International Journal of Cyber Criminology
Vol 8 Issue 2 July - December 2014

The Greening of Canadian Cyber Laws: What Environmental Law can Teach and Cyber Law can learn

Sara M. Smyth[1]
Bond University, Australia

Abstract

This article examines whether Canadian environmental law and policy could serve as a model for cyber crime regulation. A wide variety of offences are now committed through digital technologies, including thievery, identity theft, fraud, the misdirection of communications, intellectual property theft, espionage, system disruption, the destruction of data, money laundering, hacktivism, and terrorism, among others. The focus of this Article is on the problem of data security breaches, which target businesses and consumers. Following the Introduction, Part I provides an overview of the parallels that can be drawn between threats in the natural environment and on the Internet. Both disciplines have innate characteristics that make them difficult to regulate, and which set them apart from other subjects. Part II looks at the current situation of cyber crime threats in Canada, as well as the Canadian government's regulatory response. It then goes on to trace the history of Canadian environmental law, as well as the many successes and failures that have been achieved in law and policy in this area. Indeed, policy-makers can learn a great deal from these efforts about the kinds of laws and policies that might be workable in the cyber-realm. Following this, Part III examines what specifically cyber-law theorists and policy-makers can learn from those in the environmental law field so as to move down a more appropriate, and effective, regulatory path. The article concludes with summary and further recommendations.

Keywords: Cyber crime, Regulation, Environmental Law, Policy, Comparative Law, Data Security Breach, Notification, Privacy.

Introduction

This article examines whether Canadian environmental law and policy could serve as a model for cyber crime regulation.[2] For the purposes of this Article, the term "cyber crime" will refer to the unlawful activities undertaken by criminals using the Internet and other electronic systems, primarily for financial gain. A wide variety of offences are now committed through digital technologies, including thievery, identity theft, fraud, the

[1]Associate Professor, Director, Canadian Law Program, Bond University, Gold Coast, Queensland, 4229, Australia. Email: ssmyth@bond.edu.au

[2] Note that this Article examines major trends in environmental law during the past several decades and does not purport to offer any statement or opinion on specific environmental laws or issues.

misdirection of communications, intellectual property theft, espionage, system disruption and interference, the destruction of data, money laundering, hacktivism, and terrorism, among others (Deloitte, 2010).

The focus of online threats continues to be aimed at compromising end-users for monetary gain, and attackers have honed their online victimisation techniques through the use of cutting-edge technologies and innovative networking strategies (Symantec, 2013). They have also taken advantage of the lack of inter-jurisdictional cooperation and regulatory enforcement in cyberspace. This places individuals and organizations in a position of significant risk because the threats posed to digital information and assets have far outpaced the ability of cyber-security professionals and law enforcement officials to respond (Deloitte, 2010).

This Article centres on the problem of data security breaches, which target businesses and consumers. Cyber criminals focused on profit can readily breach corporate security measures to commit identity theft, steal and then sell sensitive information to competitors, appropriate customers' confidential data, or otherwise misuse corporate name or product brands (Cisco, 2008). These attacks can be perpetrated through a variety of means, including spam, phishing and malicious software, or 'malware,' and they can expose a number of different types of confidential or sensitive information, including trade secrets, intellectual property, customer data, and employee information (Ponemon, 2013). Customer information includes consumers' credit card information, birth dates, government identification numbers, financial information, email addresses, home addresses, medical records, passwords, and other personal information (Symantec, 2013).

Once the victim's credentials have been stolen, individuals can be hired through the online underground economy to obtain currency directly from the accounts attached to them (Abad, 2006). Alternatively, stolen credentials can be sold in bulk through underground fraud forums, with the attacker taking a commission on the net proceeds (UK House of Lords, 2006). How can Canadian policy-makers deal with these threats? Without careful deliberation, attempts to mitigate danger can have the opposite effect of introducing new harms into the network, as well as stifling innovation, through invasive censorship and surveillance techniques.

We live in a world replete with risk and we typically use regulation as the best means of dealing with it; however, as is the case with many areas of the law, including environmental law and cyber-law, we also need industry to participate in the risk mitigation process (Sossin, 2014). At the same time, we cannot assume that businesses will make the best decisions because they have a powerful self-interest in maximizing their profits (Sossin, 2014). As well, political actors are motivated by popularity, and they must choose between, on the one hand, giving industry enough autonomy to achieve financial growth, especially given that global trade and competition are crucial in today's economy, versus, on the other hand, effectively responding to ever more complex and wide-reaching concerns (Wood, et. al., 2010).

Information security is one of the most critical aspects of the successful operation of any business (Prislan & Bernik, 2010). Virtually every organization, large and small, wants its information systems to operate securely; however, even the most robust security system remains vulnerable to exploitation by sophisticated attackers (Prislan & Bernik, 2010). Just as with the environment, information security is best achieved through the implementation of formal risk management programs by industry, and these initiatives can also promote proficiency, credibility and competitiveness in the global marketplace

(Prislan & Bernik, 2010). However, the decision to implement a risk-mitigation strategy is influenced by a variety of factors, including cost, the size of the organization, management awareness/concern for the threats, and the presence or absence of qualified personnel (Prislan & Bernik, 2010). Effective risk management can be realized through government-mandated legal requirements; however, Canadian legislators have been lax in developing legal remedies to address the problems arising from high rates of Internet penetration around the world.

In the uncertain yet rapidly evolving field of cyber crime, there is much to learn from those who spent the past fifty years or so trying to avert catastrophe in the natural world. Environmental law originated in response to a widespread social crisis during the 1960s about the threats posed by pollution and resource degradation (Lazarus, 2010). Before this, environmental laws were almost entirely absent from the North American legal landscape (Lazarus, 2010). Today, we can tell the story of how environmental law transitioned from one broad "generational" era to the next as extensive studies have been conducted, reports have been written, hearings have been held, and international discussions have occurred at the highest levels of policy on countless issues including the dumping of hazardous wastes, pollution reduction, oil transportation safety, and genetically modified foods (Arnold, 2010). Legal scholars have disputed the exact means of characterizing the generations, such as disagreeing about which generation of environmental law we are currently in; however, the precise categorization of the generations is not essential to this Article (Arnold, 2010).

From this perspective, one of the "richest and most relevant resources" in all regulatory law is the environmental movement (Hirsch, 2006). It has been at the forefront of the longstanding, passionate debate about the most effective way to regulate a widespread problem with international implications, involving public and private actors (Hirsch, 2006). As with other areas of the law, Canadian policymakers relied on American law and policy in shaping Canadian environmental law. In fact, in many areas of Canadian environmental law, legislators mimicked what had already been implemented south of the border, often in watery versions, after lengthy setbacks and delays (Wood et. al., 2010).

A primary objective of this Article is to trace the rise and fall of environmental law in Canada, from a labyrinth of complex and costly regulations through to deregulation, including voluntary or 'self' regulation,[3] which has become popular in Canada, the United States and Europe (Brouhle & Harrington, 2009). The observations are primarily restricted to developments in Canada, and the goal is to provide a general account of the growth of environmental law in Canada over a period of several decades. Of course, this approach may be criticized for being overly subjective; however, the focus is on identifying the broad social, political and economic underpinnings of Canadian environmental law and policy in order to discern what Canadian cyber-law scholars and policy-makers can draw from this expansive narrative.

[3] Voluntary, or 'self,' regulation is an alternative to command and control style regulation which allows regulated entities to be exempted from some command and control conditions, provided that they put forward different mechanisms for achieving the stated environmental objectives. The government generally sets out expansive performance standards but leaves it up to the regulated entity to come up with how it will achieve those goals.

One of the significant barriers of the past has been the over-reliance upon command-and-control style regulatory systems,[4] and the climate of hostility that they can generate (Fiorino, 1996). While these regulations were helpful in mitigating significant pollution problems during the first couple of decades of environmental law, their appropriateness for resolving complex challenges over the long term has been questioned since the early 1980s (Fiorino, 1996). Command-and-control style environmental regulation originated in the United States and was applied to a much greater extent in that country than it ever was in Canada (Fiorino, 1996). The Canadian style of environmental lawmaking was, in fact, largely consultative, whereby rules were established behind closed doors, in private consultations between government and industry (Fiorino, 1996). Canadian regulators also relied more substantially on voluntary industry cooperation and industry self-monitoring (Fiorino, 1996).

From the 1980s onward, Canadian politicians, particularly those with a conservative bent, criticized the bureaucratic nature of environmental law, while promising to be less heavy-handed. As a result, environmental law witnessed a shift away from command-and-control regulation, to deregulation, and an increased reliance on market-oriented policy instruments, including financial incentives and voluntary agreements with industry (Sossin, 2014). Nonetheless, as explained in greater detail below, Canadian environmental laws have not been effective for many reasons including reduced government spending, jurisdictional overlap, the lack of satisfactory market-based instruments, and insufficient enforcement (Boyd, 2003).

Following this Introduction, Part I provides an overview of the parallels that can be drawn between threats in the environment and on the Internet. Indeed, both the environment and cyberspace have innate characteristics that make them difficult to regulate, and which set them apart from other disciplines (Sparrow, 2008). As well, threats can evolve over generations and be incapable of a complete 'fix' in the long-term (Sparrow, 2008). This presents a dynamic challenge for policy-makers because it requires regulator to develop partnerships with industry and executives may question why the risk-reduction or harm-control techniques are justified, given the potential harm to the firm's reputation, objectives and culture. This problem is compounded by the fact that low rates of detection and reporting may make the problem uncertain and the effects of mitigation hard to measure; in addition, the desired outcomes may not even be achievable within the firm's budgetary timeframes (Sparrow, 2008).

Part II sets out an overview of the current state of cyber crime threats in Canada, as well as the Canadian government's regulatory response. It then goes on to trace the history of Canadian environmental law, as well as the many successes and failures that have been achieved in law and policy in this area. Indeed, policy-makers can learn a great deal from these efforts about the kinds of laws and policies that might be workable in the cyber-realm. Part III examines what specifically cyber-law theorists and policy-makers can learn from those in the environmental law field so as to move down a more appropriate, and effective, regulatory path. The article concludes with final summary and further recommendations.

