CHAPTER XII

Ethical-Hacking Challenges in Legal Frameworks, Investigation, Prosecution, and Sentencing

There is often a false belief among law makers that if the right legislation is enacted, and if enough resources are allocated to the task, that the law can rise to the challenge and overcome a myriad of obstacles to combat cyber security and cybercrime. Cybercrime investigations, whether it be for online-identity theft, selling counterfeit products via spam, or hacking (unauthorized access, modification of or impairment/interference with data or data systems), involve unique challenges. The challenges involve difficulty with the harmonization of laws, jurisdictional issues, resource implications, lack of training, ambiguity in terms of how a criminal provision will be interpreted alongside human-rights protections, and, above all, a host of technical hurdles that makes tracing back to the "offender" difficult. In spite of advances in machine learning, big-data techniques, and artificial intelligence, attribution remains a formidable challenge. If these hurdles are overcome, there remain issues with inconsistency in sentencing and, where relevant, in determining appropriate damages. These challenges are the same for ethical hacking

The following chapter addresses hurdles to the investigation and prosecution of an ethical hacker. In some contexts—where ethical hacking moves toward vigilantism—where prosecution is desirable as a deterrent to escalating acts. But there are also good arguments, as previously discussed, for exemptions to apply to many

ethical-hacking incidents, especially in situations where the online activity corresponds with legal off-line activity.

12.1 Criminal Landscape: Convention on Cybercrime and the Canadian Criminal Framework

The Convention on Cybercrime, an agreement between member nations of the European Union, is the only international agreement in the area of cybercrime. It is unique in that it is open for signature by non-EU states. The United States, Canada, and Japan have all signed the convention, with the United States also ratifying it.

The convention may be divided into three key divisions: substantive law, procedural requirements, and international cooperation. All signatories to the convention must criminalize certain activities.

The convention creates four main categories of substantive offences:

1. offences against the confidentiality, integrity, and availability of computer data and systems, comprising interference and misuse of devices;
2. computer-related offences, such as forgery and computer fraud;
3. content-related offences, in particular the production, dissemination, and possession of child pornography; and
4. offences related to copyright infringement.

Canada already criminalizes these four categories of conduct. One would presume that only the first category would be relevant to ethical hacking. Indeed, the computer offences are the most relevant area to ethical hacking, but some ethical-hacking incidences may also be relevant to areas such as copyright, child pornography, and fraud.

The convention also addresses the procedural aspects of cybercrime. The main categories here are:

1. expedited preservation of stored computer data,
2. expedited preservation and partial disclosure of traffic data,
3. production orders,
4. search and seizure of stored computer data,
5. real-time collection of traffic data, and
6. interception of content data.

Each of the procedural requirements is of some relevance to botnets and malware investigation.

Finally, the convention contains provisions relating to international cooperation. While some of these provisions are contentious, the convention allows a certain amount of flexibility in terms of how a nation might negotiate some of the issues. These may broadly be categorized as:

1. extradition,
2. mutual assistance, and
3. designation of a 24/7 network contact.

Each of these international-cooperation components of the convention exists to combat cybercrimes.

Table 3 lists the substantive provisions of the convention with the Canadian Criminal Code. While there are some minor differences between Canadian law and the substantive provisions found in the convention, there is significant overlap between them. An expanded version—table 4—is found at the end of this chapter.

Table 3. Comparison of Convention on Cybercrime and Canadian Criminal Framework

Convention on Cybercrime	Canada
Offences against the confidentiality and availability of computer data and systems	
Article 2—Illegal access	Section 342.1 of the Criminal Code
Article 3—Illegal interception	Section 342.1 of the Criminal Code
Article 4—Data interference	Section 430 (1.1) of the Criminal Code
Article 5—System interference	Section 430 (1.1) of the Criminal Code
Article 6—Misuse of devices	Section 326 (1)(b) of the Criminal Code Section 327 (1) of the Criminal Code
Forgery and online fraud	
Article 7	Section 366 of the Criminal Code
Article 8	Part X of the Criminal Code
Child sexual-exploitation materials	
Article 9	Section 163.1 of the Criminal Code
Copyright infringement	
Article 10	Section 42 of the Copyright Act Criminal Remedies

