Dalhousie University
Faculty of Computer Science

CSCI 4192 Report 2:
Legal Risk in Computer Security Research in Canada

Author:
Mike Doherty
doherty@cs.dal.ca

Produced for:
Kirstie Hawkey
hawkey@cs.dal.ca
Directed studies supervisor

Prepared in partial fulfillment of the requirements of the Computer Science Directed Studies program.

December 10, 2013

Contents

1 Introduction

In the first paper for this research project, "Problematic Computer Crime Law in Canada" [3], I described four areas of law that affect computer security researchers: the criminal offences "mischief in relation to data" and "unauthorized use of computer"; the security and encryption research exceptions in copyright law; and the cyberbullying law in Nova Scotia. In this paper, I try to translate the cases of Andrew Auernheimer and Aaron Swartz into the Canadian legal context. Both cases illustrate how the law might be applied to real-world cases, and illustrate the legal risk involved in computer security research.

The hypothetical cases should serve to illustrate that while successful defences to computer crime charges can be made for security researchers and other technologists who might be targeted for prosecution, this occurs late in the process. A defence can only be mounted during a trial, and the dearth of precedent makes this a risky proposition.

This legal risk has the potential to chill security research, while public policy should be encouraging it. As computers become ubiquitous, and expand into new realms of our lives, we will need more and better security research. There are critical questions of computer security in burgeoning areas like e-voting, healthcare records, medical devices, and self-driving cars. Each of these presents unique challenges which researchers might be disinclined to pursue if the legal risk in doing so is not addressed.

The history of such cases in Canada is promising, however. I've been unable to find legal cases targeting computer security researchers improperly, in stark contrast to the recent record in the US. Hamed Al-Kabaz was expelled from Dawson College's computer science program for "professional misconduct", and was threatened with police involvement, but was never charged [8]. Other cases have involved extradition to the US, as with the case of Peter Alfred-Adekeye,

whose extradition was blocked by a Canadian court [14]. While these are troubling, they are not criminal cases, and the US record is worse.

There are likely many factors at work here. First, the critical difference between the American and Canadian legal landscapes is that the US Computer Fraud and Abuse Act (CFAA) is a hybrid civil/criminal statute. This means that private parties may bring civil cases which argue for broad readings of the CFAA. If precedent is set, then it can apply to criminal CFAA cases as well. By contrast, only the Crown can bring cases in Canada. Prosecutors in the US have been aggressive in several prosecutions, including the Swartz and Auernheimer cases discussed in this paper.

In Canada, neither the police nor the Crown seem to have a focus on pursuing "hackers" (the other term for disfavoured computer security researchers) aggressively. Instead, they seem more interested in busting child pornography rings [17] and serious organized crime than exploiting public fears about "hackers" and "cybercriminals"—an attitude which the US has enshrined in law. The USA PATRIOT ACT [12] deals with terrorists and hackers side-by-side, while Canada's stance has been much more restrained.

Instead of attempting to separate bad actors, as the law does now, it should identify the specific conduct that is criminalized. In particular, what constitutes unauthorized access. Until the law changes, the risk to security researchers and other technologists will remain real, constrained mainly by the reluctance of police and prosecutors to investigate and bring cases. I provide some practical advice for computer security researchers for mitigating risk as early in the research process as possible at the end of the paper.

2 Translating US prosecutions into Canada

2.1 Andrew Auernheimer

2.1.1 Case summary[1]

Andrew Auernheimer—known online as "weev"—worked with Daniel Spitler to discover a security hole in one of AT&T's websites. AT&T had configured their website so that when new iPad owners came to register, the email address AT&T already had on file would be pre-filled in the registration form. But Auernheimer and Spitler discovered that there was no authentication mechanism protecting those email addresses. Any request to AT&T's system using the iPad user agent string and requesting a URL like `https://dcp2.att.com/OEPClient/openPage?ICCID=X&IMEI=0` where X is an ICCID number for which AT&T had an email address on file would get a response from the AT&T server which included the email address.