[4] As discussed below, command-and-control regulations impose detailed limits on regulated entities with respect to the amount of pollutants that can be discharged, and the regulated body is further required to implement the best available control technologies to meet those standards, and to monitor emissions frequently, on the basis that everything should be done to drastically decrease levels of harmful emissions

I. The Nexus between Cyber-Law and Environmental Law

At the heart of the both cyber-law and environmental law is the question of how their far-reaching causes and effects can be managed, despite the lack of a central lawmaking authority (Lazarus, 2013). Both problems have persisted far longer than the political term of any elected official (Lazarus, 2013). As well, the scope and magnitude of the harm is often difficult to ascertain and the effects of mitigation and remediation can be hard to measure (Sparrow, 2008). Lawmakers must also grapple with national and international agreements, negotiations, and obligations (Sparrow, 2008). Agreement between the various stakeholders about how to best regulate is also by strained differences in perspective and belief (Sparrow, 2008). And, while cyber-law is not hampered by the federal/provincial jurisdictional issues that plague lawmakers in the environmental law field, as discussed below, both are influenced by fickle voters with fleeting attention spans.

In the cyber-law sphere, there is also a sophisticated international network of criminals, including organized crime groups and technical experts, who quickly adapt and change their behaviour in order to avoid detection and apprehension. Regulators often find themselves caught up in an elaborate game of cat-and-mouse with savvy opponents who are actively seeking to avoid discovery. In contrast, most environmental harms are not perpetrated by individuals or groups of criminals, with perhaps the limited exceptions of toxic waste dumping, and the illegal harvesting, poaching or cultivating of resources, such as logging or fishing (Sparrow, 2008). The environmental law sphere is more concerned with 'catastrophic harms,' including nuclear power plant disasters, major oil leaks and spills, global warming and species extinction, among others.

Another way of examining the similarities between environmental law and cyber-law is to think about a number of different properties, or features, that are common to both disciplines, apart from the specific challenges they present to regulators. What follows below are five unique features that apply to both cyber-law and environmental law which reinforce this Article's central theme that there is much that cyber-law scholars and policy makers can learn from environmental law policy and regulation (Lazarus, 1995).

(a) Novelty

Environmental consciousness only recently emerged on the scene (Brickey, 1996). In fact, environmental threats weren't widely talked about until the publication of Rachel Carson's infamous book *Silent Spring*, in the late 1960s, along with television discussions and documentaries that widely exposed environmental degradation and mismanagement (Boyle, 1997). This suggests, quite correctly, that the enactment of environmental laws is also an embryonic trend (Brickey, 1996). Similarly, the advent of an astonishing number of powerful, inter-connected computers around the globe, which are run by diverse, skilled and unskilled users, is another landmark challenge of the late twenty-first century (Zittrain, 2009). And, while cyber crime hasn't inspired the same degree of public outrage as the environment, members of the general public are very much at risk, and thus have a genuine reason to be widely alarmed.

Moreover, when it comes to the destruction of the environment, as well as online crime, everyday activities carried out by ordinary people, such as ourselves, are largely to blame (Levin, et. al., 2012). These are not like other sorts of problems with discrete adversaries; instead, everyday activities, as well as commercial decisions, are the underlying causes of many, if not most, environmental and cyber crime threats (Levin, et. al., 2012). For example, when it comes to climate change, many commonplace activities, such as

automobile transportation, result in the emission of harmful greenhouse gases (Levin, et. al., 2012). Similarly, cyber crime attacks are proliferating at an alarming rate due to the increasing numbers of unsophisticated users conducting transactions online; indeed, users can be blamed for opening infected email attachments and downloading malicious files onto their computers (Chandler, 2006).

The continued growth of the Internet and the dramatic rise in the number of people using it for a wide range of activities also provides attackers with an extensive pool of targets and a variety of means to carry out malicious activities (Symantec, 2013). An attacker no longer needs to trick his victim into opening an email and clicking on an attachment. Instead, he can exploit a weakness in a legitimate website to gain control and insert malicious content, or embed links that can redirect the user's browser to another Web server that is under the his control (Symantec, 2013). Indeed, Symantec, which monitors cyber-threat activity in over 157 countries throughout the world, reports that it carried out "vulnerability scans" of legitimate public websites in 2013 and found that as many as 77% of sites contained vulnerabilities; and, of these, 16% were significant un-patched weaknesses that could allow a cyber criminal to access restricted information, modify the contents of the website, or compromise a user's computer (Symantec, 2013).

It is also significant that the inherent trust provided by online social networks, such as *Facebook* and the innate curiosity of users, leads to a high click rate on malicious links, making these kinds of attacks against ordinary users very successful. Consequently, cyber criminals routinely place baits in social networking sites because users have proven to be highly trusting in these environments and readily click on links and other invitations to download and view content (Symantec, 2013). These are just two of the many examples of how those who advocate for greater cyber-security also participate in the Internet's demise, just as those who call for harmful emissions reductions also contribute to the problem in a multitude of different ways (Levin, et. al, 2012). This makes both problems hard to contain because they require regulators to change the behaviour of many diverse participants who may not even be aware of the fact that they are contributing to the problem. This issue will be further discussed Part III below.

(b) Evolutionary Nature and Global Reach

Practically any place in the world can be the source of an environmental threat or cyber crime (Brickey, 1996). Both disciplines are also in a perpetual state of transformation. Indeed, both cyberspace and the natural world have been in continuous flux, and have been highly unpredictable, virtually since their inception. Many in the global scientific community have identified worldwide environmental threats, like increases in carbon dioxide and greenhouse gas emissions, as accelerating and likely to cause significant damage to the environment (Levin, et. al, 2012). Despite decades of focused involvement, at the domestic and international levels, there is no single legal framework, protocol, instrument, or solution that can deal with this threat, and there is also not likely to ever be a point at which we can say the problem is fully resolved (Levin, et. al, 2012). The cyber crime threat can also be seen as gathering momentum, despite many years of international and domestic efforts to combat it. Similarly, there is no legal framework or instrument that exists to effectively mitigate this threat, largely because it is a distinctively multifaceted problem, and, thus, it defies many of our commonly-used legal and policy techniques.

Given the magnitude of the global environmental crisis, particularly when it comes to extensive problems like climate change, there is the dire warning that *time is running out*

(Levin, et. al, 2012). What this means is that as our global predicament is continually getting worse, and since solutions to combat it are not imminent, at some point the problem will be too severe, or have had too much of an effect, or simply be too large and difficult to reverse (Levin, et. al, 2012). Although we cannot say that the Internet is in as dismal a state as many global climate change scientist believe the planet's ecological health to be, cyber criminals are increasingly honing their victimization techniques and cyber-threats against individuals and organizations are steadily on the increase, despite our best global efforts to combat them. Moreover, the inherent nature of the Internet, which progressively evolves over time, makes it unlikely that we will ever be able to turn back the clock and stop these threats from surmounting over time.

The reason is that generative systems like the Internet can be put at risk by their widespread success as new participants ignore or defy the system's openness and spread malicious software, or malware, with ease. Those who pay tribute to the openness of the Internet must therefore accept the corresponding danger that lurks within (Zittrain, 2009). Indeed, the generative forces of the Internet welcome contribution and enable a vast number of people to express themselves in a multitude of formats without any form of central organization or control (Zittrain, 2009). The very fact that the Internet has no control is what gives it so much power and significance, and encourages innovation, which attracts more participants to the system, and further enables it to grow and change in ways that enrich and benefit us all (Zittrain, 2009).

However, this unique advantage is also what can lead to the system's downfall. As the Internet accepts contributions from a wide variety of anonymous participants all at once, without any central authority or gatekeeper, it isn't hard for rogue users to introduce malicious code into the network; and, even for well-guarded systems to be vulnerable to this threat (Zittrain, 2009). The problem is that the system is in a continuous state of metamorphosis, and it responds to human intervention through transformation, for better or for worse. The environment is very much the same, and one day these highly regarded domains may simply be too far gone for policy-makers to deal with.

(c) No Central Authority

Clearly, there is no central authority or police force for the Internet or the environment. What is more, decision-makers within domestic public bodies do not have authority over all of the alternatives, decisions, and instruments of control that are needed to make a considerable change to either of these two global problems (Levin, et. al, 2012). The difficulty in coordinating policy across multiple economic and political sectors also makes it tricky to achieve workable collective action (Levin, et. al, 2012). The evolutionary nature of the harm creates further uncertainty about what the law is, or should be, including what behaviour should be considered illegitimate over time.

Many environmental threats span multiple generations and given that it can take many months or years for them to materialize, there's a built-in assumption on the part of many policy-makers that there's plenty of time to react, even in the face of credible evidence that there is a serious risk of unavoidable and disastrous harm from not taking action (Levin, et. al, 2012). In other words, poor policy decisions can be made in response to unrealistic assumptions about the speed at which a problem is likely to arise, and the unpredictable nature of these distant outcomes reduces the public and political resolve to take action (Jaccard, 2006).

But if things happen much more quickly than policy-makers anticipate, and they are operating in a fog, they cannot respond to what's on the horizon. This problem is compounded by the tendency of politicians to deal with only the most pressing issues of the day (Levin, et. al, 2012). Consideration of the available policy alternatives also reminds us of the need to provide incentives for individuals and groups to constrain their short-term behaviour in order to achieve a greater future benefit (Levin, et. al, 2012). The question, though, is how to achieve this goal on a sizeable scale when there is no central authority to manage it. This is explored in further detail in Part II below.

As with the environment, the open and widely distributed nature of the Internet suggests that it is all but impossible to create a regulatory structure to govern it. This is especially true given that cyberspace was designed to be a network of networks, without any single point of control at the operations level. As a global network, the Internet allows for the instant exchange of information between users throughout the world. And given that the Internet is simply a neutral device for routing packets of data, which means that it doesn't discriminate between packets or route certain kinds of data differently than others, it imposes no restrictions upon end users and (paraphrasing an insightful remark made by Internet pioneer John Gilmore), when it comes to censorship, it simply skirts around it (Elmer-DeWitt & Jackson, 1993). The Internet's design means that when regulators try to impose restrictions, they are forever chasing a moving target (Deibert & Rohozinski, 2010). As well, cyber criminals can conceal their identities and operate from jurisdictions where the laws are weak, or where network service providers have trouble monitoring and filtering traffic across their networks. This makes it time-consuming and expensive to enforce conventional legal measures on the Net.