As has been demonstrated throughout this book, ethical hacking almost always involves a form of unauthorized access, modification, or interference with data, a network, a computer, or a device connected to a network. Both the convention and Canadian law cast the net wide, with broad provisions. Indeed, all jurisdictions who have ratified the convention cast a wide net, with no security research or public-research exceptions to the criminal provisions. Curiously, the exceptions only apply to copyright. For instance, in Canada there are exceptions to the infringement of copyright found in sections 29 through to 32 of the Copyright Act. The most relevant exceptions are Security (s. 30.63) and Encryption Research (s. 30.62). Where a person has consent/authorization to perform a range of cybersecurity functions, such as assessing the vulnerability of a computer, the exception applies. This makes perfect sense given that criminal laws don't apply where hackers are authorized to "hack" a system. Under the Canadian Copyright Act, encryption research is exempted provided it is not practical to do the research without making a copy, the work has been lawfully obtained, and the copyright owner has been informed. Note, informed—this is a lower threshold than consent. Curiously, there is no exception for encryption research under the Criminal Code. So, if a researcher informed a copyright owner, and the other conditions were met but the copyright owner did not want the researcher to continue with the research, there would be an exemption for copying the code. However, the researcher could still foreseeably be charged with a computer offence under the Criminal Code, where there are no exemptions.

Less relevant to ethical hacking are the online-fraud and child-pornography provisions. In the examples where credit-card information was copied and then used to make donations to charity as an act of protest, the law has clearly been broken, with no exemptions in place. There should not be any exemptions for theft, even when done for a seemingly altruistic motive. Likewise, where ethical hackers work to expose people who engage with child pornography, or where ethical hackers take down Dark-Net forums dedicated to such, they will likely inadvertently have accessed child pornography. There are no exemptions for these acts either. Ethical hackers are always at the mercy of law enforcement, under prosecutorial guidelines, as to whether they will be charged with an offence. Though, as will be explored below, attributing an act to an individual and pressing charges with a successful prosecution are made difficult

due to attribution, jurisdiction, and evidence collection, among other factors.

12.2 Attribution

Many different techniques exist to make attack traceback difficult. These technologies/techniques are tools of obfuscation, as they allow people to evade technological controls and legal sanction.[1] As discussed in chapter 2, commonplace obfuscation techniques include dynamic DNS, multihoming, fast flux DNS, distributed C&C (super botnet), encryption, proxy servers, TOR, virtual platforms, rootkits, cloud, IoT, and the use of P2P channels. These tactics allow people to hide behind a cloak of anonymity and lower the possibility of attack traceback.

Take the example of traceback to an IP address. Security researcher Guillaume Lovet describes the difficulty of traceback to the IP address of a botnet master in the following persuasive manner:

> To put it simply, when a stateful Internet connection (a.k.a. a TCP connection) is established between Alice and Bob, Alice sees Bob's IP address. Thus if Bob does bad things to Alice via this connection, his IP address can be reported. Now, if Cain connects to Bob, and from there, connects to Alice with bad intentions, Alice will still only see Bob's IP address. In other words, Cain has masked his IP address with Bob's. The component which allows Cain to use Bob as a relay is called a proxy (there are various types of proxies, though in cybercriminal schemes socks4 and socks5 proxies are mostly used). Such a component, of course, may have been installed on Bob's computer without his knowledge, by Cain. Or by Daniel, and Cain just rented or purchased access to it. As a matter of fact, most trojans and bots embed a proxy, and in any case, have the capability of loading one after prime infection. Given the prevalence of bot-infected machines (a.k.a. zombie computers), that makes a virtually endless resource of proxies for cybercriminals, all sitting on machines of innocent, unaware users. This is something cybercriminals understand perfectly and exploit ruthlessly, sometimes on a large scale.[2]

When an obfuscation method such as a proxy or fast-flux is utilized, traceback will often only lead to the infected bots that form part of the botnet. Once the IP address is known for the bot, the individual who has registered the Internet connection from that computer to the ISP may be contacted. Of course, bots are devices of innocent third parties. An IP address of a bot does nothing to show you who is in control of the botnet. Even in the rare event that the botnet master is discovered, this won't necessarily tell you who launched the DDoS protest because someone could have rented out the botnet, or hired the botnet master to perform the protest.

