Dalhousie University
Faculty of Computer Science

CSCI 4192 Report 1:
Problematic Computer Crime Law In Canada

Author:
Mike Doherty
doherty@cs.dal.ca

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

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

October 31, 2013

Contents

1 Introduction

The Computer Fraud and Abuse act (CFAA) is the main computer crime law in the United States, and has come under fire lately[1], after a spate of questionable prosecutions, most prominently the cases of Aaron Swartz, and Andrew Auernheimer.

1.1 Troubling prosecutions

1.1.1 Aaron Swartz[2]

Aaron Swartz called himself an "applied sociologist" and was a renowned computer programmer and an advocate for digital civil liberties. He helped create the first version of RSS, an important internet standard, when he was 14 years old. Later, he took up the cause of open access.

US court judgments are stored in a computer system called PACER, which charges an access fee 10¢ per page. 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. Believing this open access tool must somehow be wrong and criminal, prosecutors tried and ultimately failed to charge Swartz with a crime. People close to Swartz believe the Department of Justice later targeted him in retaliation for this frustrated attempt at prosecution.

Swartz also came to believe it was wrong for academic research papers funded by public money to be locked up like the judicial decisions in PACER. He used MIT's open computer network to access the JSTOR database of academic

[1] See [47, 28, 11, 29, 54]

[2] This account is drawn from [40, 54, 32, 46, 51, 1].

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 data sets without planning any particular use for them.

Anyone is allowed to access MIT's network, and anyone accessing MIT's network is allowed unrestricted access to JSTOR's archives. His downloading program overloaded the JSTOR servers, and access to JSTOR was blocked for larger and larger segments of MIT's network, as Swartz tried to evade these measures. Eventually, he entered a wiring closet and physically connected a laptop with an external hard drive to MIT's systems, and continued downloading.

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 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.

1.1.2 Andrew Auernheimer[3]

Andrew Auernheimer—better known as "weev"—worked with Daniel Spitler discovered 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 would get a response from AT&T which included the email address.

Spitler wrote a program which downloaded thousands of pages, incrementing the ICCID value each time, to obtain thousands of 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.

AT&T convinced the FBI to investigate, and 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.

These, and other, cases are troubling, because if the arguments and precedents stand, they would criminalize much of everyday users' behaviour online. The laws are being applied too broadly, criminalizing conduct that should more

[3]This account is drawn from [18, 17, 24, 53].

properly be considered breach of contract, or a matter for discipline within an employer-employee relationship, or which is already sufficiently criminalized by other laws, such as wire fraud or identity theft. Swartz' case in particular raises questions about prosecutorial discretion, and whether the overlapping provisions of the CFAA allow prosecutors to double-dip, leading to outsize potential punishment for minor infractions. The prosecutors in the Auernheimer case used state laws to double-dip, ratcheting up the punishment.

While some of the conduct in these cases might be troubling, or even criminal (Swartz' entering MIT's wiring closet, for example), the charges relating to computer crime would apply broadly to conduct that computer security researchers might perform daily.

1.2 Computer security research

Computer security research is a broad field, and includes both academic and industrial research. The kind of research ranges from applied mathematics, to monitoring networks for signs that an attack is taking place.

Academic researchers might do basic research to create new encryption, or to evaluate existing cryptographic systems. They might investigate new classes of security vulnerabilities, and how to mitigate them. They might build tools for collecting data—like Zmap, the internet scanner—relevant to further research.

Academics and industry practitioners also research specific vulnerabilities in specific software. "Penetration testing" is when a company hires a security professional to attempt to breach their security systems, identifying and reporting on the vulnerabilities, and often helping to resolve them once the testing is complete.

This kind of research is also done by independent researchers, who might do the research without being hired to do so. Several vendors now reward

researchers for disclosing the vulnerabilities they find in confidence, so they can be fixed before making the flaw public. Other researchers might give the information they discover to an intermediary, either for free or for a fee, who might dislose the flaw to the affected vendor, or sell it to other companies or governments in the form of raw vulnerabilities or exploits, or services like scanning for signatures indicating the vulnerability is being exploited.

Security research also encompasses building security and privacy tools, and bleeds into adjacent fields, like usability research in relation to privacy and security tools.

The CFAA is sufficiently broad so as to endanger much of the activity that computer security professionals engage in on a daily basis.

1.3 The Canadian context

By comparison with the United States, Canada has both fewer computer crime prosecutions and proportionately fewer questionable prosecutions. As a consequence, Canadian security researchers and computer scientists are likely much less familiar with computer crime laws in Canada than they are with US laws like the CFAA and DMCA.

I will give an overview of some of the Canadian laws which are most relevant to computer security researchers, and discuss ways in which those laws might be problematic by being overbroad or vague in ways that could lead to prosecutors arguing that the legitimate conduct of security researchers is criminal. First, I'll discuss the Criminal Code offences "unauthorized use of a computer" and "mischief in relation to data". Second, I'll discuss the Copyright Act, which has carved out exceptions for encryption and computer security researchers. Third, any law which impinges on freedom of speech can have an impact on researchers, so I will consider the new Nova Scotia cyberbullying legislation as

one such example.

