IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA	§	
	§	**No. 3:12-cr-413-L**
v.	§	
	§	
BARRETT LANCASTER BROWN		

BRIEF *AMICUS CURIAE* OF
ELECTRONIC FRONTIER FOUNDATION,
REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS,
REPORTERS WITHOUT BORDERS,
FREEDOM OF THE PRESS FOUNDATION,
AND PEN AMERICAN CENTER
IN SUPPORT OF DEFENDANT BARRETT BROWN'S
MOTION TO DISMISS THE SUPERSEDING INDICTMENT

TABLE OF CONTENTS

STATEMENT OF INTEREST

Amici curiae Electronic Frontier Foundation (EFF), Reporters Committee for Freedom of the Press, Reporters Without Borders, Committee to Protect Journalists, Freedom of the Press Foundation, and PEN American Center respectfully urge this Court to grant Defendant Barrett Brown's Motion to Dismiss the Indictment.

Collectively, *Amici* are the leading organizations representing the interests of journalists and the public in the free flow of ideas and information.

The ***Electronic Frontier Foundation*** ("EFF") is a member-supported civil liberties organization working to protect free speech and privacy rights in the online world. With more than 29,000 dues-paying members nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law—including the First Amendment—in the digital age. As part of its mission, EFF has often served as counsel or amicus in cases involving free speech online. *See, e.g.*, *Doe v. Harris*, 2013 WL 144048, 12-cv-5713-TEH (N.D. Cal. Jan. 11, 2013); *Backpage.com v. McKenna*, 881 F. Supp. 2d 1262 (W.D. Wash. 2012); *Free Speech Coalition, Inc. v. Holder*, 729 F. Supp. 2d 691 (E.D. Pa. 2010); *Savage v. Council of American-Islamic Relations, Inc.*, 2008 WL 2951281, No. 07-cv-06076-SI (N.D. Cal. July 25, 2008).

The ***Reporters Committee for Freedom of the Press*** is a voluntary, unincorporated association of reporters and editors that works to defend the First Amendment rights and freedom of information interests of the news media. The Reporters Committee has provided representation, guidance and research in First Amendment and Freedom of Information Act litigation since 1970.

Reporters Without Borders is the largest press freedom organization in the world with almost 30 years of experience. Thanks to its unique global network of 150 local correspondents investigating in 130 countries, 12 national offices (Austria, Belgium, Finland, France, Germany, Italy, Libya, Spain, Sweden, Switzerland, Tunisia, USA) and a consultative status at the United

Nations and UNESCO, Reporters Without Borders is able to have a global impact by gathering and providing on the ground intelligence, conducting cybersecurity workshops, and defending and assisting news providers all around the world.

Freedom of the Press Foundation is a non-profit organization that supports and defends public-interest journalism focused on transparency and accountability. The organization works to preserve and strengthen First Amendment rights guaranteed to the press through a variety of avenues, including 1) accepting and distributing tax-deductible donations to a variety of transparency journalism organizations; 2) supporting organizations and individuals that have been unjustly censored or cut off from funding for doing their job as journalists; 3) promoting the development of open-source tools that protect sensitive digital communications between journalists and their sources; and 4) advocating for the rights of journalists, whistleblowers, and the public's right-to-know in both the public sphere and courtroom.

PEN American Center is a non-profit association of writers with approximately 3,700 members, including poets, playwrights, essayists, novelists, editors, screenwriters, journalists, literary agents, and translators ("PEN"). PEN is affiliated with PEN International, a global writers' organization with 144 centers in more than 100 countries, which was founded in the aftermath of the first World War by leading writers who believed that the international exchange of ideas was the only way to prevent disastrous conflicts born of isolation and extreme nationalism. Today, PEN works with the other chapters of PEN International to advance literature and protect freedom of expression wherever it is imperiled. It advocates for writers all over the world who are persecuted because of their work.

INTRODUCTION

The First Amendment protects Mr. Brown's publication of a publicly-available and lawfully-obtained web address linking to millions of pages of documents discussing suspect activities of the United States government intelligence contractor Stratfor Global Intelligence. Mr. Brown is a well-known and published journalist, and this publication was a necessary part of routine newsgathering and news reporting activities. The publication concerned matters of public

significance—namely, the brazen hack into Stratfor's servers and the fact that Stratfor had been discussing rendition and assassination with its clients along with methods to subvert journalists, political groups and foreign leaders. Speech on matters of public concern such as these is "at the heart of the First Amendment's protection." *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 758-759 (1985) (Powell, J.) (citations omitted).

The First Amendment reflects "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964). Charging Mr. Brown with trafficking in stolen authentication features and aggravated identity theft for the simple act of publishing a web address linking to the Stratfor files contravenes this national commitment. Not only does it violate Mr. Brown's First Amendment rights, it creates a chilling effect on other journalists and the public at large. Linking to online sources and files in articles and through emails and social media is an integral part of communicating on the Internet. Allowing the government to proceed with its charges would threaten this communication; if faced with the prospect of criminal prosecution for linking to questionable sources, many journalists and the public likely will choose to remain silent. Because this case has the strong potential to adversely impact First Amendment-protected speech, *Amici* respectfully request this Court grant Defendant's Motion to Dismiss Counts 1 and 3-12 of the Indictment.

BACKGROUND

I. Anonymous and the HBGary and Stratfor Hacks

In 2010 and 2011, large decentralized associations of loosely-coordinated individuals, some affiliated with the group "Anonymous," launched hundreds of attacks on government, financial services, and company websites around the world,[1] bringing down those websites for periods of time in what some called acts of civil disobedience and others called cyber-terrorism.[2]

[1] David Kravets, *Anonymous Unfurls "Operation Titstorm,"* Wired (Feb. 10, 2010), http://www.wired.com/threatlevel/2010/02/anonymous-unfurls-operation-titstorm/.
[2] Matt Krupnick, *Freedom Fighters or Vandals? No Consensus on Anonymous*, Contra Costa Times (Aug. 16, 2011), http://www.mercurynews.com/top-stories/ci_18686764.

Many of their actions were in response to what the groups saw as government, corporate and organizational corruption and attempts to silence the publication of important information about government actions.[3] The groups' actions were widely reported on by the media.[4]

In February 2011, these groups hacked into the private servers of HBGary, Inc. and HBGary Federal—security firms known to provide services to the United States Government.[5] The groups published the records found on the company servers, including 70,000 emails.[6] These records showed that HBGary and other government contractor security firms, along with the law firm Hunton & Williams LLP, were engaging in questionable and potentially illegal practices that included plans to undermine journalists reporting negatively on U.S. government activity and to foment dissent within social organizations and advocacy groups with positions counter to their clients' interests.[7]

Many journalists and media outlets around the world reported on these attacks and the subsequent release of corporate documents and emails.[8] The companies' actions, as revealed

---

[3] Andy Greenberg, *Wikileaks Supporters Aim Cyberattacks at PayPal*, Forbes (Dec. 6, 2010), http://www.forbes.com/sites/andygreenberg/2010/12/06/wikileaks-supporters-aim-cyberattacks-at-paypal/.