As always, an IP address does not necessarily reveal who used a computer to perform a crime. If a computer is used by several people, identifying the botnet master will require additional evidence other than a mere IP address. The botnet master may only be targeted upon discovering where the C&C is occurring and tracing back through proxies to the original source. Discovering the C&C point where a botnet receives its instructions from, however, neither reveals the exact computer source nor the identity of the botnet master. Increasingly, cloud services and the IoT are used to connect to botnets. In the rare chance that the identity of a botnet master can be traced, the botnet master can always use Trojan-horse or bot defences, which may or may not prove successful (see below). Of course, whether it's a botnet or other, the botnet master may not even be the perpetrator of an act. They could have merely rented out their services on the Dark Net. This is common.

As noted in previous chapters, many online civil-disobedience participants do not have the computer skills required to use such obfuscation techniques. They are often limited to using open-source LOIC. That tool does not use measures to hide IP addresses. As was seen in the case of Matthew George, he did not use other anonymizers such as a VPN or TOR to connect to LOIC because he believed that he was participating in a lawful protest. Only those with limited technical skillsets are likely to be prosecuted for DDoS as a form of protest. Those with a modicum of technical savvy will either use a different technology or use LOIC with TOR and/or VPN. This then makes attribution difficult.

12.3 Jurisdiction

Computer crimes often involve parties located abroad. These crimes may involve people located in different jurisdictions, whether they are different states or provinces within a country or different countries altogether. Each jurisdiction may have its own laws dealing with an issue as well as its own unique set of evidence procedures in courts. Uniformity is a real problem. Successful prosecution often involves assistance and cooperation of authorities from an outside jurisdiction. For a variety of reasons, some jurisdictions may or may not be willing to cooperate. Such cooperation generally must proceed through the cogs of bureaucracy in cases where time and access to good digital evidence (unaltered) is of the essence. This often means applying for warrants in multiple jurisdictions, which may translate into a loss of valuable time, and perhaps a loss of obtainable evidence.

The greatest challenge, however, remains in identifying and determining the physical location of the computer, and then the actual individual(s) who used the computer/network to commit a crime. Police in Canada, for example, cannot obtain a warrant to wiretap someone in Mongolia, and they cannot compel an ISP in Papa New Guinea to provide data logs. This type of international policing requires the cooperation of law enforcement and courts in other jurisdictions. Law enforcement could contact authorities in the location of the hacker, but cooperation may not be forthcoming. First, inter-jurisdictional investigations rely on the offence being given similar priority in both jurisdictions. For truly repugnant cases, such as child pornography, jurisdictions tend to have similar strong mandates.[3] In the case of hacking (i.e., unauthorized access), the priorities are often disparate. This is especially true in jurisdictions without computer-misuse offenses. It is of no coincidence that WikiLeaks servers are located in protective jurisdictions. The LulzSec website is rumoured to be located in a protected cloud space.

The situation is somewhat reversed when subpoenas for data logs are sent to US-based communication services such as Google, Twitter, or Facebook. In this instance, the law of the server—where the server is physically located where possible—prevails. For example, if I am a Twitter user located in Australia, an American law-enforcement entity may issue an administrative subpoena without a warrant or transparent declaration of the scope of a criminal investigation to actively retrieve all data logs connected to a hashtag.

For example, one could request all communications, IP addresses, and subscriber information for everyone who communicated in the Occupy Wall Street movement, including those of people around the world. In this sense, the international criminal-justice system, by way of established treaties and data protection of citizens in foreign countries, is subverted. The law of the server (often in the United States) prevails. Where data is hosted on a cloud server, and the physical location is unknown, jurisdiction is even more difficult to ascertain.

The second challenge is related to the first in that police tend to use their resources to respond to local problems. Where there is no victim in the locale of a particular police force, priority there will not be given to an overseas investigation. Third, there is the "de minimus rule," whereby in order to justify valuable police resources, a certain threshold of damages must be met. The jurisdictional hurdles stem from practical considerations as well as a lack of criminalization of an act across jurisdictions.

IFW Global is a company that conducts private investigations of cybercrime and, in particular, criminal-fraud syndicates. In our work (recall that I am on the board of directors) we took down the international fraud group known as the Bristol Boys. The investigation lasted over two years and involved twenty-five separate jurisdictions with registered companies, physical locations of servers and offices, virtual offices, bank accounts, and more—see figure 20.

Figure 20. Jurisdictions Involved with the Bristol Boys Investigation.

Although the case involved online organized cyber fraud, the jurisdictional issues for ethical hacking are similar, especially when people from various points in the world anonymously participate in an ethical-hacking incident.

