CHAPTER XIII

Ethical Hacking, Whistle-Blowing, and Human Rights and Freedoms

If we accept Martin Luther King Jr.'s statement "injustice anywhere is a threat to justice everywhere" as true—as I believe we must—we should be grateful that, in the twenty-first century, the Internet provides an effective medium to expose grave injustices perpetuated around the world. While it is not suggested that the Internet itself offers a solution to correct these problems, its existence enables the facilitation of the first of King's four basic steps in a non-violent campaign: "[C]ollection of the facts to determine whether injustices are alive." While it is accepted that the quality of information provided might be affected by personal opinions and beliefs, or may be manipulated, it still enables the collection and discussion of injustices throughout the world. King's discussion of being "caught in an inescapable network of mutuality, tied in a single garment of destiny" reminds us of metaphors of the Internet as a net or a web. King's remarks portend the capability of the Internet to enable protest from anywhere about activities anywhere because of the Internet's proliferation, and because it is not tied down to a geographical location.

In my interview with hacker and hacktivism expert Dr. Dreyfus, she stated that there was usually a correlation between the number of participants in an online protest and the worthiness and morality of the cause.[1] While this finding suggests that the unnoticed pleas for support using social media are less meritorious in the eyes of

the masses, this must be considered against King's assertion that "if repressed emotions do not come out in these nonviolent ways, they will come out in ominous expressions of violence." It is worth considering here a movement by Ronny Edry, an Israeli graphic designer, who posted an image on Facebook showing himself with his daughter along with the graphic: "Iranians, we will never bomb your country. We [heart] you." The image garnered such international support it became a catalyst for dialogue between the people of two nations on the brink of war.[2] The point of this is to illustrate the effectiveness of non-violent forms of protestation and really emphasize the values exposed by King. "I [heart] Iran," however, is very different from the acts of hacktivism and online civil disobedience covered in this book.

In many instances, it is not difficult for us to look at some of these hacking acts differing only with regard to intent. While we may agree, for instance, that hacking into the Sony database as an act to contest Sony's lapse security practices breaks the law, we might also agree that such hacktivists should not be prosecuted or punished in the same fashion as someone who hacked into the system for personal and financial gain (e.g., stole and then used third-party credit-card information). It becomes more difficult to see acts of denial of service or online defacements as criminal acts attracting harsh sentences of computer offences under the criminal law. Should DDoS attacks be seen more as acts of political barricades? Should online defacements be considered as a form of leafleting or picketing? What role does freedom of expression and freedom of peaceful association play in this equation?

13.1 The Canadian Charter of Human Rights and Freedoms

The Canadian Charter of Human Rights and Freedoms[3] is the constitutional framework in Canada that legally provides for rights and freedoms for not only Canadian citizens but for those physically in Canada. The Charter is used in this chapter as a way of engaging the content through the lens of human rights. The Charter is further considered one of the strongest protections of human rights of any legal framework in the world. Courts around the world look to decisions rendered under the Charter for guidance in their own jurisdictions.

Online civil-disobedience participants are motivated by the same reasons as participants in traditional off-line acts of civil

disobedience. For example, consider the off-line and online acts of civil disobedience in table 5.

Table 5. Off-line and Online Comparison

Off-Line	Online
Sit-ins	Virtual sit-ins
Barricades	Denial-of-service attacks and website redirection
Political graffiti	Website defacements
Wildcat strikes	Denial-of-service attacks and website redirection
Underground presses	Site parodies, blogs, Facebook protests
Petitions	Web petitions (e.g., Facebook likes)
Whistle-blowing	Unauthorized taking of information (often via hacking) and leaking it to another organization or to the media

Table 6 presents some off-line acts and provides the relevant Charter protection as well as leading case law and legal principles.

Table 6. Leading Case Law and Legal Principles

Action	Charter Protection	Legal Principles	Leading Case Law
Picketing	• Freedom of Expression (s. 2b of the Canadian Charter and art. 3 Quebec Charter of Human Rights and Freedoms) • Freedom of Peaceful Assembly and Association (s. 2(c) of the Canadian Charter and art. 3 of the Quebec Charter)	• Picketing falls under freedom of expression. • It does not extend to acts of violence. • It does not extend to destruction of property, assault or other unlawful conduct. • Picketing may be restricted if it is inconsistent with the function of the place it takes place in. • Injunction is unlikely to be granted if the police can control the situation.	• *K Mart Canada Ltd v. United Food and Commercial Workers* • *R.W.D.S.U., Local 558 v. Pepsi-Cola Canada Beverages* • *Dolphin Delivery Ltd v. RWDSU* • *Chum Ltd v. NABET* • *Blackstone Industrial Products Ltd. v. Parsons (1979)* • *Ontario Public Service Employees Union v. Ontario (Attorney General)*