(d) Inspirational Qualities

Both environmental law and cyber-law are inspirational in that they aspire to effect substantial changes in human behaviour in order to combat a colossal threat to the public's wellbeing (Brickey, 1996). In the environmental sphere, this has lead to the implementation of technology-driven requirements, some of which have been labelled unrealistic, inefficient, or even irrational. Indeed, the first "generation" of environmental laws were so inspirational that they had to be implemented regardless of their economic or technical feasibility (Lazarus, 2001). When these measures proved ineffective, regulators turned to market-based strategies, and voluntary initiatives, which also failed to completely address the problem.

Similarly, cyber crime attacks are becoming more sophisticated and effective, despite our best efforts to combat them globally. According to Symantec, hacking was the number one cause of data breaches in 2013 (Symantec, 2013). When an organization's network is hacked, not only are customers' identities at grave risk of being compromised, the company also faces the threat of losing business or harming their reputation in the marketplace (Smith & Urbas, 2001). What accounts for this dramatic rise in targeted cyber crime attacks? Are businesses not prioritizing security? Are regulators failing to take action, or regulating in unsuitable or ineffectual ways? These issues are explored further in Part II.

(e) High Level of Complexity

It goes without saying that the Internet is a system of continuous transformation and complexity, and since complexity is the adversary of security, computer systems are inherently insecure (Schneier, 2000). Few would dispute that the Internet is highly

scientific and complex; particularly given its inception as an American military tool, which was later expanded to promote social, economic, educational, recreational, military, commercial and other policy-driven priorities, including the provision of numerous public and private goods and services (Hafner, 1998). Similarly, the environment is highly technological, scientific and intricate; and its complexity is compounded by a plethora of environmental law statutes and regulations, which themselves are notoriously elaborate and technical (Brickey, 1996). In contrast, the lack of regulatory oversight on the Internet contributes to the uncertainty about what content or conduct is harmful, and raises questions about the soundness of regulatory policy in this area. For further clarity on this issue, the next Part examines various policies and regulations in both the environmental law and cyber-law spheres in Canada.

II. Threat Evolution and the Canadian Regulatory Response

(a) Cyber-Law

In today's cyber-world, security experts are continually seeing attacks against all sorts of devices including laptop computers, Smart phones, tablets, USB devices and desktop PCs, through malware, spyware, malicious downloads, phishing and spam, which poses a significant risk to an organization's networks, vulnerable data, and, inevitably, its revenue and reputation in the marketplace (Ponemon, 2012). Indeed, Symantec recently described 2013 as the "year of the mega breach (Symantec, 2013)." What this means is that not only have targeted attacks against businesses been on the rise, the total number of breaches against organizations was significantly higher than in the past, and the number of identities exposed during these incidents has also skyrocketed (Symantec, 2013). For instance, Symantec reports that there was a 62% increase in the number of breaches in 2013 from 2012 (during which the number of breaches was also higher than any previous year), and eight of the breaches in 2013 exposed more than 10 million identities apiece; moreover, one breach earned attackers a shocking 150 million identities, which is greater than any previous year (Symantec, 2013). What is more, the average number of identities revealed *per data breach* for hacking incidents was roughly 4.7 million (Symantec, 2013).

Symantec reports that 2013 further witnessed an increase in targeted attacks which use malware directed at a specific user or group of users within an organization, delivered, for example, through a spam email message, in order to open up a covert channel through which to breach the targeted organization (Symantec, 2013). The reason that specific employees, or groups of employees, are being targeted is that they have access to classified or sensitive company information as a result of their position within the organization (Symantec, 2013). And, through the use of Internet search engines, like *Google* and *LinkedIn*, amongst others, it's not difficult for an attacker to locate and reach out to these company insiders. In 2013, attackers became ever more sophisticated and aggressive in perpetrating these scams, often combining a variety of modes of contact, such as impersonating high-ranking employees within an organization, and emailing then telephoning victims to con them further in order to steal data from the breached organization (Symantec, 2013).

A negligent but well-meaning employee can also inadvertently expose customers' confidential data to theft or misuse by failing to exercise diligence and by engaging in risky behaviours that he or she may be completely unaware are unsafe (Symantec, 2013). This may result from the lack of understanding about internal security policies, or the failure to

comply with them, given the absence of corporate security policy or insufficient communication of those policies to employees. For example, Internet users continue to fall for scams on social media sites, such as a recent *Facebook* hoax that purported to offer free cell phone minutes (Symantec, 2013). Victimization through social media can also happen when a user's account is unknowingly hacked, or when the user engages in risky online behaviour, such as sharing passwords with others, or connecting with strangers online (Symantec, 2013).

These threats are not only harmful for individual users. As social media is increasingly pursued through the use of mobile devices, many organizations have experienced data loss or more serious exploits resulting from employees' use of insecure devices, such as Smart phones, while at work (Ponemon, 2012). It is also significant that mobile devices have become a popular new target for scams and malware attacks, and this threat is increased by the fact that users are storing sensitive data on these devices, including putting workplace and personal information in the same online storage area, which makes their employer's data highly susceptible to attack (Symantec, 2013).

Another common example of negligent employee behaviour includes leaving computer passwords in sight or unprotected, accessing malicious websites from work (including legitimate, compromised websites which are used to distribute malware), or misplacing corporate devices, such as a laptop or USB device, containing sensitive company information, which is then recovered by an outsider with malicious intent (Cisco, 2008). In fact, accidental exposure to risk, through the theft or loss of digital devices, increased substantially in 2013 and ranked as the third leading source for identities exposed that year (Symantec, 2013). In the case of both public and private organizations, victims may suffer damage to their corporate reputation, brand integrity, customer confidence, and share price as a result of security breaches (UK House of Lords, 2007). In addition, breaches can significantly affect the security of the data of individual consumers.

Data loss may also result from internal activities, such as when a rogue employee engages in malicious conduct, including network sabotage, stealing data or devices containing corporate data, accessing someone else's computer to search for unauthorized corporate information or intentionally leaking and/or selling confidential corporate information (Cisco, 2008). Indeed, employees with a disgruntled or malicious agenda and a profit motive can use their insider standing to engage in activities that cause an even larger financial loss than the external threats discussed above (Cisco, 2008). These individuals also have insider knowledge of the inner-workings of the company, so they don't need to go to the trouble of stealing passwords from another person, and if the company has substandard security practices, they may operate with a heightened sense impunity (Symantec, 2013).

One must also consider the risks posed to the provision of goods and services, as well as threats to the national critical infrastructure, as a result of network security breaches. One such example is the distributed denial of service (DDoS) attack whereby many computers, which have been infected by malicious programs, can be directed to send multiple requests to a single server, which, in turn, becomes overwhelmed and cannot respond to legitimate traffic (Symantec, 2013). Another concern is the presence of botnets, or robot networks, on the Internet. Malware is often designed to create a 'botnet,' or a network of as many as more than a million infected computers, that can be used for a wide diversity of purposes, including sending out spam email messages, stealing banking details, or launching a DDoS attack against a government website, or even an air traffic control

tower (Morgan, 2014) without the awareness of the individuals behind the infected machines (Symantec, 2013).

Accurate figures on the scope and scale of these problems are hard to ascertain, which makes it very difficult to determine what sort of response would be the most effective. Indeed, Internet fraud and identity theft are rarely reported to law enforcement authorities in Canada and the mechanisms for detection and reporting are not particularly advanced (Smyth & Carleton, 2011). As such, there are few reliable statistics on the prevalence of cyber crime in Canada, and there is no precise way of assessing how often victimization occurs, largely because a major proportion of incidents will not be reported, identified or even detected by victims (Smyth & Carleton, 2011). The more time that passes between the victimization and the discovery of the incident, the more difficult it is for the offender to be identified and located; and longer delays are also associated with larger monetary losses for the victim and additional efforts to clear his or her name (White & Fisher, 2008). This is particularly significant when one considers that identity fraud-related offences in Canada were recorded by the RCMP's Commercial Crime Branch, in 2013, to be greater than $11 million, whereas the total reported dollar loss from mass marketing fraud during the same year was close to $58 million (Canadian Anti-Fraud Centre, 2013).

One of the few cyber crime surveys that focus on Canadian industry professionals is the national TELUS-Rotman survey. In 2013, approximately four hundred IT and security professionals in Canada were surveyed on various aspects of IT security in their businesses or organizations, including IT security posture (i.e. satisfaction); IT security procedures; IT security awareness; IT security breaches; IT security initiatives and policies; the extent to which organizations outsource IT security; and the extent to which Canadian organizations are, on the whole, "IT security responsible (Baros & Hejazi, 2014)." The study found that compared to previous years, Canadian businesses are allocating only slightly more of their IT budgets to security (although this figure remains low at just 7.5%) (Baros & Hejazi, 2014). In addition, the researchers reported that 68% of organizations surveyed reported experiencing some form of attack via viruses/worms/ spyware/malware/spam in the previous twelve months, and 42% experienced laptop or mobile hardware device theft (Baros & Hejazi, 2014).

When asked about their ability to monitor and respond to new IT security threats, as many as 60% reported that they routinely or vigorously monitor and act; whereas, a surprisingly high 40% reported that they either don't actively monitor for new threats, or that they occasionally review new threat information but never act on it (such as taking new security precautions and/or educating employees) (Baros & Hejazi, 2014). This is vital because the researchers found that threat monitoring can significantly reduce breaches (Baros & Hejazi, 2014). Yet, only 27% of Canadian organizations surveyed conduct IT security awareness training upon hire and 15% never conduct such training (Baros & Hejazi, 2014). These findings paint a bleak picture of the IT security of Canadian businesses today.

Given that Canada and the United States share a common border, similar socio-economic systems and policy concerns, cyber crime figures from that country can also be useful to policy-makers and academics. According to data published by Symantec, the cost to US companies *per breached record*, after suffering a malicious attack, is, on average, now USD $277; and, this amount includes detection, notification, and response to victimized customers (Symantec, 2013). The amount is substantial when one considers that tens of millions of identities can be compromised in a single data breach incident.

