No. 13-1816

IN THE UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,*

v.

ANDREW AUERNHEIMER, *Defendant-Appellant.*

Appeals from the United States District Court for the District of New Jersey, Case No. 11-CR-470, Judge Susan D. Wigenton

---

BRIEF OF MEREDITH PATTERSON, BRENDAN O'CONNOR, SERGEY BRATUS, GABRIELLA COLEMAN, PEYTON ENGEL, MATTHEW GREEN, DAN HIRSCH, DAN KAMINSKY, SAMUEL LILES, SHANE MACDOUGALL, BRIAN MARTIN, C. THOMAS, AND PEITER ZATKO AS AMICI CURIAE SUPPORTING APPELLANT

ALEX MUENTZ
Adjunct Instructor
Department of Criminal Justice
Gladfelter Hall, 5th floor
Temple University
1115 Polett Walk
Philadelphia PA 19122
(215) 806-4383

Table of Contents

Table of Authorities

Cases

Statutes

Interest of Amici Curiae

The *amici*, Meredith Patterson, Brendan O'Connor, Professor Sergey Bratus, Professor Gabriella Coleman, Peyton Engel, Professor Matthew Green, Dan Hirsch, Dan Kaminsky, Professor Samuel Liles, Shane MacDougall, Brian Martin, C. "Space Rogue" Thomas, and Peiter "Mudge" Zatko, are professional security researchers, working in government, academia, and private industry; as a part of their profession, they find security problems affecting the personal information of millions of people and work with the affected parties to minimize harm and learn from the mistakes that created the problem. Members of the *amici* have testified before Congress, been qualified as experts in federal court, and instructed the military on computer security; they have been given awards for their service to the Department of Defense, assisted the Department of Homeland Security, and spoken at hundreds of conferences. Their résumés, representing more than two centuries of combined experience, are attached as an Appendix for the information of the Court. They are concerned that the rule established by the lower court, if not corrected, will prevent all legitimate security researchers from doing their jobs; namely, protecting the populace from harm. Accordingly, they wish to aid this Court in understanding the implications of this case in the larger context of modern technology and research techniques.

Non-Party Statement

This brief has been written without the authorship or contribution of any party to the case; the work has been done on a *pro bono* basis, without financial support for its creation coming from any individual.

Consent to File

Both parties to this litigation have consented to the filing of this brief.

Summary of Argument

The Computer Fraud and Abuse Act, 10 U.S.C. §1030, as construed by the United States in this case, allows a private corporation to make, and the government to enforce, a secret, after-the-fact declaration that access to information made public through standard technological processes was "unauthorized;" this determination, when used to trigger criminal liability, is a private law, which violates the United States Constitution. Though this determination was a non-governmental action, it may also constitute a violation of the Ex Post Facto Clause through its binding legal effect, as adopted by the United States. Allowing unknowable laws to be written on an ad-hoc basis by private corporations is not only unconstitutional, but also harms the public at large by preventing consumer-protecting functions in the digital world. The Court should overturn the judgment of conviction in this case.

Argument

1. Allowing a corporation to serve data publicly, then state after the fact that access was secretly restricted and thus impose criminal liability, amounts to a private criminal law, and may also violate the Ex Post Facto Clause.

Mr. Auernheimer's conviction on charges of violating the Computer Fraud and Abuse Act, 10 U.S.C. §1030, implies that his actions are in some material way different than those of any web user, and that beyond this, his actions violated a clearly-delineated line of authorization as required by §1030(a)(2)(C). Neither of these statements is true. The data Mr. Auernheimer helped to access was intentionally made available by AT&T to the entire Internet, and access occurred through standard protocols that are used by every Web user. Since any determination that the data was somehow nonpublic was made by a private corporation in secret, with no external signal or possibility of notice whatsoever, such a determination amounts to a private law of which no reasonable Internet user could have notice. On this basis alone, Mr. Auernheimer's conviction must be overturned. In addition, since AT&T's after-the-fact determination created a binding legal effect upon Mr. Auernheimer, it may violate the Ex Post Facto Clause of the United States Constitution, which would provide a separate legal basis upon which Mr. Auernheimer's conviction must be overturned.

1.1 *How a World Wide Web server works*

The HyperText Transfer Protocol, or HTTP, is the language that both web clients, such as web browsers, and web servers, which host all content on the World Wide Web, speak. Internet protocols are defined by a standards body called the Internet Engineering Task Force (IETF), through documents called Requests For Comments, or RFCs; HTTP, as it is used today, was defined in RFC 2616.[1] This document, promulgated by the Internet Engineering Task Force in 1999,[2] specifies the required behavior of web servers and web clients of all types on the Internet. Much as speaking a common human language allows two individuals to communicate by speech, HTTP allows two computers, whether they be desktops, laptops, servers, tablets, phones, or other devices, to be part of the World Wide Web—and it applies whether a human is using a web browser, or two computers with no user input devices are exchanging web data.

HTTP is so popular—it is used by more than a billion people, and several billion devices, each day—because it is so simple. Web servers host all content on the web, whether that content is designated to be public or private. To use a standard analogy, a web server may be thought of as a librarian; rather than a user looking in the library stacks themselves,

[1]Network Working Group, *RFC 2616 - Hypertext Transfer Protocol – HTTP/1.1*, Internet Engineering Task Force (June 1999), `http://tools.ietf.org/html/rfc2616`.

[2]Previous versions of HTTP have been standardized before 1999 by the IETF, but RFC 2616 is the most recent version of HTTP.

they ask the librarian. If the document in question is public, the librarian gives it to the user without hesitation; if the document is private, the librarian asks the user for some proof of identity, such as a username and password. If the provided username and password are on the librarian's roster for that document, the document is given to the user; if not, the librarian refuses to give the document to the user.

For a public document, a human might interact with the librarian as in Figure 1. Note the brief conversation: the human requests the document, and the librarian provides it immediately and without any check for credentials. The HTTP conversation, just as it is sent over the wire, is in Figure 2; the "200 OK" is the standard HTTP response that indicates that the document is being sent, as specified in the protocol document discussed above. In Figure 2, the client first sends a GET request for a specified page. If the server has been told by its owner that the page requested is available to the public, it will respond by sending 200 OK, indicating a successful request, along with the content (a page, photo, document, or file).

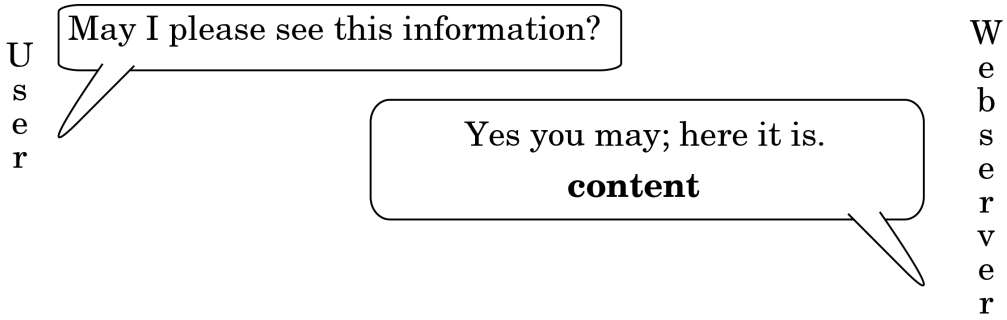

Figure 1: An HTTP request without authentication, as portrayed by humans.

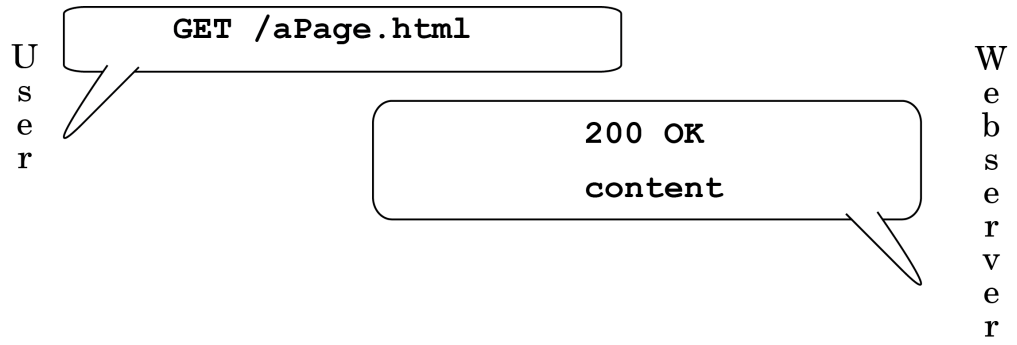

Figure 2: An HTTP request without authentication.

If the owner of a server wishes to restrict access to a particular document or set of documents, the owner can instruct the web server to do so. The librarian will ask the human for a proof of identity, and provide the document only if the identity is on the list, as in Figure 3. The server's HTTP request for identification is the code "401 Not Authorized;" this code tells the client device that some proof of identity is required. When the client receives the request, it will send an Authorization command, complete with username and password. (It may send the username and password in one of several encodings, but the command is otherwise the same.) The HTTP version of this request is shown in Figure 4. If the server recognizes the username and password, it will send 200 OK, along with the requested document—just as it did in Figure 2.

If our librarian does not accept the provided identification, he will refuse to provide the document, as shown in Figure 5. If the server does not recognize the username and password, it will send code: "403 Forbidden." This indicates that the username and password is not known to the server, or is not authorized to access the particular document. This flow is shown

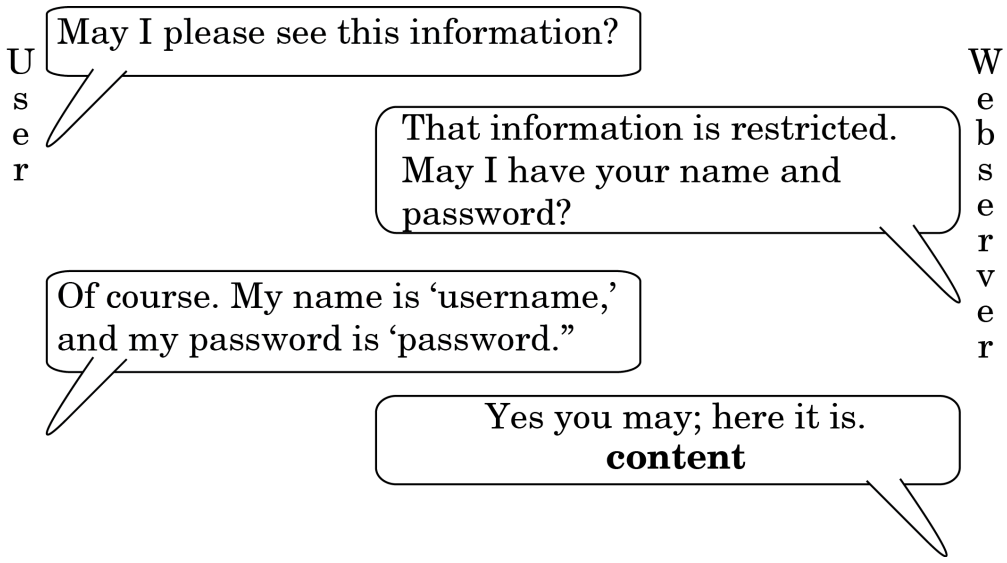

Figure 3: An HTTP request with successful authentication, as portrayed by humans.

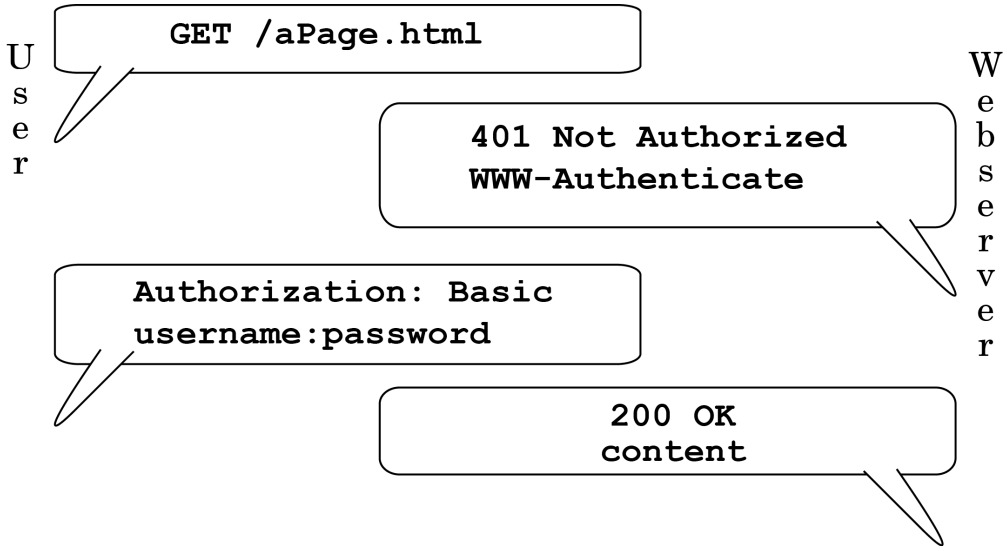

Figure 4: An HTTP request with successful authentication.

in Figure 6; note that no content is sent by the server in that case.

AT&T instructed its servers that the email addresses it had were unrestricted content, available to anyone; in essence, they were the content for a particular set of documents. The documents were named for their asso-

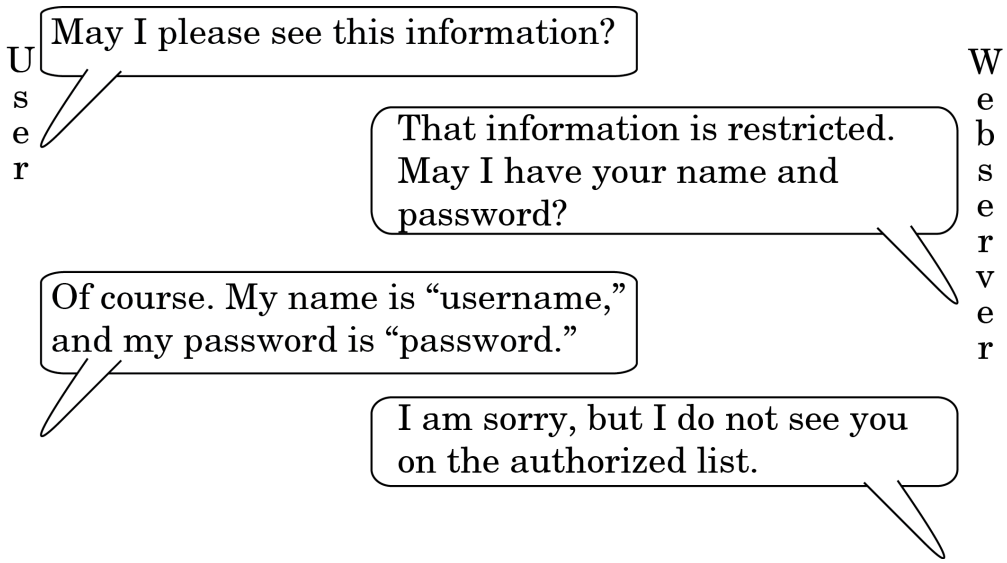

Figure 5: An HTTP request with unsuccessful authentication, as portrayed by humans.

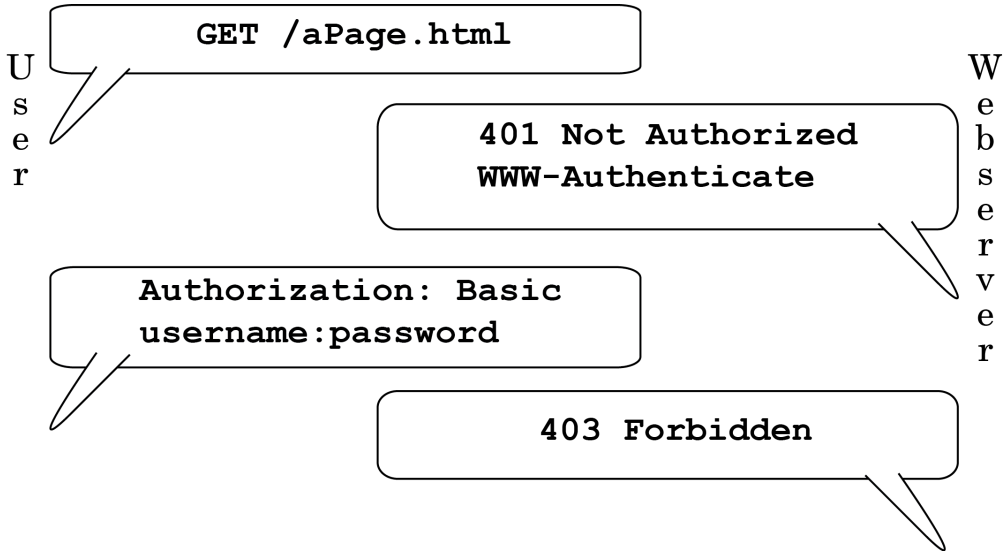

Figure 6: An HTTP request with unsuccessful authentication.

ciated numeric identifiers, called ICC-IDs.[3] If our librarian is asked for

[3]A Subscriber Identity Module, or "SIM Card," is a small replaceable chip inside mobile phones or other mobile devices that use the Global System for Mobile Communications (GSM) protocol; in the United States, AT&T and T-Mobile use GSM. An Integrated Circuit Card Identifier, or ICC-ID, is a number up to twenty digits in length that identifies a SIM card. It is important to note that an ICC-ID is not an authenticating num-

several documents in a row, each by its identifier, there is no issue; it responds to each in turn. If it cannot find a document that corresponds to an identifier, it simply responds that while it has verified that the document number is valid, it has no information to give on that document.[4] This is shown in Figure 7. Mr. Spitler simply requested many documents; for each, AT&T's server returned a "200 OK," with either the email address of a subscriber or a notice that it was not known, as shown in Figure 8.

It is crucial to realize that AT&T gave the webserver its instructions: they *explicitly* told it to respond with consumers' private information to anyone who gave the server a valid number, easily picked at random. With this action, AT&T deliberately made the information public to anyone who asked, set no limits whatsoever on who could ask or how often, and required no verification before handing out ostensibly private information to all comers. AT&T used technical means to signal to any user of the Internet that this data was public, not private, and treated the data accordingly.

While the repeated requests outlined in Figure 8 might look odd to a lay person, they in fact represent the standard operation of the Web. A

ber; it could be compared to a football player's jersey number, in that it was not designed to be used for anything more than the most transient identification.

[4]This is because AT&T's server would respond the same way to each request, regardless of whether it knew a particular ICC-ID; if it did not know an ID, it would simply fail to provide an email address in that otherwise-blank space. A server could also be configured to give the response "404 Not Found," if it encountered an ID of which it had not heard.

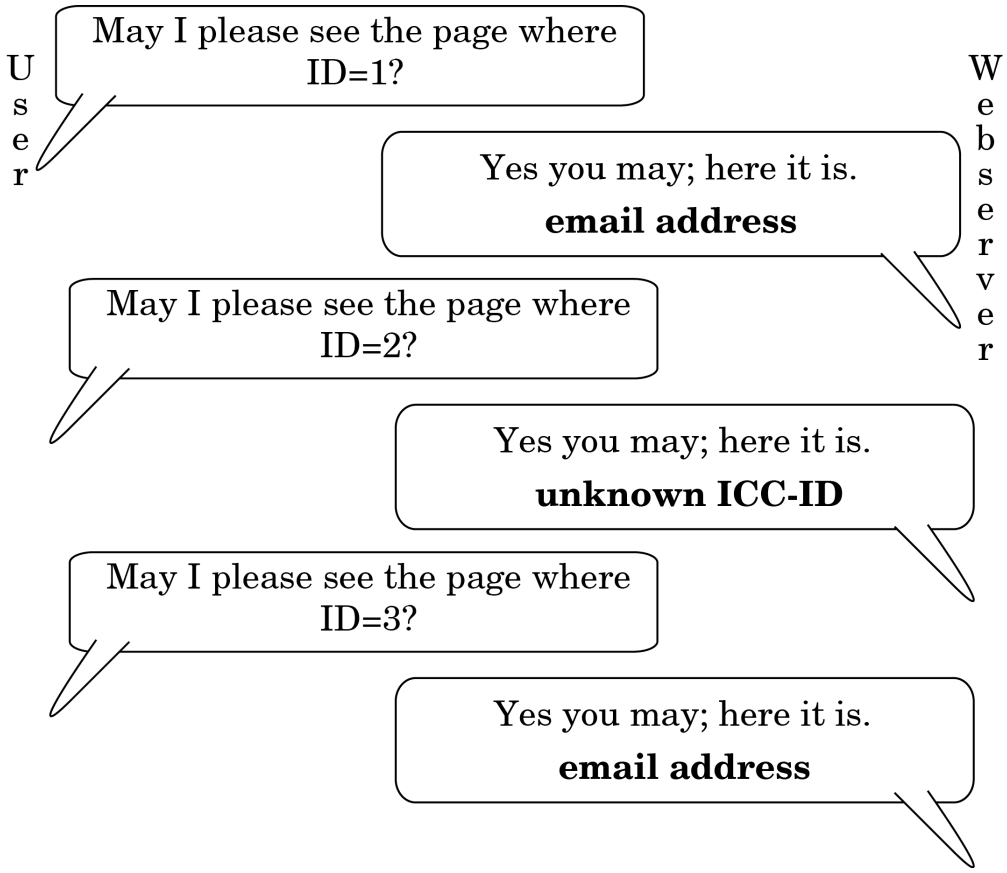

Figure 7: Mr. Spitler's requests to the AT&T server, as portrayed by humans.

user makes these same requests whenever they use a website, whether they are clicking through cat videos, using a search engine, or reading a blog. Indeed, if a person wished to read every post on a blog in order, they might first ask for `http://www.example.com/blog/1`, signifying the first post; having read that, they would ask for `http://www.example.com/blog/2`, the second post; `http://www.example.com/blog/3`, the third post; and so on. (This might be done through clicking on links, or it might be done by manually changing the address displayed to the user.) There is nothing untoward about this behavior; it is the default behavior for most of the

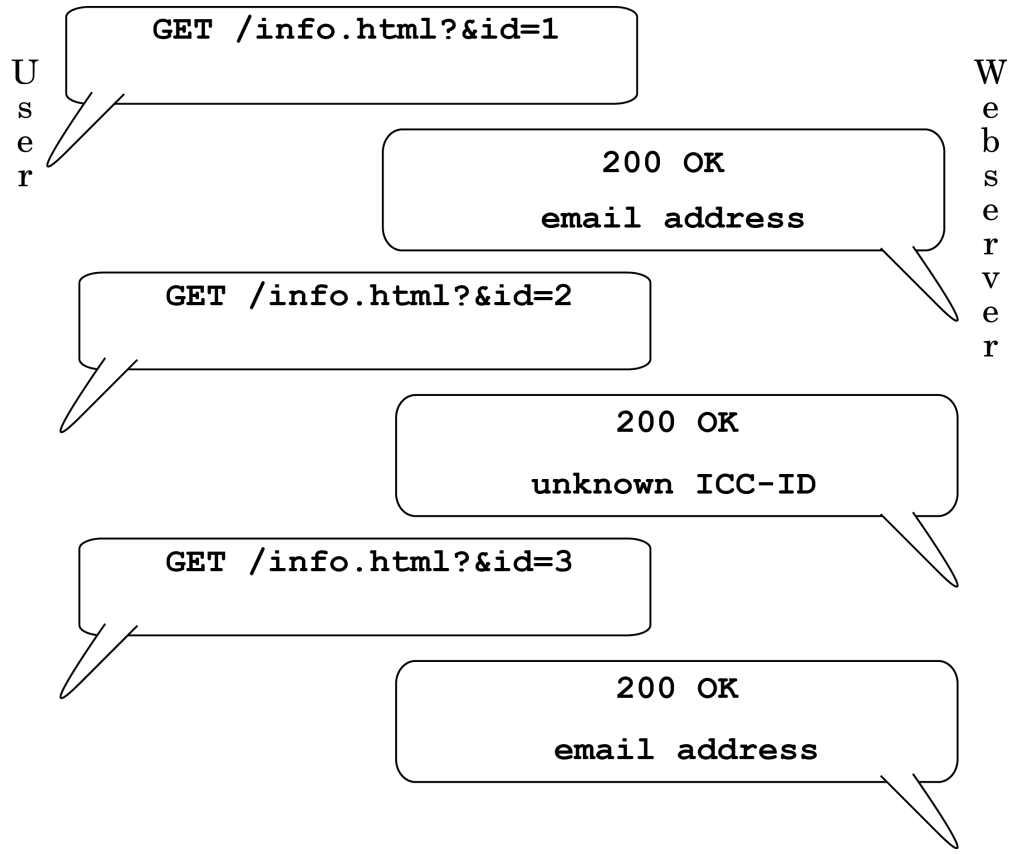

Figure 8: Mr. Spitler's requests to the AT&T server.