Spitler wrote a program which downloaded thousands of pages, incrementing the ICCID value each time, to obtain approximately $100,000$ email addresses. Auernheimer told journalists about the vulnerability in AT&T's website, and disclosed the list of email addresses as proof. AT&T fixed the information leak when the story received national attention, then convinced the FBI to investigate.

Spitler and Auernheimer were charged with CFAA violations. Spitler pled guilty and testified against Auernheimer, who was convicted and is currently serving a 41-month prison sentence while his case is appealed, with amicus briefs filed by the Standford Center for Internet and Society, the Mozilla Foundation and a slew of computer scientists and privacy experts, and the Berkman Center for Internet and Society's Digital Media Law project.

[1] This account is based on work from [3], which drew from [7, 5, 13, 23].

In Canada, this might be prosecuted under either of the two principal computer crime offences: mischief in relation to data, or unauthorized use of computer. I will consider these charges in turn.

2.1.2 Mischief in relation to data

Mischief in relation to data is an independent offence under s. 430(1.1), but it also forms part of the unauthorized use of computer offence under s. 342(1)(c). I will consider these two applications together.

Mischief in relation to data may seem like it applies straightforwardly to unauthorized obtaining of information like this. However, the statute enumerates four acts which are mischief, and none of them cover "stealing" or wrongfully obtaining data.

In *R. v. Alexander* [4], the Crown alleged that Nadine Alexander had obtained unauthorized use of a computer with intent to committing the offence of mischief in relation to data when she stole credit cards passing through the mail system. The Court considered whether the indictment alleged a crime known to law—that is, whether stealing credit cards was mischief in relation to data, which could then be used as part of an unauthorized use of computer charge:

> [G]iven that stealing is not one of the ways to commit mischief specified in s. 430(1.1), does the charge, as drafted, disclose an offence known to law?

The court ultimately declined to address the question, because it decided that Nadine Alexander had not stolen the credit cards as a matter of law (merely looking at confidential data is not theft under the law). Since there was no stealing, the court didn't need to definitively resolve the question of whether theft of data is mischief in relation to data. Justice Ducharme did, however, give a preview of what courts in future cases might consider before breaking off the analysis:

> [64] The question here is whether the charge, as drafted, does properly incorporate an offence under section 430. Certainly, the application of the *maxim expressio unius, exclusivio alterius*[a] to s. 430 (1.1) does suggest that Parliament, in enumerating various ways in which mischief to data can be committed, did not mean to include the stealing of data as a form of mischief to data. On the other hand, this is a highly technical area and it seems at least possible that if data, or some part thereof, was "stolen", this same act could possibly alter the data [s. 430(1.1)(a)]; render it meaningless, useless or ineffective [s. 430(1.1)(a)]; or obstruct, interrupt or interfere with its lawful use [s. 430(1.1)(c) and (d)]. Therefore, it would be unwise to attempt to resolve this issue without the assistance of expert evidence with respect to computer data. Fortunately, given my conclusion that there is no evidence that the applicant stole data, I need not resolve whether the charge, as drafted, does create a valid offence.
>
> [a] "expressing one thing excludes another"

The court is suggesting that theft does *not* constitute the offence of mischief in relation to data unless it affected the data in one of the ways enumerated in the statute. In the Auernheimer case, the data was stolen, but the stealing did not alter the data; render it meaningless, useless, or ineffective; or obstruct, interrupt, or interfere with its lawful use. If this reasoning were applied by a Canadian court to Auernheimer's case, I think the stealing of the email addresses would not be considered an offence under s. 430(1.1), and thus cannot form part of a charge under s. 342.1(1)(c).

2.1.3 Unauthorized use of computer

The other 3 provisions of the unauthorized use of computer offence are unrelated to mischief in relation to data, so I consider them separately here.

s. 342.1(1) defines the essential elements of the offence. The conduct must be both fraudulent and without colour of right, and the accused must obtain computer service; or intercept some function of a computer system; or use, possess, traffic in, or permit another person to have access to a computer password which would allow them to commit the offence of unauthorized use of computer.