[4] John Leyden, *Anonymous Shuts Down Hidden Child Abuse Hub*, The Register (Oct. 24, 2011), http://www.theregister.co.uk/2011/10/24/anonymous_fight_child_abuse_network/; Adrian Chen, *Anonymous Hacks Police Websites and Data to Support Occupy Wall Street*, Gawker (Oct. 21, 2011), http://gawker.com/5852297/anonymous-hacks-police-websites-and-data-to-support-occupy-wall-street; Mark Hachman, *Anonymous Publishes Internal Documents from Govt. Contractor ManTech*, PC Magazine (July 29, 2011), http://www.pcmag.com/article2/0,2817,2389447,00.asp.

[5] Peter Bright, *Anonymous Speaks: the Inside Story of the HBGary Hack*, Ars Technica (Feb. 15, 2011), http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/.

[6] *Id*.; Peter Ludlow, *The Strange Case of Barrett Brown*, The Nation (June 18, 2013), http://www.thenation.com/article/174851/strange-case-barrett-brown.

[7] Eric Lipton & Charlie Savage, *Hackers Reveal Offers to Spy on Corporate Rivals*, New York Times (Feb. 11, 2011), http://www.nytimes.com/2011/02/12/us/politics/12hackers.html.

[8] Barrett Brown, *Anonymous, Australia, and the Inevitable Fall of the Nation-State*, Huffington Post (Feb. 11, 2010), http://www.huffingtonpost.com/barrett-brown/anonymous-australia-and-t_b_457776.html; Barrett Brown, *The Aims of Anonymous*, Huffington Post (Dec. 8, 2010), http://www.huffingtonpost.com/barrett-brown/the-aims-of-anonymous_b_794182.html.

through those emails, were widely condemned,[9] and media reporting prompted Representative Hank Johnson and more than a dozen other members of Congress to call for an investigation into HBGary and other security contractors' actions.[10] In a letter, these lawmakers stated that the e-mails appeared "to reveal a conspiracy to use subversive techniques" including "possible illegal actions against citizens engaged in free speech." The representatives stated it was "deeply troubling" that "tactics developed for use against terrorists may have been unleashed against American citizens."[11]

Later in 2011, hackers broke into the servers of another government contractor, Stratfor Global Intelligence, releasing between 2.5 and 5 million Stratfor emails and internal Stratfor documents, along with tens of thousands of credit card numbers and passwords.[12] Stratfor provides intelligence for several federal agencies, including the Departments of Defense and Homeland Security, and also works for large national and international corporations, including Goldman Sachs, Dow Chemical Co., Lockheed Martin, Northrop Grumman, and Raytheon. The records released as a result of the hack were even more disturbing than the HBGary emails; they included discussions of rendition and assassination and attempts to subvert journalists, political

---

[9] Martin Kaste, *E-Mails Hacked by 'Anonymous' Raise Concerns*, NPR (Feb. 16, 2011), http://www.npr.org/2011/02/16/133811429/e-mails-hacked-by-anonymous-raise-concerns; Andy Greenberg, *Law Firm That Worked with HBGary Hit with Bar Complaint*, *Forbes* (Feb. 25, 2011), http://www.forbes.com/sites/andygreenberg/2011/02/25/law-firm-that-worked-with-hbgary-hit-with-bar-complaint/.

[10] Dan Eggen, *Democrats Call for an Investigation of Law Firm, 3 Tech Companies*, Wash. Post (Feb. 28, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/28/AR2011022805810.html.

[11] *Id.*

[12] Quinn Norton, *Antisec Hits Private Intel Firm; Millions of Docs Allegedly Lifted*, Wired (Dec. 26, 2011), http://www.wired.com/threatlevel/2011/12/antisec-hits-private-intel-firm-million-of-docs-allegedly-lifted/. The government has not alleged in this case that Mr. Brown participated in the hack in any way. In fact, in November 2013, Jeremy Hammond was sentenced to ten years after pleading guilty to one count under the Computer Fraud and Abuse Act for obtaining and releasing the Stratfor files. Ed Pilkington, *Jailed Anonymous Hacker Jeremy Hammond: "My Days of Hacking Are Done,"* The Guardian (Nov. 15, 2013), http://www.theguardian.com/technology/2013/nov/15/jeremy-hammond-anonymous-hacker-sentenced.

groups and even foreign leaders.[13]

The federal government swiftly investigated and charged the individuals responsible for the hacks.[14] In May 2012, the U.S. Attorney for the Southern District of New York announced that Hector Xavier Monsegur had pleaded guilty to numerous charges under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, in connection with the HBGary hack.[15] It also announced it had indicted Jeremy Hammond and three others in the Southern District of New York for violations of the CFAA, conspiracy to commit access device fraud, 18 U.S.C. § 1029 and aggravated identity theft, 18 U.S.C. § 1028A in connection with the Stratfor hack.[16] On November 15, 2013, Hammond was sentenced to ten years in prison.[17] Monsegur has not been sentenced yet and has been cooperating with the FBI.[18]

II. Journalist Barrett Brown Crowdsources Review of the Stratfor Files

Mr. Brown was a prolific writer for a number of publications including *Vanity Fair*,[19] *The Guardian*[20] and the *Huffington Post*[21] and had published a book, *Flock of Dodos: Behind Modern*

[13] Ludlow, *The Strange Case of Barrett Brown*, The Nation; *The Global Intelligence Files*, WikiLeaks (Feb 27, 2011), http://wikileaks.org/the-gifiles.html (see also cites on Wikipedia page for Stratfor).
[14] *See* FBI Press Release, *Six Hackers in the United States and Abroad Charged for Crimes Affecting Over One Million Victims*, (Mar. 6, 2012), http://www.fbi.gov/newyork/press-releases/2012/six-hackers-in-the-united-states-and-abroad-charged-for-crimes-affecting-over-one-million-victims.
[15] *See United States v. Monsegur*, 1:11-cr-00666-LAP (S.D.N.Y. 2011).
[16] *See United States v. Hammond,* 1:12-cr-00185-LAP (S.D.N.Y. 2012).
[17] Kevin Poulsen, *Anonymous Hacktivist Jeremy Hammond Sentenced to 10 Years in Prison*, Wired (Nov. 15, 2013), http://www.wired.com/threatlevel/2013/11/hammond-sentence/.
[18] Nate Anderson, *FBI Still Needs Hector "Sabu" Monsegur, Sentencing Delayed (Again)*, Ars Technica (Aug. 23, 2013), http://arstechnica.com/tech-policy/2013/08/fbi-still-needs-hector-sabu-monsegur-sentencing-delayed-again/.
[19] http://www.vanityfair.com/contributors/barrett-brown.
[20] http://www.theguardian.com/profile/barrett-brown.
[21] http://www.huffingtonpost.com/barrett-brown.