12.4 Evidence

One of the greatest challenges for ethical-hacking prosecutions is how evidence is obtained. If governments are outsourcing intelligence to security firms, it is likely that many of such firms will use hacking methods to obtain their information. There is no legal mechanism that allows such firms to perform such actions. There is furthermore no way to ensure the accountability of such firms at present. Nowhere was this more apparent than in the WikiLeaks Operation Payback, and the responses by LulzSec and Stratfor.

One assumes that evidence collected by law enforcement is done according to the law, but this too turns out to be a murky legal area. For example, in 2001 the US Federal Bureau of Investigation lured two Russian criminal hackers to Seattle under the guise of a job offer with an FBI-devised corporation, Invita. Alexey Ivanov and Vasily Gorshkov were arrested shortly after arriving to the US. What they thought would be a job interview quickly turned into an interrogation from law enforcement. The two had allegedly broke into the networks of banks and other companies. The FBI remotely installed keylogging Trojan horses on the suspects' computers and collected evidence, including the passwords to email accounts while the pair were at the ruse job interview, where they were asked to prove that they were competent hackers. Incriminating evidence from the suspects' computers and servers utilized for email were used to convict the two on charges under the Computer Fraud and Abuse Act, as well as on twenty counts of conspiring to commit fraud and a number of fraud counts.[4] The evidence was collected without a warrant, but a US court nonetheless deemed the evidence valid, rejecting motions for its suppression. The court ruled that the right against unreasonable search and seizure under the fourth amendment was not violated because the accused had no right to privacy when using computers at "Invita."

12.5 Integrity, Volatility of Evidence, and the Trojan-Horse Defence

Digital evidence suffers from volatility. Volatility refers to the ease by which one may alter or damage evidence, whether it is done accidentally or intentionally. This in turn makes it relatively easy to expunge volatile evidence and to create "reasonable doubt." For example, the mere making of a copy of a file and putting it onto a USB memory stick interferes with the integrity of the digital evidence. Another common example is when an employee with a company's technical division takes it upon herself to view a quick online tutorial then proceeds to install and use forensics software on the company's computer or server. When forensics software and equipment are used without proper training it is probable that the integrity of the evidence will be jeopardized. Forensics investigators, by way of example, use a device which makes tampering with evidence impossible and take a virtual snapshot of a computer or server (if possible), which can then be analyzed at a later date. Without such preventative measures, digital evidence is subject to being expunged from evidence.[5] Forensics investigators have these basic technologies which allow for proper collection and preservation of data. The concern, therefore, is not that such technologies are not widely available or that their cost is prohibitive. The concern is one of education and training. When proper forensics techniques are not used, the integrity of the evidence is lost.

Where technology is involved in a crime, the accused will often use the Trojan-horse or bot defence. In the case of the former, a party claims that they are not responsible for an action but, rather, a malicious software program such as a Trojan was unknowingly downloaded to their computer by a third party. In the bot defence, the argument is that the defendant's computer became a bot and was controlled by a malicious third party. Thus, software or a bot is to blame. In the case of a botnet, it may seem odd that a Trojan-horse defence would be tried when the criminal act is often the very installation of unauthorized software onto someone else's computer. This, however, is not necessarily the case. A botnet master, for example, could argue that his/her computer was being used as a proxy to make it look as though the botnet was installing Trojans. This argument could conceivably extend to the claim that C&Cs were orchestrated to come through his/her computer via malware, where the bots

(software programs) were installed by a third party. Alternatively, a botnet master might claim to operate a botnet but could make the argument that a third party (another botnet master) took over his/her botnet through the issuance of an unauthorized bot (software code) to perform illegal acts.

An example of such successful defence is a judgement in the United Kingdom against Aaron Caffrey. Caffrey, aged nineteen, was charged with launching a DDoS attack on September 20, 2001, affecting computers serving the Port of Houston, Texas.[6] The attack caused major havoc with shipping logistics. The accused claimed that a malicious program had been installed on his computer, that he did not perform such acts. The jury acquitted in spite of the fact that upon examination, common hacker tools were found on the defendant's computer, the defendant was a known hacker who regularly participated in discussion of how to launch DDoS attacks and other types of malware, while possible forms of malware were absent on the defendant's computer.[7] The evidence was overwhelmingly in favour of a successful prosecution, but the technical evidence was presented in a confusing manner, which one journalist described as:

> Had the jurors been technology experts, or even computer-literate, I wonder if the ruling would have been the same. I spent most of the first week of the trial in the public gallery and found it didn't take long before the jury's eyes glazed over because the technical arguments sounded like a Russian version of Moby Dick that had been translated into English using Babelfish. By the third day, one of the jury members had to be discharged because of a severe migraine, which was indubitably brought on by the jargon.[8]

This case reinforces that while digital evidence is volatile, even sound evidence can be subject to a Trojan-horse or bot defence due to the inability of jurors and judges to understand the technical complexities of some cybercrime cases.[9] While the Caffrey case did not involve an ethical-hacking incidence, rather an act that is clearly criminal with no justifiable motive, it still portrays the difficulties of prosecution.

12.6 Damages

In theory, if there has been unauthorized access or modification or impairment of data, an investigation may be mounted and perpetrators prosecuted. In practice, often a victim must be able to prove that a certain amount of money was lost or damage was done in order to prompt an investigation.[10] The amount is often pure conjecture. Many jurisdictions have predetermined thresholds amounts in order for an investigation to be launched. Arguably, many forms of unauthorized access or a denial-of-service attack for two hours may not cause enough damage to attract investigation. These thresholds are determined by prosecutorial services. Not all law-enforcement agencies have minimal monetary amounts in order to commence an investigation. In some jurisdictions, a decision to launch an investigation in the case of computer-related cybercrimes is dependent on a wide range of factors, including whether the crime is serious or organized crime, and whether the investigation is within the capabilities of the local police.[11]

That said, when the target of an act of hacktivism or online civil disobedience involves a government website, defence website, or other entities connected to critical infrastructure such as water, electricity, banks, and hospitals, the mere target of the protest makes it a priority for law enforcement.

12.7 Sentencing and Dealing with Mental Disorders—Addiction and Autism Spectrum (with PhD candidate Hannah Rappaport)

Cybersecurity legal cases often involve young men who have autism, are addicted to computers, and sometimes are both autistic and addicted to computers. The medical conditions are first explained below, followed by why cyber security, and in particular hacking, might be appealing to people on the autism spectrum, and why these characteristics may make people on the spectrum particularly talented at cyber security.

Autism is a lifelong neurodevelopmental condition that occurs in approximately 1 per cent of the global population. The term "autism spectrum" is used to reflect the wide scope of abilities and difficulties found within the autism community. The most recent version of the Diagnostic and Statistical Manual of Mental Disorders

defines autism-spectrum disorder as a deficit in social communication and social interaction, marked by restricted and repetitive behaviour, interests, or activities, with early onset. Unfortunately, this description focuses solely on the difficulties experienced by people on the autism spectrum and fails to acknowledge strengths that are often found in autistic individuals. A study investigating rates and types of savant skills in 137 autistic individuals found that thirty-nine individuals (28.5 per cent) met criteria for a savant or exceptional cognitive skill, although previous estimates have been lower. A postal survey of 5,400 parents of autistic children found that 531 (9.8 per cent) were reported to have savant abilities. Of this subset, the most common skills were music (53 per cent), memory (40 per cent), mathematical/calculation skills (25 per cent), and art (19 per cent).

A growing body of research suggests that autistic individuals who are considered high functioning (i.e., average or above average intelligence) outperform their neurologically typical counterparts in a variety of visual local perceptual processing tasks, such as finding shapes embedded in a complex background. Autistic individuals also perform better in Raven's matrices, a nonverbal fluid-intelligence test in which participants use analytical abilities to complete visual patterns. One study found that autistics were on average 40 per cent faster than neurotypicals in solving the matrices.

Capabilities in visual perception are invaluable to the cybersecurity sector, where the ability to spot anomalies in large data sets is paramount. Indeed, there is a growing interest in the skills and talents that people on the autism spectrum can bring to the workplace. For example, in 2012 the Israel Defense Forces established an intelligence unit, called Ro'im Rachok ("seeing far"), which specifically recruits high-functioning autistic teenagers and young adults to analyze aerial reconnaissance photographs. The unit was founded by two former Mossad agents who recognized that certain individuals on the autism spectrum may be uniquely skilled in noticing anomalies in complex images. While software may one day replace the human decipherer, the leaders of the unit believe that this is not yet on the horizon. In addition to the military benefits, the Ro'im Rachok program facilitates social interaction, encourages independence, and helps participants to prepare for future careers.