Affected corporations are also susceptible to the threat of consumer class action lawsuits, as well as the loss of customers who move their business over to a competitor (Symantec, 2013).

The Ponemon Institute in the United States recently completed their fourth annual Cost of Cyber Crime Study (Ponemon, 2012). That study was based on a sample of 60 organizations in various industry sectors in the United States, many of which are multinational corporations. The researchers found that cyber-victimization has become a common occurrence for the organizations they surveyed and that attacks have continued to be costly. On average, the mean annualized cost of cyber crime incidents for the organizations they surveyed is USD $11.6 million, and the companies in their study experienced 2.0 successful attacks per week, which was an 18% increase from the previous year (Ponemon, 2012). The most common types of attacks were those caused by denial of service, malicious insiders and web-based attacks (Ponemon, 2012).

The researchers also found that all industry sectors are impacted by cyber crime; however, small organizations incur a significantly higher per capita cost as a result of these incidents than large organizations (Ponemon, 2012). Generally speaking, the costs of cyber crime can be broken down into a number of components, including the following: losses to victims (i.e. the amount defrauded); costs of preventing the breach or attack before the event (i.e. anticipatory costs, including investing in security measures, including shredders and hardware/software upgrades); and expenses associated with responding to the breach after the event (i.e. internal or out-sourced private investigations, costs to the criminal justice system, improvements to network security, as well as loss of goodwill and customers in the marketplace). The Ponemon researchers found that the average time to contain a cyber-attack was 32 days, with an average cost to organizations of USD $1,035; and malicious insider attacks can take more than 65 days on average to resolve, thereby increasing the cost to the business (Ponemon, 2012).

These findings indicate that companies that experience cyber-attacks incur significant costs overall. The most significant external costs result from the loss or theft of information (43%), as well as disruption to business operations and loss of productivity (36%), followed by revenue loss and equipment damage (Ponemon, 2012). Recovery and detection are the most costly internal cost activities (accounting for 49%), followed by containment, investigation and incident management (Ponemon, 2012). However, the employment of security intelligence and a strong security posture was found to significantly increase the chance of detecting and containing an attack, thereby substantially decreasing the cost of a breach (by up to as much as USD $1.5 million on average) (Ponemon, 2012).

Together, these studies indicate that data security breaches and attacks against sensitive company information are extremely costly for organizations in North America. It is apparent that a significant number of North American companies, across a variety of industry sectors, have experienced data breach incidents, and that more are likely to occur in the future. However, the good news is that the deployment of a robust security posture makes a genuine difference in helping to reduce cyber-attacks, and thereby avoid, or substantially limit, the costly effects of data security breaches.

Data protection should thus form a critical component of an organization's overall business strategy. A key question is why so many North American organizations, particularly those surveyed in the Canadian TELUS-Rotman study, are not making data security a priority. One of the crucial factors to consider is the sufficiency of applicable

laws and regulations. Legislation in this area is faced with the complexity of protecting consumers and encouraging e-commerce growth without placing unnecessary restrictions on the trans-border flow of data (Davis, 2003). Perhaps this is why Canada has been one of the last G8 nations to modernize its laws in this area (Smyth, 2012).

In fact, it wasn't until late 2009 that Parliament created a legal framework to deal with the growing problem of identity theft. Prior to the enactment of *Bill S-4, An Act to Amend the Criminal Code (Identity Theft and Related Misconduct),* the *Criminal Code* did not contain an identity theft offence at all. The *Code* does contain provisions dealing with unauthorized access to computer systems, as well as mischief to data, and a general fraud provision which predates computer technology and the Internet (see, for example, ss. 341.1, 342.2 and 380 of the *Criminal Code*). However, these instruments are unlikely to be effective, by themselves, at mitigating cyber crime in Canada because attacks can be carried out anonymously from remote locations across the Internet.

There are also a number of provisions in the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) that can significantly reduce the risk of identity theft and fraud by placing limits on the collection, use and disclosure of personal information. *PIPEDA* requires organizations engaged in commercial activities to adopt a number of safeguards with respect to the personal information they collect.[5] Both private and public sector organizations are also beginning to establish policies that address the risks associated with widespread Internet penetration in Canada. However, these measures are not adequate to address the steady occurrence of data breaches and attacks against sensitive and confidential information in the hands of Canadian businesses.

It is also relevant that as early as 2001, Canada signed the Council of Europe's *Cyber crime Convention* which requires each signatory state to make it an offence to commit certain crimes using computer systems and to grant new powers of search and seizure to its law enforcement officials, including the power to require an ISP to preserve a citizen's Internet activity records and the power to monitor user activity in real time. It also requires law enforcement officials in each signatory state to assist those in other participating states by cooperating with "mutual assistance requests" from police "to the widest extent possible."[6] However, for a variety of reasons, the Canadian government has not been able to ratify the Convention and implement the required measures into its domestic law (Smyth, 2011).

In 1997, cyber-law scholar James Boyle argued that Internet law and policy was in roughly the same position that the American environmental law movement was during

[5] It requires organizations to comply with ten principles set out in the Model Code (Schedule 1), which include: collection limitation (the parties should limit how information is collected and collection must be with consent and knowledge that the information is being collected); data quality (the data must be accurate and relevant); purpose specification (the party must specify the purpose for which the information will be collected); use limitation (once information is collected for one purpose it cannot be used for another purpose unless the individual consents or this is authorized by law); security safeguards (the information must be secured from risk, e.g. from attacks by hackers); openness (transparency i.e. the individual should know what is being done with her information); individual participation (the individual should have access to her information and be able to look at it and correct inaccuracies); and accountability (there must be an oversight mechanism). Note also that *PIPEDA* imposes limits on how long an organization can retain personal information. This means that even if personal information is collected with the consent of the individual, it cannot be stored in perpetuity. This helps to reduce the risk of identity theft by making it clear that organizations should get rid of information that they no longer need.

[6] See Article 25.

the 1960's (Boyle, 1997). In fact, there are still many similarities between the two. Both involve complex socio-legal problems, which are influenced by many forces, and which require continual adaptation to shifting conditions in a rapidly-evolving technical environment (Arnold, 2011). Regulators must grapple with conflicting expectations in seeking to enact ever more complex and far-reaching laws (Arnold, 2011). The environmental movement further provides a sad reminder of how market-based forces can fail to make a small number of firms absorb the costs of their actions, creating far-reaching socially unacceptable outcomes, such as the destruction of ecological systems for one and all (Boyle, 1997). Yet environmental regulation also provides an illustrative example of distributed benefits and localized costs, whereby the public can benefit from having better air, water and soil quality, while the expenses are shouldered by a small group of regulated entities and individuals (Harrison, 1996).

Much the same is true in the cyber-law context where decisions can be made to benefit a few individuals, while the costs are spread over a much larger group (Boyle, 1997). For example, if a company is hacked because it fails to maintain a secure network and the data pertaining to thousands of individuals is lost, and if they do not report this to anyone, the company will not necessarily lose any revenue from the breach, whereas affected consumers face the threat of identity theft, credit card fraud, and up to hundreds of hours clearing their names, and damage to their credit rating (Hirsch, 2006). To deal with this negative outcome, it is necessary to shift the costs of the breach onto the company, as only then will it have an incentive to deal with it. From this perspective, cyber-regulators may have a great deal to learn from policy-makers in the environmental law field. This is explored further in the next section below.

(b) Environmental Law

It is significant that an environmental "intellectual revolution" occurred in the 1960s in North America, which was fuelled by dire warnings about the use of pesticides in Rachel Carson's 1962 book *Silent Spring*, as well as television news coverage of local ecological disasters occurring around that time (Lazarus, 2001). There was public indignation on both sides of the border over looming environmental disasters, which led to a dramatic rise in the level of public awareness about environmental harms and galvanized people to take action (Lazarus, 2001).

Indeed, Carson's book, which dealt with the harmful effects of pesticide use, made the middle and upper classes take notice and grasp the fact that "...pollution affected complex ecological systems in ways that put even the wealthy at risk – that deteriorating ecosystems affect everyone" (McKenna, Finsterbusch & Baroni-Harris, 1996). According to Boyle, this thinking was influenced by two major ideas: the first is ecology, which rests at the heart of the environmental movement; and the second is welfare economics, which addresses the ways that economic actors do not internalize the full costs of their actions (Boyle, 1997). This brings up what economists refer to as the tragedy of the commons, which applies to both environmental law and cyber-law (Hardin, 1968).

In this narrative, Garrett Hardin discusses how resource depletion can occur as a result of individuals acting in their immediate self-interest. He postulates that a number of cattle herders graze their animals on a commonly-held field of grass. From the perspective of the individual cattle herder, it makes sense to increase the number of his cattle in the field. He enjoys the full benefit of another fat cow, whereas the other cattle herders must shoulder the burden of the wasted grass. However, the individual herder, if he pursues his

direct self-interest, will keep adding new cattle to the field in order to maximize his revenue. Eventually, all the grass will be eaten and the collective group of cattle herders will suffer from the loss of the field. The heart of the problem is the cattle herder's short-term focus on his own self-interest; thus, there is a need to manage or restrict access to avoid overexploitation of the commons (Levin, et. al., 2012).

One can easily see how this pertains to the environment; think, for example, of when a fishing company over-exploits a water resource and destroys the fish population in the process (Hirsch, 2006). In this example, the imposition of a negative externality on the whole is borne by the individual to the same extent; however, a negative externality can also occur when someone uses a resource and is able to impose the costs of that use onto others but not themselves (Hirsch, 2006). For example, burning greenhouse gas causes negative effects upon society, including rising sea levels, which are borne by individuals; yet, since the company doesn't have to bear these costs directly, it has little motivation to reduce them (Hirsch, 2006). To stop the problem of the company continuing to emit greenhouse gasses, the company must be required to shoulder the costs of the harm that it is creating. The focus is on providing incentives for individuals to constrain their short-term behaviour in order to achieve a future benefit for everyone (Levin, et. al., 2012). This idea will be explored further below.