Creationism, Intelligent Design, and the Easter Bunny in 2007.[22] Long before the HBGary and Stratfor hacks, Brown had written on political issues, including Wikileaks and Anonymous.[23]

After the release of the HBGary files, Mr. Brown, like other journalists, wanted to sift through the voluminous records as source material for future stories. But the quantity of records made public through the attacks was so large that it was virtually impossible for one person or one media outlet to review them all. Mr. Brown decided to employ a technique that has become more and more widely used among journalists and others needing to look through vast quantities of documents—crowd-sourced review.[24]

Crowdsourcing allows news media organizations to work with others—including outside journalists, select groups of volunteers, or even the general public—to review huge troves of records. It has become common in an era when the quantity of documents produced and retained by the government and private organizations increases exponentially every year, where Internet tools make working remotely with others increasingly possible, and where diminishing media budgets have cut newsroom staff significantly over the last 20 years.

Several examples of crowdsourcing in media show just how powerful and important this technique has become. In 2007, the website *Talking Points Memo* and its blog, the *TPM Muckracker*, asked its readers to crowdsource the review of thousands of emails and records released by the Department of Justice, exposing the politically motivated firing of eight United

---

[22] Barrett Brown, *Flock of Dodos: Behind Modern Creationism, Intelligent Design & the Easter Bunny*, Cambridge House Press (2007), http://books.google.com/books/about/Flock_of_Dodos.html?id=X_1BAAAACAAJ

[23] *See, e.g.,* Barrett Brown, *Anonymous: A Net Gain for Liberty*, The Guardian (Jan. 27, 2011), http://www.theguardian.com/commentisfree/cifamerica/2011/jan/27/anonymous-internet; Barrett Brown, *The Aims of Anonymous*, Huffington Post (Dec. 8, 2010), http://www.huffingtonpost.com/barrett-brown/the-aims-of-anonymous_b_794182.html; Barrett Brown, *Wikileaks and War; Secrecy and Context*, Huffington Post (Apr. 13, 2010), http://www.huffingtonpost.com/barrett-brown/wikileaks-and-war-secrecy_b_534627.html; Barrett Brown, *Wikileaks Blows Whistle; Most Miss the Point*, Huffington Post (Apr. 7, 2010), http://www.huffingtonpost.com/barrett-brown/wikileaks-blows-whistle-o_b_525066.html.

[24] Ludlow, *The Strange Case of Barrett Brown*, The Nation.

States Attorneys.[25] *TPM*'s reporting led to the resignation of Attorney General Alberto Gonzalez and garnered a prestigious journalism award in the process.[26]

In another example, in 2009, the British paper, *The Guardian*, successfully employed crowdsourcing to engage the public in reviewing and reporting on 2 million pages of Members' of Parliament expense records and allowed the paper to document and report on extensive financial improprieties.[27] And in 2011, the *Washington Post*, *New York Times*, *MSNBC*, *Mother Jones*, *ProPublica* and *The Guardian* all asked the public to help crowdsource the review of 24,000 pages of Sara Palin's emails from her time as governor of Alaska.[28]

Crowdsourced review has also been crucial in the last year to the reporting on the thousands of pages of leaked documents about the NSA provided by Edward Snowden. Journalists have teamed up across newsrooms and with non-journalist security researchers to

---

[25] Noam Cohen, *Blogger, Sans Pajamas, Rakes Muck and a Prize*, N.Y. Times (Feb. 25, 2008), http://www.nytimes.com/2008/02/25/business/media/25marshall.html; Paul McLeary, *How TalkingPointsMemo Beat the Big Boys on the U.S. Attorney Story*, Colum. Journalism Rev. (Mar. 15, 2007), http://www.cjr.org/behind_the_news/how_talkingpointsmemo_beat_the.php.

[26] Jeff Howe, *A Coup for Crowdsourced Journalism…*, Crowdsourcing (Feb. 25, 2008), http://www.crowdsourcing.com/cs/2008/02/a-coup-for-crow.html.

[27] Michael Andersen, *Four Crowdsourcing Lessons from The Guardian's (Spectacular) Expenses-Scandal Experiment*, Nieman Journalism Lab (June 23, 2009), http://www.niemanlab.org/2009/06/four-crowdsourcing-lessons-from-the-guardians-spectacular-expenses-scandal-experiment/; *How to Crowdsource MP's Expenses*, The Guardian (June 18, 2009), http://www.theguardian.com/news/datablog/2009/jun/18/mps-expenses-houseofcommons; *Who Have MPs Been Having for Dinner?*, The Guardian, http://www.theguardian.com/politics/blog/2010/feb/04/mps-expenses-crowdsourcing (last visited Mar. 5, 2014); MPs' Expenses: What You've Told Us, *The Guardian*, http://www.theguardian.com/news/datablog/2009/sep/18/mps-expenses-westminster-data-house-of-commons (last visited Mar. 5, 2014).

[28] *WaPo, NYT to Crowdsource Palin Emails*, Politico, (June 9, 2011) http://www.politico.com/blogs/onmedia/0611/WaPo_to_crowdsource_Palin_emails.html; *Crowdsourcing the Sarah Palin Emails: User Guide*, The Guardian, http://www.theguardian.com/world/datablog/2011/jun/10/crowdsource-sarah-palin-emails. For other examples, *see* Dave Maas, *The Darrell Issa Cables*, San Diego City Beat (Sept. 14, 2011) http://www.sdcitybeat.com/sandiego/article-9525-the-darrell-issa-cables.html; Amanda Zamora, *Crowdsourcing Campaign Spending: What ProPublica Learned From Free the Files*, ProPublica (Dec. 12, 2012) http://www.niemanlab.org/2012/12/crowdsourcing-campaign-spending-what-propublica-learned-from-free-the-files/.

better report on the material, ensuring its broader impact on society.[29]

Crowdsourced review, whether with the public or other contributors, has become so useful, that in 2009, editors from the *New York Times* and *ProPublica* teamed up to start the website DocumentCloud, which allows journalists, researchers and archivists to upload, annotate, review and share primary source documents.[30] DocumentCloud is now used by newsrooms from the *New York Times* to *National Public Radio* to the *Dallas Morning News* as well as non-profit organizations like EFF and the ACLU. It allows contributors to annotate their own and others' documents and to discover relationships among documents and sources that would not have been evident had the records remained in an individual organization's files.[31]

Against this backdrop, in 2011, Mr. Brown crowdsourced the review of the thousands of emails contained in the HBGary records by creating a type of webpage called a "wiki" that allows people to collaborate and add, modify, or delete content.[32] Mr. Brown invited other investigative journalists to join the wiki, called "Project PM," to review and discuss the released HBGary records.[33] This led to extensive reporting on the troubling information contained in the

---

[29] *See, e.g.*, James Ball, Bruce Schneier & Glenn Greenwald, *NSA and GCHQ Target Tor Network that Protects Anonymity of Web Users*, The Guardian (Oct. 4, 2013) http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption; Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, Wash. Post (Dec. 4, 2013) http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

[30] *Who We Are: Meet the People Behind DocumentCloud*, DocumentCloud, https://www.documentcloud.org/about; *Document Contributors*, DocumentCloud, https://www.documentcloud.org/contributors.