The two-prong "fraudulent and without colour of right" test will be the focus of this analysis.

Auernheimer's conduct may have been fraudulent. *Essentials of Canadian Law: Computer Law* [22] explains the meaning of "fraudulently":

> "Fraudulently" means dishonestly and unscrupulously, and with the intent to cause deprivation to another person.

US prosecutors argued, and Canadian prosecutors likely would argue as well, that Auernheimer's conduct was dishonest and unscrupulous. The argument is that it was dishonest because "He lied to the AT&T servers in order to get the information" [10], even though user agent strings are not taken to be true representations of fact, and are not intended used for security authentication[2]. Most web browsers "lie" about what software they are, and have done for decades. This is a normal part of the functioning of the internet. Prosecutors might argue the conduct was unscrupulous because Auernheimer bragged about "hacking" AT&T's systems, or wanted to gain noteriety off the discovery, or because he went to the press with proof of the vulnerability.

Accepting that Auernheimer's conduct was dishonest and unscrupulous (which the court is likely to do, given Auernheimer's abrasive character and past conduct), the question of whether Auernheimer's conduct deprived another would decide the "fraudulent" half of the two-prong test. Auernheimer did not intent to deprive AT&T or their customers of the email addresses themselves. However, the kind of deprivation required to show fraudulent intent includes concepts such as liberty and security of the person. In this context, prosecutors would argue that this includes privacy, and that Auernheimer intended to deprive AT&T customers of their privacy by obtaining and then revealing their

[2] "[The user agent string] is for statistical purposes, the tracing of protocol violations, and automated recognition of user agents for the sake of tailoring responses to avoid particular user agent limitations." [9]

email addresses. Counterarguments might include the fact that Auernheimer only disclosed the email addresses to the press as proof of the vulnerability, and this was done to pressure AT&T into fixing the security flaw, not to violate the customers' privacy; or that since Auernheimer had no other identifying information, the email addresses were not private information. The definition of "private information" in the Personal Information Protection and Electronic Documents Act (PIPEDA) bolsters the latter argument: "'personal information' means information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization" [11]. Without any other information, a database of e-mail addresses might not be considered personal information. PIPEDA would also apply to AT&T's security breach, which might offer Auernheimer some protection, since he would argue that it is AT&T that is in the wrong.

2.1.4 Disposition of the case

If Auernheimer had been tried under Canadian jurisdiction, the Crown would likely have attempted to charge him with unauthorized use of computer under s. 342.1(1)(a), (c), or (d). As well, the Crown would likely have pursued a separate offence of mischief in relation to data under s. 430(1.1), and a charge of unauthorized use of computer with intent to commit mischief in relation to data under s. 342.1(c) (which relies on s. 430(1.1) again). In each case, I think there are compelling arguments which could result in an acquittal.

For the independent mischief in relation to data charge, merely obtaining information is not an enumerated way that mischief can be committed, so the allegations don't disclose an offence known to law, and nobody can be convicted on such a charge.

If the charge of unauthorized use of computer is under section (a)—obtaining computer service—then it should fail on the "fraudulent and without colour of

right" test. If it was under section (c)—with intent to commit mischief in relation to data—it fails twice: once as with the other unauthorized use of computer charge, and once as with the independent mischief charge.

Co-ordinated disclosure—working with the vendor to agree upon a timetable which allows reasonable time to generate and deploy a patch which fixes the flaw prior to disclosure—is generally considered an industry best practice. However, it isn't always appropriate or possible, and there are legitimate reasons to prefer other approaches to vulnerability disclosure. Auernheimer didn't attempt co-ordinated disclosure in the instant case, and there are good reasons Auernheimer might not have felt that co-ordinated disclosure was appropriate, but even if not, failure to follow industry best practices shouldn't be a crime.