The first period of heightened interest in the environment occurred during the late 1960s through to the late 1970s. During this time, the surge in public interest and political capital devoted to protecting the environment generated considerable progress, including the implementation of innovative legislative initiatives at the federal and provincial levels in Canada (Boyd, 2003). Environmental groups also surfaced, reinforced by external funding and individual 'policy entrepreneurs' who believed that they could address environmental problems through extensive lobbying and legislative reform (Harrison, 1996). This rare combination of forces is significant because disinclination, on the part of the political elite, as well as industry, is the prevailing norm in this field (Harrison, 1996).

One of the underlying reasons is that ecological and other scientific forces dictate that the benefits and costs of environmental laws are unavoidably spread over great distances and time. Indeed, costs may be imposed by regulating activities today; whereas, the benefits may not be felt for years, or even whole generations (Lazarus, 2003). As a result, pollution-emitting entities are more likely to resist the imposition of environmental laws in the short-term, which may have a disproportionately negative impact upon them (Lazarus, 2003). Indeed, an industry executive can simply ignore risks, and flout the law, knowing that the long-term damaging effects won't necessarily happen during his or her lifetime. They may treat fines as just another cost of doing business, or simply allow themselves, or their assets, to be rendered insolvent. However, through the use of market-based instruments, such as resource pricing and fiscal incentives like taxes, or tradable permits, we can force industry emitters to internalize costs in the here and now, and marshal change on significant, long-term scale (Doern, 1992).

Canada has a long history of environmental regulation, and a number of statutes have been implemented at the federal and provincial levels. However, the strength of environmental law reform never equalled its intensity in the United States (Wood, et. al., 2010). In both countries, environmental laws were virtually nonexistent prior to the 1970s, except for common law property and tort doctrines (which enabled private individuals to pursue claims following a range of wrongdoings or torts, such as nuisance,

trespass, negligence, and so on) in addition to a few laws in the U.S. states and the province of Ontario (Lazarus, 2001). Then in the 1970s, governments in both Canada and the United States faced mounting public concern about environmental degradation and demands for the implementation of environmental protection policies (Van Nijnatten, 1999). This led to the creation of what came to be known as the "first generation" of environmental laws.

At this juncture, it is critical to note that the Canadian political structure is heavily influenced by federalism and the constitutional division of powers significantly constrains legislators in the area of environmental law. Both the federal government and the provinces have authority over the environment, which is enumerated by different constitutional sources of power. For instance, s.109 of the Constitution grants the provinces ownership of all lands, mines, and minerals in the public domain within their borders; and this enables them to exercise a great deal of control over these resources (Harrison, 1996). As well, s. 92(13) gives the provinces control over "Property and Civil Rights in the Province," which enables them to legislate in respect of private and public lands in the province. In addition, s.92A of the Constitution verifies provincial jurisdiction over the exploration, development, conservation and management of non-renewable natural resources, as well as forestry and hydroelectricity. Together, these sections limit provincial power to matters that have no extra-provincial consequence; and, moreover, the provinces cannot legislate in areas of federal jurisdiction, and in the event of a conflict, the federal law is pre-eminent (Harrison, 1996). At the same time, the provinces are responsible for administering both local and federal regulations, without much supervision from the federal Parliament (Van Nijnatten, 1999).

The federal power over the environment is broad and ambiguous, although the federal government has authority to legislate with respect to environmental harms that traverse international or inter-provincial boundaries, and that pose a threat to public health (Harrison, 1996). The federal power largely stems from s. 91(1A) of the constitution which gives the federal government authority to regulate in respect of its own resources and a number of federal statutes, including the *Arctic Waters Pollution Prevention Act* and the *Northern Inland Waters Act*, rely on this jurisdictional source of power (Harrison, 1996). Section 91(12) also grants the federal government exclusive jurisdiction over "Sea Coast and Inland Fisheries" and laws such as the *Fisheries Act* were created under this head of power, which gives the federal government extensive jurisdiction over important environmental issues like water pollution (Harrison, 1996).

As well, the federal government has power under s. 91(2) of the constitution over trade and commerce, taxation, spending, criminal law, and 'Peace Order and Good Government." This gives the federal government authority to use taxation as a regulatory instrument to encourage environmentally sound behaviour, and to also subsidize federal environmental initiatives, through its spending power, such as to monitor the environmental practices of industrial emitters and to carry out research activities (Harrison, 1996). Nevertheless, the scope of federal regulatory power over the environment has been contested in the courts, and general disagreement remains within Canada over the extent of federal authority in this area (Harrison, 1996).

Given that federal regulatory power over the environment is so uncertain, and considering the fact that the provinces have significant power over the environment as a result of their legislative jurisdiction over 'property and civil rights' and their ownership of Crown resources within the province, the federal government has historically taken a

back-seat role in environmental regulation and limited its activities to carrying out research, providing technical support, regulating automobile emissions, and urging the provinces to adopt uniform nationwide standards (Harrison, 1996). The provinces, for their part, have traditionally set benchmarks for emissions targets, distributed pollution permits, and enforced provincial and federal rules (Harrison, 1996). At the same time, though, the federal government is motivated by the demands of the voting public and, as discussed below, is more likely to enact environmental regulations during times of increased anxiety. This, in turn, affects the balance of power within the tenuous framework of Canadian federalism, which is marred by jurisdictional overlap (Harrison, 1996).

(i) First Generation Environmental Law

The first generation of environmental laws originated in the United States during the 1970s and focused on command-and-control regulations to curb pollution (Arnold, 2011). Command-and-control regulations impose stringent requirements upon industry, to scale back pollution to a socially desirable level, by mandating that they adopt specialized pollution control technologies, and adhere to strict timelines, regardless of economic or practical feasibility (Lazarus, 2001). These efforts were highly determined and forward-thinking in that they did not rely on voluntary shifts in industry practice, nor use market incentives to obtain cooperation from polluters. They simply categorized various types of harm and imposed rigid requirements upon industry, with the aim of curbing pollution as much as technologically feasible (Lazarus, 2001).

The underlying policy rationale for command-and-control regulation includes the need to address the tragedy of the commons and rectify market failures arising from emissions externalities, including physical and economic "overflow" costs (Esty, 1996). This approach is grounded in a deterrence-based theory of enforcement which assumes that regulated entities are rational entities acting in their own self-interest to maximize profit (Rechtschaffen, 1997). Thus, it is essential for regulators to make the chance of detection high, and the speed/certainty of penalties great (e.g. fines for being found in violation, as well as implementing the required control measures), such that there will be an economic disincentive for firms to violate the requirements in the first place (Rechtschaffen, 1997).

It is notable that the Canadian government and businesses are inclined toward "importing" regulatory standards from other jurisdictions, whether they are motivated by customers, foreign head offices, or international trade agreements (Wood, et. al., 2010). Nonetheless, Canada has always had a more gentle regulatory posture toward environmental issues than the United States, and it has resorted more frequently to the use of negotiated initiatives rather than command-and-control regulatory instruments (Brouhle and Harrington, 2009). Indeed, the shared nature of environmental jurisdiction between the federal government and the provinces, as well as the lack of federal leadership, has led to a heavy reliance on the multi-stakeholder consultation approach (Henriques & Sadorsky, 2008).

Yet, public awareness of environmental hazards dramatically rose during the 1960s and Canadians jumped on the global "greening" bandwagon alongside their southern neighbours (Smith, 2008). The consciousness-raising of Canadians was due to a combination of events, including similar shifts in American public opinion at the time; increased media coverage of pollution and other environmental concerns in both countries; and a series of high-profile environmental disasters in England and the United

States, during the 1960s, in addition to Canadian environmental problems, during the 1970s, such as the mercury contamination of waterways in the Maritimes (Harrison, 1996). The surge in public awareness led to the creation of environmental groups in Canada, including Greenpeace, and to environmental issues being debated in the House of Commons (Harrison, 1996). Indeed, increased public and political pressure led to the problem becoming very prominent in the wake of the 1968 election, and subsequently, another important milestone was when Prime Minister Trudeau announced the creation of a five new environmental statutes in his 1969 Throne Speech (Wood, et. al., 2010). As well, in 1971, the Trudeau administration established Environment Canada, to combine all of the environmental agencies of the federal government into a single department (Wood, et. al., 2010).

At the same time, though, the federal government was loath to confront the provinces, which were highly defensive of their jurisdiction over natural resources, and, as an example, new federal statutes, such as the *Canada Water Act*, greatly encouraged cooperation between the federal government and the provinces in the protection and management of resources (Harrison, 1996). During this period, each of the ten provinces also enacted environmental statutes, some of which, like the provinces of Ontario and British Columbia, pre-dated the federal government's scheme, and as a result, the four largest provinces (Ontario, British Columbia, Alberta and Quebec) were quite outspoken against the federal government's proposals, or even opposed federal involvement in the environmental protection area altogether (Harrison, 1996). Indeed, going forward, the federal government resisted the assertion of further federal power in this area, perhaps because it dreaded provoking conflict with such large and influential provincial stakeholders (Harrison, 1996).

One of the other reasons for the federal government's retreat away from enforcement was the shift in public opinion toward more pressing concerns of the day, including high unemployment and inflation (Harrison, 1996). Given the slump in public support for pollution control initiatives, combined with the economic and political price of implementing new legislation in this area, the federal government stressed the importance of provincial jurisdiction (Harrison, 1996). In fact, there was no discussion of environmental protection in federal throne speeches from the mid-1970s through to the mid-1980s (Harrison, 1996). During much of that time, federal policy efforts were focused on the need to restore national unity and a national identity, in the wake of the growing Quebec separatist movement, and to repatriate the constitution (Doern, 1982).

(ii) Second Generation Environmental Law

The second generation of environmental laws came into fruition during the anti-government, neo-liberal movement of the 1980's, associated with Margaret Thatcher in the United Kingdom, Ronald Regan in the United States, and, to a somewhat lesser extent, Brian Mulroney in Canada. One might think that command-and-control style regulation would immediately fall out of favour, especially given that neo-liberalism embraces free-market ideology (Gunningham, 2009). It is highly significant, though, that in both Canada and the United States, environmental concerns became politically momentous during the 1980s (Wood, et. al., 2010). New policy initiatives in the environmental law sphere thus played an important role during this period.