[31] Steve Myers, *Archived Chat: ProPublica, NYT Team on How DocumentCloud Will Improve Investigations*, Poynter (June 17, 2009), http://www.poynter.org/latest-news/top-stories/96362/archived-chat-propublica-nyt-team-on-how-documentcloud-will-improve-investigations-2/.

[32] *Wiki*, Wikipedia, https://en.wikipedia.org/wiki/Wiki. Wikipedia, itself, is a type of a "wiki," an online encyclopedia in which any member of the public can make changes to entries or create new entries.

[33] *Project PM*, http://wiki.echelon2.org/wiki/Main_Page; Ludlow, *The Strange Case of Barrett Brown*, The Nation.

records.[34] For example, in the summer of 2011, Mr. Brown wrote an article in *The Guardian* detailing a secret U.S. intelligence program called Romas/COIN which allowed for large scale monitoring of social networks and data mining appearing to target the Middle East.[35] The details of this program were culled by reviewing the more than 70,000 emails obtained from the HBGary hack. Other media organizations, including *Raw Story* and *Network World*, reported on Mr. Brown's story.[36]

After success with the crowdsourced review of the HBGary files and as part of his reporting on the server attacks and on the secret world of government security contractors, Mr. Brown appears to have attempted to crowdsource the review of the even larger trove of Stratfor records.[37] According to documents filed in the prosecution of Jeremy Hammond, the Stratfor records were available to the public via many sources on the Internet,[38] including at the web address (or "URL"[39]): http://wikisend.com/ download/597646/stratfor_full_b.txt.gz.[40]

---

[34] *See, e.g.*, Mike Masnick, *Leaked HBGary Documents Show Plan to Spread Wikileaks Propaganda for BofA… And "Attack" Glenn Greenwald*, TechDirt (Feb. 10, 2011), http://www.techdirt.com/articles/20110209/22340513034/leaked-hbgary-documents-show-plan-to-spread-wikileaks-propaganda-bofa-attack-glenn-greenwald.shtml. *See also* Project PM, *Media Reports*, *available at* http://wiki.echelon2.org/wiki/Media_Reports (listing & linking to articles).

[35] Barrett Brown, *A Sinister Cyber-Surveillance Scheme Exposed*, The Guardian (June 22, 2011), http://www.theguardian.com/commentisfree/cifamerica/2011/jun/22/hacking-anonymous.

[36] Ms. Smith, *Project PM Leaks Dirt on Romas/COIN Classified Intelligence Mass Surveillance, NetworkWorld* (June 22, 2011), http://www.networkworld.com/community/blog/project-pm-leaks-dirt-romascoin-classified-in; David Edwards, *U.S. Conducting "Mass Surveillance" Against Arab World: Report*, The Raw Story (June 22, 2011), http://www.rawstory.com/rs/2011/06/22/u-s-conducting-mass-surveillance-against-arab-world-report/.

[37] *See* Ludlow, *The Strange Case of Barrett Brown*, The Nation. WikiLeaks later made the Stratfor files available to the public on its website and partnered with several media outlets in reviewing the records. *The Global Intelligence Files*, WikiLeaks (Feb 27, 2011), http://wikileaks.org/the-gifiles.html.

[38] *See Def. Mot. to Dismiss the Indictment*, 5-6 (filed March 5, 2014) (citing to Hammond Complaint and noting "[t]he web pages referenced above are all still available online, as are the links they contain").

[39] A "URL" or "uniform resource locator" is, like the address of a house or business, an address that directs a user's browser (a program running on the user's computer such as Microsoft Explorer, Apple Safari or Firefox) to go to a specific web page. For example, if a user typed in the URL, "http://www.txnd.uscourts.gov/index.html," into his browser bar, and hit "return," the browser would be directed to the home page for the United States District Court for the Northern District of Texas. For more, *see* http://en.wikipedia.org/wiki/Uniform_resource_locator.

Wikisend is a web service that allows its customers to share files with one another.[41] Users can upload a file to wikisend's server—where the file is then stored—and the service generates a unique web address for that file.[42] The user can then share the web address for the file with others, who can type the address into a browser to download a copy of the original file. Often a web address acts as a "link" or "hyperlink," which means that it essentially automatically enters the address of the page for the user.[43]

According to the government, Mr. Brown transferred the wikisend web address for the Stratfor files from one Internet Relay Chat or "IRC" channel to another—making the wikisend web address available to people who had access to the Project PM wiki. *See* Superseding Indictment at p. 1.[44] IRC is one of the most common forms of real-time communication over the Internet. *ACLU v. Reno*, 929 F. Supp. 824, 834 (E.D. Pa. 1996). It operates much like the old-fashioned telephone "party lines," in that it "allows two or more [users] to type messages to each

---

[40] The wikisend URL ends in ".txt.gz." This format indicates the original file was a ".txt" or "text" file, which is a file with little or no formatting that can be opened by any program that reads text. *See* http://en.wikipedia.org/wiki/Text_file. The fact that the URL ends in .gz indicates the original file was compressed to make it smaller using an open source compression utility called "gnu zip." *See* http://www.gzip.org/.

[41] *Wikisend*, http://wikisend.com/.

[42] Wikisend.com Terms and Conditions, http://wikisend.com/terms/. "Servers" are computers that store "documents and make them available over the Internet…. Users access documents by sending request messages to the servers that store the documents. When a server receives a user's request…, it prepares the document and then transmits the information back to the user." *See In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001).

[43] Sometimes the text accompanying a link reveals the underlying URL; for example, the text on a webpage might say "the website, http://www.dallasnews.com/, has up-to-date news on Dallas, Texas." But sometimes the URL is not apparent from the text until the user clicks on the link, and the browser goes to the linked address. In the above example, the text could instead say, "click here for up-to-date news on Dallas, Texas," where clicking "here" would direct the computer user's browser to the same http://www.dallasnews.com/ web page.

[44] *See also* U.S. Attorney's Office, Northern District of Texas Press Release, *Dallas Man Associated with Anonymous Hacking Group Faces Additional Federal Charges* (Dec. 7, 2012) ("According to the indictment, Brown transferred a hyperlink from an Internet Relay Chat (IRC) channel to an IRC channel under his control. That hyperlink provided access to data stolen from the company Stratfor Global Intelligence (Stratfor), which included more than 5,000 credit card account numbers…") available at http://www.justice.gov/usao/txn/PressRelease/2012/DEC2012/dec7brown_barrett_ind.html.

other that almost immediately appear on the others' computer screens." *Id*. at 835.

If a person copied the URL for the wikisend page into his browser or clicked on the link, his browser would open the page for the Stratfor files, and he could choose to download a copy from the wikisend server. The web address "http://wikisend.com/download/597646/stratfor_full_b.txt.gz" did not contain the actual Stratfor files; the URL acted only as a pointer to the server where the files resided. A person who shared that web address with another did not transmit or transfer the actual files, because the files remained on the wikisend server. Even when the second person clicked on the wikisend link or copied the URL into his browser—seeking to download the files—the second person received only a copy of the original document, while the original remained on the wikisend server.

