*. *Id.* at 205. Because WEC's company policies regulated use of information not access to that information, even if the defendants' purpose in accessing information made available to them as employees was contrary to company policies regulating use, there could be no liability under

the CFAA. *See also Nosal*, 676 F.3d at 857 (“If Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better suited to that purpose.”). Thus, if initial access to a website is authorized, the CFAA simply does not regulate an individual’s subsequent decision to report the information she learns to the public.

A narrow reading of the CFAA is especially important here. Reporting the results of research on computers to the press, to colleagues at conferences, and by publishing are core academic activities protected by the First Amendment. Hinging CFAA liability on the dissemination of information could dangerously impact legitimate research practices and dissuade *Amici* and others from otherwise lawful and valuable publication.

B. A Researcher’s Attitude and Motivations are Irrelevant to CFAA Liability

The government may argue that Auernheimer’s conduct was unauthorized and he knew it. *See* App2. 132, 606-12. At trial, the government introduced evidence that Auernheimer referred to collection of the email addresses as a “theft.” App2. 166. In his testimony, the co-defendant agreed that his program “tricked” and “lied” to the AT&T website. App2. 264. According to the

government, these words “first and foremost” proved Auernheimer’s guilt. App2. 132.

First, CFAA liability should not hinge on the terms Auernheimer used to describe his conduct. Explaining computer security practices in English inevitably requires some translation from computer language to human language. In translation, descriptions sound nefarious when they are not. For example, in the academic paper reporting on respawning flash cookies, researchers described their methodology as “mimick[ing]” a “typical” user’s session on the investigated site. Soltani, *Flash Cookies and Privacy*, at 2. Someone who wished to describe the research in a negative light might call the technique “impersonation.” Neither word is exactly right. The words mean to convey that the test machine was programmed to send the same commands typical user machines would send. But the words chosen to convey this idea can improperly bias the listener towards a moral conclusion unwarranted by the facts.

Similarly, in the Wall Street Journal price discrimination investigation, the paper “simulated” visits from computers around the country. Jeremy Singer-Vine et al., *How the Journal Tested Prices and Deals Online*, Wall. St. J. Digits Blog (Dec. 23, 2013), <http://blogs.wsj.com/digits/2012/12/23/how-the-journal-tested-prices-and-deals-online/>. An angry company might critique the technique as “faking.” The words are inevitable approximations which suggest legal or moral

weight the conduct as a matter of computer science does not have. From our expert perspective, selecting a new user-agent is neither “tricking” or “lying.” Nor is collecting unsecured data from an open website “theft.”⁷

Second, Auernheimer has repeatedly made provocative statements in public and to the trial court. Some of us see Defendant-Appellant as typifying a strong anti-authoritarian tradition familiar to the computer security community. *See, e.g.,* E. Gabriella Coleman, *Phreaks, Hackers, and Trolls: The Politics of Transgression and Spectacle*, in *The Social Media Reader* 191 (Michael Mandiberg ed., 2012) (“There is a rich aesthetic tradition of spectacle and transgression at play with trolls, which includes the irreverent legacy of phreakers and the hacker underground.”). Others of us may simply dislike him. But motive, character, and attitude are not elements of a CFAA violation. As scientists, researchers, and academics, we have diverse reasons for the work we do. The merits of our research should not be judged by our motivations for conducting it.

VI. Criminalizing Computer Security and Privacy Research would Frustrate Congressional Intent and Policy

A. Congress Funds Applied Computer Security and Privacy Research

The U.S. Government provides financial support to applied security and privacy research. The Cyber Security Research and Development Act of 2002, for

⁷ Some unsecured information may be protected by copyright and duplicating it may constitute infringement, but that is not an issue in this case.

example, allocated over \$200 million in computer security and privacy research funding, including for “vulnerability assessments” that identify security flaws in deployed systems. 15 U.S.C. § 7401 (“The Congress finds . . . Federal investment in computer and network security research and development must be significantly increased to . . . improve vulnerability assessment . . .”); *id.* § 7403(a) (directing grantmaking). The National Science Foundation provides financial support through its Secure and Trustworthy Cyberspace program and Team for Research in Ubiquitous Secure Technology initiative. Nat’l Sci. Found., Program Solicitation 12-596, *Secure and Trustworthy Cyberspace*, <http://www.nsf.gov/pubs/2012/nsf12596/nsf12596.htm> (last visited July 5, 2013); TRUST Research, <http://www.truststc.org/research/> (last visited July 5, 2013). The Department of Homeland Security funds through its Cyber Security Research and Development Center, and the Air Force provides grants through its Office of Scientific Research. Dep’t Homeland Security, *Cyber Security R&D Center*, <http://www.cyber.st.dhs.gov/> (last visited July 5, 2013); Robert Herklotz, *Funding Research for a Science of Cybersecurity: The Air Force Makes It a Mission*, *The Next Wave*, 2012, at 16, *available at* http://www.nsa.gov/research/tnw/tnw194/articles/pdfs/TNW_19_4_Web.pdf. These are but a few of the federal funding opportunities for applied security and privacy researchers. This Court should not interpret CFAA to criminalize conduct

