United States Court of Appeals

for the

Third Circuit

Case No. 13-1816

UNITED STATES OF AMERICA

– v. –

ANDREW AUERNHEIMER

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY (WIGENTON, J.),
CRIMINAL NO. 11-CR-470 (SDW)

ADDENDUM OF *AMICUS CURIAE* NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS IN SUPPORT OF APPELLANT

STEVEN P. RAGLAND
JENNIFER A. HUBER
BEN D. ROTHSTEIN
KEKER & VAN NEST LLP
633 Battery Street
San Francisco, California 94111
Tel.: (415) 391-5400
Fax: (415) 397-7188

Attorneys for Amicus Curiae National Association of Criminal Defense Lawyers

Of Counsel:
JENNY CARROLL
Seton Hall University School of Law
Newark, New Jersey 07102

PETER GOLDBERGER
50 Rittenhouse Place
Ardmore, Pennsylvania 19003

Third Circuit Co-Vice-Chairs, National Association of Criminal Defense Lawyers Amicus Curiae Committee

TABLE OF CONTENTS

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNTANGLING THE WEB

A Guide To Internet Research

The opinions expressed in this article are those of the author(s) and do not represent the official opinion of NSA/CSS.

(b)(3)-P.L. 86-36

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

Untangling the Web: An Introduction to Internet Research
by [redacted], Center for Digital Content
Last Updated: February 28, 2007
Cover Design by [redacted]

(b)(3)-P.L. 86-36

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~

~~This product has been produced for official use only. This product is not approved for public release. The information contained herein is for the exclusive use of the original recipient and is not for further distribution outside the recipient's agency or organization. The original recipient may make copies for distribution only within the recipient's agency or organization.~~

~~Ultimate responsibility for the protection of this product from public disclosure resides with the user, with severe penalties for non-compliance.~~

~~For additional information, please contact:~~

[redacted]
9800 Savage Road
Suite 6324
Fort Meade, MD 20755-6324

(b)(3)-P.L. 86-36

This Page Intentionally Left Blank

Table of Contents

Preface: The Clew to the Labyrinth

One of the most famous stories about libraries tells of the tenth century Grand Vizier of Persia, Abdul Kassem Ismael who, "in order not to part with his collection of 117,000 volumes when traveling, had them carried by a caravan of 400 camels trained to walk in alphabetical order."[1] However charming this tale may be, the actual event upon which it is based is subtly different. According to the original manuscript, now in the British Museum, the great scholar and literary patron Sahib Isma'il b. 'Abbad so loved his books that he excused himself from an invitation by King Nuh II to become his prime minister at least in part on the grounds that four hundred camels would be required for the transport of his library alone.[2]

A 21st Century version of the story might feature any number of portable electronic devices—a laptop, a PDA, or even a mobile phone—designed to overcome this difficulty. Today, 1000 years later, the Persian scholar/statesman would have to find a new excuse for declining the job offer. Abdul Kassem Ismael (aka Sahib Isma'il b. 'Abbad) would be hard pressed to explain why he couldn't just find what he needed on the Internet. The message seems to be that books are passé, replaced by ones and zeroes, the real world replaced by a virtual one, knowledge supplanted by information at best and chaotic data at worst. Have we shrunk the world or expanded it? Or have we in some way replaced it?

Untangling the Web for 2007 is the twelfth edition of a book that started as a small handout. After more than a decade of researching, reading about, using, and trying to understand the Internet, I have come to accept that it is indeed a Sisyphean task. Sometimes I feel that all I can do is to push the rock up to the top of that virtual hill, then stand back and watch as it rolls down again. The Internet—in all its glory of information and misinformation—is for all practical purposes limitless, which of course means we can never know it all, see it all, understand it all, or even imagine all it is and will be. The more we know about the Internet, the more acute is our

---

[1] Alberto Manguel, *A History of Reading*, New York: Penguin, 1997, 19. Manguel cites as his source Edward G. Browne's *A Literary History of Persia*, 4 vols., London: T. Fisher Unwin, 1902-24. I found the specific reference to this story on pages 374-375 of Vol. 1, Book IV, "Decline of the Caliphate." There is, sadly, no mention of the alphabetical arrangement of the library. This entire masterpiece is available online at The Packard Humanities Institute, Persian Texts in Translation, 23 February 2006, <http://persian.packhum.org/persian/pf?file=90001011&ct=0> (15 November 2006).

[2] Edward G. Browne. Vol. 1, Book IV, "Decline of the Caliphate," *A Literary History of Persia*," 4 vols., London: T. Fisher Unwin, 1902-24, 374-375. Available online at The Packard Humanities Institute, Persian Texts in Translation, 23 February 2006, <http://persian.packhum.org/persian/pf?file=90001011&ct=0> (15 November 2006).

awareness of what we do not know. The Internet emphasizes the depth of our ignorance because "our knowledge can only be finite, while our ignorance must necessarily be infinite."[3] My hope is that *Untangling the Web* will add to our knowledge of the Internet and the world while recognizing that the rock will always roll back down the hill at the end of the day.

I will end this beginning with another story and a word of warning. "Tlön, Uqbar, Orbis Tertius" describes the discovery of an encyclopedia of an unknown planet. This unreal world is the creation of a secret society of scientists, and gradually, the imaginary world of Tlön replaces and obliterates the real world. Substitute "the Internet" for Tlön and listen. Does this sound familiar?

> "Almost immediately, reality yielded on more than one account. The truth is that it longed to yield...The contact and the habit of Tlön have disintegrated this world. Enchanted by its rigor, humanity forgets over and again that it is a rigor of chess masters, not of angels...A scattered dynasty of solitary men has changed the face of the world. Their task continues. If our forecasts are not in error, a hundred [or a thousand] years from now someone will discover the hundred volumes of the Second Encyclopedia of Tlön. Then English and French and mere Spanish will disappear from the globe. The world will be Tlön."[4]

As we enjoy, employ, and embrace the Internet, it is vital we not succumb to the chauvinism of novelty, that is, the belief that somehow whatever is new is inherently good, is better than what came before, and is the best way to go or best tool to use. I am reminded of Freud's comment about the "added factor of disappointment" that has occurred despite mankind's extraordinary scientific and technical advances. Mankind, claims Freud, seems "to have observed that this newly-won power over space and time, this subjugation of the forces of nature, which is the fulfillment of a longing that goes back thousands of years, has not increased the amount of pleasurable satisfaction which they may expect from life and has not made them feel happier."[5] Indeed, most of the satisfactions derived from technology are analogous to the "cheap enjoyment...obtained by putting a bare leg from under the bedclothes on a cold winter night and drawing it in again."[6] What good is all this technology and information if, instead of improving our lot, it only adds to our confusion and suffering? We are continually tempted to treat all technology as an end in itself instead of a means to some end. The Internet is no exception: it has in large

---

[3] Karl Popper, *Conjectures and Refutation: The Growth of Scientific Knowledge*, London & New York: Routledge, 2002, p. 38.

[4] Jorge Luis Borges, "Tlön, Uqbar, Orbis Tertius," in *Labyrinths*, ed. Donald A. Yates and James E. Irby, New York: New Directions Books, 1962, 17-18.

[5] Sigmund Freud, "Civilization and Its Discontents," tr. James Strachey, New York: Norton, 1962, 34-35.

[6] Freud, 35.

measure become the thing itself instead of a means of discovery, understanding, and knowledge.

Like Tlön, the Internet, "is surely a labyrinth, but it is a labyrinth devised by men, a labyrinth destined to be deciphered by men." We must avoid getting lost in the labyrinth without a clew. My hope is that *Untangling the Web* will be something akin to Ariadne's clew,[7] so that as you unravel it, you can wind your way through the web while avoiding some of its dangers. Remember also that those who use the Internet to do harm, to spread fear, and to carry out crimes are like the mythical Minotaur who, as well as being the monster in the Minoan maze, was also its prisoner.

8

[7]Daedalus, the architect of the infamous labyrinth on Crete, purportedly gave King Minos' daughter Ariadne the clew, a ball of thread or yarn, to use to find a way out of the maze. Ariadne in turn gave the clew to Theseus, who slew the Minotaur and found his way out of the labyrinth. Theseus repaid Ariadne's kindness by leaving her on an island on their way back to Athens.

[8] "Minotaurus," WikiMedia Commons, <http://commons.wikimedia.org/wiki/Image:Minotaurus.gif> (6 February 2007). This image is in the public domain because its copyright has expired.

Specialized Search Tools & Techniques

This section, which first appeared in the 2006 edition, was born of the rapid growth of both unconventional search techniques such as Google hacking and the wildfire spreading of such tools as online maps. This year, I have added a new section on Wikipedia and expanded the maps and mapping section.