III. Linking Is an Integral Part of Journalism

This act of sharing a hyperlink is nothing remarkable in today's digital age. Every day, people around the world routinely share links with one another over email, social media and other forms of digital communication. On social media like Facebook, linking to pictures stored on Facebook's servers or articles found on outside websites is a crucial part of interacting with friends, family and business associates. The frequency with which people share links online caused Twitter, a service that allows its users to compile short public messages of no longer than 140 characters, to automatically shorten any hyperlinks in a post (known as a "tweet") to allow a user to fit more text within the character limits.

For journalists, "linking" is crucial to effectively providing readers with background and context to stories. For example, since the summer of 2013, media organizations from around the world have been linking to hosts of sensitive government documents obtained by former NSA employee Edward Snowden. Indeed, the controversy began on June 5, 2013 when *The Guardian* published a top-secret order issued by the Foreign Intelligence Surveillance Court ("FISC")

ordering Verizon to disclose telephone metadata of all of its customers.[45] The *Guardian* article linked to the top-secret order itself, and that order is still available online.[46] As other organizations, including the *New York Times*,[47] the *Washington Post*[48] and CNN,[49] reported on this breaking news, they too linked to not only the *Guardian's* article, but to the order itself on the *Guardian's* website. And as more revelations about the NSA programs were reported in the press, these media organizations began linking to other top-secret orders and classified intelligence materials.[50] These organizations shared the links with the public at large through social media like Facebook and Twitter, hoping it would prompt others to read their stories on the NSA's surveillance.[51] But by sharing these links, these media organizations were also disseminating classified and top-secret national security information—information protected by

---

[45] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The Guardian (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[46] *Verizon Forced to Hand Over Telephone Data – Full Court Ruling*, The Guardian (June 6, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.

[47] Charlie Savage & Edward Wyatt, *U.S. is Secretly Collecting Records of Verizon Calls*, N.Y. Times (June 5, 2013), http://www.nytimes.com/2013/06/06/us/us-secretly-collecting-logs-of-business-calls.html?_r=0.

[48] Timothy B. Lee, *Report: NSA Asked Verizon for Records of All Calls in the U.S.*, Wash. Post (June 5, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/05/nsa-asked-verizon-for-records-of-all-calls-in-the-u-s/.

[49] Chelsea J. Carter, *Report: Secret Court Order Forces Verizon to Tur Over Telephone Records of Millions*, CNN (June 6, 2013), http://www.cnn.com/2013/06/05/politics/nsa-verizon-records/.

[50] *See, e.g.,* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (linking to PRISM slides); James Glanz, Jeff Larson & Andrew W. Lehren, *Spy Agencies Tap Data Streaming from Phone Apps*, N.Y. Times (Jan. 27, 2014), http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html (linking to slides detailing NSA collecting phone app data).

[51] *See* N.Y. Times, Twitter (June 6, 2013 7:01 AM EST), https://twitter.com/nytimes/status/342642404442128384 (linking to NYT story on order to Verizon); The GuardianUS, Twitter (June 5, 2013 4:13 PM EST), https://twitter.com/GuardianUS/status/342419047134150656 (linking to Guardian story on order to Verizon).

statute no less than the credit card records at issue in this case.

Linking is also common in news reports involving stories of public interest beyond the NSA scandal. The *New York Times* has an enormous cache of documents, including emails, reports and analyses, concerning the mining of shale gas obtained from confidential sources not authorized to share the documents with the media.[52] In 2009, the *Wall Street Journal* published emails obtained from a hack into computers at a U.K. university concerning climate change.[53] And NPR linked to leaked internal documents taken from the American Legislative Exchange Council (ALEC) detailing its attempts to influence conservative politicians in the United States.[54]

ARGUMENT

I. THE FIRST AMENDMENT PROTECTS THE PUBLICATION OF LAWFULLY-OBTAINED, TRUTHFUL INFORMATION ABOUT A MATTER OF PUBLIC CONCERN

The First Amendment to the U.S. Constitution guarantees freedom of speech and the press. At "the heart of the First Amendment's protection" is the freedom "to discuss publicly and truthfully all matters of public concern without previous restraint or fear of subsequent punishment." *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 776 (1978) (quoting *Thornhill v. Alabama*, 310 U. S. 88, 101-102 (1940) (quotations omitted). This is because this kind of speech "is more than self-expression; it is the essence of self-government." *Garrison v. Louisiana*, 379 U.S. 64, 75 (1964). By protecting "the free discussion of governmental affairs," the First Amendment ensures "the individual citizen can effectively participate in and contribute to our republican system of self-government." *Globe Newspaper Co. v. Super Ct., Cty of Norfolk*, 457 U.S. 596, 604 (1982) (quoting *Mills v. Alabama*, 384 U.S. 214, 218 (1966) (quotations

---

[52] *Documents: Leaked Industry E-Mails and Reports*, N.Y. Times, http://www.nytimes.com/interactive/us/natural-gas-drilling-down-documents-4-intro.html.
[53] *Climate Emails: Science and Candor*, Wall Street Journal (Nov. 24, 2009), http://online.wsj.com/news/articles/SB10001424052748704779704574553652849094482.
[54] *How ALEC Serves as a "Dating Service" for Politicians and Corporations*, NPR (Dec. 10, 2013), http://www.npr.org/2013/12/10/249956329/how-alec-serves-as-a-dating-service-for-politicians-and-corporations (linking to leaked documents obtained by *The Guardian*).

omitted)). The First Amendment has a broad reach, subject only to "well-defined and narrowly limited classes of speech." *Brown v. Entm't Merch. Ass'n*, 131 S. Ct. 2729, 2733 (2010) (citation omitted).

The First Amendment protects Mr. Brown's publication of a publicly-available and lawfully-obtained web address linking to several million pages of documents discussing suspect activities of a United States government security contractor. The application of a statute to prohibit the publication of lawfully obtained information is subject to strict scrutiny. *Fla. Star v. B.J.F.*, 491 U.S. 524, 541-42 (1989); *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 103 (1979); *see also Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829, 845 (1978) (applying clear and present danger standard). As such, the government must show that its application of the criminal statutes to the facts of Mr. Brown's case is "narrowly tailored to serve a state interest of the highest order." *Fla. Star v. B. J. F.*, 491 U.S. at 541; *Bartnicki v. Vopper*, 532 U.S. 514, 528 (2001). This it cannot do.