2 Criminal law

The most important regulation on computer security research is the computer crime provisions of the Criminal Code [21]. The most specific computer crime provisions are "mischief in relation to data"[4] and "unauthorized use of computer"[5]. "Counselling offence that is not committed"[6] is relevant to vulnerability disclosure, but jurisprudence on the question of whether an offence was *counselled* seems entirely sensible. Consequently, I believe it does not pose a problem for security researchers who want to disclose security vulnerabilities, even if the disclosure includes how it can be exploited, so I have not discussed this provision of the law.

2.1 Mischief in relation to data

Theft is the crime where a person takes another person's property, intending to deprive them of it permanently. A lesser crime, called criminal conversion, is taking (as in theft) or exerting unauthorized control over someone else's property, but without intent to permanently deprive the owner of that property. A still lesser crime is *mischief*, which is when a person damages or defaces another's property but without conversion (the exertion of unauthorized control). Consider three crimes in relation to a person's car. Stealing the car would be a theft. Joyriding would be criminal conversion, as it involves taking the car, but without intent to permanently keep it. Spraying graffiti on the car would be mischief.

[4] [21] at s 430(1.1)
[5] *Id.* at s 342.1
[6] *Id.* at s 464

"Mischief in relation to data"[7] creates an offence which is meant to be analagous to mischief in the physical world.

> 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.
>
> Punishment
>
> **(2)** Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.
>
> [...]
>
> **(4)** Every one who commits mischief in relation to property, other than property described in subsection (3)[8],
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
>
> (b) is guilty of an offence punishable on summary conviction.
>
> **(5)** Every one who commits mischief in relation to data
>
> (a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
>
> (b) is guilty of an offence punishable on summary conviction.

s 430(1.1)(c) and (d) seem to apply fairly straightforwardly to distributed denial of service (DDoS) attacks, which overwhelm the target website or service with excess requests, making it inaccessible to others. Researchers like Gabriella Coleman [8, 9, 10], Molly Sauter [44], and others [25] are developing an understanding of at least some DDoS as a form of civil disobedience akin

[7] *Id.* at s 430(1.1)

[8] Subsection 3 refers to a will, or physical property valued at greater than $5000.

to sit-ins, widely considered a legitimate political activity. Equating what we might understand as a political act with truly destructive computer crime is a serious category error. While physical sit-ins are criminal acts, we don't treat them as severely as we treat DDoS. A typical street protestor might be arrested, but not charged with any crime, or charged with an offence like trespassing and given a suspended sentence, a fine, or community service. Comparable actions online carry a potential penalty of 10 years in prison under Canadian law. The huge gulf between the treatment of civil disobedience performed with one's own body and with one's computer is unjust.

s 430(2) provides for life in prison if your mischief causes actual danger to life. This might apply in the commonly-cited but overblown[9] scenario of "cyberterrorists hacking the power grid." If that were to happen, it could cause actual danger to life, and if caught and successfully prosecuted, the attackers would face a sentence of life in prison.

s 430(4) provides the punishment for physical mischief. Because "property" is defined as "real or personal corporeal property", this doesn't apply to mischief in relation to data. This allows a useful comparison between how computer crimes and non-computer crimes are treated. The non-computer mischief punishments have a dollar value requirement, which is missing from the punishments for computer mischief (s 430(5)). This dichotomy means that similar conduct is assessed differently for punishment depending on whether it was committed against data or tangible property.

The monetary requirement is also notable because the US CFAA included a felony enhancement for damages over $5000. That is, if the damages were more than $5000, then the conduct could be charged as a felony instead of a misdemeanor. $5000 is already quite a low bar[10] for a misdemeanor, but the

[9]The power grid likely faces a greater threat from being physically hacked-at with a power saw; see [45].

[10]The EFF's legal director, Cindy Cohn, gave a good explanation of how the CFAA counts

comparable statute in Canada has no bar at all. It is entirely up to the prosecutor's discretion whether to proceed by indictment or by summary conviction. In Canada this also affects the options available to the accused. If the Crown proceeds on summary conviction, there is no option for a trial by jury.

Elsewhere (s 429(3)), the Criminal Code provides that it is not a crime to destroy anything if you own it and have exclusive interest in it, so long as you are not attempting fraud. For example, you can't burn down your house in an attempt to defraud your insurance company, even if you own it outright. The intent here seems to be to criminalize destroying others' "digital property", just like it's a crime to destroy others' physical property, but imposes much more onerous maximum sentences. This is perhaps justifiable on the grounds that computer networks allow much more damage to be done than in non-digital offences.

Notably, the definition does not seem to include "theft" of data which does not deprive the owner of that data. In R. v. Alexander [16], a fraudster was charged with mischief in relation to data for stealing credit card numbers. But theft of data is not included in the definition. The court did not need to determine whether the charge of theft constituted a crime under the statute because it found that the accused did not steal the data in question. Nevertheless, it seems likely that such a charge would fail as a matter of law even if the theft had been committed.