Web, and these requests are set out and sent in the same way, regardless of what device sends them, or whether a user is present.

1.2 *AT&T's secret determination of "authorized access" creates an unconstitutional private law*

It is a fundamental violation of the basic concept of due process for an act to be secretly criminal; AT&T's determination that access to documents it had made public was unauthorized, without making such a determination public in any way, amounts to the creation of a private law.

> "The rule that 'ignorance of the law will not excuse' is deep in our law, as is the principle that of all the powers of local government,

> the police power is 'one of the least limitable.' On the other hand, due process places some limits on its exercise. Engrained in our concept of due process is the requirement of notice." *Lambert v. People of the State of California*, 355 U.S. 225, 228, 78 S.Ct. 240 (1957) (citations omitted).

In *Lambert*, the Supreme Court set out a theory of actual notice of a law. In the case at hand, however, Mr. Auernheimer had not even the *possibility* of notice of the law in question; in effect, AT&T's determination was secret, making it impossible for any legal scholar—let alone, any reasonable user of the Internet—to have knowledge of the legality of the action beforehand. AT&T did not use any means at its disposal, whether through the display of a warning, or through utilizing the fundamental protocol of the World Wide Web's authorization mechanism, as described in Section 1.1, to give notice that access of the type Mr. Auernheimer aided was unauthorized. In fact, AT&T declared, at the time that the documents were accessed, that the access was authorized; instead of using the "403 Forbidden" code to signify a lack of authorization, as shown in Figure 6, it instead used the "200 OK" code that signifies that no further authorization is needed, as shown in Figure 2. This means that Mr. Auernheimer cannot be held legally responsible for exceeding his "authorized access," since he had no way of finding out what access was "unauthorized," and was indeed told by AT&T's computers that his access was authorized.

Moreover, to affirm the district court would provide for the enforcement of such private laws, and the handling of litigation about them, at public expense. The criminal justice system is ill-suited to serve as a tool

for corporate policy interests. If a business fails to take care to avoid unwanted consequences associated with its publication of information, it cannot later be allowed to convert those consequences into felonies for the criminal justice system to handle; to permit that path would allow businesses to shirk their duty to safeguard private information, and simply pass the workload onto an on already overburdened court system.

The Ninth Circuit has already rejected a system of private laws, even *with* notice, being used to turn a user's access to data into a felonious act under the CFAA. In *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012), the Ninth Circuit ruled that it would not allow "every violation of a private computer use policy [to be] a federal crime." *Id.* at 859.

> "[T]he government's proposed interpretation of the CFAA allows private parties to manipulate their computer-use and personnel policies so as to turn these relationships into ones policed by the criminal law." *Id.* at 860.

We invite this Court to adopt the Ninth Circuit's determination that this sort of private legal scheme is unacceptable in a society of laws.

1.3 *AT&T's post-hoc determination of "authorized access" violates the Ex Post Facto Clause*

The Computer Fraud and Abuse Act criminalizes the act of exceeding authorized access to a computer, and defines authorization solely as what the user is "entitled" to access. 18 U.S.C. §1030(e)(6). As explained in Section 1.1, AT&T used technical means to make public the private in-

formation of its customers, as a response to anyone who asked for it; a reasonable user of the World Wide Web would assume that data explicitly made public would be public. However, after the data was accessed, AT&T decided that this information that it had made public should, in retrospect, have been private, and thus no user should have access to it (despite the fact that it was being handed out by their server, at their behest). This determination, insofar as it is adopted by the United States, and used as the threshold for criminal liability, makes an action criminal that was non-criminal when it was taken; as such, it amounts to a violation of the Ex Post Facto Clause of the United States Constitution.

Ex post facto laws are prohibited by Article 1, Section 9 of the United States Constitution; this means that something cannot be made illegal, and a person thereby be held liable, for an action taken before the illegality had been designated. Ex post facto laws have been broadly defined:

> "1st. Every law that makes an action done before the passing of the law, and which was innocent when done, criminal; and punishes such action. 2d. Every law that aggravates a crime, or makes it greater than it was, when committed. 3d. Every law that changes the punishment, and inflicts a greater punishment, than the law annexed to the crime, when committed. 4th. Every law that alters the legal rules of evidence, and receives less, or different, testimony, than the law required at the time of the commission of the offence, in order to convict the offender." *Calder v. Bull*, 3 Dall. 386, 390, 1 L.Ed. 648 (1798) (emphasis deleted).

Particularly relevant here, an ex post facto law need not be a complete legislative action for it to violate the Ex Post Facto Clause (i.e., it need not

be an actual law). Instead, it need only have "binding legal effect," as the Supreme Court restated in *Peugh v. U.S.*, 569 U.S. ___, at *12, 133 S.Ct. 2072 (2013).

In *Peugh*, the Supreme Court held that even non-binding sentencing guidelines—guidelines that did not carry the force of law, and were not created through direct Congressional action—could violate the Ex Post Facto Clause. Here, the imposition of liability is actually more concerning than the stricken sentence in *Peugh*: AT&T, a non-governmental, non-neutral corporation, created the rule Mr. Auernheimer is charged with violating, after the time at which it is claimed that he violated it. While *Peugh* dealt with sentencing guidelines, the *amici* believe that the rule put forward need not be restricted to strictly governmental action; this non-governmental action created the requisite "binding legal effect," and, crucially, the determination was subsequently adopted by the government when it chose to indict Mr. Auernheimer. In this case, AT&T made an after-the-fact determination that an action, already taken, had violated some previously-unarticulated rule; this determination meant that an action that in other respects was simply a request to view a web page, as explained in Section 1.1, was now criminal. This determination, and its subsequent adoption by the United States, has had the requisite "binding legal effect" upon Mr. Auernheimer in the form of the case at bar.

In *Peugh*, the Supreme Court held that even intervening discretionary acts could not save a sentencing guideline: "[O]ur cases make clear that

'[t]he presence of discretion does not displace the protections of the Ex Post Facto Clause.'" *Peugh*, 569 U.S. at *12 (citation omitted). In this case, AT&T issued much more than a mere guideline—it, through the government's adoption of its determination, issued the new rule of law itself, after the act had been committed. *Peugh* holds that no discretion between then and now, such as the issuance of an indictment, prevents the situation from violating the Ex Post Facto Clause. As such, Mr. Auernheimer may not be held criminally liable for violating a law not fully actualized until after his act.

2. Criminalizing access to publicly-offered material is not in the public interest, because it prevents the security research community from exercising its consumer-protecting role.

Mr. Auernheimer is one example of a security researcher, a profession of which the amici are also a part. There are many thousands of security researchers worldwide[5] who work in government, academia, and for private industry. They have a shared goal: to protect people from dangerous computer systems, whether they be websites that leak personal information, implantable cardioverter-defibrillators that are susceptible to remote disabling, or dams that can be controlled—or even destroyed—

[5]One security research conference, the annual DEF CON conference in Las Vegas, NV, had more than 13,000 attendees in 2012.

from anywhere in the world.[6] The security research community is a part of the larger consumer safety community: as with more traditional product safety researchers, security researchers form an important part of the system of consumer protection.

The role that consumer safety and advocacy organizations and researchers play in ensuring the safety of the population has been recognized throughout the legal system. *See, e.g.,* The Consumer Product Safety Act, 15 U.S.C. §2051, *et seq*. (2006) (providing protection for those who "blow the whistle" on violations of consumer safety), *National Ass'n Of State Utility Consumer Advocates v. F.C.C.*, 457 F.3d 1238 (11th Cir. 2006) (cellular telephone service billing irregularities), *International Healthcare Management v. Hawaii Coalition For Health*, 332 F.3d 600 (9th Cir. 2003) (medical care pricing), *Kaiser Aluminum & Chemical Corp. v. U. S. Consumer Product Safety Commission*, 574 F.2d 178 (3d Cir. 1978) (aluminum house wiring), *Grimshaw v. Ford Motor Co.*, 191 CA3d 757, 236 Cal. Rptr. 509 (Cal. Ct. App. 1981) (the Ford Pinto case), *In re Harvard Pilgrim Health Care, Inc.*, 434 Mass. 51, 746 N.E.2d 513 (Mass. 2001) (medical care organizations), *Porter v. South Carolina Public Service Com'n*, 333 S.C. 12, 507 S.E.2d 328 (S.C. 1998) (BellSouth statewide rate-setting corruption), *Utah State Coalition of Sr. Citizens v. Utah Power and Light Co.*, 776 P.2d 632 (Utah 1989) (protecting the elderly from a state power monopoly). These organizations do not ask for, nor do they require, the

[6]Talks on each of these were presented at DEF CON in 2012, among many other presentations.

permission of the companies whose publicly-accessible products they test for problems that endanger the safety of society at large, and every member of society specifically. If there were such a requirement, the permission would in reality never be given; as in the case at hand, the existence of the problem in the first place, combined with either a lack of awareness on the part of the responsible company, or the company's unwillingness to fix the problem, would be embarassing to the company.

There are relatively few sources of pressure to fix design defects, whether they be in wiring, websites, or cars. The government is not set up to test every possible product or website for defects before its release, nor should it be; in addition, those defects in electronic systems that might be uncovered by the government (for instance, during an unrelated investigation) are often not released, due to internal policies. Findings by industry groups are often kept quiet, under the assumption that such defects will never come to light—just as in *Grimshaw* (the Ford Pinto case). The part of society that consistently serves the public interest by finding and publicizing defects that will harm consumers is the external consumer safety research community, whether those defects be in consumer products or consumer websites. In the situation at hand, AT&T was improperly safeguarding the personal information of hundreds of thousands of consumers. When Mr. Auernheimer discovered this fact, he publicized it, in precisely the same way that Consumers Union, publisher of *Consumer Reports*, does with each consumer-safety violation that it uncovers:

he made it available to the press.

The United States would like this Court to create a rule that would allow private corporations to control the right of researchers to examine public accommodations, as long as those accommodations were on the Internet. If that rule were applied to the physical world, it would be unlawful for a worker to report a building code violation on a construction site. It would be unlawful for an environmental activist to sample water for contaminants, lest they come across things a company (which had illegally dumped waste in a river) deemed secret. It would be unlawful for a customer at a restaurant to report a rat running across his or her table to the city health authority. It would be unlawful for a newspaper to investigate whether a business is illegally discriminating against racial minorities. It would even be illegal for Ralph Nader to have published (or have done the research for) "Unsafe at Any Speed;" his analysis of design flaws inherent to certain automobiles, found while examining the design of those automobiles without permission from their manufacturers, would be illegal under a system that required that a company give its consent to any research of which it might not approve.

In fact, every car sold today contains a great deal of computers that control every facet of the car's operation—from entertainment systems, to how the engine runs, and even braking. The CFAA interpretation proposed by the government could be used to criminalize Mr. Nader's research; if such research were done today, analysis of the car would nec-

essarily involve its computers. General Motors should not have been allowed, after the fact, to decide that it had not meant to allow Mr. Nader access to the Chevrolet Corvair when Mr. Nader, rather than simply driving the car (with its inherent risks) as they had intended, instead used the car to discover its design risks and flaws and to make that information available to the public. In short, private corporations would, under the rule proposed by the United States, be able to silence critics with the threat of imprisonment for publishing unfavorable research.

In addition, the government, private corporations, and indeed the whole world have benefited from the research being done by independent security researchers. One flaw, discovered by one of the *amici*, Dan Kaminsky, affected the core naming infrastructure of the Internet; his publication of the vulnerability to the affected entities—private corporations, governments, and open source projects—resulted in the aversion of a catastrophe; in essence, the flaw would have meant the complete destruction of the Internet. Members of the *amici* have reported vulnerabilities in software created by Microsoft, VeriSign, McAfee, and many others of the world's largest corporations, whose software is used by millions of people every day. These researchers have prevented untold financial and privacy losses to entities large and small; it is therefore crucial that their continued right to research be protected.

There is no reason why the electronic world and the physical world should differ so mightily: as an increasing amount of an average per-

son's day-to-day life moves online (from paying bills to registering cars, and from shopping, to trading stocks, to musical performance and art appreciation), any conceivable rationale for this difference becomes facially unconvincing. The increased prominence of the digital world means that more scrutiny, not less, should apply to those who offer up public accommodations on the Internet (or in any digital forum). If, as Justice Brandeis once said, sunlight is to be a disinfectant, then it is imperative that if a public corporation chooses to endanger the safety of consumer information, we allow security researchers to publish their results and warn the public at large.

Conclusion

The United States asks this Court to endorse the use of the criminal justice system to cover up a private corporation's failures. AT&T published private consumer data in an inappropriate fashion. Rather than take responsibility for their act, they have asked the criminal justice system to punish the researcher who uncovered their mistake. If this tactic is allowed to flourish, it will allow corporations to choose to terminate any safety oversight of their actions, and instead rely on the criminal process to serve as a cover-up for bad acts. Corporations will have no incentive to treat consumer data with adequate care in the future, since no one but the corporations themselves will be aware of any possible danger. In essence, the precedent that the respondent seeks to create is one that will make

the American taxpayer subsidize the irresponsibility and misfeasance of private corporations through the courts on a scale never before seen.

With this case, this Court has an opportunity to state that it is not acceptable for private corporations to warp the criminal justice system to shield themselves from public scrutiny in their digital public accommodations, any more than it is acceptable in any physical accommodation. Mr. Auernheimer's "crime" was to discover that a public corporation was giving anyone access to private consumer information; he discovered this by, in essence, repeatedly adding 1 to a number. The Court should not condone the metaphorical shooting of a messenger who acted for the safety and security of all. We ask that this Court overturn Mr. Auernheimer's conviction.

Respectfully submitted,

/s/ Alexander Muentz

Alexander Charles Muentz
Attorney for Amici

Certificate of Bar Membership

I, Alexander Charles Muentz, certify that I am a member in good standing of the Bar of the State of Pennsylvania, with Attorney ID 204459. I certify further that I am admitted to practice in the United States Court of Appeals for the Third Circuit.

Certificate of Compliance With Word Count Requirements

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) and Fed. R. App. P. 29(d) because this brief contains 4,983 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using TeX 3.1415926 in 14-Point New Century Schoolbook.

Certificate of Service

This brief was submitted through the CM/ECF system of the Third Circuit Court of Appeals; notice of its filing has been made through that system's Notice of Docket Activity.

Certificate of Identical Compliance of Briefs

The text of this brief is identical as submitted both in electronic format and in hard copy.

Certificate of Virus Check

This brief has been checked for malicious software by Wepawet, in the version made available on June 15, 2013.

No. 13-1816

IN THE UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,*

v.

ANDREW AUERNHEIMER, *Defendant-Appellant.*

Appeals from the United States District Court for the District of New Jersey, Case No. 11-CR-470, Judge Susan D. Wigenton

---

APPENDIX OF MEREDITH PATTERSON, BRENDAN O'CONNOR, SERGEY BRATUS, GABRIELLA COLEMAN, PEYTON ENGEL, MATTHEW GREEN, DAN HIRSCH, DAN KAMINSKY, SAMUEL LILES, SHANE MACDOUGALL, BRIAN MARTIN, C. THOMAS, AND PEITER ZATKO AS AMICI CURIAE SUPPORTING APPELLANT

ALEX MUENTZ
Adjunct Instructor
Department of Criminal Justice
Gladfelter Hall, 5th floor
Temple University
1115 Polett Walk
Philadelphia PA 19122
(215) 806-4383

Meredith L. Patterson

Skills

Languages

- C/C++
- Python
- Java
- Javascript
- Haskell
- Lua
- PHP
- Objective-C
- Scala
- Lisp
- lex/yacc
- Prolog
- SQL
- XSLT/XPath

Specialized Skills

- Language-theoretic security
- Compiler design
- Formal language analysis and design
- Database deployment, tuning and migration
- Technology education
- Machine learning
- Database backend internals
- Data analysis, modeling and mining
- Bioinformatics (genomics/ proteomics)
- Test-driven/Agile development

Work Experience

October 2012–Present **Principal NLP Engineer**, *Nuance Communications*, Ghent, Belgium.
Productization, build and release engineering, development, troubleshooting, and security analysis for a hybrid (statistical and rule-based) natural language semantics product in the medical domain, in collaboration with a team of researchers from Nuance and the IBM Thomas J. Watson Research Center.

August 2012–Present **Managing Partner**, *Upstanding Hackers, LLC*, Brussels, Belgium.
Co-founder. Principal architect for open-source security offerings, including Hammer, a DARPA-funded parser generator library (https://github.com/UpstandingHackers/hammer).

January 2011–August 2012 **Senior Research Scientist**, *Red Lambda*, Orlando, FL.
Worked as part of a team of eight developers to build a scale-free distributed computing platform. Wrote analysis tools for Netflow v5 and v9. Developed tools (based on Scala's parser combinators) and GUI to enable non-expert users to quickly build bespoke parsers for custom log formats, including recursive and non-greedy matching. Wrote a binary parser combinator library in Scala to parse pcaps and other binary protocol data. Audited other developers' code in Java and C++. Prototyped novel machine learning techniques and locality-sensitive hashes.

January 2009–January 2011 **Independent Researcher**, Leuven, Belgium.
Collaborated with academic and industry security researchers on cross-implementation X.509 vulnerabilities and generalized language-theoretic attack and defense techniques. See publications list for further details.

Rue Notre Dame du Sommeil 24 – 1000 Brussels
✉ *mlp@thesmartpolitenerd.com* • *http://github.com/abiggerhammer*

May–December 2008 **Programmer/Analyst**, *UC Berkeley Phylogenomics Group*, Berkeley, CA.
Ported a PHP web application for proteomics analysis to Python/Django. Redesigned schema for and migrated a 10GB proteomics database from MySQL to PostgreSQL. Performed technology evaluation and made recommendations. Audited web application security. Led disaster recovery efforts.

May 2006–May 2008 **Chief Technical Officer**, *Osogato*, San Francisco, CA.
Led a team of engineers and system administrators, distributed across the US and Europe, in the development of a client application for algorithmic analysis and recommendation of music. Architected, specified, and prototyped the application in C++ and Objective-C. Prototyped and developed a web-based version of the application in Python and Javascript. Raised $250,000 in angel funding.

January 2006–April 2006 **Software Engineer**, *Mu Security*, Sunnyvale, CA.
Developed and extended core internals of a smart fuzzing appliance, using C++ and XML. Wrote tools to automatically generate RPC service fuzzers from RPC interfaces, using bison and XSLT. Developed and maintained Python scripts for text and packet parsing, code generation, and documentation generation. Handled assistant database administrator duties.

June 2005–September 2005 **Summer of Code Participant**, *Google*.
Implemented a fast, templatized C++ machine-learning library for various classes of support vector machines (regression, binary classification, and ranking), extensible to other machine learning methods. Extended the PostgreSQL parser and backend to learn a discriminant function from sets of tuples already present in a table, then return results based on applying the discriminant function to the rest of the table.

August 2003–December 2005 **Bioinformatics Intern**, *Integrated DNA Technologies*, Iowa City, IA.
Developed standalone and web-based tools for DNA and RNA sequence design and site-directed mutagenesis. Audited and refactored co-workers' code. Deployed a local installation of the EnsEMBL genomic database.

August 2001–December 2005 **Teaching and Research Assistant**, *University of Iowa*, Iowa City, IA.
Designed and implemented a provably secure method of validating SQL input to prevent injection attacks. Contributed to a system for biomedical named-entity disambiguation. Teaching assistant for Computational Theory, Introduction to Knowledge Discovery and Data Mining, Discrete Structures, Computer Science II and III, Programming Language Concepts, Language and Formal Reasoning, and Language and Society.

Education

2003–2005 **University of Iowa**, *PhD in Computer Science (unfinished)*, Iowa City, IA.
Research in data mining and its integration with database internals. Left ABD in December 2005, having finished all coursework and qualifying exams.

2001–2003 **University of Iowa**, *M.A. in Linguistics*, Iowa City, IA.
Concentration in Computational Linguistics.

1994–2001 **University of Houston**, *B.A. in English*, Houston, TX.
Concentration in Linguistics.

Selected Publications and Talks

LANGSEC 2011-2016, *CONFidence*, 2013.

Shotgun Parsers in the Crosshairs, *BruCON, ShmooCon*, 2012–2013.
With Sergey Bratus and Dan Hirsch.

Rue Notre Dame du Sommeil 24 – 1000 Brussels
✉ *mlp@thesmartpolitenerd.com* • *http://github.com/abiggerhammer*

Hammer: Smashing Binary Formats Into Bits, *BerlinSides, DEFCON SkyTalks*, 2012.
With Dan Hirsch.

A Patch for Postel's Robustness Principle, *IEEE Security and Privacy, vol. 10, no. 2*, March/April 2012.
With Sergey Bratus and Len Sassaman.

The Science of Insecurity, *TROOPERS 12, ShmooCon, 28th Chaos Computer Congress*, 2011–2012.
With Sergey Bratus.

Exploit Programming: from Buffer Overflows to Weird Machines and Theory of Computation, *USENIX ;login:*, December 2011.
With Sergey Bratus, Michael E. Locasto, Len Sassaman and Anna Shubina.

The Halting Problems of Network Stack Insecurity, *USENIX ;login:*, December 2011.
With Sergey Bratus, Len Sassaman and Anna Shubina.