When the Mulroney Conservatives first came to power in 1984, there was no urgent effort to step up federal involvement in the environmental protection arena (Harrison,

1996). This was consistent with the protracted period of budget cuts and deference to the provinces (following a brief flurry of Liberal enthusiasm for environment in the 1970s) which had been on-going under the Liberal regime (Doern, 1992). Yet by the late 1980s, public awareness about environmental mismanagement had reached a fever pitch in Canada, such that in July 1989 a Gallup poll indicated that Canadians viewed the environment as the most important problem facing the country (Harrison, 1996). In fact, a number of global environmental disasters, including the Bhopal chemical disaster in India, the Exxon Valdez oil spill in Alaska, and the Chernobyl nuclear disaster in the former USSR were given widespread media attention and these catastrophes (along with widening fears about global warming and acid rain) thrust the environment onto centre stage once again (Harrison, 1996). It was also significant during this period that two watershed cases came before the Canadian courts on the Rafferty-Alameda and Old Man Dam projects in Saskatchewan and Alberta whereby environmental groups successfully used the courts to force the federal government to accept its broad jurisdictional responsibility in this area, rather than retreat from the limelight and defer to the provinces on all-things-environmental (Harrison, 1996).

The new era of renewed public concern about the environment, combined with ground-breaking court decisions that paved the way for a more dominant role by the federal government in environmental law, provided the impetus for the Mulroney administration's Green Plan (Doern, 1992). In the 1991 budget, the federal government sought to reassert its involvement in the environmental arena, as its Green Plan was announced, which ambitiously sought to commit $3 billion to environmental protection over a five (which was soon changed to six) year period (Doern, 1992). The Plan was largely put forward under the guise of increased government-industry partnerships and greater financial investment in the private sector (Doern, 1992). What is most important, for the purposes of this Article, is the fact that it combined traditional command-and-control regulation with market-based solutions. Overall, though, the plan was far more heavy-handed (while this was hidden in the rhetoric of partnership building) than it was committed to the use of economic instruments, such as environmental taxes (Doern, 1992).

Nevertheless, the public's interest in environmental issues waned again after the historic Rio Earth Summit of 1992, and when the Liberals were elected to government in 1993, the Plan lost momentum (Wood, et. al., 2010). What followed during the 1990s was a period of substantial environmental cutbacks in both the federal and provincial spheres (particularly in Ontario), such that the Plan that was to be the cornerstone of the government's environmental policy was quietly dropped, and 70% of the money was never distributed (Paehlke, 2000).

(iii) Third Generation Environmental Law

Environmental law subsequently moved into a third generational era in which increasing emphasis was placed upon the use of "participatory" and "collaborative" processes (Arnold, 2011). This shift was the consequence of a number of factors, including disillusionment with environmental law (Wood, et. al., 2010). During 1990s, other concerns, such as government cutbacks, unemployment, and budget deficits monopolized the media, and buttressed political apathy toward the environment (Paehlke, 2000). Politicians also had an incentive to focus on reducing the cost of government and lessening the financial burden on industry in order to generate support and encourage

economic growth (Paehlke, 2000). This trend was consistent with the broader political mood at the time, which opposed 'big government,' and sought to decrease the federal government's incursion into all areas of domestic affairs (Long, 2007).

Indeed, in the early 1990s, a backlash occurred, whereby businesses, large and small, called for reform of the command-and-control environmental law strategy (Steinzar, 1998). They challenged the idea that this was the best way forward, and pointed to other options, including more flexible laws, the greater use of market incentives, and a focus on cost reduction (Steinzar, 1998). The argument was that by mandating unachievable goals, environmental law imposed impossibly high standards and guaranteed the inability of regulated firms to comply (Lazarus, 1991). Over time, the system morphed into a mess of complex, conflicting, and unworkable requirements that beleaguered businesses and bureaucrats alike (Steinzar, 1998). In turn, this led to a cycle of diminished credibility and mistrust (Lazarus, 1991).

While command-and-control style regulation is easy to monitor and fair (because all industry must meet the same standard), it is also inflexible and achieves small returns for a substantial cost (Hirsch, 2006). It is also inefficient, and according to some critics, "wastes many billions of dollars per year," (Ackerman & Stewart, 1987) because it ignores differences between industries by mandating that the best available technologies be installed by *all* pollution emitters *in exactly the same way*, without regard to whether the same results could be achieved by less costly, more flexible methods (Steinzar, 1998). It also provides no incentive to exceed the requirement, and it risks being rendered obsolete in the face of rapidly evolving knowledge and expertise (Hirsch, 2006). Similarly, a number of scholars have also pointed to the high degree of complexity and uncertainty in environmental law (Esty, 2001), and cautioned that the more complex the environmental problem, the more unlikely it is that command-and-control regulations can sufficiently deal with it (Gunningham, 2009).

One of the most dynamic arguments raised by critics of command-and-control regulation is that the model is based on an outdated approach toward corporate behaviour (Rechtschaffen, 1997). Rather than act exclusively as rational economic actors that seek to maximize profit, many companies try to comply with environmental laws because they have a sense of civic and social responsibility (Rechtschaffen, 1997). As well, firms have concerns other than only profit, including their reputation, and their public perception as law abiding and socially responsible (Rechtschaffen, 1997). Moreover, environmental values are now deeply embedded within societal norms (Esty, 2001), and environmental responsibility is an economically sound goal for business leaders because it helps to bolster one's public image in today's competitive marketplace; it saves time and money through the reduction of energy costs, reduced waste management and disposal prices; and it can help to win customers who are dissatisfied with the environmental track-record of a competitor (Rechtschaffen, 1997).

The climate of fiscal restraint in the 1990s also placed emphasis on alternative environmental law measures, including agreements with industry on a variety of issues (Toner & Frey, 2005). It goes without saying that when economic fears are at their highest, politicians, industry, members of the public, as well as the media, are far less likely to focus their attention on environmental concerns (Paehlke, 2000). Thus, with the sense of urgency around environmental protection having all but vanished, it is perhaps not surprising that under Prime Minister Chretien, who came into office in 1993, Canada began trying out new regulatory approaches, including having industry flesh out their own

process standards, and developing new management practices, which could achieve comparable, or even better, degrees of environmental protection (Gunningham, 2009).

For example, memorandums of understanding were negotiated with a variety of different industry emitters, including motor vehicle manufacturers, chemical and petroleum producers, dry cleaners, and the printing industry; and, in addition, the Canadian government implemented deposit refund systems for pesticide containers and rechargeable batteries (Henriques & Sadorsky, 2008), as well as environmental taxes on emissions, in order to elicit changes in industry and consumer behaviour (Long, 1997). Other notable examples include the Canadian Chemical Producers Association's Responsible Care Program, which was started by the chemical industry in Canada in 1985, and has since been adopted by chemical industries in over 45 countries around the world (Brouhle & Harrington, 2009).

Responsible Care is a complex environmental management system, around the conscientious management of chemical products, which is intended to improve the chemical industry's environmental record, as well as to improve its relationship with government and promote greater public trust, particularly after the Bhopal, India industrial catastrophe in 1984 (Henriques & Sadorsky, 2008). It requires chemical facilities to publicly report their environmental performance (Darnall, Henriques & Sadorsky, 2008). This type of self-regulation, through information disclosure, has become a model for industries in many other countries and it is a consequence of the developments in information technologies made over the past several decades. In fact, the Internet has substantially reduced the cost of gathering, managing and disseminating information relating to a wide variety of social harms (Schott & Wing, 2006).

In the five year period leading up to the signing of the Kyoto Protocol, in December 1997 (Vaughn, et. al., 2005), Canada opened up its environmental policymaking process to a range of participants, and a multi-stakeholder consultation process was implemented in order to bring together multiple levels of government, various stakeholders, administrative agencies and industry emitters (Henriques & Sadorsky, 2008). In 2005, with *Project Green*, the government announced that it would regulate large emitters through emissions trading, offsets and a technology fund (Henriques & Sadorsky, 2008). These market-driven initiatives supplemented the Canadian Voluntary Challenge Registry (VCR), which was started as an important joint federal/provincial partnership to encourage industry to reduce its greenhouse gas emissions, and which remained in operation from 1997-2004 (Henriques & Sadorsky, 2008).

In 1997, the VCR became a privatized non-profit government and industry organization, with the majority of its funding coming from the private sector (Henriques & Sadorsky, 2008). The VCR is one of the first recognized environmental management systems (EMS) centred on the problem of global climate change. An EMS can be adopted either at a facility or a parent company level; and it can involve a range of practices, including developing a written environmental policy with specific performance indicators and goals, training employees about environmental threats, conducting internal environmental audits, and implementing procedures to enhance environmental stewardship (Brouhle & Harrington, 2009).

The VCR sought greenhouse gas emitters to voluntarily report their emissions on an annual basis, as well as details of environmental management practices undertaken in the past, or to be implemented in the future, to the VCR (Brouhle & Harrington, 2009). Industry emitters that adopted more inclusive and effective management practices were

awarded with high scores from the VCR that could then be used by the individual companies to achieve public appreciation and support (Brouhle & Harrington, 2009). The VCR was acquired by the Canadian Standards Association on January 1, 2005, and it was eliminated from the federal climate change plan (Henriques & Sadorsky, 2008). This initiative will be further discussed in Part IV below.

Despite the lack of U.S. participation, and in defiance of strong opposition from the provinces and industry, on December 13, 2002, cabinet ratified the Kyoto Protocol (Munroe, 2012). Sadly, though, most signatory states, including Canada, have admitted that they will not be able to meet their commitments under this agreement because few have been able to impose stern restrictions on industry greenhouse gas emitters (Brouhle & Harrington, 2009). Indeed, while the Liberal governments of both Jean Chretien and Paul Martin supported Kyoto's promise, they were painfully slow to develop climate change policy and failed to implement any important policy changes before they were defeated in the 2006 election (Wood, et. al., 2010).

When the politically conservative Stephen Harper government was elected in January 2006, he sought to abandon the previous government's policies toward environmental regulation (Munroe, 2012). In fact, he has been overtly adamant against taking action on climate change; for instance, he has candidly acknowledged that Canada cannot meet its Kyoto targets, while taking no steps to meet them (Smith, 2008). At the same time, the federal government has been unwilling to increase its regulation, or taxation, of Canadian businesses in order to achieve environmental progress (Wood, et. al., 2010).