"Google Hacking"

This topic has received a great deal of attention in the world of Internet search in the past few years. While this activity is generically referred to as "Google hacking,"[61] this is a double misnomer. First, to limit this practice to "Google" is a mistake because many of these kinds of searches can be run using any search engine, though they are clearly going to be most effective with a large, powerful search tool that offers many search options, such as Google. Second, this is not hacking in the sense that most people use the term, i.e., gaining access to a computer or data on a computer illegally or without authorization. Nothing I am going to describe to you is illegal, nor does it in any way involve accessing unauthorized data. ***"Google (or search engine) hacking" involves using publicly available search engines to access publicly available information that almost certainly was not intended for public distribution***. In short, it's using clever but legal techniques to find information that doesn't belong on the public Internet.

To understand how this information has found its way into search engine databases, we need a quick overview of how search engines work. Very simply, search engines deploy "spiders" (aka crawlers or bots), which is actually software that "crawls" websites looking for new sites, updating old ones, following links, and dumping all that data into search engine databases where it is stored, sorted, and eventually accessed by users. There is nothing illegal, immoral, or even fattening about search

[61] Let's talk about the term *hacking* for a minute. A hacker is someone who is proficient at using or programming a computer; in short, a computer expert. While there is no universal agreement on a preferred term for someone engaged in illegal/illicit computer or network activity, I will call these "black hat" hackers "malicious hackers" to distinguish them from "white hat" or neutral "hackers," meaning proficient or expert computer users.

engine spiders. Indeed, without them, we would have little or no idea what is "out there" and available to us. The problem for webmasters is that it is their responsibility to keep the search engine spiders out of any parts of their websites they do not want to be accessed and indexed by a search engine. The spider is not smart; it simply knows that if a "door" is open, it can—and will—go in and crawl around. Webmasters must tell spiders "do not enter" (primarily) by the use of the Robots Exclusion Protocol.

Robots Exclusion[62] comes in two basic flavors: either a metatag that can be inserted into the HTML of a web page (usually used by an individual) or a Robots Exclusion Protocol (robots.txt) file, a specially formatted file inserted by the website administrator to tell the spider which parts of the website may and may not be indexed by the spider. If a robots exclusion is missing or improperly configured, the spider will index pages that the website owner may not have wished to have been accessed.

The whole problem of keeping information on the Internet private dramatically worsened almost overnight a couple of years ago when Google quietly started indexing whole new types of data. Originally, most of what got spidered and indexed was HTML webpages and documents, with some plain text thrown in for good measure. However, the ever-innovative Google decided this wasn't good enough and started to index PDF, PostScript, and—most importantly—a whole range of Microsoft file types: Word, Excel, PowerPoint, and Access. Problem was, lots of folks had assumed these file types were "immune" to spidering not because it couldn't be done but because no one had yet done it. As a result, many companies, organizations, and even governments had quite a lot of egg on their faces when sensitive documents began turning up in the Google database.

That was then, this is now. You might think people would have learned, but judging by the amount of "sensitive" information still available, many have not. Even though search engines now routinely index many non-HTML file types, many individuals and organizations still do not protect these files from the long reach of search engine spiders. Furthermore, there are many ways for sensitive information to end up in search engine databases. An improperly configured server, security holes, and unpatched software can give search engine spiders unintended access. Quite frankly, most of the problems boil down to one thing: human error, either through ignorance or neglect.

What kinds of sensitive information can routinely be found using search engines? The types of data most commonly discovered by Google hackers usually falls into one of these categories:

---

[62] For additional information, see: <http://www.robotstxt.org/wc/exclusion.html> (14 November 2006).

- personal and/or financial information
- userids, computer or account logins, passwords
- private, confidential, or proprietary company data
- sensitive government information
- vulnerabilities in websites and servers that could facilitate breaking into the site

Now, you may be thinking to yourself, "I use Google all the time and I've never encountered this type of information." That's not surprising. It's not usually the kind of thing you would stumble across inadvertently. Normally, one would have to be actively looking for this type of information. Of course, many of the documents Google hackers find using these techniques are not sensitive and indeed are intended for the public Internet. Only a tiny fraction of the over eight billion pages in the Google index were not meant to be made available to the public. *And, it so happens, these techniques are excellent unconventional ways of finding useful information that might not be discovered using routine search engine queries.* Here are some of the typical techniques used in Google hacking:

- search by file type[63], site type, and keyword: many organizations store financial, inventory, personnel, etc., data in *Excel spreadsheet format* and often mark the information "Confidential," so a Google hacker looking for sensitive information about a company in South Africa might use a query such as:

  [filetype:xls site:za confidential]

  a similar but more specific search could involve use of a keyword such as *budget* to search for Excel spreadsheets at Indian websites; for example: [filetype:xls site:in budget]

- one of the most popular Google hacking technique is to employ ***stock words and phrases*** such as *proprietary, confidential, not for distribution, do not distribute*, along with a search for specific file types, especially Excel spreadsheets, Word documents, and PowerPoint briefings.

- search for files containing ***login, userid, and password*** information; note, even at international sites, these terms usually appear in English. This type of information is typically stored in spreadsheet format, so a typical search might be:
  [filetype:xls site:ru login]

---

[63] It is critical that you handle all Microsoft file types on the Internet with extreme care. Never open a Microsoft file type on the Internet. Instead, use one of the techniques described here.

- ***misconfigured web servers*** that list the content of directories not intended to be on the web often offer a rich load of information to Google hackers; a typical command to exploit this error is:

  [intitle:"index of" site:kr password]

- <u>numrange search</u>: this is one of the least known and (formerly) one of the scariest searches available through Google. Numrange uses two number separated by two periods (dots) and no spaces. While "***legitimate***" numrange users probably will want to indicate what the numbers mean, e.g., weight, money, pixels, etc. Google does not require any special words or symbols to run a successful numrange search; hence its power. *Numrange* can be used with keywords and other Google search options, such as:

  [site:www.jordanislamicbank.com 617..780]

How is numrange typically used in Google hacking? It used to be extremely effective in finding credit card numbers and social security numbers. Because of the publicity about criminals using Google to look for private data, this particular search no longer works for credit card and Social Security numbers, which is not a bad thing.

The disabled "hack" was:

[numrange:4567000000000000..4567999999999999 visa] or

[numrange:222000000..250999999 ssn]

Now if you try these searches, you will see this message:

Lest you think I am spilling the beans here, I assure you I am not revealing anything that is not already widely known and used on the Internet both by legitimate and illicit Google hackers. I am fully indebted to Johnny (johnnyihackstuff) Long for many of the "Google hacking" techniques[64] I have learned. Please use the information he provides judiciously because many of the Google *hacking* techniques he discusses are really designed for *cracking*, i.e., breaking into websites and servers. That is not

[64] Johnny Long, *Google Hacking for Penetration Testers*, Syngress: Rockland, MA, 2004.

something I encourage or advocate. I do encourage you to "hack" your own website to see what kinds of information is being revealed inadvertently via Google and other search engines.

Also, a lot of the best information Johnny offers is for his site members only, and I do not want to suggest you register there. Nonetheless, Johnny's briefing slides from the 2004 Black Hat and Defcon12 conferences are available at the official Black Hat Briefings website and elsewhere (so much for registration). I have also found his excellent white paper "The Google Hacker's Guide" at other sites that do not require registration; there is another very good briefing on the dangers of Google by Sebastian Wolfgarten.

There was a fair amount of sniping following Long's talks at Black Hat and Defcon, mostly of the "big deal" variety, i.e., it is not "real" hacking and therefore not worthy of presenting at Defcon. However, this is a very shortsighted point of view when one considers the kinds of information that is so very easily available via Google, et al. How would you like to see your Social Security Number, credit card number, and that very handy little three digit number on the back of your credit card used for "verification," bank routing information, mother's maiden name, etc., in the next Google hacking briefing? Yes, all this kind of information is readily available (I know...I've uncovered quite a bit of it myself). And this doesn't even take into consideration all the other website weaknesses, such as multiple vulnerabilities with IIS 6.0 Web-based administration, that can be exposed using Google.

Johnny Long's Googledorks Page http://johnny.ihackstuff.com/ghdb.php

Johnny Long's "The Google Hacker's Guide"
http://www.securitymanagement.com/library/Google_Hacker0704.pdf

Johnny Long, "You Got That With Google?" Black Hat Briefings and Defcon12, July 2004.
http://www.blackhat.com/html/bh-media-archives/bh-archives-2004.html#USA-2004

Johnny Long, "Google Hacking Mini-Guide," *Informit.com*, 7 May 2004
http://www.informit.com/articles/printerfriendly.asp?p=170880

Sebastian Wolfgarten, "Watch Out Google"
http://www.wolfgarten.com/downloads/Watch_out_google.pdf

Joe Barr, "Google Hacks are for Real," *Newsforge.com*, 6 August 2004
http://www.newsforge.com/article.pl?sid=04/08/05/1236234

Taken all together, the information Johnny Long has found using Google (he sticks with this one search engine), combined with the techniques he details at his website, provide an excellent tutorial on using Google to find stuff that really should not be on the public Internet or easily accessible via a search query. Furthermore, the greatest value of his efforts may not be in finding useful information but in demonstrating the vulnerabilities of any given website and the necessity of taking strong measures to ensure the information that gets into Google (as well as other search engine databases and the Internet Archive) is only that which is intended.