2.2 Aaron Swartz

2.2.1 Case summary[3]

Aaron Swartz was a renowned computer programmer who helped write the first RSS standards when he was just 14 years old. Later, he was involved in Creative Commons, the Wikimedia Foundation, and other similar "free"/"open" culture and digital civil liberties organizations. He became particularly interested in open access.

US court dockets and case documents (briefs filed by the parties, court decisions, etc) are stored in a computer system called Public Access to Court Electronic Records, better known as PACER. The system is a critical tool for lawyers, reporters, and other observers of the legal system. Congress allowed the a fee to be charged to recoup costs in maintaining the system and making the documents available. As a result, PACER charges a 10¢ fee per page, with some exceptions. The revenue from PACER is $150 million more than the cost

[3]This account is based on work from [3], which drew from [18, 24, 15, 20, 21, 1, 19].

to run the system.

Swartz thought it was wrong to charge the public for access to judgments that govern them and which were produced at public expense, so he built RECAP (PACER, backwards). RECAP is a web browser plugin that uploaded a copy of any PACER documents you paid for and accessed to a public archive, maintained for free. When a RECAP user searched in the PACER system, the browser would first check the RECAP archive, obtaining the document for free if available, and only performing the paid search on PACER otherwise. Believing this open access tool must somehow be wrong and criminal, prosecutors tried and ultimately failed to prosecute Swartz. People close to Swartz believe the Department of Justice later targeted him in retaliation for this frustrated attempt at prosecution.

Later, Swartz took up another open access issue–journal articles, mostly the result of public funds, being hoarded in academic databases. He targeted JSTOR in particular, which has a large archive of scientific papers, including many which are so old they're in the public domain, but all are behind a paywall.

Swartz used MIT's open computer network to access the JSTOR database of academic journals, and download articles by the thousand. Nobody knows for certain what Swartz planned to do with them. It could have been a research project to look at funding sources—Swartz had done similar research on legal papers in the past. He might have been intending to release the public domain documents. He might not have made a decision about what he planned to do with them—Swartz was known to acquire large data sets without planning any particular use for them.

Anyone on campus, even visitors, are allowed to access MIT's network, and anyone accessing MIT's network is allowed unrestricted access to JSTOR's archives. MIT pays a blanket license fee to JSTOR for this access. Swartz's

downloading program overloaded the JSTOR servers, and JSTOR blocked access for larger and larger segments of MIT's network in an effort to mitigate the performance degradation. Swartz tried to evade these measures by switching IP addresses, for example. Eventually, he entered a wiring closet and physically connected a laptop with an external hard drive to MIT's network, and continued downloading. He was recorded by a security camera, but used a bike helmet to shield his face. Swartz's identity was unknown to MIT and JSTOR during most of the conduct in question.

Police were called, and a team subsequently arrested Swartz and charged him with a myriad of offences including wire fraud and CFAA violations. JSTOR refused to press charges, saying there was no permanent damage, but prosecutors proceeded regardless, and ratcheted up the charges to a maximum 35 year sentence. Later, the indictment was amended with even more charges, bringing the possible penalty to 50 years in prison and a one million dollar fine.

Swartz refused plea bargains because he felt he'd done nothing wrong. He was authorized to access MIT's network and the JSTOR archive, so conviction on the wire fraud and CFAA charges would have been unacceptable. Two years after he was arrested, Swartz hung himself in his apartment. Swartz had long struggled with depression, but it is likely the pending charges were relevant to his suicide.

2.2.2 Mischief in relation to data

Swartz's downloading program overloaded the JSTOR servers, thereby depriving others of their use. Interfering with lawful use of data is part (d) of s. 430:

> Mischief in relation to data
>
> **430(1.1)** Every one commits mischief who wilfully

(a) destroys or alters data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with the lawful use of data; or

(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Swartz's defence might include arguing that the denial of service was accidental, which it almost certianly was. Swartz believed there should be wider access to academic work, so it seems unlikely he would have deliberately overloaded JSTOR's servers in order to interfere with other users of the JSTOR archives. Since Swartz's ideological commitment to information freedom is a critical part of the prosecution's argument, it would be difficult to argue the contrary in an attempt to obtain a conviction on this charge.