The Israelis are not the only ones who have noticed the employment potential in the autism community. In March of 2017, the

Defence Academy of the United Kingdom hosted a collaborative industry event to discuss the skill sets of people on the autism spectrum and how these skills could fill gaps in the cyber sector.

A number of companies, including Microsoft and EY, are also beginning to recognize that people on the autism spectrum may provide invaluable skills to their workforce, and such companies are now dedicated to training and employing autistic adults. Burgeoning interest in recruiting autistic individuals is an exciting development, given that currently only 16 per cent of adults with autism are estimated to be in full-time employment. Autistic talent is often missed due to overreliance on the interview process in employment or to the lack of flexibility on the part of companies.

While some governments and organizations are looking to use the unique skillset of individuals on the spectrum, the unemployment rate remains very high among this group. It is of no surprise, then, that a higher than normal portion of "hackers," ethical or otherwise, are on the spectrum.

We have seen in previous chapters participation in ethical hacking by LulzSec member Ryan Cleary, activist Aaron Swartz, and hacker Adrian Lamo—all identified as being on the autism spectrum, having Asperger's syndrome. Recall that Cleary was involved in the highly controversial WikiLeaks MasterCard showdown with Stratfor.[12]

The nineteen-year-old Cleary was also arrested in Essex in the United Kingdom, where was charged under the Computer Misuse Act for his hacking effort of the UK's Serious Organised Crime Agency. He is alleged to have broken into many other law-enforcement agencies, both in the United Kingdom and the United States. Cleary is purportedly a member of LulzSec. He is said to suffer from agoraphobia and he has been diagnosed with Asperger's and attention-deficit disorder. Similar cases against hackers in the United Kingdom, Australia, and New Zealand in the last ten years have involved people addicted to computers, those who suffer from agoraphobia, and others on the spectrum disorder or have attention-deficit disorder. A hacker who went by the handle Wandii was acquitted on all counts of computer misuse in the United Kingdom due to a computer addiction. A nineteen-year-old New Zealand hacker, Owen Walker, was brought up on several charges of computer misuse. The first charge was under section 252(1) of the New Zealand Crimes Act 1961, accessing a computer system

without authorization. The second charge related to interfering with a computer system under section 250(2)(c) of the act. The third charge was the use of a computer system for dishonest purpose under section 249(2)(a). He was additionally charged under section 251(a) and (b) of the act for possession of software for the purpose of committing a crime. Walker pleaded guilty to all charges. He could have been sentenced to up to sixteen years of imprisonment under the four offences, but was instead discharged without conviction and was ordered to pay NZD$9,526 in reparation, as well as to relinquish any assets acquired as a result of gains he achieved through the use of his botnet. The court noted that Walker committed the crimes over a two-year period when he was aged sixteen to eighteen. The court heard evidence of Walker's difficulty in socializing due to Asperger's syndrome. Walker now works in Melbourne, Australia, for Telstra (the largest telecoms and ISP in Australia). There has been no study that has looked at the link, if any, between agoraphobia, Asperger's, or attention-deficit disorder and hackers.

Aaron Swartz, a renowned computer-science genius and passionate human-rights advocate, was arrested by MIT campus police and a US Secret Service officer on break-and-enter charges in 2011. Swartz had been downloading the JSTOR repository[13] (JSTOR is a non-profit organization that compiles academic journal articles, many of which, held in its digital library, are protected by copyright laws), and it was suspected that Swartz intended to put the contents of the database online so that everyone—whether rich or poor, educated or not—could have open access to these articles.

The threat of thirteen separate counts of wire fraud and other serious computer offences, which could have seen him jailed for over thirty-five years and liable for US$1,0000,000 in fines, proved to be too much for Swartz, who committed suicide, aged twenty-six. Swartz had authorized access to several of MIT's databases, including JSTOR, and there is a good chance that he would not have been found guilty of the charges. Clearly an action for copyright infringement would have provided the most appropriate remedy if Swartz was liable, yet the government chose a different path, to prosecute.