Action	Charter Protection	Legal Principles	Leading Case Law
Protesting	• Freedom of Expression (s. 2b of the Canadian Charter and s. X Quebec Charter) • Freedom of Peaceful Assembly and Association (s. 2(c) of the Canadian Charter and art. 3 of the Quebec Charter)	• Comes within freedom of expression because it is an effort to influence social/political decisions. • Comes within peaceful assembly because it allows assembly for the purposes of protesting state action. • Unlawful strikes are still protected as "expression." • However, not all government property can be used as a physical areas on which to protest. • Public streets can be. • As with picketing, it can be restricted if it is inconsistent with the function of the place it occurs in.	• *HEU & BCTF et al. v. HEABC & BCPSEA* • *Re General Motors*
Graffiti	• Freedom of Expression (s. 2b of the Canadian Charter and art. 3 Quebec Charter)	• Graffiti falls under freedom of expression because the forms of "expression" can be written and/or artistic. • If the graffiti contains political commentary and social expression, it is protected by the Charter.	• *Ontario (Attorney-General) v. Dieleman, 1994 CanLII 7509 (ON SC)* • *Cherneskey v. Armadale Publishers Ltd. (1978), 1978 CanLII 20 (SCC), 90 D.L.R. (3d) 321 at p 330*

Action	Charter Protection	Legal Principles	Leading Case Law
		• This protection also extends to pictures or photos. • Offensive or insulting graffiti is not reason enough to restrict it. • If the act involves violence it is not protected by the Charter. • Some suggestion that neither Canadian nor Quebec Charters protect property damage.	• *Irwin Toy Ltd. v. Quebec (Attorney-General), supra, at p 606-8* • *R. c. Quickfall, 1993 CanLII 3509 (QC CA)*

Let us use Anonymous's Operation Titstorm as an example for our discussion. Participating in a denial-of-service attack against a parliamentary website is a form of protest. In this case, it was to protest censorship in Australia. The DDoS attack could be considered similar to a barricade. In this instance, images of penises and breasts were also displayed on the parliamentary website. It is difficult to see this SQL injection as being different from a form of picketing or leafleting outside of a parliament with similar images, or similar to spraying graffiti, albeit distasteful. The intent is the same—protesting government censorship.

In the Canadian context, freedom is a constitutional right under subchapter 2(b) of the Charter.[4] It has never been an absolute right in Canada. Freedom of expression is rationalized under three main ways: it is essential to democracy, it is an instrument of truth, and it is an instrument of personal fulfilment.[5] The Supreme Court of Canada accepted these rationales in *Irwin Toy v. Quebec*.[6] In *Irwin Toy*, the province of Quebec had introduced legislation targeting commercial advertising to children under the age of thirteen. This meant, for example, that commercial advertisements for toys during morning television cartoon programs were not allowed. Irwin Toy company unsuccessfully challenged the Quebec legislation on the grounds that it was an unlawful restriction on freedom of expression.

A number of cases following *Irwin Toy* further articulated these freedom-of-expression rationales.[7]

The Supreme Court's decision in *Kmart*[8] held that consumer leafleting was to be distinguished from other forms of picketing, such as striking employees. In *Kmart*, the court found that statutory regulation of labour strikes could be justified, but that such acts differed substantially from acts such as consumer leafleting. Depending on the content of an SQL injection, one could easily see the act as a form of consumer leafleting or of a public protest—both acts are protected under the Charter. *Irwin Toy* gave a broad power of freedom of expression, while *Kmart* gave a limited power for, as per the Charter, "freedom of peaceful assembly."

In *Dolphin Delivery*,[9] the Supreme Court of Canada, as per Justice McIntyre, stated that:

> There is always an element of expression in picketing. The Union is making a statement to the general public that it is involved in a dispute. This freedom doesn't extend to threats of violence. It would not protect the destruction of property, or assaults, or other clearly unlawful conduct.

In the case of a DDoS protest to a government website, such as the parliamentary website, which acts as an online a directory of Members of Parliament, it is difficult to see how blocking access for a short period of time would constitute the destruction of property. Once the protest stops, the website commences functioning again exactly as it did pre-protest. Indeed, there is no physical damage or destruction of property.