Towards a formal theory of computer insecurity: a language-theoretic approach, *Invited lecture at Dartmouth College*, February 2011.
With Len Sassaman.

Exploiting the Forest with Trees, *Black Hat Briefings*, July 2010.
With Len Sassaman.

Exploiting Computational Slack in Protocol Grammars, *ph-neutral 0x7da*, May 2010.
With Len Sassaman.

PKI Layer Cake: New Collision Attacks Against the Global X.509 Infrastructure, *Financial Cryptography*, January 2010.
With Dan Kaminsky and Len Sassaman.

Freezing More Than Bits: Chilling Effects of the OLPC XO Security Model, *USENIX Usability, Psychology and Security*, FIXME 2008.
With David Chaum and Len Sassaman.

Subliminal Channels in the Private Information Retrieval Protocols, *28th Symposium on Information Theory in the Benelux*, FIXME 2007.
With Len Sassaman.

Some of These Things are Just Like the Others, *PostgreSQL 10th Anniversary Summit, O'Reilly Emerging Technologies, CodeCon*, 2006.

Stopping Injection Attacks with Computational Theory, *Black Hat Briefings*, July 2005.

SciTools: the grand unified web-based toolkit for genetic design and analysis, *CodeCon*, February 2005.

Rue Notre Dame du Sommeil 24 – 1000 Brussels
✉ *mlp@thesmartpolitenerd.com* • *http://github.com/abiggerhammer*

Brendan Francis O'Connor

bfo@ussjoin.com

(406) 545-0430 http://ussjoin.com

Education

The University of Wisconsin - Madison *September 2011 - May 2014 (Ongoing)*
Juris Doctor

Top 35% of Class
Dean's List, Spring 2012, Spring 2013
Member, Pro Bono Society
Technology Administrator, Student Bar Association

The Johns Hopkins University *September 2006 - May 2009*
Master of Science in Engineering in Computer Science

Thesis Title: **Mnikr: Reputation Construction Through Human Trading of Distributed Social Identities**
President of the CS Honor Society, Upsilon Pi Epsilon

The Johns Hopkins University *September 2004 - May 2008*
Bachelor of Science in Computer Science

Graduated with Departmental Honors

Legal Experience

Wisconsin State Public Defender *Summer 2013*
Legal Intern (With Practice Certificate)

This summer, I will be working with the Forensics Specialty Practice Group of the Wisconsin State Public Defender, assisting in cases with significant questions of scientific evidence across the state. I will be supervised by Anthony Rios under Wisconsin SCR 50, meaning that I will be able to make court appearances and work on behalf of clients.

Wisconsin Supreme Court *Fall 2012*
Judicial Intern

I served as a legal intern for Justice N. Patrick Crooks of the Wisconsin Supreme Court. My duties included examining cases requesting review by the Court, writing legal analyses of the issues raised by cases before the Court, and assisting the clerks in the performance of their duties.

The Rutherford Institute *Summer 2012*
Legal Intern

The Rutherford Institute is a public interest firm focusing on civil liberties litigation at both the trial and appellate levels, whose primary topics of interest are the First and Fourth Amendments as well as school "zero-tolerance" policies. I was responsible for legal research on current cases, drafting memos and briefs, and researching and writing legislation and policy statements for TRI on electronic privacy and UAV issues.

Technical Experience

Malice Afterthought, Inc. *2010 - Present*
CTO / DSS

Malice Afterthought provides software and security consulting services to a range of clients, from small businesses to large corporations, in addition to creating and releasing its own commercial and open source software. From January - July 2011, I taught information and network warfare (CNO) to students of the Department of Defense. In January, 2012, we won a DARPA Cyber Fast Track research proposal to fund research entitled "Reticle: Leaderless Command and Control," and in November, an additional CFT proposal entitled "NOM: Novel Object Mapping." Please visit http://www.maliceafterthought.com for more information.

SET Corporation *2009 - 2010*
Senior Research Associate

I worked as a technical lead on software projects in a variety of areas, including natural language processing and user modeling, and a project to create an augmented reality application to add real-time data and intelligence analysis to a multi-viewpoint 3D holographic display using the iPhone 3GS. These software projects were for a variety of government agencies, including DARPA, AFRL, INSCOM, and the DoD.

Six Apart *2008 (Internship)*
Open Platforms Group

I worked as an engineer on the Open Platforms team, dealing with furthering the goals of data portability across technologies and corporate boundaries while maintaining a focus on user control of data. I worked as an intern full-time during the summer of 2008, and then part-time through the remainder of the year.

Sun Microsystems *2007 (Internship)*
Solaris Security Technologies Group

I ported and integrated software into Solaris allowing users to authenticate using true PKCS#11 interfaces, then worked with a variety of teams and people across Sun (despite my status as an intern) to move these smartcard services into Solaris. I also had the opportunity to work with DTrace on Solaris Kerberos.

VeriSign *2006 (Internship)*
Security Services

I worked primarily with the Unified Authentication group, specifically with One-Time Passwords; I also did some work for VeriSign Labs (the Advanced Projects Research Group) on the VeriSign Personal Identity Provider. Over the course of 12 weeks, I was responsible for major projects in C♯, Ruby, and Java, as well as JSP/Struts/Spring web applications, JNI, C/C++, and various technologies. Despite being an intern, I had the honor of winning the VeriSign Labs "PIP Challenge" for integrating one-time password technology with the VeriSign Personal Identity Provider.

Publications and Invited Lectures

How to Fight a War Without Actually Starting One

Presentation on international war law as it pertains to computer security, to be presented at DerbyCon 3.0 in Louisville, KY, September 28-29, 2013.

Stalking a City for Fun and Frivolity

Original computer security research, to be presented at DEF CON 21 in Las Vegas, NV, August 1-4, 2013.

CreepyDOL: Cheap, Distributed Stalking

Original computer security research, to be presented at Black Hat USA in Las Vegas, NV, July 31 - August 1, 2013.

Panel - The Global 'Gamification' of Online Gaming

Panel on the intersection between legal issues and cybersecurity research, especially as they affect the international online gambling industry. At the conference of the International Bar Association, Dublin, Ireland, on October 1, 2012.

Reticle: Dropping an Intelligent F-BOMB

Hardware remote sensor design and implementation for security applications, presented at the Security B-Sides (BSidesLV 2012) conference in Las Vegas, NV on July 26, 2012. Video and slides at `http://blog.ussjoin.com/2012/07/reticle.html` . The acceptance rate for talks was 53.75% (43/80).

Hack the Law

Presentation on why security researchers should consider going to law school, presented at the Hackers on Planet Earth (HOPE Number Nine) conference in New York, NY on July 15, 2012. Video/slides at `http://tinyurl.com/llynv9m`.

Sacrificial Computing for Land and Sky

Presented at the ShmooCon security conference in Washington, D.C. on January 27, 2012. The acceptance rate for talks at the conference was 16.6% (36/216). Average attendee review score: 4.52/5. Video and coverage (including Forbes, Wired, and MSNBC) collected at `http://tinyurl.com/84kmz8c`.

A "Fair and Balanced" Look at Online Privacy in the Age of Location-Based Social Networking

Presented to the students and faculty of the United World College of the American West in their symposium on social networking, April 9-11, 2010.

Mnikr: Reputation Construction Through Human Trading of Distributed Social Identities

O'Connor, B. F. and Griffin, J. L. Proceedings of the 5th ACM Workshop on Digital Identity Management. Presented at the ACM Computer and Communications Security conference in Chicago, IL, on November 13, 2009, and selected as the best paper at the workshop. The workshop acceptance rate was 33% (7/21) for full papers.

Federal Government and Major Organizational Endorsements

Department of Defense

Security Clearance (Contact for Details)

International Information Systems Security Certification Consortium, ISC²

Certified Information Systems Security Professional (CISSP®)

Department of Homeland Security

IS-{100, 200, 700, 800, 802} - ARES/RACES Series
IS-{139, 230, 235, 240, 241, 242, 244} - FEMA Professional Development Series
IS-{1, 120, 130, 250, 288} - ARRL Advanced Emergency Communications Series
FEMA Professional Development Certificate

Federal Communications Commission

Amateur Extra Radio License, `K3QB`
Volunteer Examiner (Accredited through ARRL)

Amateur Radio Relay League

Public Service and Emergency Communications Management for Radio Amateurs (EC-016)
Amateur Radio Emergency Communications Course (ARECC)
Full Member, Dane County (Wisconsin) Amateur Radio Emergency Services

Sergey Bratus, Ph.D.

Institute for Security, Technology, and Society
Dartmouth College
ph. 603-646-9224

EMPLOYMENT

- **Research Assistant Professor**, Computer Science Dept., Dartmouth College (2008–present)
- **Principal Security Technology Advisor to Kiewit Computing**, Dartmouth College (2008–present)
- **Senior Research Associate**, Institute for Security Technology, and Society, Dartmouth College (2005–2008)
- **Consultant**, BAE Systems (2006–2009)
- **Research Associate**, Institute for Security Technology Studies, Dartmouth College (2002–2005)
- **Scientist**, BBN Technologies/Verizon (1999–2001)
- **Instructor**, Northeastern University, College of Computer Science (1997–1999)
- **UNIX system administrator**, Northeastern University, Dept. of Mathematics (1997–2001)
- **Teaching Assistant**, Northeastern University, Dept. of Mathematics (1993–1996)

RESEARCH AND SOFTWARE ENGINEERING

- **Computer security, Intrusion Analysis, Reverse Engineering**

  Institute for Security, Technology, and Society, Dartmouth College, 2002–present time

  · Worked on distilling security practitioner methodologies behind the discovery of high-impact vulnerabilities by vulnerability researchers, hackers

  · Studied the security challenges of composition of software modules in terms of Formal Language Theory and Theory of Computation

  · Led a security assessment of a Control Center network of a Fortune 500 utility company.

  · Managed the Dartmouth Internet Security Testbed (DIST) wireless, an 802.11 research infrastructure of over 200 Air Monitors distributed throughout diverse locations of the Dartmouth College campus (`http://www.cs.dartmouth.edu/~dist/`)

  · Proposed new hardware security primitives for Trusted Computing systems and security context separation in virtualized environments (Best Paper Award at the TRUST 2008 conference)

  · Performed fuzz-testing of proprietary SCADA protocols and equipment `http://lzfuzz.cs.dartmouth.edu/`

  · Researched link layer fingerprinting techniques for 802.11 stations and designed an active fingerprinting tool (`http://baffle.cs.dartmouth.edu/`)

  · Designed and developed automated log analysis tools for host and network logs for the Kerf project (`http://kerf.cs.dartmouth.edu/`)

  · Applied statistical machine learning, data organization and information theory techniques to log and network trace analysis tasks

- Extended a research Linux kernel system call logging and policy enforcement framework and developed tools for visualization and analysis of resulting system call traces
- Analyzed rootkit deception techniques, their detection and defensive applications
- Studied UNIX kernel security mechanisms, including LSM and NSA SELinux security policies, Linux Vserver, BSD jails and other virtualization solutions, and researched ways to improve their usability
- Performed security assessment of PlanetLab Central, for the PlanetLab project
- Directed parts of the campus-wide Dartmouth computer security assessment, organized various graduate and undergraduate student efforts
- Performed analysis of compromised systems, data recovery, OS hardening
- Directed student research related to Linux kernel security and Xen virtualization security mechanisms
- Reviewer for ACSAC, SecSE, PST, SiS, ATC and other conferences, subreviewer for CCS, NDSS, USEC.

BAE Systems, National Security Solutions, Inc., 2006—2009

- Windows kernel mode rootkit detection software
- Defensive reverse engineering protection measures
- Participated in developing research proposals

Publications:

- *"Composition Patterns of Hacking"* with Julian Bangert, Alexandar Gabrovsky, Anna Shubina, Daniel Bilar, Michael E. Locasto, in Proceedings of Cyberpatterns 2012
- *"A Patch for Postel's Robustness Principle"* with Len Sassaman, Meredith L. Patterson, IEEE Security and Privacy Journal, Volume 10, Issue 2, March-April 2012
- *"Identifying Vulnerabilities in SCADA Systems via Fuzz-Testing"*, with Rebecca Shapiro, Edmond Rogers, Sean Smith, in IFIP Advances in Information and Communication Technology, 2011, Volume 367, 2011
- *"Packets in Packets: Orson Welles In-Band Signaling Attacks for Modern Radios"* with Travis Goodspeed, Ricky Melgares, Rebecca Shapiro, Ryan Speers, in Proceedings of the 5th USENIX Workshop on Offensive Technologies, August 2011
- *"Exploiting the Hard-working DWARF: Trojan and Exploit Techniques with No Native Executable Code"* with James Oakley, in Proceedings of the 5th USENIX Workshop on Offensive Technologies, August 2011
- *"Exploit Programming: from Buffer Overflows to Weird Machines and Theory of Computation"* with Michael E. Locasto, Meredith L. Patterson, Len Sassaman, Anna Shubina, in USENIX ;login:, December 2011
- *"The Halting Problems of Network Stack Insecurity"* with Len Sassaman, Meredith L. Patterson, Anna Shubina, in USENIX ;login:, December 2011
- *"Intrusion Detection for Resource-constrained Embedded Control Systems in the Power Grid"* with Jason Reeves, Ashwin Ramaswamy, Michael Locasto, Sean Smith, International Journal of Critical Infrastructure Protection, 2011
- *"Beyond SELinux: the Case for Behavior-Based Policy and Trust Languages"* with Michael E. Locasto, Boris Otto, Rebecca Shapiro, Sean W. Smith, Gabriel Weaver, Dartmouth Computer Science Technical Report TR2011-701, August 2011
- *"Security Applications of Formal Language Theory"* with Len Sassaman, Meredith L. Patterson, Michael E. Locasto, Anna Shubina, Dartmouth Computer Science Technical Report TR2011-709, 2011

- *"Api-do: Tools for Exploring the Wireless Attack Surface in Smart Meters"* with Travis Goodspeed, Ricky Melgares, Ryan Speers, Sean W. Smith, Hawaii International Conference on System Sciences, January 2012
- *"On Tuning the Knobs of Distribution-Based Methods for Detecting VoIP Covert Channels"* with Chrisil Arackaparambil, Guanhua Yan, Alper Caglayan, Hawaii International Conference on System Sciences, January 2012
- *"Assessing the Vulnerability of SCADA Devices"*, with Rebecca Shapiro and Sean Smith, Fifth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, 2011, August 2011
- *"Lightweight Intrusion Detection for Resource-Constrained Embedded Control Systems"*, with Jason Reeves, Ashwin Ramaswamy, Michael Locasto, and Sean Smith, Fifth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, 2011, August 2011
- *"Using Hierarchical Change Mining to Manage Network Security Policy Evolution"*, with Gabriel A. Weaver, Nick Foti, Dan Rockmore, and Sean W. Smith, USENIX HotICE, Boston, 2011
- *"Exploiting the hard-working DWARF"* with James Oakley. Shmoocon 2011, Washington, DC
- *"Exploiting the hard-working DWARF"* with James Oakley. Hackito Ergo Sum 2011, Paris, France
- *"Detection of Rogue APs Using Clock Skews: Does It Really Work?"*, with Chrisil Arackaparambil and Anna Shubina, Shmoocon 2010, Washington, DC
- *"Detection of Rogue APs Using Clock Skews: Does It Really Work?"*, with Chrisil Arackaparambil and Anna Shubina, Toorcon 2009, San Diego, CA
- *"SegSlice: Towards a New Class of Secure Programming Primitives for Trustworthy Platforms"*, with Michael E. Locasto, Brian Schulte, TRUST 2010, Berlin, Germany, 2010
- *"Software on the witness stand: what should it take for us to trust it?"*, with Ashlyn Lembree, Anna Shubina, TRUST 2010, Berlin, Germany, 2010
- *"The diversity of TPMs and its effects on development: a case study of integrating the TPM into OpenSolaris"*, with Anna Shubina, Wyllys Ingersol, Sean W. Smith, 5th ACM Workshop on Scalable Trusted Computing (STC '10), New York, NY, USA, 2010.
- *"VM-based security overkill: a lament for applied systems security research"*, with Michael E. Locasto, Ashwin Ramaswamy, Sean W. Smith, 2010 Workshop on New Security Paradigms (NSPW '10). New York, NY, USA, 2010.
- *"Automated Mapping of Large Binary Objects Using Primitive Fragment Type Classification"*, with Gregory Conti et al., 10th Annual DFRWS Conference, `http://www.dfrws.org/2010/`, Portland, OR, 2010
- *"A Visual Study of Primitive Binary Fragment Types"* with Gregory Conti et al., BlackHat USA 2010
- *"On the reliability of wireless fingerprinting using clock skews"*, with Chrisil Arackaparambil, Anna Shubina, David Kotz, 3rd ACM Conference On Wireless Network Security, Hoboken, NJ, 2010
- *"Teaching the principles of the hacker curriculum to undergraduates"*, with Anna Shubina, Michael E. Locasto, 41st ACM technical symposium on Computer science education, Milwaukee, WI, 2010

- *"Distributed Monitoring of Conditional Entropy for Anomaly Detection in Streams"*, with Chrisil Arackaparambil, Joshua Brody, Anna Shubina, 10th Workshop on Communication Architecture for Clusters, International Parallel and Distributed Processing Symposium, Atlanta, GA, 2010
- *"Katana: A Hot Patching Framework for ELF Executables"*, with Ashwin Ramaswamy, Michael E. Locasto, Sean W. Smith, 4th Workshop on Secure Software Engineering (SecSE), part of the ARES conference, Krakow, Poland, April, 2010
- *"Katana: Towards Patching as a Runtime Part of the Compiler-Linker-Loader Toolchain"*, with James Oakley, Ashwin Ramaswamy, Sean W. Smith, Michael E. Locasto, International Journal of Secure Software Engineering (IJSSE), Volume 1, Issue 3, 2010
- *"What Hacker Research Taught Me"*, Keynote at TROOPERS 2010, Germany, `http://www.troopers10.org/`
- *"What Hacker Research Taught Me"*, Defcon 802, May 2010, Burlington, VT, `http://dc802.org/`
- *"Bickering In-Depth: Rethinking the Composition of Competing Security Systems"*, with Michael E. Locasto, Brian Schulte, IEEE Security and Privacy Journal, vol. 7, no. 6, pp. 77–81, 2009
- *"The cake is a lie: privilege rings as a policy resource"*, with Peter C. Johnson, Ashwin Ramaswamy, Sean W. Smith, Michael E. Locasto, 1st ACM workshop on Virtual Machine Security (VMSec), Conference on Computer and Communications Security, Chicago, IL, 2009
- *"Dartmouth Internet Security Testbed (DIST): building a campus-wide wireless testbed"*, with David Kotz, Keren Tan, William Taylor, Anna Shubina, Bennet Vance, Michael E. Locasto, USENIX 2nd Workshop on Cyber Security Experimentation and Test (CSET), Montreal, Quebec, 2009
- *"Using Domain Knowledge for Ontology-Guided Entity Extraction from Noisy, Unstructured Text Data"*, with Anna Rumshisky, Rajendra Magar, Paul Thompson, 3rd Workshop on Analytics for Noisy Unstructured Text Data, Barcelona, Spain, 2009
- *"Traps, Events, Emulation, and Enforcement: Managing the Yin and Yang of Virtualization-based Security"*, with M.E.Locasto, A.Ramaswamy, and S.W.Smith, 1st Workshop on Virtual Machine Security (VMSec), Washington, D.C., 2008
- *"Why Do Street-Smart People Do Stupid Things Online?"*, with Chris Masone, Sean W. Smith, IEEE Security and Privacy Journal, vol. 6, no. 3, pp. 71–74, May 2008
- *"Embedded Systems – "Invisible" Devious Devices"*, TROOPERS 2009, Munich, Germany, `http://www.troopers09.org/`
- *"Backhoe, a packet trace and log browser"*, with Axel Hansen, Fabio Pellacini, and Anna Shubina, 5th International Workshop on Visualization for Computer Security (VizSec '08), Boston, 2008
- *"Streaming Estimation of Information-theoretic Metrics for Anomaly Detection (Extended Abstract)"*, with Joshua Brody, David Kotz and Anna Shubina, 11th International Symposium on Recent Advances in Intrusion Detection (RAID '08), Boston, 2008
- *"New Directions for Hardware-assisted Trusted Computing Policies (Position Paper)"*, with Michael Locasto, Ashwin Ramaswamy and Sean Smith, Future of Trust in Computing, Berlin, 2008
- *"Fuzzing Proprietary SCADA Protocols"*, Black Hat USA 2008, Las Vegas, NV, 2008
- *"LZfuzz: a fast compression-based fuzzer for poorly documented protocols"*, with Axel Hansen and Anna Shubina, Dartmouth Computer Science Technical Report TR2008-634, 2008

- *"TOCTOU, Traps and Trusted Computing"*, with Nihal D'Cunha, Evan Sparks and Sean Smith, **Best Paper Award** at TRUST 2008, Villach, Austria
- *"Active behavioral fingerprinting of wireless devices"*, with Cory Cornelius, David Kotz, and Daniel Peebles, 1st ACM Conference on Wireless Network Security (WiSec '08), Alexandria, VA, March 2008
- *"Active 802.11 Fingerprinting: Gibberish and "Secret Handshakes" to Know Your AP"*, with C.Cornelius and D.Peebles, Shmoocon 4, February 2008
- *"Attacking and Defending Networked Embedded Devices"*, with J.Baek, S. Sinclair and S.Smith, 2nd Workshop on Embedded Systems Security, Salzburg, Austria, October 2007
- *"Dumbots: Unexpected Botnets through Networked Embedded Devices"*, with J.Baek, S.Sinclair and S.Smith, Dartmouth technical report TR2007-591, May 2007,
- *"Hacker Curriculum: How Hackers Learn Networking"*, IEEE Distributed Systems Online, vol. 8, no. 10, 2007
- *"What Hackers Learn that the Rest of Us Don't: Notes on Hacker Curriculum"*, IEEE Security and Privacy, vol. 5, no. 4, pp. 72–75, July/August 2007
- *"Entropy-based data organization tricks for browsing logs and packet captures"*, Defcon 15, August 2007
- *"Simple entropy-based heuristics for log and traffic analysis"*, Shmoocon 3, March 2007
- *"Pastures: Towards Usable Security Policy Engineering"*, with A.Ferguson, D. McIlroy and S. Smith, 1st Workshop on Secure Software Engineering (SecSE), part of the ARES conference, April, 2007
- *"Semi-supervised Data Organization for Interactive Anomaly Analysis"*, with J.Aslam and V.Pavlu (Northeastern University), International Conference on Machine Learning and Applications (ICMLA) , December, 2006
- *"The Kerf Toolkit for Intrusion Analysis"*, with J. Aslam, D. Kotz, D. Rus, R. Peterson, B. Tofel (Dartmouth College), IEEE Security and Privacy, 2(6):42-52, November/December, 2004.
- *"The Kerf Toolkit for Intrusion Analysis"*, with J. Aslam, D. Kotz, D. Rus, R. Peterson (Dartmouth College), IAnewsletter, 8(2):12-16, Summer, 2005.
- *"Ubiquitous Redirection as Access Control Response"*, with G. Bakos, Privacy, Security and Trust Conference, 2005
- *"Kerf: Machine Learning To Aid Intrusion Analysis"*, Work-in-progress report at USENIX Security Conference 2004

◇ **Information Extraction, Natural Language Processing**

BBN Technologies, Speech and Language Dept., 1999–2001

- Worked on statistical Text Understanding systems, in particular on name and fact extraction from natural English text.
- Designed and/or implemented:
  - Statistical and rule-based algorithms for NLP tasks such as parsing, name and descriptor finding and classification, coreference, pronoun resolution, summarization of natural English text.
  - XML-based architecture for processing and storing natural language documents.
  - XML and HTML-based visualization tools for annotated and processed documents and training data.
  - Web front-ends and relational database back-ends for the above.