2.2 Unauthorized use of a computer

The "unauthorized use of a computer"[11] offence conceives of a crime akin to tresspass. Instead of trespassing into a physical location, this offence is trespass into a computer.

up the $5000 of damages at DEF CON 11. See [7].

[11] [21] at s 342.1

There are four kinds of conduct which are criminalized: use of a computer; intercepting computer communications; using a computer to do "mischief in relation to data" (s 430(1.1)) ; and having computer credentials that would allow someone to commit one of the first three offences.

> Unauthorized use of computer
>
> **342.1 (1)** Every one who, fraudulently and without colour of right,
>
> (a) obtains, directly or indirectly, any computer service,
>
> (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system,
>
> (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or
>
> (d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c)
>
> is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.[12]

2.2.1 "Fraudulently and without colour of right"

The two prongs of this test— "fraudulently" and "without colour of right"—are not defined here, but they are explored in case law. *Essentials of Canadian Law: Computer Law* [52] explains the meaning of "fraudulently":

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

If this first prong of the test fails, the conduct is not criminal. The requirement of intent seems to provide a useful narrowing of what conduct falls afoul

[12]Immediately following the quoted text, the Criminal Code lists several definitions. I omitted them for brevity, and because they appear to be quite straightforward.

of this prong of the test. If a researcher didn't intend to deprive another person, then there is at least an argument that the conduct was not fraudulent. Perhaps the researcher can demonstrate that the intent was to demonstrate a security flaw to the vendor, or expose the vulnerability publicly. If data was copied (rather than permanently destroyed), then your defence might be that no deprivation was caused or intended to be caused.

The second prong of the test is "without colour of right". *Essentials of Canadian Law: Computer Law* [52] again:

> "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 helpful explication can be found in these instructions to the jury in *Lilly v. The Queen* [30]:

> The phrase 'colour of right' simply means a bona fide belief or an honest belief. And a bona fide belief or an honest belief may arise from a genuine mistake or in some cases even from ignorance. Therefore the phrase in the definition of theft, 'without colour of right', simply means the lack of a bona fide or honest belief. It is up to you to determine from the evidence whether the accused, in regard to Count No. 1 acted dishonestly and without colour of right when monies were taken, as is alleged, from the trust account of the company to the general account. You will note that the definition reads 'fraudulently and without colour of right' takes, not 'fraudulently or [without] colour of right' takes. If you find that the accused did take the monies and the actions of the accused were fraudulent and without colour of right, and that he took the said monies from the

> trust account with intent to deprive the owner, you must – you, in that case, would find the accused guilty of Count No. 1.

Although *Lilly* was a case about theft of money, the "fraudulently and without colour of right" test is the same as in the unauthorized computer use provisions.

If someone mistakenly accessed a computer, or subjectively believed they were authorized to use it, their conduct would not be criminal. For example, if someone sat down at a computer in the library thinking it was open for anyone to use, but it was really unlocked by someone who had stepped away, this second prong of the test would fail because the use *would have been* authorized if their subjective (but mistaken) belief had been true.

2.2.2 What is unauthorized?

While the "without colour of right" standard is flexible, it seems to simply postpone difficult questions about what "authorization" means in relation to computers. Now we must answer whether the accused subjectively and reasonably believed that their use of the computer was authorized, but without any guidance as to what "authorized" means. Could it really be the case that checking your personal email on a work computer is a crime that carries a potential ten year prison sentence? After all, employers typically provide computers to their employees with an implicit or explicit understanding that they are to be used only for the employee to perform their contracted duties on behalf of the employer, and working as an agent of the employer in the employer's interests.

While a person might subjectively believe that they were not authorized to use their work computer to check their personal email account, it should not follow that this conduct is criminal. That is a matter for discipline within an employer-employee relationship, or a matter for contract law to resolve. How-

ever, it might be true that such a violation would be considered criminal. In *R. c. St-Martin* [41], a police officer was convicted of unauthorized use of a computer for using his access to police systems to obtain information for purposes unrelated to police duties. Because the purpose for which he accessed the data was not police business, the access was unauthorized. This seems to apply straightforwardly enough to conduct that might be problematic, but which we might not consider criminal. Indeed, this result seems to criminalize huge swathes of extremely common, everyday conduct, which might result in only trivial harms. We all understand that checking personal email with company time and resources is in some small way wrong, but which should be punished—if at all—by an employee's supervisor, not by the government imposing criminal sanctions.

The legislators in 1985 [27] did not foresee the extraordinary proliferation of computing into every facet of our lives coming—the World Wide Web was introduced in 1991, six years *after* these provisions were added to the Criminal code—and ever since, the government has failed to modernize the law.