In *Ontario Public Service Employees Union*,[10] strikers picketed in front of provincial courts, thereby blocking access to the courts. The Supreme Court held that while picketing falls within the ambit of freedom of expression, an injunction to limit the activity was considered reasonable as access to courts is seen as an integral part of the rule of law. The question then becomes whether blocking access to a website can be seen as interfering with the rule of law. Here there are two hurdles. The first is how does one impose an injunction restricting a DDoS attack? This may be very difficult as it requires knowledge of who is protesting, addresses to serve notice (usually information links back to an IP address or a device and not an individual), and can only be served (at least easily) to people

participating in the attack in Canada. The second hurdle is one of rule-of-law threshold. Preventing people from accessing a court runs clearly in the face of impeding the law and rule-of-law principles. A DDoS attack against a website or portal for electronic submission of court documents might also be seen as impeding the rule of law. Impeding access, however, to information found on parliamentary websites strays far from principles of the rule of law. The Parliament of Australia website has information about senators and members, information on how the Senate and House of Representatives works, list of the various committees, current bills, and provides access to the Parliamentary Budget Office and Parliamentary Library.[11] The website provides information and is not the sole provider for such widely available public information. If the DDoS protest had occurred on a more specific government website preventing people from accessing health portals, social assistance, or immigration portals, then this becomes more about restricting access to essential services, which could be argued to limit sections 2(b) and 2(c) of the Charter. Not being able to access the parliamentary website, however, for a day or two neither impedes the rule of law or essential services. It is difficult to see how such activity should not be seen as a legitimate and protected protest.

Of course, online acts of civil disobedience and hacktivism have a unique feature—they are potentially more inclusive. There may be 100,000 people spread across North America who wish to protest army deployment or climate-change policy, but it is extremely difficult, and for some impossible, to meet up in person to protest on the ground. Online platforms by their very nature can enable people from disparate backgrounds and physical locations to join in solidarity for a cause.

As we saw in chapter 7, the #TellVicEverything Twitter campaign was lawful and fell outside of criminal-law provisions on unauthorized access and use of interference. However, we noted that if the same volume of traffic for the exact same purpose would have been directed at a website, causing it to crash, this would become a DDoS event, subjecting participants to the possibility of being prosecuted. Same method, same intent. Because one cannot "crash" or "DDoS" Twitter or a Twitter feed (or it would be extremely difficult), this is considered a legitimate form of protest. Using LOIC to launch a DDoS event at a website or server could trigger a response from prosecutors seeking to apply criminal-law legislation. It will

be interesting to see how higher courts deal with similar online acts of protests in the years to come.

13.2 Whistle-Blowing and Ethical Hacking

Hacktivism, as we have seen, goes beyond mere barricades and political graffiti, escalating to acts more aligned with whistle-blowing, as systems are often broken into to retrieve data. There is either unauthorized access where the person did have authority to view or copy documents and/or there is an unauthorized use where the person may have had authority to access the documents but such authority was subject to restrictions on consequent uses.

Whistle-blowing is the disclosure of illegal, immoral, or illegitimate practices of an organization by a member or employee of the organization.[12] Disclosure could be to the media, to a regulatory authority, or to the public in general (such as via disclosure on a website). Whistle-blowing involves the disclosure of otherwise confidential information where it is a matter of "public interest." Many jurisdictions have enacted legislation that shields a whistle-blowing member or employee of a government, corporation, or organization from criminal sanction and legal liability, including copyright. As will be seen, this protection is not, however, absolute.

The concepts of external and internal whistle-blowing are somewhat confusing.[13] The terms "external" and "internal" refer to the recipients of the information and not to the person who exposes the information. An internal whistle-blower is a member or employee of an organization who sends leaked information to someone within the organization. External whistle-blowing occurs when the person chooses to share the information with someone external of the organization. In some jurisdictions, both internal and external whistle-blowers are protected under the law, while in other jurisdictions the recipient must be internal.

Whistle-blowers enjoy legal protection in many jurisdictions. The United States, the United Kingdom, Canada, and Australia all have whistle-blowing legislation. Depending on which jurisdiction, whistle-blowers are protected from criminal charges, civil liability, and being fired for disclosing information about corrupt, illegal, or immoral practices of governments and corporations.