The Crown might, however, argue he was reckless with respect to the possibility he might overload the servers, and that the various contortions he used to evade JSTOR's attempts to block him indicate that he knew he was causing problems. This is an argument with the benefit of hindsight. At the time, it wouldn't have been obvious to Swartz why his program's access to JSTOR periodically failed. There would have been no clear indication of whether access was deliberately cut off, or the specific reason for doing so. There was no communication from JSTOR to inform him, so while Swartz might have guessed any number of reasons for the access disruptions, it would be difficult to show that he knew he was causing problems. As time went on, Swartz's attempts to evade the blocks JSTOR put in place became more and more drastic. Swartz eventually connected a laptop directly to MIT's network, which could be charged as unauthorized use of computer.

2.2.3 Unauthorized use of computer

A charge of "unauthorized use of computer" (s. 342.1) requires that Swartz do one of the enumerated acts "fraudulently and without colour of right".

Swartz would have to show that MIT's network was an open one, and convince the court that this meant he was permitted access to the network, and thus also permitted to access JSTOR's archive. MIT is well-known for having such a network, so this is likely to succeed.

Even failing to convince the court that MIT's network was so open that Swartz was permitted to access the network (and, through it, JSTOR's archive), it is sufficient to argue that Swartz *believed* this to be the case, because "colour of right" is a subjective standard. Recall this description from *Essentials of Canadian Law: Computer Law* [22]:

> "Without colour of right" means without an honest belief that one had the right to carry out the particular action. To establish "colour of right," one would need to have an honest belief in a state of facts that, if they existed, would be a legal justification or excuse.

Another explication comes from the 1973 case *R. v. DeMarco* [16]:

> "The term 'colour of right' generally, although not exclusively, refers to a situation where there is an assertion of proprietary or possessory right to the thing which is the subject matter of the alleged theft. One who is honestly asserting what he believes to an honest claim cannot be said to act 'without colour of right' even though it may be unfounded in law or fact... The term 'colour of right' is also used to denote an honest belief in a state of facts which, if was actually existed would in law justify or excuse the act done... The term when used in the latter sense is merely a particular application of the

doctrine of mistake of fact."

So, if Swartz can show that he subjectively believed that he was permitted to access MIT's network, and thus was also permitted to access JSTOR's archive though that network, *and* that this state of facts would have been a legal justification or excuse had they actually been true, then the charge fails. "Without colour of right" is an essential element of the "unauthorized use of computer" crime, so the Crown cannot prove its case without proving this element.

This argument applies to the downloading Swartz did while a guest on the MIT network, but it would be harder to argue that entering a network closet and wiring a laptop to the network directly was permitted, even on an open network. Nevertheless, there is an argument to be made on this. The network closet's walls are covered in years of graffiti, demonstrating that accessing that closet was normal. If that is the case, then connecting to the MIT network in the closet might be permitted as well. On the other hand, Swartz felt the need to hide his identity from security cameras while doing so. The Crown would argue that this shows a guilty conscience—that Swartz knew his conduct was wrong. I'm inclined to be pessimistic; the argument that shielding your face from the security camera is evidence of a guilty mind would probably succeed, and a single charge of "unauthorized use of computer" would succeed. While the sentence for such a conviction would be up to ten years in prison, the Canadian judicial system is less inclined to issue maximum penalties, and the prosecutor might proceed by summary conviction, as the putative victims expressed no interest in pursuing charges.

2.2.4 Other charges

Swartz was also charged with breaking and entering and wire fraud. While I have focused on computer crimes, this serves as a reminder that many non-

computer crimes might be alleged to have been committed alongside computer crimes.