The kinds of relationships one would have with computer systems in the 1980s are very different from the relationships one has today. In the 2010s, most computer systems that we interact with are publicly available by default—think of most popular web services, where anyone can sign up for an account. We also interact with many more of them. In the 80s, one would likely encounter computers only at work, or at university. In the 90s, personal computers proliferated, and home access became common. Since the introduction of the World Wide Web in 1991, personal computers and mobile devices have enabled us to access not only the computer systems we own, or use for work and school, but a huge number of public computing services. Correspondingly, the potential impact that the government's regulation of computer access has on the life of

any particular citizen has expanded. That expansion is worrying because the law does not envision the kind of always-on public-by-default service-oriented computing environment Canadians inhabit. The risk of criminalizing normal behaviour is thus heightened.

It is normal for operators of computer services to communicate their authorization to the user of a computer system through terms of service documents in the case of public internet services, employment contracts in the case of an employer providing a computer to an employee, or implicitly through a principle of agency – that a computer system can be used so long as it is used in the computer owner's interests, and the authorization ends if you use the system in a disloyal manner (because you are no longer acting as the owner's agent). All of these have the potential to give the power of criminal law to what might not even rise to the level of an enforceable contractual agreement. Terms of service documents are famously problematic because they are so one-sided, serving only the interests of the server owner, and because they may not even be enforceable [38, 3]. Yet the "fraudulently and without colour of right" standard potentially gives them the power to define illegal conduct. It is also relevant that most terms of service allow the service provider to unilaterally change the terms, without notice to the users of the service.

Terms of service agreements often include provisions we should never want to enforce as a matter of criminal law. A few examples, selected from the most popular internet services:

Facebook: "You will not use Facebook to do anything unlawful, misleading, malicious, or discriminatory. You will not provide any false personal information on Facebook. You will keep your contact information accurate and up-to-date."[13]

[13] `https://www.facebook.com/legal/terms`

This means you are not allowed to lie about your age on Facebook. If you move, or get a new phone number, you must update that information.

Seventeen.com: "YOU MAY NOT ACCESS OR USE THE COVERED SITES OR ACCEPT THE AGREEMENT IF YOU ARE NOT AT LEAST 18 YEARS OLD." [31]

This makes it illegal for a seventeen-year-old to visit Seventeen.com. The terms of use have been updated to decriminalize the magazine's readership.

Google Plus: "You must provide a two-part name."[14]

This requirement means that people whose legal name is a one-part name (for example, people from Iceland, Indonesia, or southern parts of India, or people who have legally changed their name to a mononym, like Teller [15], people who are known by a single name they chose for themselves (like the technologist Skud [49] or the pseudonymous graffiti artist Banksy), and people who have a name with more than two parts (anyone commonly referred to by their first, middle, and last names, for example) can't use Google Plus without violating the terms of service, and thus the criminal law.

YouTube: "Graphic or gratuitous violence is not allowed. If your video shows someone getting hurt, attacked, or humiliated, don't post it."[15]

This means you are not permitted to post video of violent police crackdowns on the Arab Spring protests.

Reddit: "You agree not to use any obscene, indecent, or offensive language."[16]

This means you are not allowed to swear on Reddit.

[14] `https://support.google.com/plus/answer/1228271`

[15] YouTube's terms of service (`https://www.youtube.com/t/terms`) require adherence to the Community Guidelines (`https://www.youtube.com/t/community_guidelines`).

[16] `http://www.reddit.com/help/useragreement#section_rules_of_usage`

OKCupid: You agree that your use of the Website shall be for bona fide relationship-seeking purposes (for example, you may not use the Website solely to compile a report of compatible singles in your area, or to write a school research paper).[17]

This means it is impermissible to find and quote OKCupid's terms of service for a research paper like this one.

Some of these provisions are problematic on their face, but service providers may write their Terms of Service document more or less however they see fit. Even if these terms rise to the level of enforceable contract, breaching them is a civil matter between the parties to the contract. Breach of contract carries no great moral opprobrium, and the law recognizes this. Any party to a contract is allowed to breach a contract when it is economically advantageous to do so—if companies A and B have a contract together, but B can get a better deal from C, they simply break the contract with A and pay them the amount A expected to make on the deal. This is normal and common conduct, and the criminal justice system isn't involved. Granting terms of service the power of criminal law is pernicious because it gives the service provider an unfair extra weapon in enforcing the contract—the threat of reporting the breach to the police, which could lead to prosecution and a long prison sentence.

More worryingly, the "fraudulently and without colour of right" standard doesn't make any distinction between serious computer crimes and dishonestly and knowingly violating the terms of use, for examply by providing an incorrect age on your online dating profile. This would punish Canadians for reading and understanding the terms of service – if they didn't read the terms, they wouldn't fall afoul of the "fraudulently and without colour of right" test.