Given the large amount of "sensitive" or private data readily available via Internet search engines, people naturally wonder why companies and individuals do not actively try to remove this information. Sometimes they do, but much still remains accessible. Why? ***Getting private information "back" is harder than preventing its disclosure in the first place.*** There are steps you can take to remove your data, but as hacker Adrian Lamo says, "removing links after the fact isn't a very elegant solution." Nor is it likely to be terribly effective. There are a number of reasons for this, but what it boils down to is: it's very hard to put the genie back in the bottle.

First of all, you have to find out if your data is "out there" in order to ask search engines to remove it and, clearly, many people and organizations are not playing defense, that is, they are not routinely checking to see what is indexed from their websites. Let's say you find something on Google that shouldn't be on the public Internet. The first thing you have to do is to protect the sensitive pages on your site or remove them entirely. However, even when you have removed those pages from your website, this doesn't mean they can't be accessed. Once documents are indexed in a search engine database, a publicly available copy of those documents (usually referred to as the cache copy) may remain behind for days, weeks, even months.

The next step is to ask Google to remove your sensitive pages from its database. However, even when Google removes your data, there are literally hundreds of other search engines around the world, and who knows what they have indexed from your site. It will not be an easy task finding out. And I'll hazard a guess that not all of them will be quite so accommodating as Google in removing pages.

To make matters worse, if something really "juicy" shows up in a search engine, chances are someone will find it and copy it to another website. Once this happens, you can forget about removing that information from the Internet. To further complicate matters, even if no individual comes across your sensitive data, the Internet Archive[65] spider is almost certainly going to find that webpage and index it in the Archive, and there it will remain until and unless you find it first and ask the Archive to remove it. As you can see, the genie is running amuck! Prevention is much easier (though certainly not easy) than curing this particular disease, so it's vital to pay close attention to anything you put on a website, especially something you do not want the whole world to see.

---

[65] The Internet Archive is a non-profit organization that was founded to "build an 'Internet library,' with the purpose of offering permanent access for researchers, historians, and scholars to historical collections that exist in digital format. Based in San Francisco, the Internet Archive has been harvesting the World Wide Web since 1996, to create one of the largest data collections in the world. The Internet Archive's web archive contains over 100 terabytes of data, and the collection is growing at a rate of 12 terabytes per month." <http://www.archive.org/> (14 November 2006).

Because of the vast amount of information available using public search engines, it's relatively easy to find lots of interesting, amusing, shocking examples of sensitive information. While this is all fine and good for entertaining yourself and impressing your friends, what we are really after is useful, meaningful, and actionable information. Put succinctly:

It's Easier to Find Anything Than It Is to Find Something

So how do you find "something" useful? While it isn't easy to do so, I can make some suggestions that might help. The most valuable assets you have are your subject matter knowledge and your creativity. Add these to a few search engine strategies, and you can probably find many relevant and genuinely useful pieces of information. The strategies I recommend for finding "something" rather than just "anything" are:

<u>Limit the search by site</u>

This can be as broad as a county [site:fr] or as specific as an individual server on a company website [site:office.microsoft.com].

<u>Try to be as specific as possible</u>

You will have a lot more success searching for information within the Chinese Ministry of Foreign Affairs [site:fmprc.cn.gov] than looking at all the sites indexed for China [site:cn] or even for the government of China [site:gov.cn]

<u>Add keywords</u>

Here's where your subject matter knowledge and creativity really help. You are the best source of information about what words are most likely to yield the best quality and quantity of useful information. As a general rule, more uncommon words work best (consider using unusual proper names).

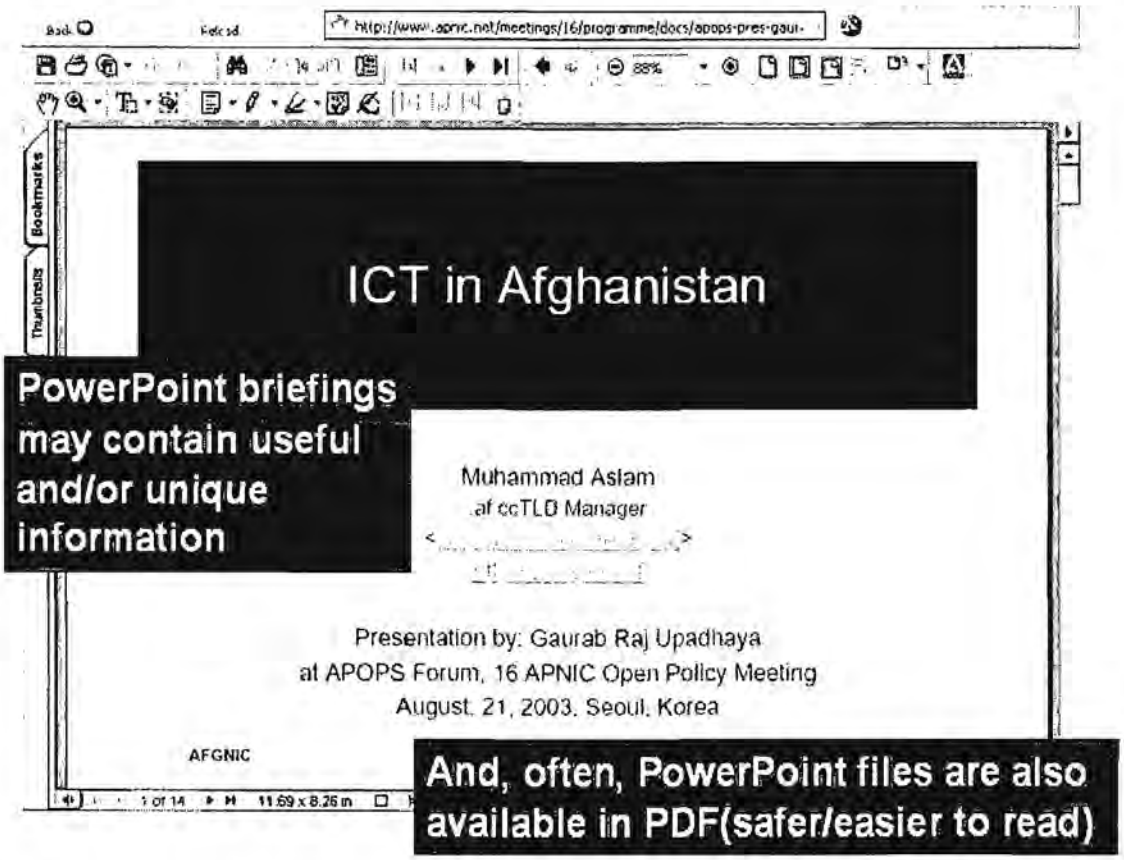
<u>Limit the search by file type</u>

Most of the best information found by Google hackers is not on webpages (HTML) but in other types of files. Try all or most of the file types one at a time (these are not the only searchable file types; check the particular search engine's documentation (*Help* page) for others):

filetype:pdf—good for large documents of all types; widely used in academia, government, and business; many PowerPoint briefings are also made available in PDF at the same website

filteype:doc—good for internal working documents, reports, etc.

filetype:xls—good for personnel data, computer records, financial information filetype:ppt—good for briefings, which often contain company or government plans for the future



<u>Use Google hacking techniques to search inside websites requiring registration</u>

You will frequently encounter a website, perhaps a database, that requires registration to view its contents. On occasion, you can use Google to get at that data without registering. For example, let's say you find a database of international companies that requires *free* registration. Without registering, you may be able to use Google to list all the companies and even get a look at the individual entries. Try this series of queries or something similar:

[site:www.companyname.com inurl:database] or

[site:www.companyname.com inurl:directory] or

[site:www.companyname.com inurl:index]

Then, look for keywords, such as *companies*, and move to the next level query:

[site:www.companyname.com inurl:companies]

You may be able to browse through the list of companies and get names, addresses, phone numbers, etc.

Search in the native language

I cannot emphasize strongly enough how important it is to use keyword search terms that are in the native language of the entity you are researching. The Internet is becoming much less dependent upon English, and sites written in languages that do not use the Latin alphabet are growing by leaps and bounds. For example, a search term written in the native language and encoding is far more likely to yield interesting, useful results than the same word transliterated into English. Most good quality search engines now correctly render non-Latin search terms regardless of how the term is transliterated in English. A search on the Arabic محمد returns very different results than searching on [muhammad], [mohamet], [mohammed], etc.