that Congress *pays for*, both through direct allocations and through agency programs.

B. Sweeping Security and Privacy Research Within CFAA Undermines the Very Purpose of the Statute

In enacting and amending CFAA, Congress has expressed a consistent policy and intent: protecting the security and privacy of information technology. *See, e.g.,* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Websites*, 63 Md. L. Rev. 320, 323 (2004) (“The CFAA was originally enacted in 1984 as a criminal statute to address hacking and the growing problem of computer crime.”). The 1986 Senate Report on CFAA indicates that the statute is targeted at “a new kind of criminal—one who uses computers to steal, to defraud, and to abuse the property of others.” S. Rep. No. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479. When Congress added 1030(a)(2)(C) in 1996 to cover non-government computer systems, a related Senate report reaffirmed that CFAA is intended to “address[] . . . the problem of computer crime”. S. Rep. No. 104-357, at 5, 7 (1996). Congress intended to prohibit “inherently wrongful” conduct “such as *breaking into a computer.*” *Nosal*, 676 F.3d at 859 (emphasis added).

The examples Congress employed when passing and amending the CFAA show its intention to criminalize breaking into secured computers, and not “misusing” public websites. The 1986 Senate Report invokes an instance where

hackers “broke into” a hospital computer system, as well as message boards for “trafficking in other people’s computer passwords.” S. Rep. No. 99-432, at 2-3. The 1996 Senate Report references security breaches of systems at an Air Force laboratory, Harvard University, the Defense Department, and NASA. S. Rep. No. 104-357, at 4-5 (1996). As information technology has progressed, more people interact with more computer systems in more ways than ever before; judicial interpretations of the CFAA are, consequently, more difficult. *See* Orin S. Kerr, *Cybercrime’s Scope*, 78 N.Y.U. L. Rev. 1596, 1640-42 (2003) (explaining the difficulty of interpreting “access” and “authorization”). The hallmark should remain preventing break-ins, not prohibiting research that prevents break-ins.

CONCLUSION

Researchers serve a critical, effective role in safeguarding security and privacy. Without a plain indication that Congress intended the CFAA to limit independent security and privacy research on public websites, the Court should find that such access is authorized and lawful under the statute. This means reversing Auernheimer’s conviction. It also means dispelling, at least in part, a cloud hanging over independent researchers’ heads as a result of his conviction. Mozilla and the wide array of experienced, renowned, and respected computer scientists and practitioners listed in Exhibit A filed this brief because they are convinced that overturning this conviction will help security and privacy, not harm

it. The alternative empowers private entities to force the public to turn a blind eye to their security and privacy missteps, on pain of a federal lawsuit or criminal prosecution.

Dated: July 8, 2013

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for Amici Curiae

EXHIBIT A

Mozilla Foundation

Mozilla is a global, nonprofit organization dedicated to making the Web better. We emphasize principle over profit, and believe that the Web is a shared public resource to be cared for, not a commodity to be sold. We work with a worldwide community to create open source products like Mozilla Firefox, and to innovate for the benefit of the individual and the betterment of the Web. The result is great products built by passionate people and better choices for everyone.

INDIVIDUALS (Titles Given For Affiliation Purposes Only)

Dave Aitel: *Founder and CEO, Immunity, Inc.*

Professor Matt Blaze: *Associate Professor of Computer and Information Science, University of Pennsylvania*

Dominique Brezinski: *Principal Security Engineer, Amazon.com*

Katherine Carpenter, J.D. M.A.: *Privacy, Data Security, and Health Consultant*

Cesar Cerrudo: *Chief Technology Officer, IOActive Labs*

Sandip Chaudhari: *Information Security Researcher*

Professor E. Gabriella Coleman: *Wolfe Chair in Scientific and Technological Literacy, Department of Art History & Communication Studies, McGill University*