Another potential issue with the subjectivity of the "colour of right" stan-

[17] `http://www.okcupid.com/legal/terms`

dard is that there is a notable cultural divide between computer experts and casual computer users (not to mention the gulf across which we find typical Crown prosecutors and the judiciary). A young computer science student might have a very different understanding of what they are allowed to do with a computer system than the Crown Attorney who might prosecute a criminal case against them, or the jury of "peers" who view their actions as though it were witchcraft. Jennifer Granick recounts [23] observations she and Larry Lessigmade about how this kind of cultural divide played out in Aaron Swartz' case:

> The more the Department of Justice, the more the prosecutors learned about Aaron [Swartz], the harder they were on him. And I've seen people whose reaction to stuff that Aaron's written online – things that I think of as showing a wonderful idealism, about sharing information, about making information accessible to people all around the world – were the very reasons people felt like what he did was criminal. That he *knew* what he was doing was wrong and that he meant to break the law anyway because of his ideology.

2.2.3 Proportionality

Subsection (c) is quite broad, as it makes it an offence to use a computer with the intent to commit the offences in (a) or (b), or s 430(1.1) (mischief in relation to data). *Essentials of Canadian Law: Criminal Law* [43] explains that the rationale here is that the police shouldn't have to wait for actual harm to occur. The difference between this and the other offences in this section is akin to the difference between murder and attempted murder. However, the punishment is the same for both computer crimes, while we typically punish other attempted crimes less severely.

3 Copyright law

There are two provisions in the Copyright Act [20] which are relevant to computer security researchers. They are exceptions from copyright infringement liability for performing security and encryption research – but those exceptions come with problematic strings attached.

3.1 Encryption research

It would be a violation of copyright to do encryption research of many kinds, but researchers are given an explicit exception at s 30.62:

> Encryption research
>
> **30.62 (1)** Subject to subsections (2) and (3), it is not an infringement of copyright for a person to reproduce a work or other subject-matter for the purposes of encryption research if
>
> (a) it would not be practical to carry out the research without making the copy;
>
> (b) the person has lawfully obtained the work or other subject-matter; and
>
> (c) the person has informed the owner of the copyright in the work or other subject-matter.
>
> Limitation
>
> **(2)** Subsection (1) does not apply if the person uses or discloses information obtained through the research to commit an act that is an offence under the Criminal Code.
>
> Limitation – computer program
>
> **(3)** Subsection (1) applies with respect to a computer program only if, in the event that the research reveals a vulnerability or a security flaw in the program and the person intends to make the vulnerability or security flaw public, the person gives adequate notice of the vulnerability or security flaw and of their intention to the owner of copyright in the program. However, the person need not give that

> adequate notice if, in the circumstances, the public interest in having the vulnerability or security flaw made public without adequate notice outweighs the owner's interest in receiving that notice.

The basic principle here is sound – nobody should be prevented from doing research on encryption because of copyright law. However, the "responsible disclosure" (more accurately called "co-ordinated disclosure", a term now being promoted by Microsoft as the adjective "responsible" is too loaded [36]) requirements may be problematic.

3.1.1 "Responsible disclosure"

"Responsible" or "co-ordinated" describe how a researcher discloses information about a vulnerability. If a researcher uncovers a security flaw in a vendor's software or systems, they first notify the vendor privately – either directly, through their reporting program, or indirectly via security firms which might pay the researcher for their information. The vendor acknowledges that they have received the report, and that it is a security flaw. The vendor and researcher negotiate and agree on a timeline for fixing the vulnerability, testing the remedy, and providing it to the vendor's customers. Once the customer systems have had a chance to be fixed, the researcher is free to disclose their findings publicly. Depending on the vulnerability, this might be an academic paper, a talk at a conference, or just dumping information online for anyone who's interested to see. The vendor will typically also make their own announcements.

This co-ordination is contrasted with alternative methods of dealing with a security vulnerability. Researchers might sell the flaw to the highest bidder, or they might make it public immediately, without giving the vendor and the vendor's customers advance notice to try to fix the problem. The latter case is sometimes used as leverage in negotiating an appropriate timeline in co-ordinated disclosure. If the vendor doesn't admit that there is a flaw, or takes

an unreasonably long time to fix the vulnerability, or to roll out the remedy, then the researcher might publish some or all of their information. Sometimes this is done purely as a method of getting the vendor to take the flaw seriously, but often the disclosure will include mitigation information. So, although criminal hackers get access to details about the flaw, making it easier to exploit, the affected public also gets that information, which they might use to protect themselves. They're also made aware that their systems are vulnerable, which allows them to make informed risk assessments. Even without specific mitigations, they could take systems offline, for example.

Vulnerability disclosure is a perennial topic for panel discussions at security conferences. A cursory search on YouTube finds video from such panels spanning the past decade: BlackHat 2002 [5], Shmoocon 2007 [48], DEF CON 15 [13], Harvard's Kennedy School of Government [26], SOURCE Boston 2009 [50], OWASP AppSec 2010 [39], and DEF CON 2011 [14]. In the academic publications, papers arguing for various practices have been regularly appearing over the past five years (see for example [35, 33, 42, 2, 6, 34, 4]). The Copyright Act attempts to codify a conclusion on that debate into law, despite the debate being unsettled, and having little relevance to copyright in any event.