Canadians tend to think of themselves as living in one of the more environmentally progressive and exemplary "green" nations in the world; however, many commentators have observed that in recent years, particularly through the 1990s and 2000s, Canada's environmental track record has declined from poor to utterly abysmal (Paehlke, 2000). In fact, improvements that have been made in environmental performance, such as the reduction in the levels of emissions that cause acid rain, are almost entirely due to initiatives undertaken more than twenty years ago (Wood, et. al., 2010). Indeed, both Canada and the United States have experienced a precipitous decline in the enactment of ambitious and innovative environmental protection legislation, alongside waning public and political concern about the environment (Wood, et. al., 2010). At the same time, environmental threats have continued to intensify and worsen around the globe (Wood, et. al., 2010).

Clearly, the enormous decline in environmental regulation is the product of a myriad of factors, many of which have already been discussed. For example, the public's eco-friendly outlook dwindled as a result of concerns about Quebec separatism and national unity (Wood, et. al., 2010). Indeed, the cyclical nature of public concern has a direct bearing on the government's eagerness to regulate on environment issues. As well, environmental stewardship has been significantly curtailed in Canada by the neo-liberal policies of the federal government, which emphasise deregulation and the reliance on market forces. Another significant factor is the steep budget cuts in the environmental policy arena that took place from the mid-1980s onward (Wood, et. al., 2010).

Thus, perhaps it should come as little surprise that, despite nearly five decades of awareness and regulation, environmental law is really no closer to 'addressing' much less 'solving' the problems of the past, which continue to perplex scientists and others. For example, although there has been a great deal of effort to reduce greenhouse gas emissions in recent years, the uncertainties around climate change have multiplied and there is

disagreement among scientists and economists over the likelihood of various alternatives, as well as the nature of those outcomes, and their anticipated consequences (Pindyck, 2013). Global regulatory efforts have proven extremely fragile (Martin, 2009); and there is considerable apathy when it comes to industry compliance. The foregoing overview of Canadian environmental law reveals a number of persistent themes. Environmental policy historically stressed command-and-control style regulations, which are inflexible, costly and jurisdictionally awkward to administer and enforce. However, Canadian environmental laws have not been as stringent as those in the U.S.; indeed, environmental law-making in Canada has traditionally occurred in closed-door negotiations between industry and government (Martin, 2009). Even still, laws are not produced in a vacuum. Environmental policy has also been deeply influenced by competing economic and socio-political forces, including downsizing, free trade, unemployment, inflation, declining government revenues, concerns about national unity, and globalization, to name a few (Paehlke, 2000).

There has been a longstanding tension between the implementation of costly and complex environmental protection laws, which can be difficult to monitor and enforce, versus the use of market-based environmental instruments, such as economic incentives for eco-friendly business practices (Paehlke, 2000). Environmentalists tend to prefer the former while industrialists prefer the latter, and this dichotomy generates distrust and hampers efforts to produce more innovative and workable policies (Boyd, 2003). This friction, combined with the other broad systemic factors mentioned above, particularly the need to achieve federal and provincial cooperation on environmental issues, and the fact that negations continue to be dominated by government and industry, have made it extremely difficult, if not impossible, for Canada to achieve long-lasting environmental progress through the implementation of more complex and pioneering environmental laws (Boyd, 2003).

Nevertheless, lessons can be learned by examining the ways in which environmental growth has been achieved, alongside failings or limitations that have hampered environmental success (Boyd, 2003). This information can be useful to cyber-law scholars and policy-makers as they search for innovative solutions to the pernicious problems of data breach security and identity theft. In fact, there are sufficient a number of parallels to be drawn between these two global problems, such that policy-makers can learn from the generally poor environmental protection record documented above in thinking about the kind of law and policy decisions that are needed in the cyber-realm. Thus, the next Part examines the ways in which cyber-lawmakers can learn from regulators in the environmental law field in developing a number of different policy alternatives.

III. Cyber-Regulation and the Lessons from Environmental Law

Having determined that there is indeed a proximity, or nexus, between cyber law and environmental law, this Part will examine how cyber law theorists and policy-makers can learn from those in the environmental law sphere and implement an effective regulatory regime.

(a) What Environmental Law has to teach

As we have already observed, first generation environmental law involved applying traditional legal responses, primarily command-and-control style regulations, to complex problems (Tietenberg, 1998). Over time, it became obvious that these approaches were

tremendously costly and unable to achieve their targeted objectives; thus, in the second and third generation of environmental law, regulators increasingly turned to market-based approaches, including tradable permits and deposit-refunds, which provided more flexibility and cost-effectiveness than command-and-control style regulation (Tietenberg, 1998). Even still, regulators were unsuccessful at dealing with the problems at hand, largely because the scope of the global environmental crisis is now so enormous (Tietenberg, 1998). Many governments lack the means to finance initiatives from their current revenue streams; yet, regulations that raise revenues, such as through taxes, are politically risky (Jaccard, 2006). The policy tension between the imposition of present-day costs upon the public and industry, and the uncertainty of long-term beneficial outcomes, makes it extremely difficult to regulate in this area (Jaccard, 2006).

According to David R. Boyd, Canadian environmental policy fails to adequately execute and enforce the law, which is evidenced by the fact that Canada has many environmental laws on the books which are rarely, if ever, enforced (Boyd, 2003). One of the reasons is that industry executives are highly resistant to intervention, particularly where this involves the imposition of costly and bureaucratic regulatory standards (Boyd, 2003). Another example of failure in this respect is the fact that environmental policies, such as the Mulroney Green Plan, discussed above, are lauded with great political promise, then quietly shelved and never fully implemented (Boyd, 2003). Substantial government budget cutbacks are clearly to blame; and, this problem is compounded by the government's delegation of responsibility to the provinces on key environmental issues (Boyd, 2003).

Boyd also points to the considerable reliance on voluntary programs and industry self-regulation as a reason for the lack of enforcement in the environmental law sphere (Boyd, 2003). Voluntary policy approaches have often been criticized for being ineffective by those who would prefer the imposition of stronger measures to look after the environment (Jaccard, 2006). And it's true that, for a variety of reasons discussed below, the Canadian government's VCR initiative, which was launched by the Liberals in 1993 as part of their National Action Program on Climate Change, did not reduce emissions over time (Jaccard, 2006).

Yet if we are to learn from the history of environmental law, we can see that command-and-control regulation, by itself, is not the most appropriate option for dealing with the data breach security problem. As we have seen, it is expensive because it requires all firms to adopt the same technology, and to achieve the same regulatory target, regardless of cost or feasibility (Hirsch, 2006). It also stifles innovation because it mandates requirements without allowing firms to exceed the targets by acting differently (Hirsch, 2006). This regulatory method is clearly not appropriate in the area of computer technology, which rewards innovation and advancement.

Thus, allowing firms to customize their approach, particularly when it comes to the adoption of new technologies, would work better than the employment of a rigid, top-down, command-and-control style of regulation. Indeed, individual firms know their facilities, and their limits, far better than regulators do, and are thus more likely to come up with a workable solution if they are motivated to do so (Hirsch, 2006). This is consistent with the third generation of environmental law and policy in Canada, which involves placing greater emphasis on flexible initiatives, and recognizing that there are new ways of approaching regulation from a collaborative perspective, with greater transparency, and far less conflict.

Two of these third generation environmental regulation methods are likely to be particularly helpful in combating the data security breach issue in Canada. As discussed further below, *disclosure strategies* have become common in environmental law because they are justified on a number of grounds, including fostering greater corporate social responsibility, enhancing stakeholders' right to know, and providing valuable information that can contribute to, or improve, pollution control policies (Tietenberg, 1998). Consistent with this approach, *environmental management systems* involve firms putting into practice a set of guidelines that can that can be implemented by any type of organization to articulate various strategies and processes for enhancing environmental outcomes. These approaches are likely to be the most effective at dealing with the data security breach program, for the reasons set out below.

As mentioned above, the VCR is an example of a public voluntary program that was an important underpinning of Canadian climate change policy during the 1990s through to the early 2000s. The program was set up by a joint federal/provincial initiative in 1995 (Henriques & Sadorsky, 2008), which was later privatised and run as a non-profit government and industry organization, with the majority of its profit coming from industry, in 1997 (Henriques & Sadorsky, 2008). It could be considered public because it operated through government bureaucracy and statutes/regulations (as opposed to through purely private channels, including business firms, outside the 'public' realm of government) and it was voluntary in the sense that it was not *required* to be undertaken by firms through government regulations mandating participation) (Wood, 2002). The VCR provides an example of an environmental management system that incorporated disclosure strategies.

The VCR required the implementation of environmental management systems on the part of industry to reduce greenhouse gas emissions (Brouhle & Harrington, 2009). On a yearly basis, participating firms were also to submit an action plan to the government setting out the actions they took and their future plans to reduce emissions. The plans, along with their VCR-based environmental responsibility rating, were then made available to the public on the VCR website (Brouhle & Harrington, 2009). Through voluntary information disclosure, the VCR succeeded in promoting industry knowledge and openness (Henriques & Sadorsky, 2008).

However, as time went on, it became obvious that the VCR was not able to rein in "free riders" and this, combined with the lack of specific emission reduction targets, meant that the program was not going to achieve substantial greenhouse gas emissions reductions on its own (Henriques & Sadorsky, 2008). This speaks to the need for command-and-control style regulations to supplement voluntary initiatives, and this idea is explored further below. Even still, since then, EMS has been used for many kinds of environmental threats, including toxic chemicals, waste disposal, and others (Brouhle & Harrington, 2009).

EMSs emerged in the late 1980s, as a management technique, in response to a number of global environmental catastrophes, including the chemical disaster in Bhopal, India and the Exxon Valdez oil spill in Alaska (Wood, 2002). Given the negative publicity that followed these events, amid public outrage and calls for tougher environmental regulation, a number of firms, including a number of large, multinational corporations, looked to the use of new management techniques that enabled them to identify and manage the environmental effects of their activities more effectively (Wood, 2002). At the heart of this approach is the notion that bad environmental outcomes can often be linked to

substandard management practices on the part of the business as a whole, and that improved management processes will lead to better environmental results (Wood, 2002).