Remember that Diacritics Also Affect Searches

Most search engine algorithms are now set up to "read" accented search terms differently from those without accents. It's easy to test this by searching first for a term without any diacritical marks and then the same word with the marks, e.g., resume vs. résumé.

Types

Some common types of diacritical marks:

- acute accent (´)
- ring[1] above (°) used for angstrom (Å), aka krouzek
- breve (˘)
- caron or háček (ˇ)
- cedilla (¸)
- circumflex (^)
- umlaut[1] or diaeresis (¨)
- double acute accent (˝)
- grave accent (`)
- macron (¯)
- ogonek (˛)
- spiritus asper
- spiritus lenis

[1]/ Strictly taken not diacritics but parts of the character.

[66]

Look for Misspellings (Intentional or Accidental)

I am constantly amazed by the frequency of misspelled words, urls, file names, etc., I encounter on the Internet. By far, most appear to be simple mistakes, often made by non-English speakers trying to cope with our confusing language. These mistakes tend to propagate as users copy and paste them again and again, which is what I believe happened here:

[66] Fact Index, <http://www.fact-index.com/d/di/diacritic.html>

UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~


Google Web Images Groups News Froogle more »
enlgish site:www.chinadaily.com.cn Search Advanced Search Preferences

Web Results **1** - **10** of **10** from **www.chinadaily.com.cn** for **enlgish**. (**0.30** seconds)

jobs
Chinadaily.com.cn Recruitment 中国日报网站招聘. 网站设计部-
高级制作师(1名) (北京市). 要求 有良好的美术基础 ...
www.chinadaily.com.cn/**enlgish**/ doc/2004-03/16/content_315314.htm - 23k - Cached - Similar pages

jobs
Chinadaily.com.cn Recruitment 中国日报网站招聘. 网站设计部-
设计师(1名) (北京市). 要求 有专业美术设计基础 ...
www.chinadaily.com.cn/**enlgish**/ doc/2004-03/16/content_315316.htm - 23k - Cached - Similar pages

jobs
Chinadaily.com.cn Recruitment 中国日报网站招聘. 市场部-项目经理（
发行推广业务）(2名) (北京市). 要求： 30 ...
www.chinadaily.com.cn/**enlgish**/ doc/2004-03/16/content_315317.htm - 23k - Cached - Similar pages

jobs
Chinadaily.com.cn Recruitment 中国日报网站招聘. 《21
世纪少年英文报》诚聘各地发行代理. 《21世纪少年英文报 ...
www.chinadaily.com.cn/**enlgish**/ doc/2004-04/06/content_321050.htm - 9k - Cached - Similar pages

jobs
Chinadaily.com.cn Recruitment 中国日报网站招聘. 英语学习栏目编辑(
2-3名) (北京市). 工作所在地：北京 职责 ...
www.chinadaily.com.cn/**enlgish**/ doc/2004-03/16/content_315312.htm - 30k - Cached - Similar pages

Finally, the enormity of the task of finding meaningful and useful information on the Internet is both daunting and comforting: daunting because we know we can only scratch the surface of all the data and comforting because there is an almost limitless pool of possibilities. I find it useful to keep the challenge in perspective by recalling that a study published in 2000 showed "*the sixty known, largest deep Web sites* contain data of about 750 terabytes (HTML-included basis) or *roughly forty times the size of the known surface Web*."[67] In short, there is just so much data and information available via the Internet that no institution, no government, no computer, and certainly no individual can possibly grasp more than a small portion of all there is.

---

[67] Michael K. Bergman, "The Deep Web: Surfacing Hidden Value," *BrightPlanet .com*, July 2001, <http://www.brightplanet.com/technology/deepweb.asp> (14 November 2006), Introduction.

Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act

BY ZOE LOFGREN AND RON WYDEN 06.20.13 9:30 AM

Photo: *Daniel J. Sieradski / Flickr*

The Internet is up for grabs.

Foreign countries want to control it. Military regimes use it to spy, to oppress, and to attack public and private institutions. 'Big Content' sought to censor it and dismantle its architecture. Law enforcement and intelligence agencies want to mine and monitor it. Powerful incumbent business interests seek to shape it in ways that benefit their bottom line but undermine the national interest and the interests of individuals worldwide.

In each of these areas, there is debate in Congress about how to respond. We need an informed public debate to ensure lawmakers make the right choices that fully preserve the vital openness of the Internet and the privacy and civil liberties of its users. Reforming the Computer Fraud and Abuse Act (CFAA) should be a part of that debate.

The CFAA is a sweeping Internet regulation that criminalizes many forms of common Internet use. It allows breathtaking levels of prosecutorial discretion that invites serious abuse. As Congress considers policies to preserve an open Internet as a platform for ideas and commerce, reforming the CFAA must be included.

Lying about one's age on Facebook, or checking personal email on a work computer, could violate this felony statute.

The Law Is Flawed and Prone to Prosecutorial Abuse

Vagueness is the core flaw of the CFAA. As written, the CFAA makes it a federal crime to access a computer without authorization or in a way that exceeds authorization. Confused by that? You're not alone. Congress never clearly described what this really means. As a result, prosecutors can take the view that a person who violates a website's terms of service or employer agreement should face jail time.

So lying about one's age on Facebook, or checking personal email on a work computer, could violate this felony statute. This flaw in the CFAA allows the government to imprison Americans for a violation of a non-negotiable, private agreement that is dictated by a corporation. Millions of Americans — whether they are of a digitally native or dial-up generation — routinely submit to legal terms and agreements every day when they use the Internet. Few have the time or the ability to read and completely understand lengthy legal agreements.

Another flaw in the CFAA is **redundant provisions** that enable a person to be punished multiple times … for the same crime. These charges can be stacked one on top of another, resulting in the threat of higher cumulative fines and jail time for the exact same violation.

This allows prosecutors to bully defendants into accepting a deal in order to avoid facing a multitude of charges from a single, solitary act. It also plays a significant role in sentencing. The ambiguity of a provision meant to toughen sentencing for repeat offenders of the CFAA may in fact make it possible for defendants to be sentenced based on what should be prior convictions — but were nothing more than multiple convictions for the same crime.

These problems are not hypothetical. But it took the unfortunate death of Aaron Swartz to spotlight them.

Aaron's Law

In January, Aaron Swartz, an Internet innovator and activist, decided to end his brief but brilliant life. At the time, Swartz faced the possibility of severe punishment under the CFAA — multiple felony charges and up to 35 years in prison by the government's own declaration – for what amounted to an act of civil disobedience. Aaron attempted to make documents, many created with public funding, freely available to the public.

Zoe Lofgren & Ron Wyden

Zoe Lofgren is a Democratic Representative from California and Ron Wyden is a Democratic Senator from Oregon.

READ MORE ▸

But Aaron Swartz was not the first or the last victim of overzealous prosecution under the CFAA.

That's why we're authoring bipartisan legislation — which, with the permission of Aaron Swartz's family, we call "Aaron's Law" — in the House and Senate to begin the process of updating the CFAA.

Aaron's Law is not just about Aaron Swartz, but rather about refocusing the law away from common computer and Internet activity and toward damaging hacks. It establishes a clear line that's needed for the law to distinguish the difference between common online activities and harmful attacks.

In drafting Aaron's Law — the text of which is available here, along with a detailed summary here – we did not opt for a quick fix of the CFAA that could bring with it unintended consequences.

Aaron's Law is not just about Aaron Swartz, but rather about refocusing the law away from common computer and Internet activity and toward damaging hacks.

Instead, we undertook a deliberative process for crafting this legislation. We posted drafts of the bill on Reddit to solicit public feedback. And that feedback informed revisions and solicitation of further feedback. We reviewed extensive input from a broad swath of technical experts, businesses, advocacy groups, current and former government officials, and the public. The result is a proposal that we believe, if enacted into law, safeguards commonplace online activity from overbroad prosecution and overly harsh penalties, while ensuring that real harmful activity is discouraged and fully prosecuted.

The law must separate its treatment of everyday Internet activity from criminals intent on causing serious damage to financial, social, civic, or security institutions. Our proposal attempts to accomplish this and address the fundamental problems of CFAA by doing the following:

Establish that mere breach of terms of service, employment agreements, or contracts are not automatic violations of the CFAA. By using legislative language based closely on recent important 9th and 4th Circuit Court opinions, Aaron's Law would instead define 'access without authorization' under the CFAA as gaining unauthorized access to information by circumventing technological or physical controls — such as password requirements, encryption, or locked office doors. Notwithstanding this change, hack attacks such as phishing, injection of malware or keystroke loggers, denial-of-service attacks, and viruses would continue to be fully prosecutable under strong CFAA provisions that Aaron's Law does not modify.