First, s 30.62(1)(c) requires that the encryption researcher informs the copyright owner of what they're doing. This assumes that the copyright owner is known, and that they can be contacted. It isn't clear how a researcher would contact the copyright holder for GnuPG, for example. Requiring researchers to inform the copyright holder, thus probably identifying themselves, opens them to retribution. This is a well-known problem in security research, so it's not clear why the copyright law should privilege business at the expense of security researchers (and thus, indirectly, the public).

Next, s 30.62(3) requires a very particular form of "responsible disclosure"

which understands almost none of the complexities and nuances of that debate. I doubt that disclosure rules belong in the *law*, but at least that nuance should be reflected. The only complexity to the disclosure rules are the public interest exception, which provides no guidance on what factors should be considered, how they should be weighted, or who makes that determination. For the security researcher who is considering whether to exercise the public interest exception, the legal morass they would be wading into might chill their speech and actions, which could have severe consequences for the affected public. Even if the researcher's determination that the public interest would be served by public disclosure is ultimately vindicated at trial, the trial itself is expensive (in terms of both time and money), and has extreme penalties for failure.

Finally, the disclosure requirement in s 30.62(3) is a requirement to contact the copyright holder, which is more nonsensical than s 30.62(1)(c), because the copyright holder is not who you want to notify when disclosing a vulnerability. You actually want to notify the software *maintainer/vendor* (if any). For big business, that might be the same as the copyright holder, but it is very often not (complicated licensing agreements, and open source software being the two most obviouis cases), and the law doesn't make any distinctions.

3.2 Security research

There are exceptions for security research at s 30.63 of the Copyright Act which are very similar to those for encryption research (see 3.1):

> **30.63 (1)** Subject to subsections (2) and (3), it is not an infringement of copyright for a person to reproduce a work or other subject-matter for the sole purpose, with the consent of the owner or administrator of a computer, computer system or computer network, of assessing the vulnerability of the computer, system or network or of correcting any security flaws.
>
> Limitation

(2) Subsection (1) does not apply if the person uses or discloses information obtained through the assessment or correction to commit an act that is an offence under the Criminal Code.

Limitation – computer program

(3) Subsection (1) applies with respect to a computer program only if, in the event that the assessment or correction reveals a vulnerability or a security flaw in the program and the person intends to make the vulnerability or security flaw public, the person gives adequate notice of the vulnerability or security flaw and of their intention to the owner of copyright in the program. However, the person need not give that adequate notice if, in the circumstances, the public interest in having the vulnerability or security flaw made public without adequate notice outweighs the owner's interest in receiving that notice.

The problems here are similar. Although there's no requirement as in s 30.62(1)(c) to notify the copyright holder, there is still a confused "responsible disclosure" requirement. There's no clear reason why "responsible disclosure" should be a requirement in law, much less in *copyright* law.

There's an even more stringent requirement here though – the owner or administrator of the computer system must consent to the research. This protects business from unwanted criticism, while endangering the public by creating a hostile legal environment for computer security researchers. Again, business is privileged over the safety of the Canadian public.

4 Cyberbullying laws

While the criminal law is the primary way the government regulates conduct with computers, there are several other laws which are relevant. The apparent recent rise in online harassment has resulted in many governments pursuing cyberbullying legislation, the Nova Scotia provincial government among them. In the case of Nova Scotia, the Cyber-safety Act [22] was drafted and enacted quickly. The speed with which the legislation was put into place might well have

reduced its quality [19].

The conduct this law regulates includes deliberately humiliating someone [37]. This is the definition of "cyberbullying" in the Cyber-safety Act, with the most troubling language bolded:

> **"cyberbullying" means any electronic communication** through the use of technology including, without limiting the generality of the foregoing, computers, other electronic devices, social networks, text messaging, instant messaging, websites and electronic mail, typically repeated or with continuing effect, **that is intended or ought reasonably [to] be expected to cause** fear, intimidation, **humiliation, distress or other damage or harm to another person's** health, **emotional well-being, self-esteem or reputation, and includes assisting or encouraging such communication in any way**

While that's problematic on its face—a clear violation of press freedom, for example—it is potentially problematic for security researchers in particular. Publicly disclosing a security vulnerability could certainly be considered embarassing, triggering a vendor to pursue the remedies provided in the Act. While the language specifies embarassing a *person*, there's no reason to believe that individuals within an organization couldn't be embarassed because they represent the organization. For example, a CEO might be personally embarassed, and can then take action under this law. The remedies provided include getting a court order in a non-adversarial process which identifies the target of the order, placing a prior restraint on speech, prohibiting the use of electronic communications, confiscating electronic devices, or "any other provision that the justice considers necessary or advisable for the protection of the subject."

While the Act may be unconstitutional, the first test cases will need to mount an expensive and difficult legal defence, including appeals, or simply self-censor to avoid the legal risk. This chilling of legitimate speech and conduct is detrimental to security researchers, and the public. The private right of action

also opens the door to wider abuse than the criminal law typically sees [12]—private citizens are more likely to use any means available to silence critics.