When someone external to an organization exposes wrongdoing they are not considered a whistle-blower and they are not shielded

from criminal sanction and legal liability. Third parties, therefore, are not protected by whistle-blower legislation. If an ethical hacker, for example, obtains a document by gaining unauthorized access to a computer, they are not considered a whistle-blower under legislation in the United States, the United Kingdom, Canada, and Australia. The primary goal of whistle-blowing legislation is to reduce—if not prevent—retaliation for exposure of malpractice or wrongdoing in the workplace. The goal of whistle-blowing has never been given a broad interpretation to cover third parties. Regardless of who blows the whistle and why someone blows the whistle, whether they be a government employee or an ethical hacker, the goal remains essentially the same—to expose wrongdoing.

Ethical hackers are often not afforded legal protection when they disclose corrupt, illegal, or immoral practices of governments and corporations, as they are third parties in the disclosure process. Whistle-blowing legislation only offers protection to employees or members of an organization, which does not extend to third parties. In a typical scenario, an ethical hacker will access a database without authorization to retrieve information on corrupt practices. This information will then be published to a website, given to a newspaper and/or submitted to a leak site. This unauthorized access of data, a database or computer will constitute a criminal offence in Australia, the United States, the United Kingdom, Canada, and in many other countries. Most jurisdictions have enacted computer-related offences, which are often referred to as unauthorized access, modification, or interference to data systems or electronic communications. Such criminal provisions generally address situations where any component of a computer (hard drive, software, network) is tampered with allowing for unauthorized access, modification, impairment, or interference to data or a data system. The very nature of hacking—whether it be to expose corrupt practices or out of mere curiosity—involves the exploration (and sometimes exploitation) of vulnerabilities which, at a minimum, involve unauthorized access to data. There are no public-interest exemptions to criminal-computer offences in any jurisdiction.[14]

13.3 Observations

"May you live in interesting times"… an expression that, as they say, can be a blessing or a curse. Never before has so much information

been at the disposal of humankind. We have the ability to participate in online citizenship, to hide our identities behind encryption technologies, express our opinions no matter how misinformed or treacherous to anyone anywhere, to deliberately misinform others, to set trends, to share information, to manipulate data, and to participate in online protests in whatever form they may take. Our digital ecosystem and ways of communicating and thinking are changing due to technology.

Politicians and courts are often slow to adapt to the reality of the society in which they live. People, and younger generations in particular, have grown up in a digital world. People are so reliant on technology that it is a part of their everyday ecosystem to the point where the evolution of neurological connections in a human brain are adapting to technology exposure. It is not simply that people expect to do things online or through digital technologies; cognitively, the brain works differently now than it did twenty or thirty years ago by virtue of the fact that our neurological pathways change when we use technologies.[15] Neural pathways also change when we play or listen to music or make art.

Is it acceptable for one generation to curtail and insist upon set methods for online protests for younger generations? Is this the same as an entity requiring something to be handwritten, or typed on a typewriter as opposed to using a computer? Or insisting that people get to work by horse and buggy? Or that females may not drive a car? While these questions are somewhat sensationalized, they still get at the essence of the matter. To what extent is it permissible to insist on specific mediums of protest? Does this no longer make sense? As will be seen in the next chapter, I will advocate for changes to regulatory frameworks to better accommodate forms of hacking that fall within the range of ethical hacking.

Notes

1. Interview with Dreyfus, December 2010, Sydney, Australia.
2. Edry, "Israel and Iran."
3. Canadian Charter of Rights and Freedoms.
4. Canadian Charter of Rights and Freedoms.
5. See Moon 2000.
6. *Irwin Toy v. Quebec.*

7. *Edmonton Journal v. Alberta*; *R v. Keegstra*; *Dagenais v. Canadian Broadcasting Corp.*; *R. v. Sharpe*; and *R v. Zundel*.
8. *U.F.C.W., Local 1518 v. Kmart Canada Ltd.* This followed from the earlier Supreme Court decision in *R.W.D.S.U. v. Dolphin Delivery Ltd.*
9. *R.W.D.S.U. v. Dolphin Delivery Ltd.*
10. *Lavigne v. Ontario Public Service Employees Union.*
11. https://www.aph.gov.au.
12. A. J. Brown (n.d.). See also Gobert and Punch 2000.
13. Dworkin and Baucas 1998.
14. Maurushat, A. 2013.
15. Von Ooyen A. and Butz-Ostendorg M. *The Rewiring Brain.* Academic Press (an Imprint of Elsevier), 2017.

Page left blank intentionally