Bring balance back to the CFAA by eliminating a redundant provision of the law that can subject an individual to duplicate charges for the same CFAA violation. This is, in fact, what happened to Aaron Swartz — more than a third of the charges in the superseding indictment against him were under this redundant CFAA provision. Eliminating the redundant provision streamlines the law, reduces duplicative charges, but would not create a gap in protection against hackers.

Bring greater proportionality to CFAA penalties. Currently, the CFAA's penalties are tiered, and prosecutors have wide discretion to ratchet up the severity of the penalties in several circumstances — leaving little room for non-felony charges under CFAA (i.e., charges with penalties carrying less than a year in prison). For example, under current law a prosecutor can seek to inflate potential sentences by stacking new charges atop violations of state laws. Aaron's Law would reform the penalty for certain violations to ensure prosecutors cannot seek to inflate sentences by stacking multiple charges under CFAA, including state law equivalents of CFAA, and torts (non-criminal violations of law).

Will It Work?

Some say that while the CFAA may be a broad statute, prosecutorial discretion will ensure that it is not abused. We disagree. Whether it is with respect to privacy, civil liberties, or Internet use, the government has shown itself unable to restrain its use of power. So far, government discretion has repeatedly failed to curb abuse and, in fact, has resulted in abuse itself.

The government has shown itself unable to restrain its use of power. It has repeatedly failed to curb abuse and, in fact, has resulted in abuse itself.

Other critics may argue that Aaron's Law reforms remove one specific scenario from CFAA: an authorized individual using their own authorization (such as password credentials) to access and use information in unauthorized ways. Although we do not wish to create any new vulnerabilities, the overbroad approach currently taken by the CFAA potentially criminalizes millions of Americans for common Internet activity. Moreover, numerous laws like Theft of Trade Secrets, the Privacy Act, copyright law, the Stored Communications Act, wire fraud, and HIPAA already criminalize misuse of information.

The CFAA permits private parties to sue violators, but this private cause of action is not always present in other federal laws. We've heard some concern from companies that Aaron's Law would hinder their ability to take matters into their own hands to protect their proprietary information from insider theft. We look forward to robust discussions on this issue and to addressing any warranted concerns.

Laws Can Spur Innovation … Or Halt It

The introduction of this legislation is just the beginning of a process needed to bring balance back to the CFAA. Still, achieving even the specific, important reforms in Aaron's Law will not be an easy lift.

The public can speak loudly thanks to the Internet. And when it does, lawmakers will listen.

Congress rarely moves with haste. Correcting this complex law — enacted more than a quarter century ago — to work in the Digital Age will take a significant amount of time. To successfully build meaningful CFAA reforms into law will require sustained public engagement and support.

But the events of the last couple of years have demonstrated that the public can speak loudly thanks to the Internet. And when it does, lawmakers will listen.

The consequences of inaction are all too clear. We live in an age where people connect globally by simply touching a device in the palm of their hand, empowered by online advances that have enriched the world scientifically, culturally, and economically.

But ill-conceived computer crime laws can undermine this progress if they entrap more and more people — simply for creative uses of the technology that increasingly mediates our everyday activities and our interactions with the world. This not only fails us today, it can also become an obstacle to the innovations of tomorrow.

The Internet faces broad challenges to the fundamental characteristics that have enabled it to be the transformational technology that we know. An update to the CFAA must be part of the discussion that seeks to resolve these challenges. Today, there's an entire generation of digitally-native young people that have never known a world without an open Internet and their ability to use it as a platform to develop and share ideas. It's up to all of us to keep it that way.

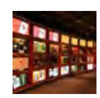
Tags: aaron swartz, hacktivism, open vs. closed, then & now
Post Comment | 82 Comments and 0 Reactions | Permalink

Share Tweet 882 +1 199

Disqus seems to be taking longer than usual. Reload?

PREVIOUS ARTICLE
Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)

NEXT ARTICLE
Everything You Need to Know About Trolls (The Patent Kind)



SITEMAP | FAQ | CONTACT US | WIRED STAFF | ADVERTISING | PRESS CENTER | SUBSCRIPTION SERVICES | NEWSLETTER | RSS FEEDS

Condé Nast Web Sites: **Webmonkey** | **Reddit** | **ArsTechnica** | **Details** | **Golf Digest** | **GQ** | **New Yorker**

Subscribe to a magazine: Condé Nast web sites: International Sites:

THE NEW YORKER

- « Making Money: Dog Runners!
- Main
- Protect and Serve »

March 18, 2013

Fixing the Worst Law in Technology

Posted by *Tim Wu*

- Print
- More

Share

Close

- Reddit
- Linked In
- Email

On the opening day of this year's South by Southwest festival, in Austin, an audience gathered in a giant conference hall to remember the life and tragic suicide of Aaron Swartz. Tim Berners-Lee, the inventor of the World Wide Web, spoke of Swartz's curious and restless mind. Swartz's girlfriend Taren Stinebrickner-Kauffman described him as a man who was constantly asking whether what he was doing was the most important thing that he could be doing. (A quality extensively documented by Larissa MacFarquhar in her Profile of Swartz.) The proceedings were yet another reminder that Swartz's suicide was heartbreaking beyond belief, and that something must be done about the law that he was aggressively prosecuted under, the Computer Fraud and Abuse Act.

As if to underline the point, last Thursday, federal prosecutors indicted that Matthew Keys, a social-media editor at Reuters, under the same law for helping with an online prank. Keys helped hackers vandalize a news story on the Web, messing with the contents of the article and changing a headline to read "PRESSURE BUILDS IN HOUSE TO ELECT CHIPPY 1337"—which was an inside joke. The damage was trivial, yet he is threatened with two hundred and fifty thousand dollars in damages and up to twenty-five years in prison.

These prosecutions have brought a rare moment of public attention to the breadth and severity of this law. Congress could change the law, but everyone knows that waiting for congressional action nowadays is a fool's game. The Obama Administration can, and should, set things right by changing its enforcement policy. And if the Justice Department declines to act, President Obama, as the ultimate enforcer of the law, should step in and set things right.

The Computer Fraud and Abuse Act is the most outrageous criminal law you've never heard of. It bans "unauthorized access" of computers, but no one really knows what those words mean. Orin Kerr, a former Justice Department attorney and a leading scholar on computer-crime law, argues persuasively that the law is so open-ended and broad as to be unconstitutionally vague. Over the years, the punishments for breaking the law have grown increasingly severe—it can now put people in prison for decades for actions that cause no real economic or physical harm. It is, in short, a nightmare for a country that calls itself free.

It wasn't always this way. The act was born, in 1984, as a narrow statute enacted for the reasonable goal of combating malicious hackers: people who break into computer systems and steal valuable data (like credit-card numbers) or do real economic damage. But it is in the nature of law to mutate and expand beyond the original justification. Over the years, Congress expanded the statute five times, adding private rights of action and making misdemeanors into felonies. Both private litigants and the Justice Department began to use the law against not only hackers but also otherwise legitimate users who violate the "terms of service" policies that come with nearly ever piece of software and service we use on computers today.

What are terms of service? Remember the last time you signed up for a Web site and clicked through several pages of fine print? Yep, that was it. Chances are, you didn't read it, and didn't think that it might be a federal felony to violate the provisions that it contained. The Justice Department has repeatedly taken the position that such violations are felonies. In the prominent cyberbullying case United States v. Drew, a federal prosecutor asserted that violating MySpace's terms of service would be a federal felony. Similarly, the indictment threatening Aaron Swartz with thirty-five years in prison depended, in part, on a terms-of-service violation: when Swartz tried to download thousands of academic articles, he did so as an authorized guest user of the M.I.T. network. He didn't actually "hack" or "break" into the network; he violated the terms of service for guests by downloading too much stuff.

The broadest provision, 18 U.S.C. §1030(a)(2)(c), makes it a crime to "exceed authorized access, and thereby obtain… information from any protected computer." To the Justice Department, "exceeding authorized access" includes violating terms of service, and "any protected computer" includes just about any Web site or computer. The resulting breadth of criminality is staggering. As Professor Kerr writes, it "potentially regulates every use of every computer in the United States and even many millions of computers abroad." You don't have to be a raving libertarian to think that might be a problem. Dating sites, to borrow an example from Judge Alex Kozinski, usually mandate that you tell the truth, making lying about your age and weight technically a crime. Or consider employer restrictions on computers that ban personal usage, like checking ESPN or online shopping. The Justice Department's interpretation makes the American desk-worker a felon.

When judges or academics say that it is wrong to interpret a law in such a way that everyone is a felon, the Justice Department has usually replied by saying, roughly, that federal prosecutors don't bother with minor cases—they only go after the really bad guys. That has always been a lame excuse—repulsive to anyone who takes seriously the idea of a "a government of laws, not men." After Aaron Swartz's suicide, the era of trusting prosecutors with unlimited power in this area should officially be over.