Wire fraud is any conduct which deprives another of property or services fraudulently, and is conducted over a wire. In Canada, fraud is criminalized by s. 380:

> Fraud
>
> **380. (1)** Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,
>
> (a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding fourteen years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or
>
> (b) is guilty
>
> (i) of an indictable offence and is liable to imprisonment for a term not exceeding two years, or
>
> (ii) of an offence punishable on summary conviction,
>
> where the value of the subject-matter of the offence does not exceed five thousand dollars.

As the documents downloaded from JSTOR were worth well over $5000[4], Swartz would face up to fourteen years in prison if convicted of fraud.

A charge of breaking and entering might also succeed, depending on whether the network closet was locked, as prosecutors allege, or not. If the closet were open, Swartz might have been able to argue that there was no breaking, which is one of the required elements of the offense.

[4]JSTOR declined to answer investigators' questions about the value of their database, and insisted on being served with a subpoena. Once served, JSTOR still tried to minimize the amount of information it provided to prosecutors. [1]

2.2.5 Case disposition

In Canada, it might be less likely that Swartz would be targeted by investigators in the first place. The US prosecutors felt frustrated that they couldn't prosecute Swartz for RECAP, which almost certainly enhanced their aggressive stance in the JSTOR case. That would probably be less likely in Canada, since RECAP wouldn't have been a problem in this country. The Canadian version of RECAP (the browser plugin) is unnecessary because our version of PACER (the legal database) is free, publicly available, and entirely mainstream – the Canadian Legal Information Institute (CanLII) is funded by the Federation of Law Societies of Canada [2]. That being the case, prosecutors would have been more likely to drop the matter as JSTOR requested, or offer a plea deal more favourable than what the US prosecutors offered, which required felony conviction and jail time.

However, assuming the case went forward, the hypothetical I've outlined is analagous to the real case against Aaron Swartz in the US. I've tried to apply the legal standards realistically. In my hypothetical, Swartz is convicted of one count of unauthorized use of computer for connecting to MIT's network in the network closet, and one count of wire fraud for downloading documents from JSTOR with the laptop in the network closet. Given the reluctance of the alleged victims to press charges, the penalties the court would impose are likely well short of the maximums.

3 Conclusion

I've tried to show with some realism the kinds of arguments which might be made in two well-known computer crime prosecutions from the US. In both cases, I have shown how the legal standards like "fraudulent and without colour of right"

might be applied, and how the subjectivity of those standards might play out. While the usbjectivity of the legal standards attempt to distinguish true bad actors as deserving of criminal sanctions, the mere fact of the subjectivity leaves much discretion in the hands of the police and Crown prosecutors as they decide who to investigate and prosecute (and, eventually, what legal tactics to use, and what sentences to seek if there is a conviction).

For legitimate security researchers, who might eventually be found not to be bad actors under the subjective legal standards, as I've argued Swartz and Auernheimer could be, this is cold comfort. Simply being investigated seriously or being charged is already to lose, since mounting a legal defense is time-consuming and costly, carries a very high potential penalty for failure to prevail, and effectively stops the research in question until the case is disposed of.

As long as computer crime investigations and prosecutions in Canada remains focused primarily on dealing with real and serious computer crimes, security researchers are unlikely to be targeted as they have been in the US.

3.1 Mitigating legal risk

Researchers wanting to enhance this protection should think about how to encourage police and public prosecutors to view them as legitimate researchers and not bad actors who should be targeted for criminal sanctions.

To mitigate legal risk when conducting and reporting on computer security research, consider making any institutional affiliations clear. If you are an academic at a research institution, a student in a computer security course, or have prior academic training in computer security, making that affiliation clear will enhance your claim to legitimacy. Even showing that a computer security research project that was graded during a university program helps show that you are participating in the normal and legitimate academic community. If you've

been awarded a bug bounty, this enhances your credibility as a good-faith actor in the security field. Research Ethics Board approval is the gold standard here—ethics approval should quash any police investigation effectively—though research approved by an REB is unlikely to be legally risky in any event.