Publications:

- *"Experiments in Multi-Modal Content Extraction"*, with L. Ramshaw, E. Boschee, S. Miller, R. Stone, R. Weischedel, A. Zamanian (BBN Technologies), Human Language Technology (HLT) Conference 2001,
- *"FactBrowser Demonstration"*, with S. Miller, L. Ramshaw, R. Weischedel, A. Zamanian (BBN Technologies), HLT 2001,

◇ **Computer Algebra and Symbolic Computation**

Developed new efficient algorithms for recognition of and computation in finite groups of various types.

Software projects:

- GAP share package for two new black box recognition algorithms (GAP/Unix,Win32)
- Package for search and computation in finite permutation groups (LISP)
- Custom package for computation with polynomials in commuting and anti-commuting variables (LISP)

Publications:

- *"Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's Conjecture"*, with I. Pak, Journal of Symbolic Computation, vol. 29, 2000
- *"On sampling generating sets of finite groups and product replacement algorithm"*, with I. Pak, ISSAC-99 Conference Proceedings
- *"Constructive recognition of black box groups isomorphic to central extensions of $PSL(n, q)$"*, with G. Cooperman, L. Finkelstein, S. Linton, preprint
- *"Recognition of finite black box groups (Algorithms for constructive recognition of finite black box groups isomorphic to symmetric and special linear groups)"* Ph.D. thesis, Northeastern University, 1999

TEACHING

◇ **Instructor**, Dartmouth College (2005–2012)

- Secure Information Systems Mentoring and Training (SISMAT)
  Developed and taught computer security hands-on "immersion" classes to students and interns of the SISMAT program (`http://www.cs.dartmouth.edu/~sismat/`).
- Advanced Operating Systems (CS108)
  Used OpenSolaris kernel code and DTrace to demonstrate and explore aspects of modern OS design.
- Computer Security (CS38) course and labs.
  Designed and implemented a virtual host and network environment for the students to practice network reconnaissance and attacks, shellcode development, live analysis of compromised hosts (described in *"Hacker Curriculum: How we can use it in teaching"*, IEEE Distributed Systems Online, vol. 8, no. 11, 2007

◇ **Instructor**, College of Computer Science, Northeastern University (1997–1999)

- Classes in C++/STL, Software Design, Data Structures.
- Wrote and ported courseware to Win32 (Visual C++ 5,6 and Cygwin)
- Teaching Assistant/Instructor, Dept. of Mathematics, Northeastern University
- Calculus and Discrete Mathematics Courses

OTHER PROFESSIONAL ACTIVITIES

Expert witness for the defence in UMG Recordings, et al. v. Mavis Roy.

EDUCATION

◇ **Northeastern University**, Boston (1993–1999)

Ph.D. in Mathematics, M.S. in Computer Science, 1999

◇ **Moscow Institute of Physics and Technology** (aka MIPT, "Phystech") (1988–1993)

REFERENCES

Available upon request.

E. Gabriella Coleman

Wolfe Chair in Scientific and Technological Literacy
McGill University

(last revised June, 2013)

Department of Art History and Communication Studies
McGill University
853 Sherbrooke St. W.
Montreal, QC H3A 2T6 Canada
http://gabriellacolman.org
[001] 514-398-XXXX
gabriella.coleman@mcgill.ca

Education

University of Chicago, Chicago, IL
Ph.D., Socio-cultural Anthropology, August 2005
M.A., Socio-cultural Anthropology, August 1999

Dissertation: "The Social Construction of Freedom in Free and Open Source Software: Hackers Ethics, and the Liberal Tradition"
Research location:: San Francisco, CA and Netherlands
Funding: SSRC and NSF, August 2001-May 2003

Columbia University, New York, NY
B.A., Religious Studies, May 1996

Positions

Faculty Associate, Berkman Center for Internet & Society
Harvard University, Cambridge, MA
September 2013-September 2014

Assistant Professor and Wolfe Chair in Scientific and Technological Literacy, Department of Art History and Communication Studies
(Affiliated with Department of Anthropology)
McGill University, Montreal, Quebec
January 2012-present

Assistant Professor, Department of Media, Culture, and Communication
Steinhardt School of Culture, Education, and Human Development
New York University, New York, NY
September 2007-December 2010

Faculty Fellow, School of Social Science
Institute for Advanced Study, Princeton, NJ
September 2010-June 2011

Izaak Walton Killam Memorial Postdoctoral Fellow, Program in Science, Technology and Society

University of Alberta, Edmonton, Alberta
September 2006-September 2007

Postdoctoral Fellow, Center for Cultural Analysis
Rutgers University, New Brunswick, NJ
July 2005-July 2006
Center Theme for 2005-2006: Intellectual Property

Grants and Fellowships

FQRSC (Fonds de recherche Société et culture du Québec)
Team Member (Principal Investigator: Christine Ross, McGill University, Department of Art History and Communication Studies). Funding for "Esthétique, nouveaux médias et la (ré)configuration de l'espace public", 2013-2016. [$12,330 CAD per year, total: $303,600 CAD for the entire team].

National Science Foundation, Program in Science, Technology, and Society
(With Christina Dunbar-Hester, Rutgers University, School of Communication and Information). Funding for "Geek Feminisms: Activism, Technical Practice, and Gender Bending", 2011-2012.[Two year funded granted for $147,500 US. One year of funding at $73,750 accepted].

Humanities Initiative, New York University, Technologies of Mediation
Co-applicant (with Ben Kafka, New York University, Department of Media, Culture, and Communication; Clifford Siskin and Robert Young, New York University, Department of English). Funding for seminars and workshops on mediation, technology, and the Enlightenment, New York, NY. September 2009-September 2012 [$5000 US].

Institute for Public Knowledge, New York University, Techniques of Liberalism
Co-applicant (with Ben Kafka, New York University, Department of Media, Culture, and Communication). Funding for a year-long seminar series to read and critique texts in liberal thought with junior faculty members and invited participants. New York, NY. September 2008-September 2009 [$5000 US].

Ford Foundation Educational Grant, Visiting Scholar (Brazil)
Funding to visit Programa de Pos Graduaçao em Antropologia Social da Universidade Federal do Rio Grande do Sul and to present my work on Free Software, Intellectual Property, and the Liberal Tradition. Porto Alegre, Brazil. June 2008 [$5000 US].

Summer Institute for Junior Scholars, Law and Society Association
University of the Witwatersrand, Johannesburg, South Africa. July 2006.

Charlotte Newcombe Fellowship, Woodrow Wilson Foundation
Dissertation writing fellowship for study of ethical and religious values. September 2003-September 2004.

Dissertation Improvement Grant, National Science Foundation
Dissertation research grant from Societal Dimensions of Engineering, Science and Technology. September 2002-May 2003.

Fieldwork Grant, Social Science Research Council
Dissertation research grant for study of non-profits and philanthropy. San Francisco, CA.

September. 2001-September 2002.

Graduate Studies Fellowship, National Science Foundation
Three-year fellowship for graduate studies. July 1998-June 2001.

Summer Travel Grant, University of Chicago
Travel funded by Center for Latin American Studies for research in Dominican Republic. July 1998.

Summer Travel Grant, University of Chicago
Travel funded by Race, Politics, and Culture Center for research in Guyana. July 1999.

Graduate Fellowship, University of Chicago
Four-year fellowship. October 1997-June 1998.

Honors and Distinctions

Anvil of Freedom Award, University of Denver
Awarded to individuals and organizations that demonstrate true leadership and commitment to democratic freedoms, ethics, and integrity. October 2013.

Gabriel Carras Research Award, New York University, Steinhardt School of Culture, Education, and Human Development
Awarded for "Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers", *Cultural Anthropology*. April 2009.

Sol Tax Dissertation Prize, University of Chicago, Department of Anthropology
Awarded for dissertation combining highest intellectual merit with relevance to anthropology and action. June 2006.

Julien Mezey Dissertation Award, Association for the Study of Law, Culture and Humanities
Awarded for dissertation most promising to enrich and advance interdisciplinary scholarship at the intersection of law, culture, and the humanities. March 2006.

Frederick K. Starr Lecturer, University of Chicago, Department of Anthropology
Lectureship awarded to four advanced Ph.D. students to teach an undergraduate course of their own design. January 2005.

Roy D. Albert Prize, University of Chicago.
Best master's thesis in Anthropology: "The Politics of Survival and Prestige: Hacker Identity and the Global Production of an Operating System". June 2000.

Publications

In Print

Books/Manuscripts

Coding Freedom: The Ethics and Aesthetics of Hacking. Princeton University Press. November 2012.

Articles in Scholarly Journals (refereed unless otherwise noted)

Am I Anonymous? *Limn*, Issue 2: Crowds and Clouds. Chris Kelty, ed. May 2012. http://limn.it/am-i-anonymous/

Our Weirdness is Free: The logic of Anonymous—online army, agent of chaos, and seeker of justice. *Triple Canopy*, (15)2012. http://canopycanopycanopy.com/15/our_weirdness_is_free [translated Gabriella Coleman: Notre etrangete est libre de droits. In *May* 9(6)2012:96-111.]

Hacker Politics and Publics. *Public Culture*, 23(3)2011: 511-516. [translated Gabriella Coleman: Politik und Öffentlichkeit der Hacker. In: Astrid Bötticher, Hans-Jürgen Lange: Cyber-Sicherheit. VS Verlag für Sozialwissenschaften. Wiesbaden.]

Ethnographic Approaches to Digital Media. *Annual Review of Anthropology*, (39)2010: 487-505.

Hacking In-Person: The Ritual Character of Conferences and the Distillation of a Life-World. *Anthropological Quarterly*, 83(1)2010: 99-124.

Code is Speech: Legal Tinkering, Expertise, and Protest among Free and Open Source Software Developers. *Cultural Anthropology*, 24(3)2009: 420-454.

Hacker Practice: Moral Genres and the Cultural Articulation of Liberalism (with Alex Golub). *Anthropological Theory*, 8(3)2008: 255-277. [First author]

Los Temps d'Indymedia. *Multitudes*, (21)2005: 41-48.

The Political Agnosticism of Free and Open Source Software and the Inadvertent Politics of Contrast. *Anthropological Quarterly*, 77(3)2004: 507-519.

Iconic Tactics: How Free Became Open and Everything Else Under the Sun (with Benjamin Hill). *M/C Journal,* 7(3)2004. [Co-author] http://journal.media-culture.org.au/0406/02_Coleman-Hill.php

High-Tech Guilds in the Era of Global Capital. *Anthropology of Work Review*, 22(1)2001: 28-32.

Chapters in Edited Books (refereed unless otherwise noted)

Anonymous and the Politics of Leaking. In *Beyond WikiLeaks: Implications for the Future of Communications, Journalism and Society*, Benedetta Brevini, Arne Hintz, and Patrick McCurdy, eds. Basingstoke, UK: Palgrave Macmillan, 2013.

Phreaks, Hackers, and Trolls and the Politics of Transgression and Spectacle. In *The Social Media Reader*, Michael Mandiberg, ed. New York: NYU Press, 2012.

Revoluções Silenciosas: o Irônico Surgimento do Software Livre e de Código Aberto e a Constituição de uma Consciência Legal Hacker. In *Estudos de Propriedade Intelectual*, Fachel Leal Ondina (Org.). Porto Alegre: Editora Tomo, 2010. *not refereed

The Politics of Rationality: Psychiatric Survivors' Challenge to Psychiatry. In *Tactical Biopolitics*, Kavita Phillip and Beatriz de Costa, eds. Cambridge: MIT Press, 2008.

The (copylefted) Source Code for the Ethical Production of Information Freedom. In *Sarai Reader 2003: Shaping Technologies*, New Delhi: Sarai, New Media Initiative, 2003. *not refereed

Book Reviews

Hacking (Tim Jordan). Book Review. *Journal of Communication*, 59(4)2010: 19-22.

Copy, Rip, Burn: The Politics of Copyleft and Open Source (David Berry). Book Review. *Times Higher Education*, February 2009.

Code: Collaborative Ownership and the Digital Economy (Rishab Aiyer Ghosh, ed.). Book Review. *The Information Society,* 23(2)2007.

Artifacts: An Archeologist's Year in Silicon Valley (Christine Finn). Book Review. *Technology and Culture,* (44)2003: 196-197.

Encyclopedia Articles and Reports

Anonymous. *A Glossary of Network Ecologies*, Carolin Wiedemann and Soenke Zehle, eds. Amsterdam: Institute of Network Cultures. November 2012.

Forthcoming Publications

Books

Doing it for the Lulz: Anonymous and the Politics of Dissent. (Manuscript in preparation, under contract with Verso).

Articles in Scholarly Journals (refereed unless otherwise noted)

The Aphorisms of Anonymous. *Journal of Visual Culture*, "Special Issue on Internet Memes and Visual Culture", 2014.

Chapters in Edited Books (refereed unless otherwise noted)

Close to the Metal (with Finn Brunton). In *Mediation, Materiality, Maintenance: Paths Forward in the Study of Media Technologies*, Tarleton Gillespie, Pablo Boczkowski, and Kirsten Foot, eds. Cambridge, MA: MIT Press, 2014.

Encyclopedia Articles and Reports (refereed unless otherwise noted)

Anonymous in Context. Centre for International Governance Innovation, Policy Report, 2013.

Hackers. *Johns Hopkins Guide to Digital Textuality*, Marie-Laure Ryan, Lori Emerson, and Benjamin Robertson, eds. Baltimore, MD: Johns Hopkins University Press, 2014.

Popular Pieces

Code Is Speech: Hackers attempt to write themselves into the Constitution. *Reason Magazine,* April 2013.
http://reason.com/archives/2013/03/21/code-is-speech

Geeks are the New Guardians of our Civil Liberties. *MIT Technology Review,* February 2013.
http://www.technologyreview.com/news/510641/geeks-are-the-new-guardians-of-our-civil-liberties/

Hackers for Right, We are Down One. *Huffington Post,* January 2013.
http://www.huffingtonpost.com/gabriella-coleman/hackers-for-right-we-are-_b_2472307.html

Beacons of Freedom: The Changing Face of Anonymous. *Index on Censorship,* December 2012.
http://www.indexoncensorship.org/2012/12/beacons-freedom-hacking-anonymous/
(republished in German in "Jahrbuch Netzpolitik 2012 - Von A wie ACTA bis Z wie Zensur")

Everything You Know about Anonymous is Wrong. *Al Jazeera*, May 2012.
http://www.aljazeera.com/indepth/opinion/2012/05/201255152158991826.html

Another Tech Pioneer, Dennis Ritchie, Passes [with Chris Kelty]. *Al Jazeera*, October 2011.
http://www.aljazeera.com/indepth/opinion/2011/10/201110171017589239 14.html

The Ethics of Digital Direct Action. *Al Jazeera*, September 2011.
http://www.aljazeera.com/indepth/opinion/2011/08/2011830845582576 9.html

Hacker Culture: A Response to Bruce Sterling on WikiLeaks. *The Atlantic*, December 2010.
http://www.theatlantic.com/technology/archive/2010/12/hacker-culture-a-response-to-bruce-sterling-on-wikileaks/68506/

What It's Like to Participate in Anonymous' Actions. *The Atlantic*, December 2010.
http://www.theatlantic.com/technology/archive/2010/12/what-its-like-to-participate-in-anonymous-actions/67860/

The Anthropology of Hackers. *The Atlantic*, September 2010.
http://www.theatlantic.com/technology/archive/2010/09/the-anthropology-of-hackers/63308/

Presentations

Invited Keynotes and Plenary Talks

Weapons of the Geek. Plenary at Personal Democracy Forum, New York, NY, June 2013.

Hacker Ethics and Aesthetics. Keynote at FOSCONS2012, Göteborg, Sweden, November 2012.

Profiling Anonymous. Keynote at 7th Annual Paul Attallah Lecture Series, Communication Department, Carleton University, Ottawa, Ontario, March 2012.

E Plurbius Anonymous: In Lulz We Trust. Plenary at Webstock 12, Wellington, New Zealand, February 2012.

From Lulz to Collective Action. Plenary at Cidadania e Redes Digitais. Universidade Metodista Sao Paolo, Brazil, October 2011.

Anonymous: From Trolling to Digital Activism and Civil Disobedience. Plenary at Re:publica, Berlin, Germany, April 2011.

'I did it for the Lulz! but I stayed for the outrage:' Internet Trolls, the Politics of Spectacle, and Geek Protests against the Church of Scientology. Keynote at Brazilian Cyberstudies Association Meeting (ABCiber), Rio, Brazil, November 2010.

A User's Guide to Lulzy Media, the Pleasure of Trickery, and the Politics of Spectacle: from Luddites to Anonymous (with Finn Brunton). Plenary at Hackers on Planet Earth, New York, NY, July 2010.

Cabals, Crisis, and Conflict. Keynote at Developing the Virtual Society: Conflict in Adoption of Collaborative Networks Conference, University of Hull, Hull, England, March 2010.

These are the Best of Times and these are the Worst of Times: F/OSS and the Global Politics of Intellectual Property Law. Keynote at Linux.conf.au Conference, Wellington, New Zealand, January 2010.

The Politics and Poetics of DeCSS. Featured Talk at Open Video Conference, New York University, New York, NY, June 2009.

Variants of Hacking. Inaugural Plenary for Digital Humanities Study Group at CUNY Graduate Center, New York, NY, October 2009.

Invited Seminars and Lectures

Weapons of the Geek: Liberation Technology Speaker Series, Stanford University, Stanford, CA, November 2012; Computer Science Privacy Speaker Series, University of Waterloo, Waterloo, Ontario, January 2013; Anthropology STANDD Lecture Series, McGill University, Montreal, Quebec, February 2013; Anthropology Speaker Series, Brown University, Providence, RI, March 2013.

*The Aphorisms of Anonymou*s. Habits of Living Conference, Brown University, Providence, RI, March 2013.

Coding Freedom. Montreal Google Speakers' Series, Montreal, Quebec, February 2013.

Anonymous. TED Global, Edinburgh, Scotland, June 2012.

*Doing it for the Lulz: Anonymous and the Politics of Dissen*t. Anthropology Department, University of Toronto, Toronto, Ontario, March 2012.

E Plurbius Anonymous: In Lulz We Trust. Building Better Speech and Globe Series.

Parsons School of Design, New York, NY, November 2011.

The Value of Opacity in the Age of Surveillance. Creative Activism Thursdays, Yes Men Labs, New York University, New York, NY, November 2011.

From Digital Direct Action to Leaking: How to Understand the Politics of Anonymous. New Media/Social Change Symposium, International Institute, University of Michigan, Ann Arbor, MI, November 2011.

*Hacktivism, Vigilantism and Collective Action in a Digital Ag*e. Brookings Institution, Washington, DC, December 2011.

Troll as Liberal Trickster. Cultures of the Internet: Identity, Community and Mental Health Conference, Advanced Study Institute, Division of Social and Transcultural Psychiatry, McGill University, Montreal, Quebec,, April 2011.

Anonymous: From the Offensive Internet to Human Rights Activism. Department of Art History and Communication Studies Speakers Series (co-sponsored by Anthropology Department and Faculty of Law), McGill University, Montreal, Quebec , March 2011.

Phreaks, Hackers, Trolls and the Politics of Spectacle. Princeton Center for Information Technology Policy, Princeton University, Princeton, NJ, October 2010.

Old & New Net Wars Over Free Speech, Freedom & Secrecy; or How to Understand the Hacker & Lulz Battle against the Church of Scientology. Radars and Fences Conference, New York University, New York, NY, March 2008; Communications Colloquium, Columbia University, New York , NY, November 2008; Information Society Project, Yale University, New Haven, CT, December 2008; Department of Communications, Drexel University, Philadelphia, PA, February 2009; Institute for Public Knowledge, New York University, New York, NY, March 2009; Science and Technology Studies Department, Cornell University, Ithaca, NY, October 2009; Faculty of Law, Victoria University of Wellington, Wellington, New Zealand, January 2010; Interactive Telecommunications Program, New York University, New York, NY, March 2010; Digital Religion: Transforming Knowledge and Practice Conference, New York University's Center for Religion and Media, New York, NY, March 2010.

The Tension between Corporate Sociality and Individual Liberalism in Debian. Copyright's Counterparts Workshop, Queens University, Kingston, Quebec , August 2008.

Silent Revolutions: The Ironic Rise of Free and Open Source Software and the Making of a Hacker Legal Consciousness. Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil and Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação, University of São Paulo, Brazil, June 2008.

On the Centers and Margins of Liberalism: How Hackers Challenge Trends in Intellectual Property Law Through the Rearticulation of Free Speech Principles. Engaged Anthropology Lecture Series, Rutgers University, New Brunswick, NJ, March 2006; Program in Science and Technology Studies, University of Alberta, Edmonton, Alberta , March 2007.

Psychiatric Survivors and the Performance of Rationality. BioArt and Public Sphere Conference, University of California Irvine, Irvine, CA, October 2005.

The Social Construction of Freedom in Free and Open Source Software: Hackers, Ethics,

and the Liberal Tradition. Franz Boas Seminar Series, Anthropology Department, Columbia University, New York, NY, November 2005.

NGO Adoption of Free and Open Source Software. Lecture at What the Hack, Boxtel, Netherlands, July 2005.

The Political Ecology of Media Activism and Computer Hacking. Institute for Social Ecology as part of summer intensive course, "Theoretical Inquiries in the Age of Globalization", Institute for Social Ecology, Plainfield, Vermont, August 2004.

Ethical Volunteerism and Debian. DebConf4, Annual Debian Conference, Porto Alegre, Brazil, May 2004.

Invited Panels and Workshops

The Camera is Everywhere. Panel discussion at Personal Democracy Forum, New York, NY, June 2013.

Information Activism, The 5th Estate: Hacking, Leaking and Investigative Journalism in the Age of Secrecy. Panel talk at Left Forum, New York, NY, June 2013.

Are Geeks the New Guardians of our Civil Liberties? Panel discussion at Free Press, National Conference for Media Reform, Denver, Colorado, April 2013.

Anonymous and the Online Fight for Justice. Panel talk at DEF CON 20, Las Vegas, NV, July 2012.

Everything You Know about Anonymous is Wrong. Panel talk at ROFLCon, MIT, Cambridge, MA, May 2012.