5 Conclusion

The principal regulation of computer security researchers comes from the Criminal Code, namely the "mischief in relation to data" (s 430(1.1)) and "unauthorized use of a computer" (s 342.1) offences. Construed broadly, both of these might criminalize the conduct of legitimate security research. That grey area could chill security research in Canada because any legal defense is time-consuming, expensive, and difficult, even if ultimately successful.

The Copyright Act also regulates copying of copyrighted works, which is commonplace in research settings. In addition to the normal fair dealing rights for research, there are explicit exceptions for encryption and computer security research, but they are tied to a particular conception of "responsible disclosure." The disclosure rules are inflexible, save for a public interest exception, which could be legally risky to use.

Finally, any legislation which could chill free speech, such as Nova Scotia's Cyber-safety Act can impact security researchers disproportionately, because their work may often involve revelations which vendors might want to retaliate against.

Despite similar legal landscapes in Canada and the United States, I've been able to find only one problematic legal precedent (*St-Martin* [41], which seems to make use of a computer for purposes your employer wouldn't want is criminal; the case is discussed in section 2.2.2) in Canada, while examples in the US abound. Further research should try to characterize the specific differences that might explain the lack of such prosecutions in Canada.

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] Arora, A., and Telang, R. Economics of software vulnerability disclosure. *IEEE Security & Privacy 3*, 1 (2005), 20–25.

[3] Bayley, E. The clicks that bind: Ways users 'agree' to online terms of service. Whitepaper, Electronic Frontier Foundation, November 2009. https://www.eff.org/files/eff-terms-of-service-whitepaper.pdf.

[4] Bilge, L., and Dumitras, T. Before we knew it: An empirical study of zero-day attacks in the real world. In *Proceedings of the 2012 ACM conference on Computer and communications security* (New York, NY, USA, 2012), CCS '12, ACM, pp. 833–844.

[5] BlackHat 2002. Vulnerability disclosure: What the feds think. Panel discussion. https://www.youtube.com/watch?v=6t1BNDnbNxo, 2002.

[6] Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Transactions on Software Engineering 33*, 3 (2007), 171–185.

[7] Cohn, C. What hackers need to know about post 9-11 legal changes. Lecture at DEF CON 11. https://youtu.be/t_aatE2UbKY?t=7m42s, August 2003.

[8] Coleman, G. Beacons of freedom. *Index on Censorship 41* (November 30, 2012), 62–71. http://ioc.sagepub.com/content/41/4/62.full.pdf.

[9] Coleman, G. Anonymous in context. *Internet Governance Papers 3* (2013). http://www.cigionline.org/sites/default/files/no3_7.pdf.

[10] Coleman, G., and Ralph, M. Is it a crime? The transgressive politics of hacking in Anonymous. *Social Text 28* (2011). Also published on owni.eu: http://owni.eu/2011/09/29/is-it-a-crime-the-transgressive-politics-of-hacking-in-anonymous/.

[11] Couts, A. Can you be arrested for sharing a link? Maybe. *Digital Trends* (September 10, 2013). http://www.digitaltrends.com/opinion/barrett-brown-link-sharing-illegal/.

[12] Cushing, T. Nova scotia's new cyberbullying law will 'make bullies of us all'. *Techdirt* (August 14, 2013). http://www.techdirt.com/articles/20130812/09495224145/nova-scotias-new-cyberbullying-law-will-make-bullies-us-all.shtml.

[13] DEF CON 15. Disclosure panel. Panel discussion. https://www.youtube.com/watch?v=8LyG2aQTiQQ, 2007.

[14] DEF CON 19. Is it 0-day or 0-care? Panel discussion. https://www.youtube.com/watch?v=71Hb6pqIzXE, 2011.

[15] della Cava, M. R. At home: Teller's magical Vegas retreat speaks volumes. *USA Today* (November 15, 2007). http://usatoday30.usatoday.com/life/lifestyle/home/2007-11-15-teller-at-home_N.htm.

[16] 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.

[17] 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.

[18] 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/.

[19] Fraser, D., and MacKay, W. Maritime Connection: What do you think of Nova Scotia's legislation to stop cyberbullying? http://www.cbc.ca/player/Radio/LocalShows/Maritimes/ID/2400296654/, August 11, 2013. Interview by Preston Mulligan.

[20] Government of Canada. Copyright Act. http://laws-lois.justice.gc.ca/PDF/C-42.pdf, 2012. RSC 1985, c C-42.

[21] Government of Canada. Criminal Code. http://laws-lois.justice.gc.ca/PDF/C-46.pdf, 2013. RSC 1985, c C-46.

[22] Government of Nova Scotia. Cyber-safety Act. http://canlii.ca/en/ns/laws/stat/sns-2013-c-2/106920/part-1/sns-2013-c-2-part-1.pdf, 2013. SNS 2013, c 2.

[23] Granick, J. Innovation or exploitation? The limits of computer trespass law. http://youtu.be/F4XdxmLUfqI?t=1h39m42s, February 19, 2013. Panel discussion at the Stanford Center for Internet & Society.