Researchers should try to follow industry best-practices when researching and reporting vulnerabilities. If possible, inform the subject of the research and get their consent. This might not always be practical, or might be inappropriate, for example if it would make the researcher vulnerable to a realistic risk of retaliation. Even if getting consent is unlikely, the attempt bolsters your claim to not be a bad actor. When reporting on your research, doing so in a way that enhances the state of knowledge in computer security, especially if presenting in mainstream academic or industry venues can enhance police and prosecutors' perceptions of you and your conduct.

When reporting vulnerabilities, attempt co-ordinated disclosure—work with the vendor to agree on a realistic timetable for creating and deploying a patch to fix the vulnerability prior to disclosing the vulnerability publicly. This might not always be possible or appropriate, but it is generally a best practice to aim for. This is doubly true since the government has enshrined co-ordinated disclosure in the Copyright Act. Researchers should keep records of communications involving the subject of their research so police and prosecutors can see this good-faith conduct. Consider whether disclosing proof-of-concept code is needed, or whether it is needed immediately. It might be sufficient to publish without code initially, and present code at a later date, perhaps after more patching has occurred. If disclosing publicly prior to patches being available or deployed, or ahead of the co-ordinated disclosure timetable, make your analysis of the public interest being served explicit, and include it in your disclosure.

Researchers should be wary of companies which are new to software devel-

opment and distribution, such as car manufacturers—these companies will have less experience working with the computer security community, and might be more inclined to overreact, including pursuing criminal or civil sanctions.

When the risk of retaliation is high, researchers might want to insulate themselves by involving a third party to act on their behalf. This might be a lawyer, but there are computer security firms who specialize in brokering vulnerability disclosures. The EFF also suggests asking the selection panel for conferences where the research is to be presented to contact the vendor [6].

Computer technologists should advocate for changing the legal standards in the Criminal Code so they encourage security research as a matter of public policy. Instead of identifying bad actors as those who can mount a successful defence against criminal charges, the law should identify the conduct that is criminal more clearly—particularly defining what "unauthorized" access to a computer means in this world of ubiquitous, always-on, public by default world of computing. Until then, these measures should enhance the apparent disinclination of Canadian police and prosecutors to pursue computer crime prosecutions against computer security researchers.

References

[1] Abelson, H., Diamond, P. A., Grosso, A., and Pfeiffer, D. W. Mit and the prosecution of Aaron Swartz. Report to the President, MIT, July 26, 2013. http://swartz-report.mit.edu/docs/report-to-the-president.pdf.

[2] Canadian Legal Information Institute. About CanLII. *CanLII website* (unknown). http://canlii.org/en/info/about.html.

[3] Doherty, M. Problematic computer crime laws in Canada. *Unpublished manuscript* (October 2013).

[4] Ducharme, J. T. R. v. Alexander. *CanLII 26480 (ON SC)* (August 1, 2006). Judicial ruling. http://canlii.org/en/on/onsc/doc/2006/2006canlii26480/2006canlii26480.pdf.

[5] Eckeland, T. B., Kerr, O. S., Hofmann, M., and Fakhoury, H. M. US v. Andrew Auernheimer. *United States Court of Appeals for the Third Circuit* (October 25, 2013). Appellant's reply brief (Case: 13-1816; Document: 003111432942). http://torekeland.com/wp-content/uploads/2013/10/Auernheimer-Reply-Brief.pdf.

[6] Electronic Frontier Foundation. A "grey hat" guide. *Coders' Rights Project* (unknown). https://www.eff.org/pages/grey-hat-guide.

[7] Fakhoury, H. You may not like weev, but your online freedom depends on his appeal. *Wired* (July 2, 2013). http://www.wired.com/opinion/2013/07/dont-hate-the-crime-hate-the-person-how-weevs-appeal-affects-all-of-us/.