We are all Anonymous: The Culture and Politics of Anonymity online. Panel discussion for Triple Canopy, New York, NY, May 2012.

Anonymous Codes: Disruption, Virality and the Lulz. Panel talk at Transmediale, Berlin, Germany, January 2012.

Anonymous and the Politics of Digital Disarray and Direct Action. Panel talk at Theory and Practice of Social Movement, Center for the Study of Ethnicity and Race, Columbia University, New York, NY, October 2011.

The Aftermaths of Wikileaks. Panel talk at Personal Democracy Forum, New York, NY, June 2011.

Is the Democratizing Potential of Technology Also Fostering Diversity? Panel discussion at National Center for Women in Technology Panel, New York, NY, May 2011.

Democracy and Technology. Panel discussion at Project Pericles Debating for Democracy National Conference. New York, NY, March 2011.

Two Ethical Moments in Debian. Discussion at Colloquium for Innovation Policy, New York University Law School, New York, NY, March 2011.

Anonymous: From Trolling to Digital Activism and Civil Disobedience. Panel talk at

Personal Democracy Forum on Wikileaks, New York University, New York, NY, January 2011.

Cameras Everywhere: Opportunities and Challenges in Human Rights Video. Panel talk with Witness at Open Video Conference, New York, NY, October 2010.

The Ethics of Peer Production (vs. The Ethics of Crowdsourced Labor). Panel talk at 2010 Future of News and Civic Media Conference, MIT, Cambridge, MA, June 2010.

Trolling! Lightning Talk at The New Everyday Unconference. Visual Culture Working Group, New York University, New York, NY, October, 2009.

#fsck Purity: Lessons about the Politics and Pleasures of Free Software. Panel talk at The Internet as Factory and Playground Conference, New School, New York, NY, November 2009.

Upgrade! NY: Free as in What? Panel debate on freedom and openness among F/OSS developers, Upgrade NY Open Source Series, Eyebeam, New York, NY, October 2009.

Anthropological Musings on the Politics of F/OSS. Pre-circulated essay for Free Culture Research Workshop, Berkman Center for Internet and Society, Harvard Law School, Cambridge, MA, October 2009.

*Silent Revolutions: The Ironic Rise of Free and Open Source Software and the Making of a Hacker Legal Consciousnes*s. Workshop presentation at Yale, Harvard, and MIT Cyberscholars Meeting, Yale Law School, New Haven, CT, March 2009.

Scaling in Networks. Institute of Network Culture "Wintercamp", On-site Coordinator and Plenary Panel, Institute of Network Cultures, Amsterdam, Netherlands, March 2009.

*Social Networks and the Public Spher*e. Round table presentation and discussion at Social Media and the Commodification of Community Workshop, University of Haifa, Faculty of Law, Haifa, Israel, May 2008.

The View from Computer Hacking: (New) Media Technologies and the (Older) Ethics of Liberalism. Paper presentation at New Trends of Socio-information in East Asia Conference, University of Tokyo, Tokyo, Japan, November 2007.

The Ideology of Medical Progress as a Problem of Political Success. Paper presentation at pre-conference workshop for Eugenics and Sterilization in Alberta: 35 Years Later, University of Alberta, Edmonton, Alberta, April 2007.

*At the Center and Margins of the Liberal Tradition: How Hacker Political Protest Led to the Stabilization of Free Speech Principle*s. Workshop presentation at Law and Science Workshop Series hosted by Program in Law, Jurisprudence, and Social Thought, Amherst College, Amherst, MA, February 2007.

The Poetics of Hacking: Humor and Liberal Selfhood. Lecture at Debconf6, Annual Debian Conference, Oaxtepec, Mexico, May 2006.

Codes of Value: Hacker Pragmatics, Poetics, and Selfhood. Presentation on pre-circulated paper at Con/texts of Invention: A Working Conference of the Society for Critical Exchange, Case Western University, Cleveland, OH, April 2006.

Silent Revolutions: How F/OSS Came to Challenge Neoliberal Trends in Intellectual Property Law. Presentation on pre-circulated paper at Globalizing Informatics, University of Indiana, Bloomington, IN, March 2006.

Three Ethical Moments in Debian: Enculturation, Legal Pedagogy, and Crisis. Presentation on pre-circulated paper at Information Society Project Speaker Series, Yale Law School, New Haven, CT, November 2005.

Ethics and Politics of Information Technology. Participant in anthropology workshop on new information technologies, Rice University, Houston, TX, May 2004.

*Every Rope Ghat Two Ends: The Caribbean Meeting Grounds of Internet Relay Cha*t. Paper presentation at Digital Genres Initiative, University of Chicago, Chicago, IL, May 2003.

Conference Presentations (refereed unless otherwise noted)

The Aphorisms of Anonymous. Talk at American Anthropological Association Meetings, San Francisco, CA, November 2011.

The Ethnographers Cunning: The Return of Arm Chair and Keyboard Anthropology (while 'hard chatting' on IRC). Talk at American Anthropological Association Meetings, Montreal, Quebec, November 2011.

STS 2.0: Taking the Canon Digital. Round table Discussion at Social Studies of Science Conference (4S), Cleveland, OH, November 2011. *not refereed.

The Troll as Liberal Trickster. Talk at American Anthropological Association Meetings, New Orleans, LA, November 2010.

In Lulz We Trust. Talk at European Association of Social Anthropology Conference, Maynooth University, Maynooth, Ireland, August 2010.

Battle Star Galactica: Hacker Battles on the Internet and the Limits of Liberal Tolerance. Talk at American Anthropological Association Meetings, San Francisco, CA, November 2008.

From Psychiatric Survivors to the Icarus Project and the Importance of a Radical Politics of (Shifting) Continuity. Paper presentation at Cultural Studies Association Meetings, New York, NY, May 2008.

The Hacker Conference Examined: How the Modern Day Conference Acts as the Ritual Underside of Virtual Publics. Talk at American Anthropological Association Meetings, Washington, DC, November 2007.

Battle Star Galactica: Hacker Battles on the Internet and the Limits of Liberal Tolerance. Paper presentation at Association of American Law Schools, Washington, DC, January 2007.

Psychiatric Survivors and the Survival of a Radical Politics of Freedom. Talk at Social Studies of Science Conference (4S),Vancouver, British Columbia , November 2006.

Crisis, Ethics, and Trust in Virtuality. Talk at American Anthropological Association meetings, Washington, DC, November 2005.

Realizing Freedom: The Culture of Liberalism and Hacker Ethical Practice. Talk at Social Studies of Science Conference (4S),Paris, France, August 2004.

An Army of Amateur Legal Scholars: How Free and Open Source Software Developers Have Come to Habituate an Ethos for Expressive Rights. Talk at Social Studies of Science Conference (4S), Paris, France, August 2004.

The Re-localization of Intellectual Property Rights and the Rise of Expressive Rights among Free and Open Source Software Hackers. Talk at Law and Society Conference, Chicago, IL, April 2004.

The Political Agnosticism of Free Software and the Politics of Contrast. Talk at American Anthropological Association Meetings, Chicago, IL, November 2003.

The (copylefted) Source Code for the Ethical Production of Information Freedom. Talk at Social Studies of Science Conference (4S), Milwaukee, WI, November 2001.

*High-Tech Guilds in the Era of Global Capita*l. Talk at American Anthropological Association Metings as part of invited session: Work as Mission: Silicon Valley and Beyond, San Francisco, CA, November 2000.

The Reconceptualization of Class, Ethnicity, and Race through Kali Mai Healing Practices. Talk at Central States American Anthropological Society Meetings, Chicago, IL, April 1998.

Teaching Experience (graduate seminars noted with an asterisk)

McGill University

Hacker Culture and Politics. Seminar, fall 2012.*

Scientific and Technological Controversies. Lecture, fall 2012.

New York University

Introduction to Human Culture and Communication. Seminar, fall 2011, fall 2007- 2009 (Course Faculty Director).

Media Theory, Masters Core Class. Seminar, fall 2011.*

Hacker Culture and Politics. Seminar, spring 2010 and fall 2008.

Technology, the Body, and Society. Seminar, spring 2009.

Politics of Digital Media: Piracy and the Commons. Seminar, spring 2009.*

Proposal Writing. Seminar, fall 2009.*

Topics in Digital Media. Seminar, spring 2008.*

Impacts of Technology. Seminar, fall 2007.

University of Chicago

Hacker Culture and Politics. Seminar, summer 2002 and winter 2005.

Introduction to Medical Anthropology. Seminar, summer 2002.

Student and Postdoctoral Fellowship Advising

McGill University

Supervisor

Alessandro Delfanti, Postdoctoral Fellow (Incoming, Media@McGill, 2013-2014).

Stéphane Couture, Postdoctoral Fellow (Incoming, FQRSC, 2013-2015).

Molly Sauter, Ph.D. (Incoming, winner of Tomlinson Arts Graduate Fellowship).

Matthew Goerzen, M.A. (Incoming).

Visiting Ph.D. Students

Kai Denker, Technische Universität Darmstadt, Darmstadt, Germany (winter and summer 2012).

Thiago Falcao, Federal University of Bahia, Salvador, Brazil (spring and summer 2012).

New York University

Committee Member (Current)

Patrick Davison, Department of Media, Culture, and Communication. "Networked Memes", Ph.D. Proposal.

Committee Chair (Past)

Renee S. Heininger, Department of Media, Culture, and Communication. "Digital Defense: Integrating New Media in the Fight Against Street Harassment", B.A. Thesis, 2009.

Charlottte Horton, Department of Media, Culture, and Communication. "The Politics of Graffitti", B.A. Thesis, 2009.

Mike Goren, Department of Media, Culture, and Communication. "Assessing Tradeoffs in the New Networked Economy", M.A. Thesis, 2008.

Zachary Sehy, Department of Media, Culture, and Communication. "Internet Access and

Regulation", M.A. Thesis, 2008.

Guy Dickinson, Department of Media, Culture, and Communication. "Hacker Representations in the Media", B.A. Thesis, 2008.

Hannah Martin, Department of Media, Culture, and Communication. "A Doctor-Patient Narrative", B.A. Thesis, 2008.

Committee Member (Past)

Alice Marwick, Department of Media, Culture, and Communication. "Becoming Elite: Social Status in Web 2.0 Cultures", Ph.D. Thesis, 2010.

Joseph Reagle, Department of Media, Culture, and Communication. "In Good Faith: The Collaborative Culture of Wikipedia", Ph.D. Thesis, 2008.

Benjamin "Mako" Hill, MIT Media Lab. "Parallel Document Management", M.A. Thesis, 2007.

Academic and Professional Service

McGill University

University Service

Academic Program Director of the Bachelor of Arts and Science Joint Undergraduate Program, March 2012-present.

Department Service

Graduate Admissions Committee Member, Art History and Communication Studies, September 2013-present.

Co-Coordinator, Art History and Communication Studies Speaker Series, April 2012-present.

Other University and Department Service

Co-organizer, Research Forum Meetings (with Matthew Hunter).
Lunch forum for graduate students, postdoctoral fellows, visitors, and sessionals for the informal exchange of ideas, ongoing research, and methodological issues, Fall 2012-current.

Undergraduate Entrance Scholarship Review Process. Review undergraduate applications for scholarship awards, March 2013.

External Examiner for Tyler Braun, Department of Art History and Communication Studies. "Priming the Senses: The Yes men and the Affective Character of Disruption", M.A. Thesis, February 2013.

External Examiner for Gretchen King, Department of Art History and Communication Studies. "The radical pedagogy of community radio and the case of Radio al-Balad: community radio news audiences and political change in Jordan", Ph.D. Proposal Defense,

February 2013.

External Examiner for Hannah Renee Mcelgunn, Department of Art History and Communication Studies. "The Discursive (Re}production and Transformation of Social Life at the General Assembly", Department of Art History and Communication Studies. M.A. Thesis Defense, April 2012.

Pro-Dean for Armen Khatchadouria, Department of Pharmacology and Therapeutics, Faculty of Medicine. Ph.D. Thesis Exam, January 2013.

Presentation on Hackers at Soup and Science, September 2012.

Panel Presentation at Symposium on Free Expression and Peaceful Assembly, May 2012.

Wolfe Chair Fellowship
Responsible for coordinating the call for fellowships, reading applications, and determining winners, April 2012-current.

New York University

Department Service

Member, Study Committee, Department of Media, Culture, and Communication, September 2009-May 2010.

Member, Undergraduate Committee, Department of Media, Culture, and Communication, September 2009-May 2010.

Member, Job Search Committee, Department of Media, Culture, and Communication, September 2009-March 2009.

Chair, Technical Committee, Department of Media, Culture, and Communication, September 2007-2009.

Member, Technical Committee, Steinhardt School of Culture, Education, and Human Development, December 2007-present.

Professional Service

Grant Reviews:

National Science Foundation [US] (2012)
Social Sciences and Humanities Research Council, Insight [CA] (2012)
Independent Social Research Foundation Early Career Fellowship [UK] (2013)

Journal Reviews*:*
(2006-2012)

American Anthropologist (2*); Journal of Cultural Economy* (1); *Ethnos* (*1); American Journal of Sociology (1); Science Studies* (1); *Human Organization* (1); *Americas Conference on Information Systems (AMCIS)* (1); *Anthropological Quarterly* (2); *Social Text* (7); *Cultural Anthropology (2); New Media and Society* (4); *Qualitative Sociology* (1);

Games and Culture (2); *Radical History Review* (1)*; International Journal of Communication* (1); *Grey Room* (4)*; Fiberculture* (1).

Book Manuscript Reviews:
(2010-2012)

MIT Press Book Manuscript (1); MIT Press Book Proposal (2); Pluto Press Book Manuscript (1); University of California Press Book Manuscript (1).

Other Service:

Tenure Evaluation Letter, Berkeley University, October 2012.

Editorial Board, Grey Room, August 2012-present.

Collective Member, Social Text, August 2010-present.

Co-organizer, *The Craft in Craftiness,* Panel at American Anthropological Association Annual Meetings (with Graham Jones, MIT Anthropology), Montreal, Quebec, November 2011.

Advisory Board, The Guardian Project (human rights organization that provides privacy applications for cell phones), April 2012-present.

Social Science Advisory Board, National Center for Women in Information Technology, May 2011-present.

Advisory Board, The Politics of Digital Culture book series, Institute for Distributed Creativity (Series Editor: Trebor Scholz), January 2011-present.

Advisory Board, Expertise book series, Cornell University Press (Series Editor: Dominic Boyer), November 2010-2012.

Discussant for *The Dark Side Of Legitimate Peripheral Participation,* Panel at American Anthropological Association Annual Meetings, New Orleans, LA, November 2010.

Co-organizer and Chair, *Exploring Digital Liberalism*, Panel at American Anthropological Association Annual Meetings (with Dominic Boyer, Rice University, Department of Anthropology), New Orleans, LA, November 2010.

Organizing Team Member, DebConf10, Annual Debian Conference, Columbia University, New York, NY, July-August 2010.

Program Committee, Free Culture Research Conference, May 2010.

Web Committee Member, *Social Text Journal,* June 2009-present.

Program Committee Member, The Politics of Open Source Conference hosted by Journal of Information Technology & Politics, University of Massachusetts, Amherst, MA, April 2010.

Co-organizer, *Contested Illnesses: Ambivalence and Advocacy in the Age of Technology*, Panel at Social Studies of Science Conference (4S) Annual Meetings (with Chloe Silverman, Penn State, Science, Technology, and Society Program, and Alex Choby, UCSF/Berkeley,

Anthropology), Vancouver, British Columbia, October 2006.

Team Member, What Sorts of People Should There Be Network. (Organizer: Rob Wilson, Department of Philosophy, University of Alberta), September 2006-2008.

Organizer, *Science, Technology, Society, and the State*.Graduate student-run workshop, University of Chicago, October 2004-June 2005.

Co-organizer, *Culture's Open Sources*, Panel at American Anthropological Association Meetings (with Chris Kelty, Rice University, Department of Anthropology), Chicago, IL, November 2003.

Board Member, Online Policy Group, a nonprofit organization dedicated to online policy research, outreach, and action on issues such as access, privacy, and digital defamation. December 2001-June 2003.

Volunteer Coordinator Intern, Electronic Frontier Foundation, a non-profit organization that protects civil liberties related to the Internet and technology. August 2001-December 2002.

Professional Memberships

American Anthropological Association
Social Studies of Science

Media and Public Appearances

Featured (web and print publications)

Q&A: Hacker Culture, Coding, and Free Speech – *Communications of the ACM*, 15 April 2013.
http://cacm.acm.org/news/163461-qa-hacker-culture-coding-and-free-speech/fulltext

Dissecting the Frog – *The New Inquiry*, 8 April 2013.
http://thenewinquiry.com/essays/dissecting-the-frog/

Hacking the World - An anthropologist in the midst of a geek insurgency –
The Chronicle of Higher Education, 1 April 2013.
http://chronicle.com/article/Hacking-the-World/138163/

E. Gabriella Coleman - Coding Freedom: The Ethics and Aesthetics of Hacking – *Neural,* 19 March 2013.
http://www.neural.it/art/2013/03/e_gabriella_coleman_coding_fre.phtml

Gabriella Coleman Knows Anonymous' Deepest, Darkest Secrets – *Huffington Post*, 27 February 2013.
http://www.huffingtonpost.com/2013/02/27/gabriella-coleman-anonymous_n_2663775.html

An anthropologist explains how hackers are changing the definition of freedom – *io9*, 25 January 2013.
http://io9.com/5978863/an-anthropologist-explains-how-hackers-are-changing-the-definition-of-freedom

Want to understand open source? Live with its developers – *Open Source.com*, 9 January 2013.
http://opensource.com/life/13/1/want-understand-open-source-live-its-developers

Author Gabriella Coleman Expands on the Role of Linux in Hacker Culture – *Linux.com,* 17 December 2012.
https://www.linux.com/news/featured-blogs/185-jennifer-cloer/682035-author-gabriella-coleman-expands-on-role-of-linux-in-hacker-culture

Top 5 influential security IT thinkers – *SC Magazine*, 3 December 2012.
http://www.scmagazine.com/anthropologist-focused-on-hacker-culture/article/269263/

La Professoressa Che Sussura Agli Hacker – *Corriere Della Sera*, 29 November 2012.
http://www.corriere.it/tecnologia/12_novembre_29/la-prof-che-ha-vissuto-tre-anni-con-gli-hacker_f3a28bf2-3a40-11e2-8e20-34fd72ebaa93.shtml

Geek Researcher Spends Three Years Living with Hackers (Interview with Robert McMillan) – *Wired*, 28 November 2012.
http://www.wired.com/wiredenterprise/2012/11/coleman/

Gabriella Coleman: Helping Hackers Infiltrate Academia – *Fast Company,* 21 June 2012.
http://www.fastcompany.com/1841040/gabriella-coleman-helping-hackers-infiltrate-academia

Digital Activism From Anonymous to Occupy Wall Street: a Conversation With Gabriella Coleman – *Death and Taxes Magazine*, 13 March 2012.
http://www.deathandtaxesmag.com/157192/digital-activism-from-anonymous-to-occupy-wall-street-a-conversation-with-gabriella-coleman/

Mr. Washington Goes To Anonymous – *The Atlantic*, 9 December 2011.
http://www.theatlantic.com/technology/archive/2011/12/mr-washington-goes-to-anonymous/249791/

The Academics of Anonymous – *Washington Post*, 12 December 2011.
http://www.washingtonpost.com/blogs/innovations/post/the-academics-of-anonymous/2011/12/11/gIQA1F8jpO_blog.html

Mr. Washington Goes To Anonymous – *The Atlantic*, 9 December 2011.
http://www.theatlantic.com/technology/archive/2011/12/mr-washington-goes-to-anonymous/249791/

TV and Film

Future Radicals – Television Documentary, Australia, *Renegade Films*, November 2012.