It is alleged within internal hacking circles[14] that the real controversy was that Swartz was the source of many confidential leaks to WikiLeaks, and in particular certain congressional research reports, which may have been part of the **Guerrilla Open Access Manifesto**, a movement that Swartz had started. The congressional reports in

question were not in the public domain; they are often used as a type of currency or bartered good among lobbyists and special-interest groups. There are many proponents to making these reports available to the public, including support from US Senator John McCain, the 2008 Republican presidential nominee (now deceased). It *might* also be the case that Aaron aided in the leak of the Manning materials, US military documents (mostly about the war in Iraq and Afghanistan) unlawfully released by US Private Bradley Manning to WikiLeaks. It is perhaps of no coincidence that Swartz's home was searched and computer equipment seized around the same time as the Manning material was published. It is also interesting to note that if you Google "the Manning materials" or "Manning materials" you will not be sent to WikiLeaks or other mirror sites. You will only find media coverage of the Bradley Manning trial and conviction. This is of no coincidence. These materials have been removed by companies such as Google by order of the United States government, though you will find no legal documents to support this removal as such requests are secret under national-security legislation.

The case of Lamo was perhaps the most curious. Adrian Lamo was convicted in 2003 for hacking into the network of the *New York Times*, among other targets and other hacks.[15] He too is identified as having Asperger's syndrome. The curious part, however, is that he was the FBI informant who handed over evidence that led to the discovery and arrest of Bradley Manning. How Lamo was linked to Manning remains surrounded with questions. What is particularly intriguing is the that you have three individuals involved with WikiLeaks in very different ways who are all on the autism spectrum.

Individuals on the autism spectrum charged with hacking offences have been treated differently depending on the jurisdiction. In New Zealand, a nineteen-year-old man charged with several counts of computer offences was given a suspended sentence, ordered to pay a modicum of damages for a DDoS attack against Carnegie Melon, then was recruited by Telstra and the New Zealand police to work for them.[16] Contrast this with the United States, where some individuals on the spectrum have been given twenty-five-year sentences.[17] Others have been given suspended sentences provided they become FBI informants and betray others, as has been the case with members of Anonymous who turned on other members.[18]

12.8 Observations

Ethical hacking is a messy area with no clear or obvious legal resolution. There has been no research to date that examines how many hackers and ethical hackers have Autism or common diagnoses. If this eventual research reveals a connection, more thought will need be given as to how to best deal with this.

A most problematic theme has emerged with hacktivism. Many hacktivists seek to rebel against what they perceive to be unjust policies or measures that infringe against civil liberties. As a consequence of the flurry of hacktivist activities, however, governments around the globe are using more and more forms of surveillance, and civil liberties are eroding further than in the pre-hacktivism era. At this point, it is a vicious circle with laws being broken by both sides.

It would be interesting to see what degree of law-enforcement resources are being allocated to hacktivist investigations compared with resources allocated to the fight of online organized crime, such as in mass fraud, identity theft, and corporate espionage. The other aspect in this area that is rarely spoken about is the visibility of hacktivists. Hacktivists often perform acts that are deliberately public or done in a matter to get media attention to a cause. Other malicious entities sit silently on systems, performing far more nefarious acts. But because they are stealthy there is less attention and certainly less prosecution. A more detailed look at the legal provisions from the Convention on Cybercrimes and the Canadian Criminal Code is found in table 4.

Table 4. Comparison of Convention on Cybercrime and Canadian Criminal Framework (expanded)

Convention on Cybercrime	Canada
Offences against the confidentiality and availability of computer data and systems	
Article 2—Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Section 342.1 of the Criminal Code** Unauthorized use of computer to commit an offence in relation to Section 430. Computer System = a device that, or a group of interconnected or related devices, one or more of which, (a) contains computer programs or other data, and (b) pursuant to computer programs, (i) performs logic and control, and (ii) may perform any other function Data = representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system
Article 3—Illegal interception Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	

Convention on Cybercrime	Canada
Article 4—Data interference 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Section 430 (1.1) of the Criminal Code** Commits mischief which amounts to an indictable offence for the wilful destroying, altering or interferes with the lawful use of data
Article 5—System interference Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	
Article 6—Misuse of devices 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a) the production, sale, procurement for use, import, distribution or otherwise making available of: i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and	**Section 326 (1)(b) of the Criminal Code** Commits theft who fraudulently, maliciously or without a colour of right uses any telecommunication facility or obtains any telecommunication services **Section 327 (1) of the Criminal Code** Without lawful excuse, the proof of which lies on him, manufactures, possesses, sells or offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for obtaining the use of any telecommunication facility or service, under circumstances that give rise to a reasonable inference that the device has been used or is or was intended to be used to obtain the use of

Convention on Cybercrime	Canada
b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.	any telecommunication facility or service without payment of a lawful charge therefor, is guilty of an indictable offence.
Forgery and online fraud	
Article 7 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Section 366 of the Criminal Code** Deals largely with forgery and offences resembling forgery. However, there are no provisions for forgery committed by the way of alteration of computer data resulting in inauthentic data with intent to be considered or acted upon as if it were authentic.