First, publication of the wikisend web address is a form of newsgathering and constitutes protected speech. *See Branzburg v. Hayes*, 408 U.S. 665, 681 (1972) ("[W]ithout some protection for seeking out the news, freedom of the press could be eviscerated."). The web address does not contain any information other than the location of a specific webpage, and as such cannot, on its own, be considered an authentication feature, access device or means of identification under 18 U.S.C. §§ 1028, 1028A or 1029. Second, even if the government could base its prosecution on the documents—including credit card numbers—available via the web address, the publication of the web address itself is protected because it was lawfully obtained and the documents available through the web address discuss matters of public concern. Finally, if the government were allowed to proceed with its prosecution against a journalist for this kind of activity, this would create a chilling effect, not just on news reporting, but also on the speech of ordinary Americans who share links to information every day through emails, blogs, Twitter, Facebook, chat and texting tools, and other novel and as yet undiscovered forms of modern communication.

A. The Wikisend URL and Hyperlink Are Protected Speech and Are Not an Authentication Feature or Means of Identification Pursuant to 18 U.S.C. §§1028 or 1028A

Mr. Brown did not transfer an authentication feature or means of identification. The only thing the government alleges Mr. Brown transferred—and, in effect, published— was the URL, "http://wikisend.com/download/597646/stratfor_full_b.txt.gz" which he appears to have copied from one IRC chat to another. This URL did not contain any information other than the address of a specific webpage; it did not contain any of the Stratfor files at issue, let alone the 5,000 or more credit card numbers alleged by the government. As merely an address containing nothing more than its 58 characters, this cannot be considered an authentication feature, access device or means of identification.

In short, when Mr. Brown published the wikisend web address to a group of people at Project PM who could help him crowdsource the review of the thousands of pages of records, he was engaging in "newsgathering"—an activity that is a necessary part of the reporting process and is entitled to First Amendment protection. *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972).

B. The Government May Not Restrict Publication of Truthful, Lawfully-Obtained Information About a Matter of Public Concern Absent a "State Interest of the Highest Order"

The Supreme Court has held repeatedly that the First Amendment prohibits state officials from restricting lawfully-obtained "truthful information about a matter of public significance . . . absent a need to further a state interest of the highest order." *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 103 (1979); *see also New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam)*; Landmark Commc'ns, Inc. v. Virginia*, 435 U.S. 829 (1978); *Fla. Star v. B.J.F.*, 491 U.S. 524 (1989). This is true whether the information came from a government source or through the use of "routine newspaper reporting techniques." *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 104 (1979) ("A free press cannot be made to rely solely upon the sufferance of government to supply it with information.") (citations omitted). Because Counts 1 and 3-12 of the superseding indictment seek to hold Mr. Brown criminally liable for publishing truthful,

lawfully obtained information about a matter of public concern, they must be dismissed.[55]

1. By Prosecuting Mr. Brown for Publishing a Web Address Linking to Other Files, the Government is Attempting to Restrict Pure Speech

In Count 1, the government alleges that, by publishing a URL linking to a webpage allowing access to the Stratfor files, Mr. Brown knowingly trafficked in stolen authentication features and means of identification in violation of 18 U.S.C. § 1028. However, by charging Mr. Brown under this statute, the government is prosecuting him for disclosure of information; this is nothing less than a regulation of pure speech—a government restriction subject to strict scrutiny under the First Amendment.

The Supreme Court has noted, "the naked prohibition against disclosures [unlike a prohibition against "use"] is fairly characterized as a regulation of pure speech." *Bartnicki v. Vopper*, 532 U.S. 514, 527. This is true, whether or not the statute at issue may be considered content neutral. *Id*. at 526-27; *see also Id.* at 528 (citing *Daily Mail*, 443 U.S. at 103) (noting that, although the section of the Wiretap Act at issue was a content-neutral law of general applicability, its application nevertheless constituted a regulation of pure speech and required the government show a need to further a state interest "of the highest order").

In *Bartnicki*, the defendants were sued under the Wiretap Act, 18 U.S.C. § 2511(c), for intentionally disclosing the contents of an illegally-recorded conversation about union activity that they received—legally—from another person. Here, although the government has charged Mr. Brown with "transferring" and "trafficking in" credit card numbers, it is actually prosecuting him in Counts 1 and 3-12 for *disclosing* a URL that he obtained—legally—from another. As in *Bartnicki*, where the activity giving rise to liability was linked to the information communicated on the wiretap tapes, *id.* at 527, n.11, here the activity giving rise to liability is inextricably linked to the information in the files available at the web address. As shown above, the web address, alone, consisted only of its 58 characters. However, by clicking on the link in the web

[55] Counts 3 through 12, which charge Mr. Brown with aggravated identity theft in violation of 18 U.S.C. § 1028A, are predicated on Mr. Brown violating 18 U.S.C. § 1028. Thus, if the Court dismisses Count 1, it must necessarily dismiss counts 3 through 12 as well.

address or copying it into a browser search bar, another person could access all the records available at the link. Therefore, the disclosure of the link is "like the delivery of a handbill or pamphlet[,]" and as such, "is the kind of 'speech' that the First Amendment protects." *Bartnicki* at 527.

2. The Speech Concerned a Matter of Public Significance

The government bases its charges on the fact that credit card information was available via the wikisend web address. However, also available via that address were millions of pages of records containing significant documentation of Stratfor and its clients' improper and potentially illegal conduct. This subject—along with the subject of the hack into Stratfor's servers and website—is, without question, a matter of public concern.

Whether a matter is of public concern is a question of law for the court to decide. *Cinel v. Connick*, 15 F.3d 1338, 1345-46 (5th Cir. 1994) (citations omitted). An issue of public concern may "'be fairly considered as relating to any matter of political, social, or other concern to the community,' or when it is 'a subject of general interest and of value and concern to the public.'" *Snyder v. Phelps*, 131 S. Ct. 1207, 1216 (2011) (citing *Connick v. Myers*, 461 U.S. 138, 146 (1983); *San Diego v. Roe*, 543 U.S. 77, 83-84 (2004) (per curiam)). To determine whether speech falls into this category, a court must independently examine the "content, form, and context," of the speech "as revealed by the whole record." *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 761 (1985). A court must review what was said, where it was said, and how it was said, and no one factor is dispositive. *Snyder v. Phelps*, 131 S. Ct. at 1217.

Here, the context in which the wikisend web address was made available to the public, combined with the content of and files available at the web address, indicate this speech concerned a matter of public significance. The government alleges Mr. Brown published the wikisend web address on December 25, 2011. Superseding Indictment at p. 1. This is one day after hackers announced they had broken into Stratfor's website and servers and the same day

several media outlets reported on the attack.[56] As the *New York Times* reported that same day, this "breach was the latest in [Anonymous'] ongoing campaign of computer attacks which, to date, has been aimed at MasterCard, Visa and PayPal as well as groups as diverse as the Church of Scientology, the Motion Picture Association of America and the Zetas, a Mexican crime syndicate."[57] As *Wired* also noted at the time, "this hack could prove particularly significant, because Stratfor serves as an information-gathering resource and open source intelligence analysis for both the U.S. military and for major corporations."[58] These contemporaneous media reports show both that the hacks into Stratfor and other companies' servers and websites were of ongoing public interest at the time Mr. Brown is alleged to have published the web address and also that the documents released from the Stratfor hack in particular had the potential to touch on significant matters of public concern. Thus, both the context and content of the speech indicate it concerns a matter of public significance.