We are Legion: The Story of the Hacktivists [consultant and featured] – Feature Film, *Luminant Media*, November 2012.

http://wearelegionthedocumentary.com/

CNN Presents: Amber Lyon Profiles 'Anonymous' – *CNN*, 14-15 January 2012.
http://cnnpressroom.blogs.cnn.com/2012/01/13/cnn-presents-amber-lyon-profiles-anonymous/

Gabriella Coleman on Open Source Culture and the Newsroom, On Tracking Anonymous, What WikiLeaks Means for the News – *The Future Journalism Project*, June 2012.
http://tumblr.thefjp.org/search/gabriella+coleman

Brian Lehrer Live with Gabriella Coleman – *CUNY TV,* November 2011.
http://www.frequency.com/video/brian-lehrer-live-with-gabriella-coleman/2944993

The revolution will not be firewalled: Gabriella Coleman on the 'hacktivist' underground – *PBS*, 22 July 2011.
http://www.pbs.org/wnet/need-to-know/tag/gabriella-coleman/

Brian Lehrer Live with Gabriella Coleman – *CUNY TV,* November 2011.
http://www.frequency.com/video/brian-lehrer-live-with-gabriella-coleman/2944993
Cyberativismo – *MTV Brazil,* 30 June 2011.
http://mtv.uol.com.br/programas/mod/blog?categoria=cyberativismo

Wer Ist Anonymous – *DCTP TV,* Germany, 19 May 2011.
http://www.dctp.tv/#/republica-2011/wer-ist-anonymus-gabriella-coleman/

Radio and Podcasts

Hacktivists: Heroes Or, Well, Hacks? – *Tell Me More, NPR*, 13 June 2013.
http://www.npr.org/templates/story/story.php?storyId=191316143

Gabriella Coleman on "Coding Freedom: The Ethics and Aesthetics of Hacking" – *To the Best of Our Knowledge, Wisconsin Public Radio,* 12 May 2013.
http://www.ttbook.org/book/gabriella-coleman-coding-freedom-ethics-and-aesthetics-hacking

Anonymous activist network – *Q*, *CBC Radio*, 22 April 2013.
http://www.cbc.ca/player/Radio/Q/ID/2381091978/

Pranks and Tricksters – *Future Tense*, *ABC*, 3 February 2013.
http://www.abc.net.au/radionational/programs/futuretense/pranks-and-tricksters/4489512

Ethical Hacking: Should good intentions get special protection from prosecution? – *The Current, CBC*, 17 January 2013.
http://www.cbc.ca/player/News/Canada/Audio/ID/2326497183/?page=12&sort=MostPopular

Gabriella Coleman on Anonymous – *Office Hours*, *The Society Pages*, 14 January 2013.
http://thesocietypages.org/officehours/2013/01/14/gabriella-coleman-on-anonymous/

Gabriella Coleman on the ethics of free software – *Surprisingly Free,* 8 January 2013.
http://surprisinglyfree.com/2013/01/08/gabriella-coleman-2/

Living with Hackers – *Word of Mouth*, *New Hampshire Public Radio*, 6 December 2012.
http://www.nhpr.org/post/living-hackers

The Hackers – *The Documentary*, *BBC*, 1 January 2013.
http://www.bbc.co.uk/programmes/p012gp95

A Modest Proposal: Recruit The Hackers – *The Story*, *American Public Media*, 26 July 2012.
http://www.thestory.org/stories/2012-07/modest-proposal-recruit-hackers

Word Watch: Hacker – *On The Media*, 13 April 2012.
http://www.onthemedia.org/2012/apr/13/word-watch-hacker

Gabriella Coleman on Anonymous and LulzSec – *Surprisingly Free*, 13 March 2012.
http://surprisinglyfree.com/2012/03/13/gabriella-coleman/

Gabriella Coleman on Anonymous – *Spark*, *CBC*, 13 March 2012.
http://www.cbc.ca/spark/2012/03/full-interview-gabriella-coleman-on-anonymous/

Feature Guest: Gabriella Coleman – *Nine To Noon*, *Radio New Zealand*, 20 February 2012.
http://www.radionz.co.nz/national/programmes/ninetonoon/audio/2510447/feature-guest-gabriella-coleman

2/8/12: Anonymous – *Radio West, KUER*, 7 February 2012.
http://www.kuer.org/post/2812-anonymous

The Many Moods of Anonymous – *On The Media*, 4 March 2011.
http://www.onthemedia.org/2011/mar/04/the-many-moods-of-anonymous/transcript/

All You Have to do is Ask (TMI Wikileaks Special) – *Too Much Information*, *WMFU*, 22 January 2011.
http://tmi.wfmu.org/all-you-have-to-do-is-ask-tmi-wikileaks-special/

TCLP 2011-01-12 Interview: Gabriella Coleman – *The Command Line*, 12 January 2011.
http://thecommandline.net/2011/01/12/gabriella_coleman/

Rise of the Hacktivist – *Day 6, CBC Radio*, 10 December 2010.
http://www.cbc.ca/day6/blog/arts/2010/12/10/episode-14/

A Look Inside The World Of Hackers – *Here and Now, NPR Boston*, 30 November 2010.
http://hereandnow.wbur.org/2010/11/30/hackers

Trolling 101 – *Search Engine*, *TVO*, 27 July 2010.
http://searchengine.tvo.org/blog/search-engine/audio-podcast-51-trolling-101

Full Interview - Gabriella Coleman on Digital Book Piracy – *Spark, CBC*, 26 November 2009.
http://www.cbc.ca/spark/full-interviews/2009/11/26/full-interview-gabriella-coleman-on-digital-book-piracy/

The Quest for a Free Culture – *Radio Berkman*, Harvard University, 29 October 2009.
http://blogs.law.harvard.edu/mediaberkman/2009/10/29/radio-berkman-135/

Mad Movement Strategies: Gabriella Coleman – *Madness Radio*, 2 February 2009.
http://www.madnessradio.net/madness-radio-mad-movement-strategies-gabriella-coleman

Cited (based on interviews unless otherwise noted)

The Geeks Who Leak – *Time Magazine*, 24 June 2013.
http://www.time.com/time/magazine/article/0,9171,2145506-1,00.html

"When Americans understand, they become outraged" – *Salon,* 11 June 2013.
http://www.salon.com/2013/06/11/when_americans_understand_they_become_outraged

Aspiring Hackers Find It's Easy to Be Anonymous – *Wall Street Journal, Risk and Compliance,* 5 June 2013.
http://blogs.wsj.com/riskandcompliance/2013/06/05/aspiring-hackers-find-its-easy-to-be-anonymous/

Attention Rapists: You've Met Your Match – *Glamour Magazine*, 1 June 2013.
http://www.glamour.com/inspired/2013/06/attention-rapists-youve-met-your-match

Exclusive: Meet the Woman Who Kicked Off Anonymous' Anti-Rape Operations – *Mother Jones,* 13 May 2103.
http://www.motherjones.com/politics/2013/05/anonymous-rape-steubenville-rehtaeh-parsons-oprollredroll-opjustice4rehtaeh?page=1

How Anonymous have become digital culture's protest heroes – *The Guardian*, 15 April 2013.
http://www.guardian.co.uk/commentisfree/2013/apr/15/anonymous-digital-culture-protest

Rehtaeh Parsons, Amanda Todd, Steubenville: Anonymous is here to stay – *The Star*, 12 April 2013.
http://www.thestar.com/news/world/2013/04/12/rehtaeh_parsons_amanda_todd_steubenville_anonymous_is_here_to_stay.html

Will Anonymous' involvement in Rehtaeh Parsons case do more harm than good? – *Global News*, 12 April 2013.
http://globalnews.ca/news/476129/will-anonymous-involvement-in-rehtaeh-parsons-case-do-more-harm-than-good/

Montreal artists get a financial kick out of crowd funding – *CBC*, 22 February 2013.
http://www.cbc.ca/news/arts/story/2013/02/22/crowdfunding-artists-buzkashi-boys-oscars-kickstarter-montreal.html

Women In Tech: 5 Analysts To Watch – *Huffington Post*, 12 February 2013.
http://www.huffingtonpost.com/2013/02/12/women-analysts_n_2546172.html

When the government approves of hacking – *Salon*, 25 January 2013.
http://www.salon.com/2013/01/25when_the_government_approves_of_hacking/

Hacktivist anger over US government's 'ludicrous' cyber crackdown – *The Guardian,* 24

January 2013.
http://www.guardian.co.uk/technology/2013/jan/24/hacking-us-government-cyber-crackdown

Digital evangelists versus the predigital thinkers – *The Toronto Star,* 19 January 2013.
http://www.thestar.com/news/world/article/1317500--digital-evangelists-versus-the-predigital-thinkers

Beyond Aaron Swartz: We Don't Need Martyrs … But Changes – *Wired,* 16 January 2013.
http://www.wired.com/opinion/2013/01/beyond-aaron-swartz-we-dont-need-martyrs-but-changes/

The Japanese cat that holds the clues to an internet prankster – *The Guardian*, 9 January 2013.
http://www.guardian.co.uk/commentisfree/2013/jan/09/japanese-cat-clues-internet-prankster-hackers

Anonymous a threat to critical infrastructure? Expert says no – *Vancouver Sun, Canada.com, Calgary Herald Report,* 21 December 2012.

Peyton Engel

Education

JD — University of Wisconsin Law School, *Magna Cum Laude* (December, 2011), Order of the Coif
Top 4% of class, 3.73 GPA, Dean's Academic Achievement Award
State Bar of WI and UW Law School Highest Achievement in Contracts I §3, Fall 2007
State Bar of WI and UW Law School Best Performance in Property §2, Spring 2008
UW Law School Top Grade in Torts I §4, Fall 2008
UW Law School Best Performance in Civil Procedure II §2, Fall 2011
Tutor for MLI sections of Contracts I (Fall 2008) and Property (Spring 2009)

MA — Russian Literature, University of Wisconsin – Madison, 1992.

BA — Russian, Grinnell College, 1990 (includes a semester at the Moscow Energy Institute)

Bar Admission Certifications — Wisconsin (Member No. 1087902); Member, Dane County Bar Association
$(ISC)^2$ CISSP (2007) and CSSLP (2009) #119476, LexisNexis Certifications: Basic (2008), Advanced (2009), Westlaw Advanced Certifications: Case Law Research, Statutory Research, and Secondary Sources Research (2009); Wisconsin State Public Defender Trial Skills Academy (2013)

Experience

2012 — Axley Brynelson, LLP: *Consulting and Forensic Expert*
Reviewed evidence including EnCase data and raw parsing of Internet Explorer history files, prepared a report, assisted with strategy for direct and cross examination, and testified in a criminal trial resulting in acquittal.

2011 (Summer) — Hurley, Burish & Stanton, SC: *Intern*
Assisted with discovery, research, and *Franks* motion briefing in a federal criminal case.

2010 (Summer) — Wisconsin Court of Appeals, Third District: *Judicial Intern*
Researched legal issues and prepared drafts of opinions in both civil and criminal matters. Analyzed no-merit briefs and responses, including rejected no-merit filings.

1997 – present — Berbee Information Networks Corporation and CDW Technologies Inc.: *Systems Engineer, Security Engineer, Technical Architect*
Lead a team of engineers specializing in computer security consultation, penetration testing, incident response, and forensics. Develop tools and service offerings; present research and briefings. Provide strategic security and compliance guidance.

1995 – 1997 — University of Wisconsin – Madison, Learning Support Services: *Network Services Coordinator*
Performed system administration and troubleshooting, managed network infrastructure components, created dynamic web content, and trained staff in the use of office productivity software.

2869 Richardson Street, Fitchburg, WI 53711
✉ peyton.engel@gmail.com ☎ 608.277.8128

1988 – 1995 GRINNELL COLLEGE and UNIVERSITY OF WISCONSIN – MADISON: *Research Assistant, Teaching Assistant, Grader*
Taught Russian language, assisted in faculty research resulting in peer-reviewed publications, graded Russian literature exams, maintained a library dedicated to the works of Pushkin.

SKILLS

BUSINESS DEVELOPMENT	Presenting nuanced service offerings to clients, explaining their value, earning client trust by persuasively differentiating competitor services, cultivating and managing a complex book of business.
CONSULTATION	Working with clients at all levels of technical expertise to gather requirements, designing solutions, managing projects, presenting findings, and recommending options.
MANAGEMENT	Leading a team of as many as ten engineers, developing project methodologies and services offerings, negotiating with customers to secure business, supervising engagements, and hiring new team members.
DOCUMENTATION	Writing for a wide variety of audiences: project proposals, marketing materials, whitepapers, technical assessment reports, and legal memoranda.
PRESENTATION	Speaking at nationally recognized conferences including DefCon (2004, 2006, 2011), USENIX/LISA (invited speaker 2003, 2005), and ToorCon (2002, 2005). Producing and delivering security training including a specialized course curriculum for software developers.
PROGRAMMING	Win32, C/C++, perl, InstallScript, Visual Basic, PHP, and UNIX shell scripting; security analysis of custom-written applications, including code review.

SELECTED PUBLICATIONS

- Daniel H. Kaiser & Peyton Engel, *Time- and Age-Awareness in Early Modern Russia*, Comparative Studies in Society and History 35:4 (October 1993), 822-39.
- Peyton Engel, *What Does This Risk Mean to Me?* Technology First–Dayton, Part 1: (May 2007) 11, 19; Part 2: (July 2007) 12, 19.

REFERENCES AND WRITING SAMPLE AVAILABLE ON REQUEST.

2869 RICHARDSON STREET, FITCHBURG, WI 53711
✉ PEYTON.ENGEL@GMAIL.COM ☎ 608.277.8128

Dan Hirsch

Rue Notre Dame du Sommeil 24
1000 Brussels
✉ *thequux@thequux.com*
http://github.com/thequux

Computer and Programming Experience

- Experience designing application-specific microcontroller boards
- Comfortable writing and debugging Linux USB drivers and embedded firmware
- Production of user-mode and kernel-mode drivers for both Linux and my hobby OS
- Fluency in low-level programming with Assembly, C, C++, and Go
- Creation of small Linux environments for specialized purposes, such as driver testing and net booting for installs
- Database performance optimization with PostgreSQL
- Usage of Common Lisp, Perl, Python, PHP for rapid development
- Troubleshooting software issues using tracing and monitoring tools.
- Creation of distributable desktop programs using C#, Java
- Development of web applications using JavaScript, jQuery, and CherryPy
- Programming user interfaces using GTK+, CLIM
- Experience with version control using CVS, SVN, Bazaar, Mercurial, and Git
- Proficiency in programming and administrating Linux/POSIX and .NET CLR environments
- Construction of build systems using Make and GNU LD scripts

Employment Experience

2010–2011 **Site Reliability Engineer**, *Google, Inc.*, Mountain View, CA.
Worked with a team of eight people to run a low-latency, highly available planet-scale storage system for petabytes of data. Debugged production issues including fiber cuts, misbehaving clients, heavy resource contention, and hardware failure. Participated in weekly on-call rotation, with an SLA requiring a five-minute response time. Helped internal clients get started using our service. Led project to automate deployment of new versions of our service across dozens of clusters; reduced SRE time spent on weekly pushes by 90%. Supported Cellbots project in 20% time. Assisted with design of the "IOIO" I/O board for Android.

2009–2010 **Co-founder**, *Flippity.com*, Los Angeles, CA.
Wrote and optimized backend for Craigslist and eBay search site using Python and PostgreSQL. Wrote core of distributed scraping tool using a Java applet with a Python server component. Implemented the use of Gerrit for code reviews.

2009 **System Administrator**, *Law Firm of Moreno, Becerra, and Casillas*, Los Angeles, CA.
Maintenance and operation of a network of two Windows servers serving twenty Windows clients as sole systems administrator, with responsibility for all network services, including Exchange and Active Directory. Resolved various systems issues such as Android clients being unable to fetch email; implemented Postini email filtering.

2008 **Systems Administration Intern**, *Google, Inc.*, Santa Monica, CA.
Debugged workaround in kernel for NFS group count limitation using KDB. Helped develop on-disk format for the TUX3 fourth- generation Linux file system. Suggested and investigated switching to GIT for internal version-control. Debugged Kerberos/LDAP integration on Google's corporate WAN.

2007–2008 **Laboratory Assistant III**, *Network Research Lab, University of California*, Los Angeles, CA, Network Research Laboratory.
Wrote kernel-mode drivers for specialized video coding hardware on a custom ST40-based board running embedded Linux for an industry-funded project seeking to develop a peer-to-peer streaming video system similar to BitTorrent.

2006–2007 **Intern**, *Northrop Grumman Corporation, Space & Technology Sector*, Los Angeles, CA.
Worked on design and implementation of a reliability calculation software package for internal use. Wrote tool to allow remote dialing of Cisco VOIP telephones from Microsoft Outlook 2003. Compared derating and Digital IC/Hybrid part specifications.

Personal Projects

2010–Present **Co-developer of GoodFET**.
Implemented Atmel AVR target support. Added support for certain subfamilies of Microchip PIC24F chips. Designed and evaluated new board design based on TI Stellaris LM3S3739 microprocessor. Designed new board variant based on TI MSP430F5510 microcontroller; reduced cost by 50% and component count by 10%.

2007–2010 **System Administrator for UCLA Linux Users' Group**.
Administered two servers for the UCLA LUG, with responsibility for email, web, shell, network authentication, server configuration, and administration procedures. Implemented Kerberos authentication. Initiated documentation of system design and operating procedures.

Fall 2008 **Tutorials for UCLA CS152B – Digital Logic Design Lab**.
Created a pair of tutorials for developing hardware systems on the Digilent XUPV2P Virtex 2 Pro evaluation board, covering interfacing custom hardware with the built-in PowerPC 405 processor cores and interfacing with the onboard AC'97 audio codec. These tutorials are currently used by the UCLA Computer Science Department as course instruction materials.

Fall 2008 **Postscript extensions for programming use**.
Used PostScript reflection to add several higher-order functions to the language, including function currying, composition, Factor-style `cleave`, `keep`, and `bi` operators. Also developed sample unit testing framework. Presented demo as a technical talk to the Southern California Functional Programmers group in November, 2008.

2006–2007 **Xenon OS – An Original X86 Protected-Mode Kernel**.
Developed a partial protected-mode kernel that handles basic memory management, keyboard, basic disk, and PCI bus access, and supports both Cirrus Logic CL-5446 and VMware built-in framebuffer devices to display high-resolution text and graphics. Makes limited use of APM.

Miscellaneous Hacks and Small-Scale Projects

- Monad tutorial for OCaml
- Testing framework for Prolog
- Tool for plotting filesystem fragmentation
- libusb-1.0 bindings for Go
- MSP430 BSLv2 client in Go
- EWMH strut support for xbattbar
- Generic constraint-satisfaction problem solver using C and Python with pluggable search strategies in Haskell

Project Team Experience

2005–2006 **Terra Engineering**, Autonomous vehicle designed and built for the 2005 DARPA Grand Challenge.
Wrote code to parse the DARPA-provided "Route Definition Data File." Worked on obstacle tracking and mapping module and Athena sensor support. Developed various stereo vision algorithms. Fixed LIDAR issues, including incorrect documentation and driver bugs. Rewrote monitor to use GTK+ toolkit, improving flexibility. Wrote a variety of system monitoring/management and data processing scripts.

Winter 2005 **Project Grant Proposal**, Research Proposal for Microsoft's External Research Digital Inclusion Program.
Researched feasibility and prior art for the design and implementation of a small IDE on the Pocket PC platform for submission with Dr. Massoud Ghyam.

2002–2003 **Palos Verdes Road Warriors**, Autonomous vehicle modified from SUV for 2003 DARPA Grand Challenge.
Worked with a software tool called "RVCad" to find optimal parameters and filters for preprocessing an image for input to a road-finding algorithm. Wrote test code to get the vehicle control actuators to work; this test code became a simple closed-loop speed control system. Also wrote init scripts to automatically start the custom servers. Debugged LIDAR and GPS systems.

Education

2006–2009 **University of California, Los Angeles**, *B.S. in EE and CS (unfinished)*, Los Angeles, CA, Completed 143 units toward Bachelor of Science degrees in Electrical Engineering and Computer Science.
Coursework included:
Computer Science 111 Operating System Principles
Computer Science 131 Programming Languages
Computer Science 132 Compilers
Computer Science 151 Computer Architecture
Computer Science 152B Advanced Logic Design Lab
Computer Science 180 Algorithms
Computer Science 181 Formal Languages and Automata Theory
Math 113 Combinatorics
Math 199 Variable Topics, Algorithms

2005–2006 **Stanford EPGY**, Distance education offered by Stanford University for college credit.
- Linear Algebra
- Ordinary Differential Equations

2003–2006 **El Camino College**.
Math/engineering coursework included:
Computer Science 1 Problem Solving and Program Design in C++
Computer Science 2 Data Structures
Math 210 Discrete Structures
Math 220 Multi-Variable Calculus

2002–2006 **Palos Verdes Peninsula High School**, *High School Diploma*.

Matthew D. Green

Curriculum Vitae

Contact

3800 N. Charles Street, 209 Maryland Hall, Baltimore, MD 21218
Phone: 410-861-0344 Fax: 928-223-2296
mgreen@cs.jhu.edu

http://www.spar.isi.jhu.edu/∼mgreen

Education

Ph.D., Computer Science, November 2008
Johns Hopkins University
Baltimore, MD
Thesis: *Cryptography for Secure and Private Databases: Enabling Practical Data Access without Compromising Privacy*
Advisor: Prof. Susan R. Hohenberger

M.S., Computer Science, December 2005
Johns Hopkins University
Baltimore, MD

B.A., Computer Science, May 1998
Oberlin College
Oberlin, OH

B. Mus., Technology in Music and Related Arts, May 1998
Oberlin Conservatory of Music
Oberlin, OH

Research Interests

Cryptography and computer security.

Employment

9/2010–present — Assistant Research Professor
Johns Hopkins University
Baltimore, MD

11/2012–present — Research Associate (Adjunct)
University of Maryland
College Park, MD

2/2005–9/2011 — CTO
Independent Security Evaluators
Baltimore, MD

6/1999–6/2003 — Senior Technical Staff Member
AT&T Labs/Research
Florham Park, NJ

Research Publications

Conference Papers

Ian Miers, Christina Garman, Matthew Green, and Avi Rubin. Zerocoin: Anonymous Distributed e-Cash from Bitcoin. In *IEEE Symposium on Security and Privacy (Oakland) 2013*, May 2013.

Joseph A. Akinyele, Matthew Green, Susan Hohenberger, and Matthew W. Pagano. Machine-generated algorithms, proofs and software for the batch verification of digital signature schemes. In *Proceedings of the 2012 ACM conference on Computer and communications security*, CCS '12, pages 474–487, New York, NY, USA, 2012. ACM.

David Cash, Matthew Green, and Susan Hohenberger. New definitions and separations for circular security. In *Public Key Cryptography (PKC '12)*. Springer, 2012.

J. A. Akinyele, M. W. Pagano, M. Green, C. Lehmann, Z. Peterson, and A. Rubin. Securing electronic medical records using attribute-based encryption on mobile devices. In *1st ACM CCS-SPSM*, 2011.

Matthew Green, Susan Hohenberger, and Brent Waters. Outsourcing the decryption of abe ciphertexts. In *Proceedings of the 20th USENIX conference on Security*, SEC'11, pages 34–34, Berkeley, CA, USA, 2011. USENIX Association.

Matthew D. Green and Aviel D. Rubin. A research roadmap for healthcare IT security inspired by the PCAST health information technology report. In *Proceedings of the 2nd USENIX conference on Health security and privacy*, HealthSec '11, Berkeley, CA, USA, 2011. USENIX Association.

Matthew Green and Susan Hohenberger. Oblivious transfer from simple assumptions. In *Theory of Cryptography Conference (TCC '11)*. Springer, 2011.

Matthew Green. Secure blind decryption. In *14th International Conference on Practice and Theory of Public Key Cryptography (PKC '11)*. Springer, 2011.

Jae Hyun Ahn, Matthew Green, and Susan Hohenberger. Synchronized aggregate signatures. In *ACM Conference on Computer and Communications Security (CCS '10)*. ACM Press, 2010.

Anna Lisa Ferrara, Matthew Green, Susan Hohenberger, and Michael Østergaard Pedersen. Practical short signature batch verification. In *Proceedings of the The Cryptographers' Track at the RSA Conference 2009: CT-RSA 2009*, volume 5473 of LNCS, pages 309–324. Springer, 2009.

Scott Coull, Matthew Green, and Susan Hohenberger. Controlling access to an oblivious database using stateful anonymous credentials. In *Proceedings of the 12^{th} International Conference on Practice and Theory in Public Key Cryptography: PKC 2009*, volume 5443 of LNCS, pages 501–520. Springer, 2009.

Matthew Green and Susan Hohenberger. Universally composable adaptive oblivious transfer. In *Proceedings of the 14^{th} International Conference on the Theory and Application of Cryptology and Information Security: ASIACRYPT '08*, volume 5350 of LNCS. Springer, 2008.

Matthew Green and Susan Hohenberger. Blind identity-based encryption and simulatable oblivious transfer. In *Proceedings of the 13^{th} International Conference on the Theory and Application of Cryptology and Information Security: ASIACRYPT '07*, volume 4833 of LNCS, pages 265–282. Springer, 2007.

Matthew Green and Giuseppe Ateniese. Identity-based proxy re-encryption. In *Proceedings of the 5^{th} International Conference on Applied Cryptography and Network Security: ACNS '07*, volume 4521 of LNCS, pages 288–306, 2007.

Stephen Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel Rubin, and Michael Szydlo. Security analysis of a cryptographically-enabled RFID device. In *Proceedings of USENIX Security '05*. USENIX Association, 2005. **Winner of Best Student Paper Award.**

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *The* 12^{th} *Annual Network and Distributed System Security Symposium: NDSS '05*. The Internet Society, 2005.

Andrea Basso, Charles D. Cranor, Raman Gopalakrishnan, Matthew Green, Charles R. Kalmanek, David Shur, Sandeep Sibal, Cormac J. Sreenan, and Jacobus E. van der Merwe. PRISM, an IP-based architecture for broadband access to TV and other streaming media. In *IEEE International Workshop on Network and Operating System Support for Digital Audio and Video*, 2000.