What can be done? Congresswoman Zoe Lofgren has drafted a bill that attempts to curtail the act's sprawling breadth. But even in the best of times, Congress rarely scales back criminal laws—and we have the do-nothingest Congress in history. The problem is compounded by industry resistance. At a recent White House meeting, Oracle and other companies made clear their suspicion of Lofgren's bill. Big data firms prefer the law just the way it is, and why wouldn't they? If you're a prosecutor or a firm with lots of data, the law is just about perfect. It's just too bad for the rest of us.

The Lofgren bill is a worthy effort, but betting on this Congress to pass a law that is opposed by industry and that diminishes prosecutorial authority is to bet on the political version of an inside straight. The memory of Swartz's suicide will fade, and we will be left with the sword of Damocles dangling. There needs to be a better way.

There is a much more immediate and effective remedy: the Justice Department should announce a change in its criminal-enforcement policy. It should no longer consider terms-of-service violations to be criminal. It can join more than a dozen federal judges and scholars, like Kerr, who adopt a reasonable and more limited interpretation. The Obama Administration's policy will have no effect on civil litigation, so firms like Oracle will retain their civil remedies. President Obama's DREAM Act enforcement policy, under which the Administration does not deport certain illegal immigrants despite Congress's inability to make the act a law, should be the model. Where Congress is unlikely to solve a problem, the Administration should take care of business itself.

All the Administration needs to do is to rely on the ancient common-law principle called the "rule of lenity." This states that ambiguous criminal laws should be construed in favor of a defendant. As the Supreme Court puts it, "When choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." So far, at least thirteen federal judges have rejected the Justice Department's interpretation of the Computer Fraud and Abuse Act. If that's not a sign that the law is unclear and should be interpreted with lenity, I don't know what is.

If neither the Justice Department nor the Attorney General will budge, it falls to the President, who bears ultimate public responsibly for law enforcement, to do what is right. The Computer Fraud and Abuse Act is egregiously overbroad in a way that has clearly imposed on the rights and liberties of Americans. With just one speech, the President can set things right.

Tim Wu is a professor at Columbia Law School and the author of "The Master Switch."

Photograph by Fred Benenson/Wikimedia Commons.

Keywords

- Aaron Swartz;
- Computer Fraud and Abuse Act;
- elements;
- technology;
- techpages

- Print
- More

Share

Close
  -
  - Reddit
  - Linked In
  - Email

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES of AMERICA v.	Criminal No. 10-114 (KSH)
KENNETH LOWSON, a/k/a ―Money", KRISTOFER KIRSCH, a/k/a ―Robert Woods", JOEL STEVENSON and FAISAL NAHDI **Defendants**	**<u>OPINION</u>**

<u>Katharine S. Hayden, U.S.D.J.</u>

I. Introduction

Defendants are charged with violations of the Computer Fraud and Abuse Act and the wire fraud statute arising from an alleged scheme to circumvent security measures put in place by Online Ticket Vendors (OTVs) in order to buy large blocks of tickets meant for the general public and then to re-sell those tickets at great profit on the secondary market. Defendants argue that their conduct is not criminal, and that in fact the government seeks to criminalize what otherwise would be a breach of contract action for violating the terms of service for ticket sales on OTVs' websites. The defendants state, ―This Indictment does not seek to punish computer fraud, it inappropriately tries to regulate the legal secondary market for event ticket sales through an overreaching prosecution." (Moving Br. 5.) The government counters that this case is anything but novel, and that ―[e]ach and every step of the way is [a] traditional fraud . . . the same thing that we see in court every day.” (Oral argument transcript 17:7−11.) The defendants, according to the government, ―lied about who they were. They lied about their business model. They lied when they impersonated thousands of individual ticket buyers. And they lied when they established thousands of false email addresses and domain names.” (Opp‘n Br. 1.)

The yawning gap between the government‘s and the defendants‘ positions is not lost on the Court, and it highlights and echoes tensions in other courts‘ viewpoints on where the line falls between what is civilly actionable conduct, and what is criminal.

Defendants now move to dismiss the Superseding Indictment (―the indictment”). For the reasons to be discussed, the Court denies the defendants‘ motion.

II. Legal Standard

An indictment, if valid on its face and returned by a legally constituted and unbiased grand jury, ―‗is enough to call for trial of the charge on the merits.’” *United States v. Vitillo*, 490 F.3d 314, 320 (3d Cir. 2007) (quoting *Costello v. United States*, 350 U.S. 359, 363 (1956)). ―An indictment is generally deemed sufficient if it[] (1) contains the elements of the offense intended to be charged, (2) sufficiently apprises the defendant of what he must be prepared to meet, and (3) allows the defendant to show with accuracy to what extent he may plead a former acquittal or conviction in the event of a subsequent prosecution.” *Id.* (quoting *United States v. Rankin*, 870 F.2d 109, 112 (3d Cir. 1989)) (internal quotation marks omitted).

Where an indictment is valid on its face, a motion to dismiss is appropriate only after the government has had an opportunity to present its proofs at trial. *United States v. Forero*, 623 F. Supp. 694, 699 (E.D.N.Y. 1985). In other words, a motion to dismiss an indictment is not a vehicle for a summary trial on the evidence, *United States v. Winer*, 323 F. Supp. 604, 605 (C.D. Pa. 1971), and any factual assertions related to a charge must be tested at trial. *United States v. Bender*, 2003 WL 282184 (S.D.N.Y. 2003). Moreover, on occasion a defendant's legal contentions may be so bound up with those facts that a court cannot grant a motion to dismiss. *United States v. Shabbir*, 64 F. Supp. 2d 479, 481 (D. Md. 1999).

III. The Wire Fraud Counts

Counts 27-36 and 37-43 of the indictment charge wire fraud by the use of CAPTCHA Challenges (counts 27-36) and e-mails (counts 37-43).

To charge the crime of wire fraud sufficiently, the government must allege three elements of the offense: (1) the defendants' "knowing and willful participation in a scheme or artifice to defraud, (2) with the specific intent to defraud, and (3) the use of the mails or interstate wire communications in furtherance of the scheme." *United States v. Al Hedaithy*, 392 F.3d 580, 590 (3d Cir. 2006); *see also* 18 U.S.C. § 1343 (2006). In addition, the object of the scheme must be a traditionally recognized property right. *Al Hedaithy*, 392 F.3d at 590.

First, the government sufficiently alleges an extensive scheme in which Wiseguys knowingly and willfully engaged to defraud Ticketmaster. The indictment alleges that Wiseguys circumvented computer code and surreptitiously obtained and resold event tickets that online ticket vendors would not otherwise sell to them. According to the indictment, defendants wrote automated software to defeat the vendors' security measures, including CAPTCHA, by opening thousands of connections and using CAPTCHA Bots to quickly solve CAPTCHA challenges. (Superseding Indict. Count 1, ¶¶ 7, 10.) The defendants allegedly acquired source code the vendors used to protect their websites, created a database of CAPTCHA challenges and their answers, and tested means of navigating to ticket "Buy Pages" without having to answer

CAPTCHA challenges at all. (Superseding Indict. Count 1, ¶¶ 9, 11, 12.) Wiseguys also allegedly used various means of deception, including mimicking the steps a human would take when answering CAPTCHA challenges (including making mistakes), using thousands of non-consecutive IP addresses to create the illusion that the addresses were not owned by a single company, using as many as 150 different credit cards to buy tickets, registering for fan clubs under fake names, creating a voicemail system with as many as 1,000 different telephone numbers, renting a mail drop in Las Vegas, renting real estate under an assumed name, and lying to lessors about the nature of their business. (Superseding Indict. Count 1, ¶¶ 14-16, 19, 20, 35-37.)

Second, the indictment sufficiently charges that Wiseguys had the specific intent to defraud the online ticket vendors. First, the alleged deceptive tactics in themselves suggest that the defendants knew what they were doing was wrong. Language in the indictment cites to the defendants' correspondence with each other and with third parties to demonstrate intent to defraud. According to the indictment, the defendants talked about pursuing ―non-human" means of buying tickets and finding backdoors at online ticket vendors' websites. (Superseding Indict. Count 1, ¶ 43.) They are charged with discussing the use of ―hacks" and breaking CAPTCHA challenges, ignoring Ticketmaster's cease and desist requests, and using tactics like the voicemail system to divert Ticketmaster's efforts to track them down. (Superseding Indict. Count 1, ¶¶ 44, 46.) The indictment also states that Wiseguys also told their employees to keep quiet about what the company did and discussed using ―stealth protocol" to go undetected. (Superseding Indict. Count 1, ¶ 47.) Moreover, the indictment alleges that Wiseguys stated that after undermining Ticketmaster's goodwill and position as an exclusive ticket distributor, it intended to become a vendor in the primary market for tickets and attract Ticketmaster's customers by providing better protection against scalpers. (Superseding Indict. Count 1, ¶¶ 41-42.)