[24] 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.

[25] Hampson, N. C. N. Hacktivism: A new breed of protest in a networked world. *Boston College International & Comparative Law Review 35*, 2 (2012), 511–542.

[26] Harvard Kennedy School of Government. Full disclosure: The perils and promise of transparency. Panel discussion. https://www.youtube.com/watch?v=rjie3FQhny0, April 11, 2007.

[27] Hébert, M., and Pilon, M. Computer crime. Background paper BP-87E, YM32-2/87-1991-11-IN, Library of Parliament, Parliamentary Research Branch, Law and Government Division, 1984, revised 1991. http://publications.gc.ca/collections/Collection-R/LoPBdP/BP/bp87-e.htm.

[28] Hill, K. When 'smart homes' get hacked: I haunted a complete stranger's house via the internet. *Forbes* (July 26, 2013). http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/.

[29] Kaplan, D. Fear of prosecution hampers security research. *SC Magazine* (July 19, 2013). http://www.scmagazine.com/fear-of-prosecution-hampers-security-research/article/303476/.

[30] Lamer, J. Lilly v. The Queen. *1 SCR* (1983), 794–800. Judicial ruling. http://scc.lexum.org/decisia-scc-csc/scc-csc/scc-csc/en/5378/1/document.do.

[31] Maass, D., Opsahl, K., and Timm, T. Until today, if you were 17, it could have been illegal to read seventeen.com under the CFAA. Electronic Frontier Foundation "Deeplinks" blog post. https://www.eff.org/deeplinks/2013/04/until-today-if-you-were-17-it-could-have-been-illegal-read-seventeencom-under-cfaa, April 3, 2013.

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

[33] Marconato, G., Nicomette, V., and Kaaniche, M. Security-related vulnerability life cycle analysis. In *7th International Conference on Risk and Security of Internet and Systems (CRiSIS)* (2012), pp. 1–8.

[34] Matwyshyn, A., Cui, A., Keromytis, A., and Stolfo, S. Ethics in security vulnerability research. *Security Privacy, IEEE 8*, 2 (2010), 67–72.

[35] McQueen, M., Wright, J., and Wellman, L. Are vulnerability disclosure deadlines justified? In *Third International Workshop on Security Measurements and Metrics (Metrisec)* (2011), pp. 96–101.

[36] Moussouris, K. Coordinated vulnerability disclosure: Bringing balance to the Force. *Microsoft TechNet, BlueHat blog* (July 22, 2010). http://blogs.technet.com/b/bluehat/archive/2010/07/22/coordinated-vulnerability-disclosure-bringing-balance-to-the-force.aspx.

[37] National Post Editorial Board. National Post editorial board: Nova Scotia's bad law. *National Post* (August 18, 2013). http://fullcomment.nationalpost.com/2013/08/13/national-post-editorial-board-nova-scotias-bad-law/.

[38] Newitz, A. Dangerous terms: A user's guide to EULAs. Whitepaper, Electronic Frontier Foundation, February 17, 2005. https://www.eff.org/wp/dangerous-terms-users-guide-eulas.

[39] OWASP AppSec USA 2010. Vulnerability lifecycle for software vendors. Panel discussion. https://www.youtube.com/watch?v=ynzcV8I7Lrg, 2010.

[40] 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.

[41] Provost, J. R. c. St-Martin. *QCCQ 575 (CanLII)* (February 2, 2012). Judicial ruling. http://www.canlii.org/en/qc/qccq/doc/2012/2012qccq575/2012qccq575.pdf.

[42] Rescorla, E. Is finding security holes a good idea? *IEEE Security & Privacy 3*, 1 (2005), 14–19.

[43] Roach, K. *Essentials of Canadian Law: Criminal Law*, 3 ed. Irwin Law, 2004.

[44] Sauter, M. Distributed denial of service actions and the challenge of civil disobedience on the internet. Masters thesis, unpublished, MIT, June 2013. http://oddletters.com/2013/05/16/726/.

[45] Schroeder, M. FBI offers large reward in power incidents. *ArkansasMatters.com* (October 7, 2013). http://www.arkansasmatters.com/story/fbi-offers-large-reward-in-power-incidents/d/story/2ERvO8ZX_EmGnRJgpsOCLw.

[46] 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.

[47] Sengupta, S. A cheap spying tool with a high creepy factor. *New York Times (Bits blog)* (August 2, 2013).

[48] Shmoocon 2007. Vulnerability disclosure panel palaver or 0 day OK, no way, or for pay. Panel discussion. https://www.youtube.com/watch?v=O7XLDJu-_Oo, 2007.

[49] Skud. My name. http://infotrope.net/attic/my-name/, unknown. Blog post.

[50] SOURCE Boston 2009. The partial disclosure dillema. Panel discussion. https://www.youtube.com/watch?v=R7wvMtYEXN4, March 12, 2009.

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

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

[53] 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.

[54] 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.