Journal Papers

Scott Coull, Matthew Green, and Susan Hohenberger. Controlling access to an oblivious database using stateful anonymous credentials. *ACM Transactions on Information and System Security (TISSEC) — To appear*, 2011.

Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green. Security through legality. *Commun. ACM*, 49(6):41–43, 2006.

Giuseppe Ateniese, Kevin Fu, Matthew Green, and Susan Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. *ACM Transactions on Information and System Security (TISSEC)*, 9(1), February 2006.

Charles D. Cranor, Matthew Green, Chuck Kalmanek, David Shur, Sandeep Sibal, Jacobus E. Van der Merwe, and Cormac J. Sreenan. Enhanced streaming services in a content distribution network. *IEEE Internet Computing*, 05(4):66–75, 2001.

Patents

- "Method and apparatus for limiting access to sensitive data", U.S. Patent 7840795 (Issue date Nov 10, 2010).
- "Method for content-aware redirection and content renaming", U.S. Patent 6954456 (Issue date Oct 11, 2005)

Grants

Co-PI, National Science Foundation award CNS-1010928, "Self Protecting Electronic Medical Records". Amount: $1,733,881.

Co-PI, DARPA PROgramming Computation on EncryptEd Data (PROCEED). Amount: $344,000.

Senior Personnel, Department of Health and Human Services Strategic Healthcare Information Technology Advanced Research Projects on Security (SHARPS), Research Focus Area: Security of Health Information Technology. Amount: $1,600,399.

Teaching

650.445 (600.454). PRACTICAL CRYPTOGRAPHIC SYSTEMS (Spring 2009, 2010, 2011). In this course I examine the issues surrounding the design and evaluation of industrial cryptographic products, and the ways that these systems fail in practice.

650.445 (600.454). PRACTICAL CRYPTOGRAPHIC SYSTEMS (Spring 2009, 2010, 2011). In this course I examine the issues surrounding the design and evaluation of industrial cryptographic products, and the ways that these systems fail in practice.

Awards

- 'Award for Outstanding Research in Privacy Enhancing Technologies (PET award), 2007.
- Usenix Security, 2005. Best Student Paper. "Security analysis of a cryptographically-enabled RFID device" (9/15/2005).

Program Committees

Usenix Security 2013. Committee chair: Sam King.

Usenix Security 2012. Committee chair: Tadayoshi Kohno.

Usenix Security 2011. Committee chair: David Wagner.

The Fifth International Conference on Provable Security **ProvSec 2011.**

The 12th International Conference on Information Security and Cryptology **ICISC 2009.**

The Third International Conference on Pairing-based Cryptography **Pairing 2009.**

Electronic Commerce and Web Technologies, Security Track **EC-Web 2009.**

Software Projects

Charm. A Python framework for rapidly prototyping cryptosystems.

The Functional Encryption Library (libfenc). A C implementation of several functional encryption and Attribute-Based Encryption schemes.

The JHU/MIT Proxy Re-cryptography Library (PRL). A prototype C++ implementation of several proxy re-encryption schemes.

Litigation Experience

Experience as a Testifying Expert

Videotron Ltee, Videotron (Regional) Ltee and CF Cable TV inc. vs Bell ExpressVu Limited Partnership (Quebec Superior Court No 500-17-027275-059)

Group TVA inc. vs. Bell ExpressVu Limited Partnership (Quebec Superior Court No. 500-17- 018324-031, 500-17-022586-047, 500-17-027276-057)

Deposition Experience

Keith Dunbar vs Google, Inc. US District Court for the Eastern District of Texas, Civil Action N 5:10CV00194

SmartPhone v. HTC., US District Court for the Eastern District of Texas, Civil Action # 6:10-cv-580

Patent and Source Code Analysis

Symbol Technologies, Inc. Et al. v. Aruba Networks, Inc., Case # 07-519-JJFF

DataSci LLC vs. Medidata Solutions, Inc, Case # 09-cv-01611-MJG

TecSec Inc vs. International Business Machines Corporation, Case # 1:10-CV 115 LMB/TCB

The PACid Group, LLC v. 2Wire, Inc., Brother Industries, Ltd., et al., Case # 6:08-cv-00498

SmartPhone v. HTC., US District Court for the Eastern District of Texas, Civil Action # 6:10-cv-580

SmartPhone v. Apple., US District Court for the Eastern District of Texas, Civil Action # 6:10-cv-00074-LED-JDL

Criminal Cases

US v. Hanjuan Jin 08-CR-192

Press Appearances

John Schwartz. Graduate cryptographers unlock code of 'thiefproof' car key. The New York Times (National Edition), January 2005.

Hackers can crack car-key codes. Consumer Reports, July 2007.

Researchers: We cracked car alarm system. USA Today, January 2005.

Samuel Greengard. 6 common IT security mistakes and how to avoid them. Microsoft UK Security Centre.

April 11, 2013

Dan Kaminsky
dan@doxpara.com
@dakami

SUMMARY

Dan Kaminsky has been a noted security researcher for over a decade, and has spent his career advising Fortune 500 companies such as Cisco, Avaya, and Microsoft. Dan spent three years working with Microsoft on their Vista, Server 2008, and Windows 7 releases.

Dan is best known for his work finding a critical flaw in the Internet's Domain Name System (DNS), and for leading what became the largest synchronized fix to the Internet's infrastructure of all time. Of the seven Recovery Key Shareholders who possess the ability to restore the DNS root keys, Dan is the American representative. Dan is presently developing systems to reduce the cost and complexity of securing critical infrastructure.

SELECTED PRESENTATIONS

- **"Introducing the Domain Key Infrastructure"** Black Hat USA 2010 – Las Vegas, NV
  Zero Configuration DNSSEC Serving, End-To-End Client Integration w/ UI Via OpenSSL and Secure Proxies, Federated OpenSSH, DNS over HTTP/X.509, Self-Securing URLs, Secure Scalable Email (Finally!)
- **Interpolique** The Next HOPE 2010 – New York, NY
  Where's The Safety in Type Safety?, Preventing Injection Attacks (XSS/SQL) With String Safety, Why Ease Of Use Matters, Automatic Query Parameterization, How LISP Was Right About Dynamic Scope, Dynamic DOM Manipulation For Secure Integration of Untrusted HTML
- **Realism in Web Defense** CONFidence 2010 – Krakow, Poland
  Why Security Fails, What's Wrong With Session Management On The Web, The Failure Of Referrer Checking, Interpreter Suicide, Towards a Real Session Context, Treelocking, The Beginnings of Interpolique
- **Staring Into the Abyss** CanSecWest 2009 – Vancouver, BC
  Middleware Fingerprinting, Firewall Rule Bypass, Internal Address Disclosure, Same Origin Attacks Against Proxied Hosts, TCP NAT2NAT via Active FTP And TCP Spoofing
- **Black Ops of PKI** Chaos Communications Congress 2009 (26c3) – Berlin, Germany
  Structural Weaknesses of X.509, Architectural Advantages of DNSSEC, ASN.1 Confusion, Null Terminator Attacks Against Certificates
- **It's the End of the Cache As We Know It** Black Hat USA 2008 – Las Vegas, NV
  DNS Server+Client Cache Poisoning, Issues with SSL, Breaking "Forgot My Password" Systems, Attacking Autoupdaters and Unhardened Parsers, Rerouting Internal Traffic
- **Ad Injection Gone Wild** ToorCon 2008 – Seattle, WA
  Subdomain NXDOMAIN injection for Universal Cross Site Scripting
- **Design Reviewing the Web** Black Hat USA 2007 – Las Vegas, NV
  DNS Rebinding, VPN to the Browser, Provider Hostility Detection, Audio CAPTCHA Analysis
- **Weaponizing Noam Chomsky, or Hacking with Pattern Languages** ShmooCon 2007 – Washington, DC
  The Nymic Domain, XML Trees For Automatically Extracted Grammar, Syntax Highlighting for Compression Depth, Live Discovered Grammar Rendering, "CFG9000" Context Free Grammar Fuzzer, Dotplots for Format Identification and Fuzzer Guidance, Tilt Shift Dotplots, Visual Bindiff

- **Pattern Recognition** Black Hat USA 2006 – Las Vegas, NV
  Net Neutrality Violation Detection, Large Scale SSL Scanning, Securing Online Banking, Cryptomnemonics, Context Free Grammar Fuzzing, Security Dotplots
- **Black Ops of TCP/IP 2005.5** Black Hat Japan 2005 – Tokyo, JP
  Worldwide DNS Scans, Temporal IDS Evasion, the Sony Rootkit, MD5 Conflation of Web Pages
- **MD5 To Be Considered Harmful Someday** Chaos Communications Congress 2004 – Berlin, Germany
  Applied Attacks Against Simple Collisions Via Malicious Appendage, Executable Confusion, Auditor Bypass, Bit Commitment Shirking, HMAC Implications, Collision Steganography, P2P Attacks Against Kazaa Hash
- **Black Ops of DNS** Black Hat USA 2004 – Las Vegas, NV
  Tunneling Audio, Video, and SSH over DNS
- **Stack Black Ops** Black Hat Federal 2003 – Washington, DC
  Generic ActiveX, SQL for Large Network Scans, Bandwidth Brokering, SSL for IDS's
- **Black Ops of TCP/IP** Black Hat USA 2002 – Las Vegas, NV
  High Speed Scanning, Parasitic Traceroute, TCP NAT2NAT
- **Gateway Cryptography** Defcon 9 2001 – Las Vegas, NV
  SSH Dynamic Forwarding, Securing Meet-In-The-Middle, PPTP over SSH

Samuel Liles
College of Technology
Purdue University
401 North Grant Street
West Lafayette, IN 47906

Phone (765) 496-2274
sam@selil.com
www.selil.com

Education – *Completed a doctorate in technology and masters and bachelors degrees in computer science*

Purdue University: West Lafayette, Indiana April 2005 to May 2012, PhD College of Technology (Digital Forensics), Dissertation Title: "*Cyber warfare as a form of conflict: Evaluation of models of cyber conflict as a prototype to conceptual analysis*", Advisor: Marcus Rogers

Colorado Technical University: Colorado Springs, Colorado July 1998 to February 1999, MSCS Software Systems Engineering

Huron University: Huron, South Dakota December 1997 to August 1998, BS Computer Science

Certifications

- Current DoD clearance
- Certified Information Systems Security Professional (CISSP), *April 2010*
- Sun Microsystems Workgroup and Enterprise GSP Certification*, August 2003*
- Colorado Technical University Certification in C++, *March 1999*

Experience – *Over 20 Years of increasing professional responsibility and experience serving and consulting as a trusted adviser to major corporate and government leadership in information security topics, over 10 years in research and higher education.*

Purdue University: Associate Professor August 2012 to Present

Activity: Serve as a tenured associate professor in the area of digital forensics and information security, focusing on live system and network based cyberforensics and cyberforensic tool development including curriculum and facilities development. Mentor and guide graduate student research and laboratory environment. Participate in both undergraduate and graduate education assignments.

Technology: Blackboard, Moodle, Forensic Took Kit, Encase, Blacklight, Autopsy, Sleuthkit, Pro Discover, Apple OSX, Apple iOS, Microsoft Windows (XP, 7, 8), Linux Red Hat, BackTrak 5.X, IdaPro

National Defense University: Associate Professor March 2011 to July 2012

Activity: Serve as a recognized expert and professor of systems management, and contribute expertise in information operations, computer network operations, computer network defense, information assurance, cybersecurity, cyberterrorism, and cyberwar. Experience encompasses the systems/network security technical and management disciplines required to ensure the security of information systems used in the federal government; including cryptography, access control, threat analysis and vulnerability assessment.

Technology: Host Based Security System, Industrial Control Systems, RedEye, Apple OSX, Apple iOS, Linux Red Hat, BackTrak 5.X

Purdue University Calumet: Associate Professor August 2003 to March 2011

Promoted from Assistant to Associate August 2008.

Activity: Held primary responsibility for the creation and delivery of information technology and security curriculum that is taught at a distance and in the classroom. Served as the lead instructor on all networking, operating system, and security courses within the department. Maintained and fostered the growth and experience of a cadre of masters degree seeking graduate students.

Technology: Blackboard, WebCT, Vista, Cisco IOS, Pix Firewalls, Cisco Routers, Cisco Switches, HP Switches, Enterasys Switches, Cisco Wireless Access Points, Microsoft Enterprise Servers (2000, 2003, etc,), Microsoft Clients (2000, XP, Vista), ProDiscover,

Samuel Liles
College of Technology
Purdue University
401 North Grant Street
West Lafayette, IN 47906

Phone (765) 496-2274
sam@selil.com
www.selil.com

Forensic Tool Kit, Java, C++, Netbeans, Visual Studio, Source Safe, Subversion, Apple OSX, Apple iOS, Linux, BackTrak 4.x to 5.x

NCR Corporation: Senior Consultant 1 – August 2000 to August 2003

Activity: Led efforts towards extensive system integration tasks on various information technology projects. Provided consulting and knowledge of SNMP traffic, firewalls, security, help desk, systems, and project management as required to customer executives and technical experts. Provided leadership and responsibility for entire architectural review prior to implementation on customer project sites. Supported any engineering activities for project enhancements internationally. Developed and wrote white papers setting project scope and methods for internal and external executives.

Technology: SNMP, RMON, Cisco IOS, Microsoft (NT, 2000, 2003, XP, etc.), Visual Studio, Source Safe, Solaris (5, 6, 7), Oracle, MySql, PostGres, Java, Netbeans, Linux

Access Data Consulting Corporation: Senior Technical Consultant - April 2000 to August 2000

Activity: Provided leadership and served as senior technical consultant providing assistance to other members of the team. Worked closely with the architectural design requirements of a web enhanced application suite. Was responsible for providing documentation and briefing materials for customer executive management. Served a customer base composed of leading e-commerce companies. Developed and implemented help desk processes and procedures for insuring customer satisfaction.

***Technology*:** Microsoft Windows (98, NT, 2000), HTML, JavaScript, Java, C++, Word, Excel, RMON, Source Safe, BugTrak, Oracle, MSSQL

Litton/TASC (Now just TASC): Senior Member Technical Staff – September 1999 to April 2000.

Activity: Managed the release of software, network enhancements, and Source-Safe code library within Department of Defense requirements. Assisted with response to technical queries, consultations with customer, and engineered technical solutions. Provided domain expertise and leadership in developing network solutions, and software engineering of project management software within the Department of Defense context. Procured, maintained, and solved issues dealing with network operating systems and hardware within the Department of Defense customer environment. Led analysis of and suggested response to customer training and solution needs at the customer site. Led and managed timelines, budgets, and project activities of vendors for the Department of Defense customer. Provided leadership and held responsibility for briefing general officers, military staff, and executive civilian staff on various assigned topics.

Technology: Dell server appliances, Microsoft Windows (98, NT, 2000), HTML, JavaScript, ToolBox, C++, Java, ADA, Oracle, MSSQL

MCIWorldcom *(Contracted Services):* Senior Program Manager – February 1999 to September 1999.

Activity: Provided leadership and subject matter expertise for systems analysis on the Y2K project. Provided technical leadership and oversight for executive management. Held primary responsibility for briefing customer executive management on technical solution strategies. Managed the development of migration paths for the known universe of network equipment. Managed a budget of over $60 million and coordinated expense documentation with the financial executive manager. Provided subject matter expertise to management on embedded network systems. Developed requirements analysis documentation for project management software. Briefed senior executive leadership on project milestone successes and issues.

Technology: Microsoft Windows (98, NT, 2000), PERL, C++, Java, ADA, Oracle, MSSQL

Basec.Net: Network Engineer - December 1997 to June 1998

Activity: Managed, implemented, and configured Internet hardware across the

Samuel Liles
College of Technology
Purdue University
401 North Grant Street
West Lafayette, IN 47906

Phone (765) 496-2274
sam@selil.com
www.selil.com

corporate enterprise. Led and developed innovative solutions for federation of customer enterprise networks. Developed and managed corporate billing and helpdesk database. Led team of technical assistance personnel who provided Tier 2 and Tier 3 help desk support. Responsible for briefing management of customer companies on product enhancements and enterprise solutions. Developed and maintained applications and performed webmaster functions developing web pages. Managed and implemented enterprise wide infrastructure enhancements.

Technology: Cisco IOS, Cisco Routers, Cisco Switches, Cisco Bridges, Livingston Portmasters, BSD Unix, Microsoft NT, Windows 95, JavaScript, HTML, C, C++

Law Enforcement and Military Experience – *Seven years experience in law enforcement with various duties and titles, three years military experience transferring from Washington State National Guard to the United States Marine Corps*

Pierce County Sheriff Department: Corrections Officer -August 1989 – December 1993

Special duties performed included court room services to the judges, and legal staff. I managed several special projects where policies were written on staffing, shift rotation, budget synopses, upgrades of phone and data networks, and implementation of computer systems.

Kitsap County Sheriff Department Corrections Officer - October 1987 - August 1989

Managed the technical workings and implementation of upgrades within the Central Control Room where the computerized alarms and surveillance gear resides. I managed the upgrade of several voice and data systems. Implemented new policies from Washington State Crime Information Computer managers, and managed local access to terminals.

United States Marine Corps: September 1984 - October 1986

Military Occupational Specialty- Small Missile Systems Technician

Washington State Army National Guard: June 1983 – August 1983

Military Occupational Specialty- Tank Driver

Publications and Presentations – *Over 20 academic peer reviewed publications, 2 technical editorships, over 15 invited speaker engagements, numerous non-peer reviewed academic publications, numerous mass-market publications, and numerous media appearances.*

Book

Devost, M., Dion, M., Healey, J., Gourley, B., **Liles, S**., Mulvenon, C., Pitts, H., Rattray G., “Addressing Cyber Instability”, Cyber Conflict Studies Association, 2012

Book Chapter

Liles, S., “ A unified generational warfare model”, The Handbook of 5th Generation Warfare, 2010

Liles, S., “The issues of non-state actors and the nation state”, Threats in the Age of Obama, 2009

Liles, S., Kamali, R., “Information Assurance and Security Curriculum Meeting the SIGITE Guidelines”, Handbook of Research on Social and Organizational Liabilities in Information Security; 2008

Journal

Borton, M., **Liles, S**., Liles, S. “Cyberwar Policy”, The John Marshall Journal of Computer & Information Law, Spring 2010, pp 303 - 324

Borton, M., **Liles, S**, “Active defense of corporate information systems”, IO Journal, May 2010

Wozniak, J., **Liles, S**. “Political and technical roadblocks to cyber attack attribution”, IO

Samuel Liles
College of Technology
Purdue University
401 North Grant Street
West Lafayette, IN 47906

Phone (765) 496-2274
sam@selil.com
www.selil.com

Journal, Inaugural Issue, April 2009

Liles, S., A review of Software Forensics by Robert Slade, Journal of Digital Forensic Practice. 2008.

Liles, S., Kamali, R., "An Information Assurance and Security curriculum implementation" The Journal of Issues in Information Systems and Information Technology Volume 3, 2006

Kamali, R., **Liles, S**., Jiang, K., Nicolai, B., "A Curriculum Model Based on the SIGITE Guidelines" Journal of Information Technology Education, Volume 5, 2006.

Amici Curiae

United States v. Ray Andrus, *On Appeal from the United States District Court for the District of Kansas,*" Brief of Amici Curiae Computer Forensics Researchers and Scientists", August 2007

Conference Proceeding

Liles, S., Dietz, J.E., Rogers, M., Larson, D., "Applying traditional military principles to cyber warfare", Fourth Annual International Conference on Cyber Conflict, Cooperative Cyber Defence, Center of Excellence, June 5 – 8, 2012, Talinn Estonia

Uzubell, S., **Liles, S**., Jiang, K., "An Analysis of the Common Body of Knowledge of Software Assurance", SIGITE, October 7 – 9, 2010, Central Michigan University, Midland MI

Liles, S. "Cyberwarfare: A form of low-intensity conflict and insurgency", In proceedings Conference on Cyber Conflict, Cooperative Cyber Defence, Center of Excellence, June 16-18, 2010, Tallinn Estonia

Liles, S., "Cyber warfare compared to fourth and fifth generation warfare as applied to the Internet". In proceedings of International 2007 International Symposium on Technology and Society: Risk, Vulnerability, Uncertainty, Technology and Society, June 1 - 2, 2007, University of Nevada Las Vegas

Rosco, R., Rogers, M. **Liles, S**., "Breaking Down Stereotypes: A Call for an ontological Model". In proceedings of the Hawaii International Conference on System Sciences Hilton Waikoloa Village Waikoloa HI January 3 - 6, 2007

Liles, S., Kamali, R., 2006. "An Information Assurance and Security curriculum implementation". In proceedings of International Informing Science + Information Technology Education joint Conference (Manchester, England, UK, June 25 -28 2006).

Kamali, R., **Liles, S**., Winer, C., Jiang, K., and Nicolai, B. 2005. "An implementation of the SIGITE model curriculum". In Proceedings of the 6th Conference on information Technology Education (Newark, NJ, USA, October 20 - 22, 2005). SIGITE '05. ACM Press, New York, NY.

Liles, S., "A vendor neutral wide area networking course" American Society for Engineering Education 2005 Illinois-Indiana Sectional Conference (Northern Illinois University, DeKalb, Illinois, USA April 1-2, 2005)

Liles, S., "A vendor neutral local area networking course" American Society for Engineering Education 2005 Illinois-Indiana Sectional Conference (Northern Illinois University, DeKalb, Illinois, USA April 1-2, 2005)

Liles, S., "Distance Education II Collaboration With Industry: Utilizing Software To Build Community and Foster Communication", ASEE CIEC 2005, February 24-25, 2005

Technical Editor

Barrett, D., Kipper, G., Virtualization and Forensics: A digital forensic investigator's guide to virtual environments, Syngress 2010

Bolt, S., Xbox Forensics, First Edition, Syngress 2010

Invited Speaker

Speaker – "Cyber security with a global perspective", Pugwash Conference, Purdue

Samuel Liles
College of Technology
Purdue University
401 North Grant Street
West Lafayette, IN 47906

Phone (765) 496-2274
sam@selil.com
www.selil.com

University, April 20, 2013

Speaker – "Cyber as a form of National Power", Institute for World Politics, Center for Culture and Security, Washington DC, November 9, 2012.