The form in which the speech occurred also proves this point. The records were voluminous, and the only way to engage others in reviewing them—assuming that was Mr. Brown's purpose in publishing the wikisend web address—would be to make them easily available by publishing a link that takes the reviewer to a compressed file that may be downloaded onto the reviewer's computer from another server.

Given the form, context and content of the speech, publication of the wikisend web address linking to the Stratfor files constituted speech on a matter of public concern.

---

[56] Nicole Perlroth, *Hackers Breach the Web Site of Stratfor Global Intelligence*, N.Y. Times (Dec. 25, 2011), http://www.nytimes.com/2011/12/26/technology/hackers-breach-the-web-site-of-stratfor-global-intelligence.html; Natalie Weinstein, *Anonymous Claims Hack on Security Think Tank*, CNet (Dec. 25, 2011), http://news.cnet.com/8301-1009_3-57348300-83/anonymous-claims-hack-on-security-think-tank/.

[57] Perlroth, *Hackers Breach the Web Site of Stratfor Global Intelligence*, N.Y. Times.

[58] Quinn Norton, *Antisec Hits Private Intel Firm; Millions of Docs Allegedly Lifted*, Wired (Dec. 26, 2011), http://www.wired.com/threatlevel/2011/12/antisec-hits-private-intel-firm-million-of-docs-allegedly-lifted/.

3. The Speech is Protected Even if it Linked to Records Illegally Obtained by Another

The First Amendment protects the publication of truthful information about a matter of public concern even when the source of that information obtained it illegally—and even when the journalist knows or has reason to know that the information was illegally obtained. *New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam) (upholding the right of the press to publish information of great public concern obtained from documents stolen by a third party); *Bartnicki*, 532 U.S. at 528, 517-18, 535 (protecting speech where publishers did not participate in the interception but knew or had reason to know that the interception was unlawful); *Fla. Star*, 491 U.S. at 546 (White, J., dissenting) (noting, in case protecting reporting on a rape, that the reporter admitted at trial that she knew that names of rape victims were not meant to be disclosed); *cf. Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000) (journalist may be held civilly liable where he participated in illegal interception of phone conversations).

There is no dispute that someone other than Mr. Brown obtained the Stratfor records unlawfully; in fact, Jeremy Hammond pleaded guilty and was sentenced to ten years in prison for hacking into Stratfor's servers to obtain the files.[59] The government has not alleged that Mr. Brown was responsible for or had anything to do with that hack or that he obtained the wikisend URL illegally. The government also has not alleged that the information accessible via the wikisend URL was untruthful. As such, it is entitled to the same protections as the speech at issue in *Bartnicki*, *Florida Star*, and *New York Times*.

4. The Government Has Not and Cannot Show that Prosecuting Mr. Brown Serves "a Need to Further a State Interest of the Highest Order"

Because the speech at issue in this case concerned a matter of public interest, the government must show that prosecuting Mr. Brown for his actions serves "a need to further a state interest of the highest order." *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 103 (1979) (the "*Daily Mail* Principle"). Here, while the state interest in preventing identity theft and access

[59] Ed Pilkington, *Jailed Anonymous Hacker Jeremy Hammond: "My Days of Hacking are Done,"* The Guardian (Nov. 15, 2013), http://www.theguardian.com/technology/2013/nov/15/jeremy-hammond-anonymous-hacker-sentenced.

device fraud is significant, it must "give way when balanced against the interest in publishing matters of public importance." *Bartnicki*, 532 U.S. at 534 (holding that privacy interests protected by statute prohibiting disclosure of illegally wiretapped conversations were outweighed by interest in publishing a matter of public concern).

The Supreme Court has held that, "[i]n addition to . . . 'the overarching public interest, secured by the Constitution, in the dissemination of truth'" there are other reasons that support application of the *Daily Mail* Principle. *Fla. Star*, 491 U.S. at 533-36. First, by limiting protection to *lawfully-obtained* information, the government "retains ample means of safeguarding significant interests upon which publication may impinge . . . ." *Id.* at 534. Here, the government interests are "to combat identity theft and the use of stolen identification documents," *United States v. Hairup*, 565 F. Supp. 2d 1309, 1312 (D. Utah 2008), as well as to deter false identification-related crimes, the manufacture and distribution of false identification, and "the unlawful use of identification documents in a wide variety of circumstances." *United States v. Luke*, 628 F.3d 114, 119 (4th Cir. 2010) (citing H.R. Rep. No. 97-802, at 8 (1982) and *United States v. Gros*, 824 F.2d 1487, 1491 (6th Cir. 1987)). However, those interests are amply protected, both by prosecuting the person who first illegally obtained the Stratfor files—which the government has already done by prosecuting Jeremy Hammond under the CFAA—and by prosecuting anyone who uses the credit card numbers illegally. Further, except in extremely rare occasions, a government interest in deterring another's criminal conduct is insufficient to justify restricting the speech of a "law-abiding possessor of information." *Bartnicki*, 532 U.S. at 529-30. The Court in *Bartnicki* noted "it would be quite remarkable to hold that speech by a law-abiding possessor of information can be suppressed in order to deter conduct by a non-law-abiding third party." *Id*.

Second, "punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act." *Fla. Star*, 491 U.S. at 535. *Bartnicki* noted, "there is no basis for assuming that imposing sanctions" upon the publisher of information will deter those who actually violated the

law: the individuals who illegally obtained the information. *Bartnicki*, 532 U.S. at 531. Here, the wikisend web address and the documents accessible through that address were already available to the public on the Internet. Mr. Brown was not the first to post the URL but obtained it through an open IRC channel in the same way any other member of the public could. Punishing him merely for disclosing this URL to others is unlikely to further the government's interests in combatting identity theft, particularly when the government can prosecute those individuals who illegally obtained the credit card numbers or used or attempted to use them.

Dismissing the indictment against Mr. Brown would not prevent the government from prosecuting others for violating the statutes at issue under different factual circumstances. *See Bartnicki*, 532 U.S. at 533 (the outcome of the case does not turn on whether § 2511(1)(c) may be enforced with respect to most violations of the statute without offending the First Amendment). As in *Bartnicki*, the application of the statutes at issue to the facts of Mr. Brown's case presents an "unusual case," *id.* at 531, and the Court here need not decide whether applying the statutes to different facts would similarly violate the First Amendment.