Mike Davis: *Principle Research Scientist, IOActive, Inc.*

Benjamin K. DeLong: *Business Analyst, Rakuten (Buy.com) Loyalty*

Professor David L. Dill: *Professor of Computer Science and, by courtesy, Electrical Engineering, Stanford University*

David Dittrich: *Research Scientist and Engineer Principal, Applied Physics Laboratory, University of Washington*

Aiden Riley Eller: *Vice President of Technology, CoCo Communications; Security Strategist, Leviathan Security Group*

Chris Eng: *Vice President of Research, Veracode*

Dan Farmer: *Security Researcher on DARPA's Fast Track Program*

Rik Farrow: *Security Consultant; Editor of USENIX ;login:*

Professor Edward W. Felten: *Professor of Computer Science and Public Affairs and Director of the Center for Information Technology Policy (CITP), Princeton University*

Dr. Richard Forno: *Director, Graduate Cybersecurity Program, University of Maryland Baltimore County; Assistant Director, UMBC Center for Cybersecurity*

Robert David Graham: *Chief Executive Officer, Errata Security*

Professor J. Alex Halderman: *Assistant Professor of Electrical Engineering and Computer Science, University of Michigan*

Stephen Haywood: *Owner, ASG Consulting*

Frank Heidt: *Chief Executive Officer, Leviathan Security*

Dan Kaminsky: *Chief Scientist, DKH*

Professor Beth Kolko: *Professor, Department of Human Centered Design and Engineering, University of Washington; Faculty Associate, Berkman Center for Internet and Society, Harvard University*

Richard Lindberg: *Information Security Professional*

Ralph Logan: *Partner, Logan Haile, LP*

Shane MacDougall: *Principal Security Engineer, Twitter; Principal Partner, Tactical Intelligence*

Brian Martin: *Independent Vulnerability Researcher and Disclosure Expert*

Jonathan Mayer, J.D.: *Doctoral Student, Stanford Security Laboratory, Department of Computer Science, Stanford University; Junior Affiliate Scholar, Stanford Law School Center for Internet and Society*

Charlie Miller: *Product Security Team, Twitter*

HD Moore: *Chief Research Officer, Rapid7 Labs*

Jameson Mott: *CompTIA Network+*

Dr. Karsten Nohl: *Chief Scientist, Security Research Labs*

Jesus Oquendo: *Chief Security Architect, E-Fensive Security Strategies*

Alexander Peslyak: *Founder and Chief Technology Officer, Openwall*

Steve Regester: *Security Software Engineer*

Jennifer Savage: *Security Researcher and Software Engineer, Tabbedout*

Bruce Schneier: *Security Futurologist, BT*

Ashkan Soltani: *Independent Researcher and Consultant*

Arrigo Triulzi: *Security Consultant and Researcher*

Vlad Tsyrklevich: *Security Engineer, Square*

Marc R. Uchniat: *Director of Technical Operations, Senico*

Matthew Watchinski: *Vice President, Sourcefire*

Nicholas Weaver: *Researcher, International Computer Science Institute*

Fyodor Yarochkin: *Security Analyst and Programmer*

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amicus Curiae In Support Of Defendant-Appellee and Reversal complies with the type-volume limitation of Fed. R. App. P.

32(a)(7)(B) because this brief contains 6,399 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

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 this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2007, the word processing system used to prepare the brief, in 14 point Times New Roman.

Dated: July 8, 2013

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for *Amici Curiae*

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the appellate CM/ECF system on July 8, 2013.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 8, 2013

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for Amici Curiae

CERTIFICATION OF VIRUS CHECK

I hereby certify that a virus check was performed on the electronically filed PDF version of the brief using Sophos v.9.5 and that no viruses were found.

Dated: July 8, 2013

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for *Amici Curiae*

CERTIFICATION OF BAR MEMBERSHIP

In accordance with 3rd Circuit LAR 46.1(e) Jennifer Stisa Granick certifies that she is a member of the Bar of this Court.

Dated: July 8, 2013

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for Amici Curiae

CERTIFICATION OF IDENTICAL COMPLIANCE OF BRIEFS

I certify that the electronically filed PDF and hard copies of the brief are identical.

Dated: July 8, 2013

By: /s/ Jennifer Stisa Granick
Jennifer Stisa Granick (CA Bar #168423)
Director of Civil Liberties
Stanford Law School
Center for Internet and Society
559 Nathan Abbott Way
Stanford, CA 94305
Telephone: (650) 736-8675
Facsimile: (650) 725-4086
jennifer@law.stanford.edu

Attorney for Amici Curiae