Third, the indictment adequately charges that Wiseguys used interstate wire communications to further their scheme. To wit, counts 27-36 allege that Wiseguys's responses to CAPTCHA challenges and automated ticket purchases generated by CAPTCHA Bots for ten sets of Bruce Springsteen tickets constitute the use of interstate wire communications. (Superseding Indict. Counts 27-36, ¶ 2.) Counts 37-43 allege that seven emails between the defendants and various individuals regarding Wiseguys' business operations constitute the use of interstate wire communications. (Superseding Indict. Counts 37-43, ¶ 2.)

Finally, the indictment charges that the object of Wiseguys's scheme was to deprive the online ticket vendors of (1) their right to be the exclusive distributor of tickets, (2) their right to define the terms of sale for tickets by refusing to sell to people who use automated programs, and (3) the goodwill value of providing event tickets to the public. (Superseding Indict. Count 1, ¶ 2(c).)

This has led to one of the more hotly debated points in the defendants' motion. While the government describes the online ticket vendors' interests as valuable property rights and this case as a ―classic wire fraud case" (Oral argument transcript 28:6–7), the defendants label the government's theory as the tail wagging the dog of secondary-market regulation.

The case law mirrors the opposing positions taken by the parties. While the property right at issue in a wire fraud indictment need not be a tangible one, *United States v. Henry*, 29 F.3d 112, 115 (3d Cir. 1994), the defendants cite to several cases that they claim stand for the proposition that the particular intangible rights asserted by the government in this case are not property rights for purposes of the wire fraud statute. For instance, in *Henry*, the Third Circuit held that competing banks‘ right to a fair bidding opportunity to be the depository for toll bridge revenues was not a property right. *Id.* In *United States v. Bruchhausen*, the Ninth Circuit held that a manufacturer‘s interest in the post-sale destination of its products did not constitute a property right under the wire fraud statute, 977 F.2d 464, 467–68 (9th Cir. 1992), and in *United States v. Alkaabi*, the Third Circuit held that a testing service‘s interest in maintaining the integrity of its testing process did not constitute a property right. 223 F. Supp. 2d 583, 590 (D.N.J. 2002).

On the other hand, the government points out that a hallmark of a property right is exclusivity, *United States v. Carpenter*, 484 U.S. 19, 26 (1987), and the property right asserted here is tied to the online ticket vendors‘ interest in being the exclusive distributor of tickets for a given event. Further, in *United States v. Al Hedaithy*, the Third Circuit held that a testing service had a property right in controlling who could take its exam and receive a score report, 392 F.3d 580, 603 (2004), and in *United States v. Alsugair*, the court held that a testing service had a property right in its goodwill. 256 F. Supp. 2d 306, 316 (D.N.J. 2003).

At the motion to dismiss stage, it would be premature for this Court affirmatively to cast its lot with one theory over the other, especially given the broad range of factual situations reflected in the cases cited in the parties‘ briefs, which are more numerous than those discussed here. For one thing, a court‘s analysis of a motion to dismiss an indictment must not be converted into a summary trial on the evidence. *United States v. Delle Donna*, 552 F. Supp. 2d 475, 482 (D.N.J. 2008) (―[A]t this stage of the proceedings the indictment must be tested by its sufficiency to charge an offense‘ rather than by whether the ‗charges have been established by the evidence.‘‖ (quoting *United States v. Sampson*, 371 U.S. 75, 76, 78–79 (1962))); *United States v. Miller*, 694 F. Supp. 2d 1259, 1267 (M.D. Ala. 2010) (court could not decide, on motion to dismiss indictment, whether defendant was a “sex offender” within the meaning of a statute because such decision would require the court to look beyond the face of the indictment and rule on the merits). It suffices now to determine whether the government has charged a required element of wire fraud, and it has. Whether the government‘s theory is correct is properly decided after it has offered its proofs. The Court‘s direct response to the defendants‘ strenuous arguments about property rights is simply that, the legal determination of whether the online ticket vendors‘ interests alleged constitute property rights under the wire fraud statute is so bound up with the facts of the case that a decision at this stage is premature. *See United States v. Shabbir*, 64 F. Supp. 2d 479, 480 (D. Md. 1999); *United States v. Nanz*, 471 F. Supp. 968, 972 (D. Wis. 1979) (“Trial of the merits of [the] charges would not only be of assistance, but would be indispensable to the proper resolution of the motion.”). It is worth noting that most of the cases cited by both the government and the defense were decided on appeal from a conviction, and one was actually a civil case decided at the summary judgment stage. Here, the alleged facts have not been developed enough for the Court to determine how the online ticket vendors conduct their businesses so as to make a considered judgment about the nature of the property rights they allegedly possessed. On its face, however, the indictment sufficiently specifies property rights that Wiseguys allegedly targeted, such that it must survive the defendant‘s motion to dismiss.

IV. The CFAA Counts:

1. Counts 2 through 10: Obtaining Information from a Protected Computer, 18 U.S.C. §§ 1030 (a)(2)(C) and (c)(2)(B)(i)

Counts 2 through 10 of the indictment charge that defendants Lowson, Kirsch and Stevenson knowingly and intentionally accessed computers without authorization and exceeded authorized access, and using an interstate communication, obtained information from protected computers used in and affecting interstate and foreign commerce and communication, for the purpose of commercial gain. In so doing, the Indictment charges a crime under CFAA § 1030 (a)(2)(C), which prohibits intentionally accessing a computer without authorization or exceeding authorized access, and thereby obtaining information from any protected computer.

The crimes charged under the CFAA—including the two additional CFAA violations alleged in counts 11 to 26— center on the defendants' alleged unauthorized access of Ticketmaster's computer network. Throughout their briefs and at oral argument, both the government and the defendants have fiercely contested what constitutes "unauthorized access" for the purpose of a prosecution under the CFAA. The central and recurring question is whether the scheme and conduct alleged here is merely an egregious breach of contract based on violations of the terms of service on Ticketmaster's website, or something criminal. Defendants assert that the indictment "unambiguously depend[s] upon alleged breaches of contract to establish criminal liability." (Def. Reply Br. 5.) The government insists that defendants' conduct amounted to a crime.

The Court is satisfied that the indictment sufficiently alleges the elements of unauthorized access and exceeding authorized access under the CFAA, and sufficiently alleges conduct demonstrating defendants' knowledge and intent to gain unauthorized access.

The indictment alleges a number of actions taken by defendants to defeat code-based security restrictions on Ticketmaster's websites. (Although the government's briefs speak of unauthorized access of the websites of Online Ticket Vendors in general, the indictment‘s CFAA charges in counts 2 through 26 reference only the network belonging to Ticketmaster.) A non-exhaustive list of the steps defendants allegedly took to defeat Ticketmaster‘s code-based security measures includes: circumventing Proof of Work protections; writing automated software to defeat CAPTCHA (itself an extensive process which allegedly involved opening thousands of connections at once and using CAPTCHA Bots to respond to CAPTCHA challenges in fractions of a second); employing optical character recognition to defeat CAPTCHA challenges; testing the vulnerability of security encryption to get directly to “Buy Pages”; and implementing “hacks” and using “backdoors” to enable automated programs to purchase tickets. The defendants also allegedly disregarded cease-and-desist letters and hired programmers, including “contract hackers,” to defeat difficult security restrictions. (*See* Superseding Indict. Count 1 ¶¶ 35–40.)

The indictment also sufficiently pleads the other elements of obtaining information from a protected computer under § 1030. The protected computers referenced in the statute are described in the indictment as Ticketmaster‘s network, which is used in interstate commerce and communication. The elements of commercial advantage and private financial gain are pleaded as 10 separate purchases of tickets for resale to concerts and sports events in 2006 and 2007. (Superseding Indict. Counts 2 through 10 ¶ 2.) Finally, the indictment alleges that the “information” obtained by defendants from Ticketmaster‘s website was a seat-map “built” by CAPTCHA Bots “to seize a number of prize seats,” which Wiseguys employees then would “cull through” in order to select and purchase the best ones. (Superseding Indict. Count 1 ¶¶ 22–25.)

The Court notes and must take seriously the arguments advanced by the defendants, as well as those made by Amici, regarding whether the unauthorized access alleged here amounts to contract-based violations of Ticketmaster‘s terms of service that are actionable under civil laws. The Court is aware, for example, that the investigation of Wiseguys, and ultimately these defendants, began after a civil case was successfully prosecuted by Ticketmaster. *See Ticketmaster LLC v. RMG Technologies*, 507 F. Supp. 2d 1096 (C.D. Cal. 2007). Courts have differed over what constitutes unauthorized access under the CFAA and where the line falls between a civil and criminal violation of the statute. Defendants point to *United States v. Drew*, in which a district court dismissed the indictment against a defendant who had been found guilty of a misdemeanor violation of the CFAA for unauthorized access based solely on the defendant‘s ―conscious breach of a website‘s terms of service." *United States v. Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009). To hold otherwise, the *Drew* court stated, would be to transform § 1030 (a)(2)(C) into a law that violates the void for vagueness doctrine by affording ―too much discretion to the police and too little notice to citizens who wish to use the [Internet]." *Id.* at 467 (quoting *City of Chicago v. Morales*, 527 U.S. 41, 64 (1999)). Defendants here go further and argue that, under the government‘s theory, a teenager hypothetically could be prosecuted under the CFAA for violating the age requirement restrictions in the terms of service when using a search engine like Google.