II. PROSECUTING MR. BROWN UNDER THESE CIRCUMSTANCES WILL CAUSE A CHILLING EFFECT ON THE PRESS

In *Florida Star*, the Court noted a final reason supporting the *Daily Mail* principle that the government may not restrict speech without showing "a need to further a state interest of the highest order." *Fla. Star v. B. J. F.*, 491 U.S. 524, 535 (1989) (citing *Cox Broadcasting*, supra, at 496); *Smith v. Daily Mail Publ'g Co.*, 443 U.S. at 103. This reason is that, allowing the media to be punished for publishing truthful information may lead to "timidity and self-censorship." *Fla. Star v. B. J. F.*, 491 U.S. 524, 535 (U.S. 1989) (citing *Cox Broadcasting*, supra, at 496). This is especially true in Mr. Brown's case, where the files accessible through the wikisend web address contained much more than the 5,000 credit card numbers alleged in the superseding indictment; they also contained the millions of Stratfor emails documenting questionable and potentially illegal practices conducted by Stratfor on behalf of the United States government,

private businesses and trade groups.[60] To allow the prosecution of a journalist for the incidental link to documents containing credit card numbers buried within thousands of records concerning matters of public concern so important that they prompted Congress to call for an investigation,[61] would create a chilling effect on all reporters' decisions to share information about and report on such matters.

The Fifth Circuit has noted that "[r]eporters must have some freedom to respond to journalistic exigencies without fear that even a slight, and understandable, mistake will subject them to liability. Exuberant judicial blue-pencilling after-the-fact would blunt the quills of even the most honorable journalists." *Ross v. Midwest Commc'ns, Inc.*, 870 F.2d 271, 275 (5th Cir. 1989). To allow this prosecution for sharing a link to go forward would not only create a chilling effect on reporters attempting to report on illegal activities and illegally-obtained information but could put the entire system of disseminating information on the Internet at risk. Modern online journalism—like most websites on the Internet—relies on linking to convey information. For example, in an online article about Mr. Brown and this prosecution in *The Nation*, there are no fewer than 15 links to outside sources.[62] As the *New York Times* has noted in another article on this prosecution:

> Journalists from other news organizations link to stolen information frequently. Just last week, *The New York Times, The Guardian* and *ProPublica* collaborated on a significant article about the National Security Agency's effort to defeat encryption technologies. The article was based on, and linked to, documents that were stolen by Edward J. Snowden, a private contractor working for the government[.][63]

---

[60] Ludlow, *The Strange Case of Barrett Brown*, The Nation; Quinn Norton, *Antisec Hits Private Intel Firm; Millions of Docs Allegedly Lifted*, Wired (Dec. 26, 2011), http://www.wired.com/threatlevel/2011/12/antisec-hits-private-intel-firm-million-of-docs-allegedly-lifted/.

[61] Dan Eggen, *Democrats Call for Investigation of Law Firm, 3 Tech Companies*, Wash. Post (Feb. 28, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/02/28/AR2011022805810.html.

[62] Ludlow, *The Strange Case of Barrett Brown*, The Nation.

[63] David Carr, *A Journalist-Agitator Facing Prison Over a Link*, N.Y. Times (Sept. 8, 2013), http://www.nytimes.com/2013/09/09/business/media/a-journalist-agitator-facing-prison-over-a-link.html.

Indeed, the myriad reports and stories about the NSA surveillance link to numerous top secret slide presentations and classified FISC opinions obtained by Mr. Snowden. But under the government's prosecution theory here, these media organizations would all be guilty of violating the law because it is a crime to disseminate classified national security information under the Espionage Act. *See* 18 U.S.C. §§ 793(d); 798.[64]

Yet no one—including, most likely the government itself—would accuse these organizations of violating the law because their stories and links to illicit material are clearly protected by the First Amendment. Indeed, a recent Congressional Research Service report on the topic reached that precise conclusion, finding "although unlawful acquisition of information might be subject to criminal prosecution with few First Amendment implications, the publication of that information remains protected."[65] Allowing the press to publish truthful information about matters of public concern—even sensitive matters of national security—is precisely what the First Amendment serves to protect.

Mr. Brown's status as an independent journalist does not change this analysis. The Supreme Court has "consistently rejected the proposition that the institutional press has any constitutional privilege beyond that of other speakers." *Citizens United v. Fed. Election Comm'n*, 558 U.S. 310, 352 (2010) (citation omitted). In *Citizens United*, the Court noted that, "[w]ith the advent of the Internet and the decline of print and broadcast media . . . the line between the media and others who wish to comment on political and social issues becomes far more blurred."

---

[64] Unsurprisingly, Edward Snowden himself has been charged with these specific crimes in a criminal complaint filed in the Eastern District of Virginia. The *Washington Post*, among other organizations, has linked to the criminal complaint in news articles about the charges despite the fact that the complaint was filed under seal and remains sealed as of this filing. *See* Peter Finn & Sari Horwitz, *U.S. Charges Snowden with Espionage*, Wash. Post (June 21, 2013), http://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html; *U.S. vs. Edward J. Snowden Criminal Complaint*, Wash. Post http://apps.washingtonpost.com/g/documents/world/us-vs-edward-j-snowden-criminal-complaint/496/ (criminal complaint against Snowden contributed by DocumentCloud).

[65] *See* Jennifer K. Elsea, *Criminal Prohibitions on the Publication of Classified Defense Information*, Congressional Research Service #R41404, September 9, 2013, at p. 31.

Id. In finding the First Amendment protected a blogger's post on the Internet, the Ninth Circuit recently noted that "First Amendment protections do not turn on whether the defendant was a trained journalist, formally affiliated with traditional news entities, engaged in conflict-of-interest disclosure, went beyond just assembling others' writings, or tried to get both sides of a story." *Obsidian Fin. Grp., LLC v. Cox*, 740 F.3d 1284, 1291 (9th Cir. 2014).

Ultimately then, the government's prosecution of Mr. Brown threatens not only journalists and the press, but the public at large. As ordinary Americans regularly share links to news and human-interest stories, medical research, gossip about movie stars, and shopping deals with friends and family through email and social media platforms like Facebook and Twitter, these communications are threatened by a broad application of the criminal statutes at issue in this case.

Faced with the threat of criminal prosecution under the government's theory here, journalists and the general public will likely remain silent rather than choose to link to data, documents or information available online they are not entitled to have. The First Amendment prohibits just such a chilling effect.

CONCLUSION

"[T]he possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted . . . ." *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973). Long ago, James Madison said, "Some degree of abuse is inseparable from the proper use of every thing; and in no instance is this more true than in that of the press." *New York Times Co. v. Sullivan*, 376 U.S. 254, 271 (1964) (citing 4 Elliot's Debates on the Federal Constitution (1876), p. 571) (citations omitted).

While identity theft is a vicious problem the government has a right to investigate and stop, prosecuting Mr. Brown does not serve that aim. Instead, it presents a significant risk to the First Amendment guarantee of freedom of speech and of the press. Allowing the government to proceed with Counts 1 and 3-12 against Mr. Brown would pose a chilling effect on the press and countless others who link to information in an increasingly networked and connected

online world.

The First Amendment requires that Counts 1 and 3-12 of the Superseding Indictment be dismissed.

Dated: March 10, 2014

Respectfully submitted,

/s/ Jennifer Lynch
Jennifer Lynch (admitted *pro hac vice*)
jlynch@eff.org

/s/ Hanni Fakhoury
Hanni Fakhoury (admitted *pro hac vice*)
hanni@eff.org
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993

Counsel for Amicus Curiae
Electronic Frontier Foundation