Convention on Cybercrime	Canada
Article 8 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a) any input, alteration, deletion or suppression of computer data, b) any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.	**Part X of the Criminal Code** Deals largely with fraud and related fraudulent conduct. However, there are no provisions for fraud committed of computer data using a computer system.
Child sexual exploitation materials	
Article 9 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct;	**Section 163.1 of the Criminal Code** Subsection 1—Definition Similar to Clause 2, 3 & 4 in corresponding Article Subsection 2—Making child pornography No indication of said offence depicting production of child pornography for the purpose of its distribution through a computer system. Subsection 3—Distribution Distribution of any child pornography guilty of an indictable offence punishable on summary convictions. No indication of said offence depicting offering or make available or distribute or transmit or procure of child pornography through a computer system. Subsection 4—Possession No indication of said offence depicting possession of child pornography in a computer system or on a computer-data storage medium.

Convention on Cybercrime	Canada
b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.	*An Act respecting the mandatory reporting of Internet child pornography by persons who provide an Internet service, SC 2011, c* 4. Act that requires mandatory report of Internet child pornography activities by Internet providers. Corresponding Regulation: Internet Child Pornography Reporting Regulations, SOR/2011-292
Copyright infringement	
Article 10 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting	**Section 42 of the Copyright Act Criminal Remedies** **Offences** **42 (1)** Every person commits an offence who knowingly **(a)** makes for sale or rental an infringing copy of a work or other subject-matter in which copyright subsists; **(b)** sells or rents out, or by way of trade exposes or offers for sale or rental, an infringing copy of a work or other subject-matter in which copyright subsists; **(c)** distributes infringing copies of a work or other subject-matter in which copyright subsists, either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright; **(d)** by way of trade exhibits in public an infringing copy of a work or other subject-matter in which copyright subsists;

Convention on Cybercrime	Canada
Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	**(e)** possesses, for sale, rental, distribution for the purpose of trade or exhibition in public by way of trade, an infringing copy of a work or other subject-matter in which copyright subsists; **(f)** imports, for sale or rental, into Canada any infringing copy of a work or other subject-matter in which copyright subsists; or **(g)** exports or attempts to export, for sale or rental, an infringing copy5 of a work or other subject-matter in which copyright subsists. **Possession and performance offences** **(2)** Every person commits an offence who knowingly **(a)** makes or possesses any plate that is specifically designed or adapted for the purpose of making infringing copies of any work or other subject-matter in which copyright subsists; or **(b)** for private profit causes to be performed in public, without the consent of the owner of the copyright, any work or other subject-matter in which copyright subsists.

Convention on Cybercrime	Canada
	Punishment **(2.1)** Every person who commits an offence under subsection (1) or (2) is liable **(a)** on conviction on indictment, to a fine of not more than $1,000,000 or to imprisonment for a term of not more than five years or to both; or **(b)** on summary conviction, to a fine of not more than $25,000 or to imprisonment for a term of not more than six months or to both.

Notes

1. Lovet 2009.
2. Lovet 2009, p. 2.
3. Wall 2007.
4. *United States of America v. Gorshkov.*
5. Klein 2010.
6. The case is not reported in law databases but was covered by the British media and is mentioned by several cybercrime researchers. See BBC News, "Questions Cloud Cyber Crime Cases." The case is cited as *R v. Caffrey* (2006) in Clayton 2006.
7. Grabosky 2007.
8. Brenner, Carrier, and Henninger 2004.
9. Walden 2010.
10. de Villiers 2003.
11. Correspondence with Detective Van der Graf, head of the fraud squad, New South Wales Police.
12. Batty 2011.
13. Poulsen 2013.
14. This information has been given to me in confidence from a reliable source.
15. Poulsen 2010.
16. *Sydney Morning Herald*, "Telstra offshoot hires teen hacker 'Akill.'"
17. Ronson 2009; Poulsen 2010.
18. Bastone and Goldberg 2014.