Speaker – "Considerations of defense in depth", Dynamic defense workshop, Sandia National Laboratory, September 5th & 6th, 2012, Albuquerque New Mexico

Panel – "Tips and opportunities in graduate school", University Symposium and Open House, Sandia National Laboratory, August 1-2, 2012, Albuquerque New Mexico

Panel – "Military Operations in Cyberspace", Fourth Annual International Conference on Cyber Conflict, Cooperative Cyber Defence, Center of Excellence, June 5 – 8, 2012, Talinn Estonia

Presented – "Cyber Threats" National War College Alumni Meeting, Naples Florida, March 2, 2012

Presented – "Cyber Threats" First Cavalry Alumni Meeting, Springfield Virginia, February 18, 2012

Panelist – "Managing Cyber Risk through Recovery Driven Resiliency", Fort Lesley J. McNair, Washington DC, February 14, 2012

Presented – "Federal Government Privacy Day: Future technology challenges to privacy", Fort Lesley J. McNair, Washington DC, October 15, 2011

Presented – "Cyber Threats", Senior Executive Seminar, John G. Marshall Center, Garmisch Germany, September 8, 2011
http://www.marshallcenter.org/mcpublicweb/en/component/content/article/4-cat-mc-news/944-senior-leaders-discuss-threat-of-cyber-war.html?directory=58

Moderator – "Cyber Security Threats" Spy Museum, Washington, DC, May 18, 2011

Panelist – "Cyber Conflict at the Operational Level", Cyber Conflict Studies Association, Washington DC September 21, 2010

Panelist – "Cyberwarfare and non-state actors", Conference on Cyber Conflict, Cooperative Cyber Defence, Center of Excellence, Tallinn Estonia, June 16-18, 2010

Poster Presentation

Liles, S., Rogers, M., Dietz, J., Larson, D., Raskin, V., "Cyberwarfare as a form of conflict: Evaluation of models of cyber conflict as a prototype to conceptual analysis", CERIAS Research Symposium 2012

Liles, S. "Risk assessment in an information centric world: Threats, vulnerabilities, countermeasures and impacts (a work in progress)", CERIAS Research Symposium 2012

Uzubell, S., **Liles, S**., Jiank, K., "Software Assurance in Academia", SIGITE, October 7 – 9, 2010, Central Michigan University, Midland MI

Bingham N., Dark M., **Liles S**., Mislan R., Rogers M., Rose M., Wedge T., "Digital Forensics Learning Objects", CERIAS Research Symposium 2006

Liles S,, Rogers M,. "Cyber warfare as low intensity conflict", CERIAS Research Symposium 2008.

Technical Publication

Liles, S., Kovacik, S., & O'Day, D. " Proposed Methodology for Victim Android Forensics", Retrieved January 31, 2011 from http://viaforensics.com/?fid=Proposed-Methodology-for-Android-Forensics.pdf, November 2010

Liles, S., Larson, D. "A Gap Analysis for the Indiana Department of Homeland Security District One Law Enforcement", Purdue University Calumet and Indiana Department of Homeland Security District 1, December 2009

Kamali R., **Liles S**., Winer C., "Report on the programs in Computer Information Sciences South Suburban Community College", April 2007

Samuel Liles
College of Technology
Purdue University
401 North Grant Street
West Lafayette, IN 47906

Phone (765) 496-2274
sam@selil.com
www.selil.com

Dark M., **Liles S**., Rose M., Rogers M., "Computer Forensics: Introduction to Computer Forensics Law", Purdue University, West Lafayette, IN, July 2005

Dark M., **Liles S**., Rose M., Rogers M., "Computer Forensics: Computer Forensics Principles", Purdue University, West Lafayette, IN, July 2005

Mass Media Publications

Liles, S., "Riding in the Wet", Wing World Magazine, Phoenix, Gold Wing Road Riders Association, AZ March 1996

Liles, S., "Even In The Cold", Wing World Magazine, Phoenix, Gold Wing Road Riders Association, AZ January 1996

Liles, S., "Tips on Trailering", Motorcycle Tour & Travel Magazine, September 1995

Liles, S., "Naming The Hazards", Wing World Magazine, Phoenix, Gold Wing Road Riders Association, AZ September 1995

Liles, S., "I Don't Get Angry I Get Even!", Wing World Magazine, Gold Wing Road Riders Association, Phoenix, AZ August 1995

Liles, S., "Group Riding Redux", Wing World Magazine, Gold Wing Road Riders Association, Phoenix, AZ July 1995

Liles, S., "Group Riding On Your Big Bike", Wing World Magazine, Gold Wing Road Riders Association, Phoenix, AZ May 1995

Media Appearances

May 15, 2013, Richard Essex, "Companies using smartphone data to track shoppers", WTHR (http://www.wthr.com/story/22265762/companies-using-smartphone-data-to-track-shoppers)

May 14, 2013, Joshua Foust, "The liberal case for drones", Foreign Policy, (http://www.foreignpolicy.com/articles/2013/05/14/a_liberal_case_for_drones?page=full)

April 24, 2013, Kent Erdahl, "Twitter increasing security after hack", FOX59 (http://fox59.com/2013/04/24/twitter-increasing-security-after-hack/#axzz2RQgv4iqi)

February 27, 2012, Bob Segall, **"**Cell phone warning: Deleted personal information often left behind", WTHR (http://www.wthr.com/story/21419450/cell-phone-warning-deleted-personal-information-often-left-behind)

February, 7, 2012, Adam Elkus, "Competition in cyberspace: Responding to the proliferation of information-based weapons", Armed Forces Journal, (http://www.armedforcesjournal.com/2013/01/12842322)

February, 4, 2013, Mark Clayton, "Cybersecurity: how preemptive cyberwar is entering the nation's arsenal" Christian Science Monitor, (http://www.csmonitor.com/USA/Military/2013/0204/Cybersecurity-how-preemptive-cyberwar-is-entering-the-nation-s-arsenal)

November 26, 2012, David McNally, "Cybershopping can have security risks", WTHR Channel 13 Indianapolis, (http://www.wthr.com/story/20190387/cybershopping-can-have-security-risks)

July 2012 Eric Beidel "iCollege Takes Nation's Cybersecurity Leaders back to School", National Defense, (http://www.nationaldefensemagazine.org/archive/2012/July/Pages/iCollegeTakesNation'sCybersecurityLeadersBacktoSchool.aspx)

Shane MacDougall

B. Comp Sci., CRISC, CICP, Two-Time Defcon Black Badge Holder

WORK EXPERIENCE

Intuit Inc, San Diego, CA (June 2012-Current)
Employed as a principal information systems threat analyst, responsible for running the corporate threat intelligence team. Duties include analyzing emerging threats, designing, implementing, and monitoring countermeasure frameworks, and deploying technologies such as honeypots or OSINT tools as needed.

Tactical Intelligence, Nova Scotia, Canada/USA/Mexico: Principal Partner (Feb 2011-Current)
Principal partner at a boutique consultancy, specializing in information gathering, risk assessments, celebrity reputation management, and social engineering engagements. Also run the company's research group, including speaking engagements and creation of white papers and responsible for marketing.

ID Analytics, San Diego, CA – Lead InfoSec Analyst (May 2003-February 2011)

Ran the information security practice for the world's largest anti-identity theft vendor. Network was attacked hundreds of times a day by everyone from organized hacking rings to state actors. The size of our identity database meant that we were regularly targeted both logically and physically (on-site social engineering attacks).

Jefferson Wells Int'l, NY, NY - Senior Information Risk Consultant (August 2000-April 2003)

Employed as a senior consultant, my focus was on performing penetration tests, leading tiger team attacks, social engineering consulting, disaster/business continuity testing, security training. I was the lead penetration tester for the company, and as such was sent to many locations around the country for client engagements and presentations.

Shane MacDougall & Associates, Toronto, Ontario – InfoSec Consultant (January 1994-August 2000)
Owned and operated my own consulting practice in Toronto, Ontario, Canada, specializing in information security, risk management and disaster recovery planning. Also performed "private label" engagements for other security firms.

KPMG, Cleveland, OH – Senior Consultant (January 1993-December 1993)
Employed by KPMG Cleveland as a Senior Consultant. Specialty was computer/telecommunications security and business resumption. Acting sys-admin for defence contractor.

- - -

LDI Disaster Recovery & Consulting, Cleveland, OH – Consultant (March 1992-

December 1992)
Employed as a computer / telecommunications security and business resumption specialist. Duties included penetration testing/red teaming of client facilities and voice/data networks.

- - -

Canadian Pacific: C+C, Toronto, Ontario (May 1990-March 1992)
Employed as computer/telecommunications security specialist. Duties included penetration testing/physical red teaming, programming, and investigations.

- - -

KPMG Peat Marwick Thorne, Toronto, Ontario (April 1989 – May 1990)

Employed as an information security specialist/disaster recovery consultant. Duties included penetration testing/red teaming, disaster planning/business resumption consulting,

- - -

EDUCATION / AWARDS

Winner, Black Badge, Defcon 19 Social Engineering CTF (2011)
Winner, Black Badge, Defcon 20 Social Engineering CTF (2012)
1989 Atlantic Provinces Council on the Sciences (APICS) Student Programming Competition
Education: Bachelor of Computer Science (Dalhousie University, 1989)
Certifications: CRISC (ISACA Risk Assessment), CICP (Core Impact Certified Professional)
Preparing for CISSP Exam

- - -

MOST RECENT MEDIA / SPEAKING ENGAGEMENTS

Author, “Effective Social Engineering and OSINT”, No Starch Press, August 2014

Keynote Speaker, ISSA San Antonio, Quarterly Meeting, May 2013

Panelist, MENA Cyber Defense Summit, Muscat, Oman, March 2013

Black Hat Abu Dhabi, “Truly Effective Social Engineering and Countermeasures”, December 2012

Presenter, ToorCon 2012 – “Truly Effective Social Engineering: A 2012 Redux” and “McAfee Secure, TrustGuard, and TrustMarks – A Hacker’s Best Friend”

ARS Technica (2012) - http://arstechnica.com/security/2012/10/mcafee-trust-guard-certifications-can-make-websites-less-safe/

Toronto Star (2012) - http://www.thestar.com/business/article/1239150--canadian-hacker-dupes-wal-mart-to-win-def-con-prize

CNN (2012) - http://money.cnn.com/2012/08/07/technology/walmart-hack-defcon/index.htm

CNN (2012) - http://cnnmoneytech.tumblr.com/post/28226562845/pro-tips-from-social-engineering-hackers

Presenter, DerbyCon 2012 – "McAfee Secure, TrustGuard, and TrustMarks – A Hacker's Best Friend"

Sophos Naked Security - http://nakedsecurity.sophos.com/2012/08/10/social-engineer-walmart/

Presenter, BSides Las Vegas 2012 – "McAfee Secure, TrustGuard, and TrustMarks – A Hacker's Best Friend"

Information Week - http://www.informationweek.com/global-cio/personnel/how-to-hire-a-hacker/240002918

Black Hat Europe, March 2012, Amsterdam, "Offensive Threat Modeling: Turning The Traditional Threat Model on its Head"

Pen Test Magazine, March 2012, "Social Engineering With Will Tarkington"

Pen Test Magazine, January 2012, "Meet The FBI's Social Engineer"

PenTest Magazine, December 2011, "Effective Social Engineering: Why The Lowest Hanging Fruit Yields a Rotten Crop"

CIO Magazine, November 1, 2011 "Tap the Social Media Stream for Competitors' Secrets http://www.cio.com/article/692945/Tap_the_Social_Media_Stream_for_Competitors_Secrets?page=1&taxonomyId=3119

Processor Magazine, Oct 21, 2011, "Data Center Physical Security" http://www.processor.com/articles//P3321/30p21/30p21.pdf?guid=

Wall Street Journal article on Social Engineering: http://online.wsj.com/article/SB10001424052970203911804576653393584528906.html

PenTest Magazine, October 2011, "The Art (And Necessity) of On-Site Social Engineering Audits" (Note: associate editor as of September 2011)

Channel World, September 21, 2011, "Black Market of Data Theft", http://www.channelworld.in/features/black-market-data-theft?page=2

Speaker, Toorcon 13 (San Diego, CA), October 2011 – Two presentations: "Effective Social Engineering: Why The Lowest Hanging Fruit Yields A Rotten Crop" and "How To Pass Audits With Badly Busted Systems"

Speaker, LASCON (OWASP Austin, TX), October 2011 - "How To Pass Audits With Badly Busted Systems"

Speaker, Bsides Las Vegas 2011 - “How To Pass Audits With Badly Busted Systems”

CIO magazine re: Web Phishing – July 2011 - http://www.cio.in/article/debarati-roy-and-shweta-rao

CBS News re: Twitter Used For Blackmail - www.cbsnews.com/2300-501465_162-10008144-4.html

Dark Reading re: SIEM Meets Business Intelligence – May 31, 2011 - http://www.darkreading.com/security-monitoring/167901086/security/security-management/229700243/siem-meets-business-intelligence.html

Fox News re: Iris Scanners – May 28, 2011 - http://www.foxnews.com/scitech/2011/05/28/iris-scanning-make-borders-secure/?test=faces

PBS Newshour, PC World (3rd Place 2010 Defcon Social Engineering Contest [attack portion]) http://www.pbs.org/newshour/bb/science/july-dec10/cyber_08-12.html

- - -

CONTACT
Email: shane@tacticalintelligence.org
Phone: 619-894-7956 / 619-261-7052

Brian Martin
1767 Pearl St #108
Denver, CO 80203
bmartin@attrition.org

Home: 303-832-9194
Mobile: 303-520-7283

SUMMARY

An industry leading information security and risk management veteran with an extensive knowledge base and international experience. Understands the application of security concepts across a broad scope of information technology areas and industries. Extensive history in network and application penetration testing, security auditing, as well as vulnerability database management. Proven leadership, client influencing, and negotiation skills.

WORK EXPERIENCE

Tenable Network Security, Denver, Colorado — July 2008 - Present
Senior Nessus Analyst
Subject Matter Expert for the Nessus vulnerability scanner and Content Group member. Performed a wide variety of writing including authoring documentation for products, knowledge base articles, and blogs. Provided feedback, quality assurance testing, and feature enhancement requests for Nessus and PVS. Helped monitor and maintain Tenable's public presence via the company blog, discussion forums, and Twitter. Contributed detailed concepts and input for the development of plugins for advanced web application assessments.

BT INS, Denver, Colorado — August 2006 – July 2008
Senior Security Consultant
Senior consultant and practice leader of the Ethical Hacking (EH) group. Performed a wide variety of security assessments focused on web applications, perimeter network, internal network, social engineering, zero knowledge and physical audits. Primary maintainer of EH group documentation for reporting, author of several internal methodologies and senior member of document quality review board.

SELF EMPLOYED, Denver, Colorado — March 2003 – August 2006
Independent Consultant
Performed a variety of subcontracting work for several companies (FuGEN, Delphinus, Wizard's Keys, True North Solutions, META Security, and more) doing network audit, ST&E/C&A evaluation, penetration testing, capacity planning, report review and more. Primary clients include US Government agencies, private banks and commercial entities.

FuGEN TECHNOLOGIES, Rockville, Maryland — September 2002 – March 2003
Senior Network Security Engineer
Primary duties include leading penetration teams, performing ST&E/C&A evaluations and developing tools to support these efforts. Primary clients include National Park Services (NPS) and Bureau of Land Management (BLM).

CACI, Lanham, Maryland — March 2000 – June 2002
Senior Network Security Engineer
Primary duties included leading penetration teams on multiple engagements for private and government sectors. Work included guiding the teams on methodology, product selection, testing methods and more. Primary clients included US Department of Justice and US Bureau of the Census.

SELF EMPLOYED, Phoenix, Arizona December 1998 – February 2000
Independent Consultant
Performed a wide range of security consulting services as an independent contractor. Work included technical editing, security auditing, security article journalism, and penetration testing. Work performed in United States and Japan. Routinely employed by New Dimensions International, Internet Security Institute, and Unitek Inc. as an instructor and designer for computer administration and security courses. Courses taught included Controlled Penetration, 'Hacker Tracker', Operating Systems, Network Security and other classes. Students have included Army Infowar Staff, several NASA labs, National Computer Security Center, Fortune 500 and others.

SELF EMPLOYED, Los Angeles, California March 1999 – May 1999
Independent Consultant
Employed by US Federal Government as technical consultant for the representation of Kevin Mitnick. Duties included examination of over ten gigs of evidence/discovery and sixteen hundred pages of witness testimony to assist the legal team.

Repsec Inc., Phoenix, Arizona March 1998 – December 1998
Senior Security Architect
Employed by RSI as Senior Security Architect in Phoenix, AZ. Duties included all manners of security consulting ranging from policy writing to penetration testing, coordination of security advisory releases with vendors and RSI staff, maintenance of a comprehensive bug/vulnerability database and research for security solutions as well as new vulnerabilities. Acted as POC to software vendors in dealing with newly discovered vulnerabilities.

Trident Data Systems, San Antonio, Texas May 1996 – March 1998
Network Security Engineer
Employed by Trident Data Systems (originally in Colorado) as a network security engineer. Duties included providing security assessment and risk posture analysis for commercial clients, general security consulting, continued upgrading of internal vulnerability database, continued research for new security solutions, guiding Penetration Teams, developing strategies and procedures for penetrations, and developing security policy for Trident and clients. Clients included Fortune 500 companies and US Air Force.

PUBLICATIONS

I have written a wide variety of articles focusing on current security trends and news since 1999. These articles have been published on several sites including linux.com, SecurityFocus, SunWorld, IBM Developer Works, ;Login, Newstrolls, eEye.com, DevX, OSALL, Synthesis, ExGame Magazine, The Register and many others. A full listing of articles is available at http://attrition.org/~jericho/works/writing_security.html.

PRESENTATIONS

- **"Cyberwar: Not What We Were Expecting"** (26 September 2012 - Ghent, Belgium)
  A debunking of the rhetoric and hype that has dominated the topic of cyberwar for years, as well as a foundation of ideas that seem to be lost on the cyberwar 'experts', that effectively broadens the topic and should make everyone reconsider what they think they know about it.
- **"Errata Hits Puberty: 13 Years of Chagrin"** (30 May 2012 - Richmond, VA)
  13 year history of the Errata project, giving a behind-the-scenes look at the nightmare and headaches involved. Both from the project, and from the security industry.
- **"Anonymous 20*20: The Beginning is Near"** (17 April 2012 - Boston, MA)
  Keynote about the hacktivist "group" Anonymous, implications of the group, and possible future direction they could take.
- **"Hacker Court"** (2002, 2003, 2004, 2005, 2006, 2007 - Las Vegas, NV.)
  Mock trials of "hacker" crimes stressing current and evolving issues of computer law.
- "**Everything is Vulnerable**" (5 May 2005 – Vancouver, Canada)
  Overview of vulnerability databases, strengths, weaknesses and why they have not evolved in the last decade.

- **“Multiple Topics”** (20 May 2002 - Manilla, Philippines.)
  Two presentations covering wide a variety of current topics related to security.
- **"Mirror Image"** (12 July 2001 - Blackhat Briefings 2001, Las Vegas, NV.)
  A summary of the two and a half year project of the Attrition Defacement Archive, including detailed statistics on web defacement computer crime.
- **“Plenary Debate: The Hacker Wars”** (1 November 2000 – COMPSEC 2000, London, England)
  Quiz the hackers face-to-face and find out more about the motives and demographics behind hacker attacks.
- **"Reflections on the Attrition Mirror"** (26 July 2000 - Blackhat Briefings 2000, Las Vegas, NV.)
  A summary of the Attrition.org defacement mirror process, parties involved and associated pitfalls.
- **"Current Hacking Trends"** (24 - 25 April 2000, Tokyo, Japan)
  An overview of existing threats and solutions for network security.
- **“Info Protect: Air Force Space Command"** (21 - 25 April 1997 – Peterson AFB)
  The demo included a live penetration of several UNIX systems, concept and theory of new and upcoming attacks, demonstration of Denial of Service attacks, and general Q&A regarding exploitation and vulnerabilities.

In addition, I have participated in a number of panel discussions on a wide range of security topics focused on both technical and sociological issues.

EDUCATION

Texas Tech University, Architecture/Civil Engineering, Attended 1991 - 1992

OTHER RELEVANT EXPERIENCE

Internet Site Development and Maintenance - I currently administrate Attrition.org, a hobby web site operating since October, 1998. The site is known for its past work as a Web Defacement Archive, the precursor to the DatalossDB, and colorful articles about the deficiencies of the computer security industry. The site has received as many as twenty three million hits from over four hundred thousand unique viewers each month.

Open Security Foundation – President and COO of the Open Security Foundation (OSF), a 501(c)(3) not-for-profit formed to empower all types of organizations by providing knowledge and resources so that they may properly detect, protect, and mitigate information security risks. Primary role since December, 2003 has been as the Content Manager to the Open Source Vulnerability Database (OSVDB.org) and concept designer / contributor to the Dataloss Database (datalossdb.org).

CVE Editorial Board Member – Since September, 2009.

University of Dayton Cybercrime Seminar - Honorary Professor, 2003 - 2004

Call-For-Papers (CFP) Reviewer - Review and guide information security conferences on submitted talks. This includes BSidesDFW 2012, BSides Denver 2013, BSides Las Vegas 2013, BSidesATX 2013, RVASec 2012/2013, and DEFCON 21.

C. Thomas

Philadelphia PA, 19123 cthomas@cristhomas.com
617-290-0938

Profile:

Commonly referred to as 'Space Rogue' and widely sought after for unique views and perceptions of the security industry, testified before the Senate Committee on Governmental Affairs and have been quoted in numerous media outlets, have also appeared as an expert on CNN, ABC, PBS and others. Spoke on a wide range of at Blackhat, Defcon, BSides, HOPE, H2K, and others.

Experience:

Trustwave – Chicago IL FEB 2012 to PRESENT
Threat Intelligence Manager
Managed the Threat Intelligence team, produced daily threat bulletins and quarterly reports. Coordinates vulnerability research and responsible disclosure. Spoke on the company's behalf at numerous global events.

SRT Studios - Philadelphia PA MAY 2009 to JUN 2011
Editor in Chief, Hacker News Network
Founder of the Hacker News Network responsible for newsgathering, script writing, filming/editing and producing weekly information security news broadcasts.

Guardent – Waltham, MA JUL 2000 to JAN 2001
Organized and Coordinated the Internet Security Vulnerability Summit

@stake - Cambridge, MA DEC 1999 to JUN 2000
Founder/Research Scientist
Co-founded the Internet Security consultancy @Stake

L0pht Heavy Industries - Watertown, MA OCT 1992 to DEC 1999
Created and release a CD collection of Macintosh security software the Whacked mac Archives. Created and ran the first incarnation of the Hacker News Network reporting on the information security industry.

Peiter “Mudge” Zatko

Google
April 2013 - Present
Advanced Technology and Projects
Performing new research and development, to deliver “breakthrough innovations to the company's product line on seemingly impossible timeframes.”

Defense Advanced Research Projects Agency, Department of Defense
February 2010 – April 2013
Program Manager
In charge of handling proposals and directing the course of research within three major programs of the Department of Defense: Military Networking Protocol (MNP), Cyber Insider Threat (CINDER), and Cyber Fast Track (CFT), the last of which funded more than 92 projects pushing the boundaries of our understanding of computer security. Won the Secretary of Defense Medal for Exceptional Public Service for my work.

BBN Technologies
Division Scientist
February 2004 – February 2010

@Stake
Vice President of Research and Development
2000 - 2002

L0pht Heavy Industries
Founder
1992 - 2000
Responsible for creating one of the most well-known security research teams. Testified before the United States Senate Committee on Governmental Affairs, at their request, on issues of security and the Internet, on May 19, 1998. Wrote L0phtCrack, AntiSniff, and L0phtwatch.