[8] Ferenstein, G. This is what's wrong with college: Student expelled for exposing network's privacy flaws. *TechCrunch* (January 25, 2013). http://techcrunch.com/2013/01/25/this-is-whats-wrong-with-college-student-expelled-for-exposing-networks-privacy-flaws/.

[9] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and Berners-Lee, T. Hypertext transfer protocol – HTTP/1.1. RFC 2616, Internet Engineering Task Force, http://tools.ietf.org/html/rfc2616#section-14.43, 1999. at §14.43.

[10] Fishman, P. J., and Moramarco, G. J. US v. Andrew Auernheimer. *United States Court of Appeals for the Third Circuit* (September 20, 2013). Brief for Appellee (Case: 13-1816; Document: 003111395511. https://m.app.box.com/view_shared/1c2i69r1x0118i68zwsv.

[11] Government of Canada. Personal Information Protection and Electronic Documents Act. http://canlii.ca/t/l29k#sec2subsec1 at s. 2(1), 2000. SC 2000, c 5.

[12] Government of the United States of America. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act. http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf, October 26, 2001. Public law 107–56.

[13] Granick, J. S. US v. Andrew Auernheimer. *United States Court of Appeals for the Third Circuit* (July 8, 2013). Brief of *Amici Curiae* Mozilla Foundation, computer scientists, security and privacy experts (Case: 13-1816; Document: 003111317316). http://torekeland.com/wp-content/uploads/2013/07/Mozilla-Amicus.pdf.

[14] Lawson, S. Canada blocks extradition of Cisco suspect. *ComputerWorld* (June 3, 2011). https://www.computerworld.com/s/article/9217300/Canada_blocks_extradition_of_Cisco_suspect.

[15] MacFarquhar, L. Requiem for a dream. *The New Yorker* (March 11, 2013). http://www.newyorker.com/reporting/2013/03/11/130311fa_fact_macfarquhar.

[16] Martin, J. R. v. DeMarco. *13 C.C.C.* (1973), 369. Judicial ruling. Quoted at ¶25 in R. v. Bahr, 2006 ABPC 360 (CanLII), http://canlii.ca/t/1vc0s retrieved on 2013-12-02.

[17] Mehta, D. Project Spade, massive international child porn bust centred on Toronto, nets 348 arrests in 'horrific sexual acts'. *National Post* (November 14, 2013). http://news.nationalpost.com/2013/11/14/at-least-386-victims-rescued-after-project-spade-a-massive-child-porn-bust-that-started-in-toronto/.

[18] Peters, J. Aaron Swartz wanted to save the world. Why couldn't he save himself? *Slate* (February 7, 2013). http://www.slate.com/articles/technology/technology/2013/02/aaron_swartz_he_wanted_to_save_the_world_why_couldn_t_he_save_himself.html.

[19] Schwartz, J. An effort to upgrade a court archive system to free and easy. *New York Times* (February 12, 2009). http://www.nytimes.com/2009/02/13/us/13records.html?pagewanted=all.

[20] Schwartz, J. Internet activist, a creator of RSS, is dead at 26, apparently a suicide. *New York Times* (January 12, 2013). http://www.nytimes.com/2013/01/13/technology/aaron-swartz-internet-activist-dies-at-26.html?pagewanted=all.

[21] Swartz, A. Sick. *Blog post* (November 27, 2007). http://www.aaronsw.com/weblog/verysick.

[22] Takach, G. S. *Essentials of Canadian Law: Computer Law*, 2 ed. Irwin Law, 2003.

[23] Walsh, K. US v. Andrew Auernheimer. *United States Court of Appeals for the Third Circuit* (July 8, 2013). Brief of *Amicus Curiae* Digital Media Law Project. http://torekeland.com/wp-content/uploads/2013/07/Berkman-Amicus.pdf.

[24] Wu, T. Fixing the worst law in technology. *The New Yorker* (March 18, 2013). http://www.newyorker.com/online/blogs/newsdesk/2013/03/fixing-the-worst-law-in-technology-aaron-swartz-and-the-computer-fraud-and-abuse-act.html.