But, as the government goes to pains to stress, and as the indictment makes clear, the unauthorized access charges at the heart of this indictment involve allegations of breaches of both contract- and code-based restrictions. In *Drew*, the conduct charged did not involve allegations of circumvention of code-based restrictions. And significantly, the *Drew* court‘s decision to dismiss the indictment came *after* trial, which allowed for the full presentation of all the government‘s proofs and a development of the factual record in what admittedly is a technology-intensive and unsettled area of the law. This Court is satisfied that a full presentation of the government‘s proofs is required to determine if the defendants‘ arguments ring true that the ―code-based restrictions . . . are red herrings . . . [and] are inextricably intertwined with the vendors‘ terms of use.” (Def. Reply 3.) For now, the indictment sufficiently alleges conduct supporting the government‘s theory of distinct code- and contract-based violations, and the government is entitled to the opportunity to fully offer its evidence, subject to cross-examination, as to why the conduct at issue here is criminal. In this case, the facts and the law are so closely related that further development of the record will shed light on crucial questions, such as what exactly the defendants did, how the alleged code-based restrictions worked, and whether the defeat of CAPTCHA challenges and circumvention of Ticketmaster‘s security measures is indeed distinct conduct from the terms of service violations described in *Drew*. It is only at that point that the Court can examine and rule on the defense theory that the CFAA and wire fraud counts are inextricably entwined, and so if the CFAA counts fall, so must the wire fraud counts.

Defendants also make a vagueness challenge. But as the Supreme Court has noted, ―vagueness challenges to statutes which do not involve First Amendment freedoms must be examined in light of the facts of the case at hand.” *Drew* at 464 (citing *United States v. Mazurie*, 419 U.S. 544, 550 (1975)). Here, the factual record before the Court remains undeveloped.

In addition, defendants argue that the indictment fails to identify the ―information” that defendants ―obtained” under counts 2 through 10. They contend that the only things they obtained were tickets, that the ―information” at issue was publicly available to ―every other member of the public that uses the online vendors‘ public websites” (Def. Br. 17), and that “[c]omprehensive seating information was available from numerous other sources.” (Def. Reply 10.) In effect, defendants argue, the government seeks to criminalize obtaining publicly available “information” and, in the process, the government will increase “exponentially” the universe of federal crimes. (Def. Moving Br. 18.) The government, however, argues that the information obtained included a detailed map of “available premium seats for each Event” that was unavailable to individual users and “confidential in the aggregate.” (Opp‘n Br. 30−32.) These clashing characterizations of what exactly defendants saw and whether it constituted “obtaining information” within the meaning of the CFAA highlights yet again the need for further factual development of the record. Applying the analysis that is proper at this stage, the Court finds that the indictment does allege sufficient facts to satisfy the element of obtaining information.

2. Accessing a protected computer with intent to defraud, 18 U.S.C. §§ 1030 (a)(4) and (c)(3)(A):

Counts 11 through 20 of the indictment allege that defendants Lowson, Kirsch and Stevenson knowingly, and with intent to defraud, accessed Ticketmaster‘s computer network and exceeded authorized access, and by doing so furthered the intended fraud and obtained things of value.

The “things of value” obtained, according to the indictment, were tickets to a July 28, 2008 Bruce Springsteen concert at Giants Stadium. (Superseding Indict. Counts 11 through 20 ¶ 2.) The key contested areas in counts 11 through 20 are the issues of unauthorized access (discussed above in counts 2 through 10), and the element of “intent to defraud.”

The "intent to defraud" is demonstrated in the indictment by the defendants' alleged scheme to, among other things, pose as individual buyers and deceive Ticketmaster into selling tickets to defendants that Ticketmaster otherwise would not sell. (*See e.g.* Superseding Indict. Count 1 ¶¶ 14–21.)

Defendants argue that the charged fraud and access violations are essentially one in the same (Def. Moving Br. 18), while the government contends that the unauthorized access and the fraud are alleged distinctly. According to the government, the unauthorized access consisted of circumventing code restrictions, defeating IP blocking and other conduct. The fraud, the government argues, consisted of the overall scheme to deprive Ticketmaster of its rights to exclusivity and to dictate terms of sale and also of its good will. (Opp'n 28–29.)

The Court finds that the indictment sufficiently pleads facts demonstrating intent to defraud and that the government is entitled to fully present its evidence on this question.

3. Transmitting a program that causes unauthorized damage, 18 U.S.C. § 1030 (a)(5)(A)

Counts 21 through 26 allege that defendants Lowson, Kirsch and Stevenson knowingly caused the transmission of programs, information, code, and commands, and as a result of such conduct, intentionally caused damage without authorization to protected computers, in and affecting interstate and foreign commerce and communication, thereby causing loss to one or more persons during a 1-year period aggregating at least $5,000 in value.

The indictment pleads a knowledge element demonstrated by allegations that, among other things, defendants discussed and implemented means to purchase tickets automatically without responding to CAPTCHA challenges; to defeat CAPTCHA using optical character recognition; and to update their CAPTCHA answer base when they encountered new CAPTCHA challenges. The pleaded ―transmission" involves defendants' responses to CAPTCHA challenges and automated ticket purchase requests for six different concerts and other events. (Superseding Indict. Counts 21 through 26 ¶ 2.) The pleaded damage element of at least $5,000 involves defendants' blocking out authorized, individual users from the website by using CAPTCHA Bots, which ―seized" the best seats for events and made those seats unavailable for purchase or consideration until their release by a Wiseguys employee. (*See* Superseding Indict. Count 1 ¶¶ 2, 25, 56.)

Defendants argue that the conduct at issue in the damage allegation essentially is identical to the conduct underlying the unauthorized access allegations, that the government again is seeking to ―criminalize a breach of contract," and that the indictment as a result contains no valid damage allegation. (Def. Reply 11.) While these arguments fit logically into the defendants' overall argument that this is a civil and not a criminal matter, the Court is satisfied that, for the purposes of deciding the motion to dismiss, the indictment sufficiently pleads the damage element of counts 21 through 26.

V. Conclusion

This case poses a good example of the complexity of criminal prosecutions under statutes written specifically about, for, and as a result of the Internet—and more, insofar as the parties are wrestling with the always perplexing issue of what constitutes criminal fraud. The challenge is to harmonize the CFAA and the government's charges of crime in the highly specialized marketplace the defendants operated in, with traditional and, indeed, sacrosanct tenets of the criminal law. The Court—and the parties as well—will be in a far better position to meet that challenge after the government presents its evidence. The motion to dismiss the Superseding Indictment is denied.

<u>/s/Katharine S. Hayden</u>

Katharine S. Hayden, U.S.D.J.

AFFIDAVIT OF SERVICE

DOCKET NO. 13-1816
---X
USA
vs.

Andrew Auernheimer
---X

I, Elissa Matias , swear under the pain and penalty of perjury, that according to law and being over the age of 18, upon my oath depose and say that:

on July 8, 2013

I served the **Addendum of Amicus Curiae National Association of Criminal Defense Lawyers in Support of Appellant** within in the above captioned matter upon:

See Attached Service List

via **electronic filing and electronic service**.

Unless otherwise noted, copies have been sent to the court on the same date as above for filing via Express Mail.

Sworn to before me on July 8, 2013

/s/ Robyn Cocho

Robyn Cocho
Notary Public State of New Jersey
No. 2193491
Commission Expires January 8, 2017

/s/ Elissa Matias

Elissa Matias

Job # 248362

Service List:

Mark E. Coyne, Esq.
email: mark.coyne@usdoj.gov.
Office of United States Attorney
970 Broad Street
Room 700
Newark, NJ 07102

Tor B. Ekeland, Esq.
email: tor@torekeland.com
Tor Ekeland
155 Water Street
6th Floor, Suite 2
Brooklyn, NY 11201

Hanni M. Fakhoury, Esq.
email: hanni@eff.org
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109

Marcia C. Hofmann, Esq.
email: Marcia@marciahofmann.com
25 Taylor Street
San Francisco, CA 94102

Mark H. Jaffe, Esq.
email: mark@torekeland.com
Tor Ekeland
155 Water Street
6th Floor, Suite 2
Brooklyn, NY 11201

Orin S. Kerr, Esq.
email: okerr@law.gwu.edu
George Washington University
2000 H. Street, NW
Washington, DC 20052