The most widely-known international EMS benchmark for environmental problems today is the International Standards Organization's (ISO) 14001 which provides international standards for the implementation of EMSs (in order to promote organizational change within corporations and self-regulation) (Henriques & Sadorsky, 2008), and which has been adopted by over 200,000 firms in roughly 150 countries, including Canada (Brouhle & Harrington, 2009). The International Organization for Standardization (ISO) is an independent, non-governmental organization and the world's largest creator of voluntary international industrial and commercial standards. It was established in 1947 in Geneva, Switzerland, "to facilitate the international coordination and unification of industrial standards" and its members are comprised of the national standards bodies of 163 member countries around the world, including Canada (ISO, 2015). To date, the ISO has published over 19,500 international standards, or technical specifications codified into voluntary agreements for products, services, and systems, covering a wide range of industry sectors, including healthcare, food safety, the environment, manufacturing, technology, and others.

A number of these standards have been adopted in Canada, through Industry Canada, such as ISO 14001. Indeed, Industry Canada has reported that, "there is a growing awareness of the business case for sustainable development by the Canadian private sector (Industry Canada, 2015)." This has resulted in a number of Canadian firms implementing corporate sustainability and social responsibility practices into their business strategies and operations, including reporting on sustainable development (Industry Canada, 2015). The growth in the number of ISO 14001 certifications achieved by Canadian industry is a critical indicator of the progress in integrating sustainability practices into operations; and Industry Canada has reported that, "although Canada still ranked behind many European countries, as well as Brazil, Australia and Korea, it has achieved steady growth in the number of Canadian companies achieving ISO 14001 certification (Industry Canada, 2015)."

ISO 1400 sets out guidelines that can be implemented by virtually any type of organization in any country to create strict environmental policies, objectives, strategies and processes for enhancing environmental outcomes (Morrow & Rondinelli, 2002). These frameworks provide a uniform standard by which a single plant, or an entire corporation, can identify environmental threats, specify goals, implement new practices and procedures, rectify problems, and improve environmental performance over the long-term (Morrow & Rondinelli, 2002). This approach has been characterized as a new kind of global environmental governance which can be credited for broadly exposing the fact that governmental and inter-governmental efforts, by themselves, are not capable of addressing our current global environmental predicament (Wood, 2002).

It is important to keep in mind that the ISO is merely an international standards-setting body, which means that it develops voluntary criteria, in the form of guidelines and standards, which represent international agreement on what constitutes best practice. However, it does not carry out conformity assessments of individual firms; that is a matter for regulatory bodies when ISO standards have been incorporated into domestic legislation, or certification bodies that provide independent assessment and confirmation that a product, system, or service meets the requirements of a standard promulgated by the ISO (ISO, 2015). Certification, through an independent certification body in Canada,

would enable individual Canadian firms to show others that it has an effective, ISO-approved, quality management system in place (ISO, 2015).

Supporters maintain that EMSs have allowed government agencies to avoid command-and-control style regulation, without leaving industry entirely on its own, while achieving environmental goals in a more business friendly and less heavy-handed manner (Gunningham, 2009). As well, this systematic approach works well within the complex field of environmental pollution mitigation, particularly given that a wide range of emissions are considered greenhouse gasses, and the fact that the industries and entities that emit these pollutants are very diverse (Brouhle & Harrington, 2009). Given that EMS initiatives are industry-driven, there are also fewer opportunities for new initiatives to be cutback, delayed, or derailed altogether, as can often be the case with government-backed initiatives (Van Nijnatten, 1999).

There is also increasing awareness of the business case for implementing EMS standards by industry, with the result being increased bottom-line performance. In fact, compliance with EMS standards such as ISO 14001 has been a good predictor of better environmental and business outcomes (Brouhle & Harrington, 2009). International surveys of companies have indicated that their primary motivations for implementing ISO 14001 standards in their workplaces include the following: the prevention of harmful environmental impacts; fostering environmental awareness in the workplace, which enhances participation and compliance; improving their corporate image and gaining increased market share (i.e. improved business performance); responding to pressure from regulatory agencies (i.e. in order to achieve regulatory compliance or other regulatory benefits, such as a tax relief); and greater legal certainty (Morrow & Rondinelli, 2002).

Curiously, a number of studies have failed to show any environmental improvements by EMS adopters compared with non-adopters; however, in many cases, this can be attributed to the lack of strong enforcement, including the lack of a stringent regulatory penalty (Brouhle & Harrington, 2009). Related to this, in the Canadian context, is the fact that environmental policy and enforcement in Canada differs between the provinces, which means that certain provinces that depend more heavily on greenhouse gas emitting industries are not likely to devote sufficient resources to regulation (Brouhle & Harrington, 2009). Thus, where a stringent regulatory threat exists, in terms of monitoring and the enforcement of penalties, it is more likely that firms will wholly undertake the transformative policy changes needed to achieve better business and environmental outcomes overall. Moreover, it may be difficult to attribute environmental improvements to the adoption of an EMS system alone, such as ISO 14001; however, it is clear that the implementation of EMS systems do produce a variety of positive results, such as increased employee awareness, and the many performance improvements discussed above (Morrow & Rondinelli, 2002).

(b) What Cyber-Law Can Learn

1. Information Disclosure as a Policy Instrument

The first point of departure for policy-makers in the cyber-law field should be to identify why information disclosure is such an effective, and necessary, policy instrument. Earlier in this Article, cyber crime was described as a widespread, pervasive, and rapidly accelerating problem, which has thus far evaded the best efforts of regulators from around the world to combat it. There are a number of reasons why cyber crime has proliferated

on a global scale, including the fact that the prospective gains from cyber crime attacks have increased along with the mainstreaming of the Internet (i.e. the globalization of the Internet has enabled offenders to reach a larger number of potential victims); and the likelihood of being apprehended and prosecuted is typically lower than compared with traditional crimes (Cardenas, et. al., 2009).

A further important challenge for regulators in this area is the fact that cyber-attacks are not always detected or reported and there is a significant need to develop a more efficient means of documenting breaches and their consequences. Without reliable information, policy decisions can be imprecise, misunderstood or even ignored (Jarvis, 2005). In other words, policy-makers must be able to detect and understand patterns of criminality in this area, including the frequency and cost of attacks, as well as the various layers of threat complexity and the opportunities they provide (Levin, et. al., 2012). It may be, for example, that public and private organizations can play different roles in helping to mitigate the threat at different stages, or in diverse contexts, and that a variety of policy instruments could be used (e.g. in the environmental sphere, policy-makers use both command-and-control methods as well as market-based approaches, like taxes and tradable permits, to address the problem) (Levin, et. al., 2012). Information disclosure not only benefits the public and the government, it also helps individual companies learn how they perform in relation to others, and this information is very valuable because it can encourage other firms to disclose and can induce laggard firms to change their business practices (Schot & Wing, 2006).

Within organizations of all dimensions, in a wide range of industry sectors, managers are under continuous pressure to enhance their company's profits and minimize costs; and effective risk management is an integral part of meeting those objectives, as it is driven by increased complexity in the business world, and an intention to promote transparency and reduce information asymmetries between corporate executives and stakeholders (Lajili & Zeghal, 2005). Effective disclosure can provide enormous guidance in identifying and responding to business uncertainties and opportunities, and, thus, it should form an integral part of managerial practice in today's competitive global business environment (Lajili & Zeghal, 2005). In addition to the more commonly identified financial and environmental risks, there are also technology risks to consider with respect to the firm's operations and in today's knowledge-based economy (Lajili & Zeghal, 2005).

Risk disclosure can occur both internally and externally; but, either way, it entails far more than simply reporting risks (Lajili & Zeghal, 2005). The detection and evaluation of risks that a firm faces is the first step in an effective risk management strategy (Lajili & Zeghal, 2005). The next step is to devise an efficient response to the risk, which includes establishing the firm's ability to shoulder the risk, then implementing risk reduction procedures, and other responses (Lajili & Zeghal, 2005). Lastly, there must be effective monitoring and revision, where necessary, of the coordinated risk response (Lajili & Zeghal, 2005). Risk information should also be disclosed internally to help the firm's employees understand and work with the risk identification, assessment, response and monitoring framework, which might also include investing in new technologies, hiring highly qualified experts, and training existing staff (Lajili & Zeghal, 2005). This approach is consistent with the requirements established through the environmental management systems, or EMSs, discussed above, which suggests that the EMS framework might provide useful model for the management of cyber-threats and risks inside firms.

Disclosure of risks and risk-management strategies can also be made externally, and this is often required by regulatory agencies and investors (Lajili & Zeghal, 2005). As within the environmental law sphere, information gaps can occur when there are minimal statutory requirements for information disclosure or confusion about public or private sector responsibilities in this area; or, if firms outright refuse to disclose information due to fear of liability and other reprisals, including being disadvantaged in the marketplace (Jarvis, 2005). Yet individual firms have complete information about technology, processes, cost and incentives, or disincentives, for information disclosure (Schot & Wing, 2006); thus, they are the most obvious ones to provide the information.

In a perfect world, companies would look beyond the interests of their shareholders and simply disclose information to the public in the interests of society as a whole (and, in fact there is a business case to be made that good environmental decisions can be captured by shareholders and investors); but we know that this is not happening on its own, and, in any event, standardized information is needed if this approach is to be an effective policy tool (Schot & Wing, 2006). One of the underlying reasons for the lack of disclosure is that a firm's decision to divulge information is heavily driven by reputational gains or losses in the marketplace (Schot & Wing, 2006).

The lesson from environmental law is that we want governments to have more information so that policy-makers can gain important insights. The advent of the Internet has drastically lowered the cost of tracking, collecting and disseminating information; thus, information disclosure has become an important policy tool in the environmental law sphere. On the one hand, some suggest that firms will voluntarily disclose information about pollution; yet, on the other hand, arguments can be made that only governments can provide a level playing field to ensure that this information is reported and used in a consistent manner, and so that free riders cannot take advantage of voluntary reporting systems.

Regardless of whether they are mandatory or voluntary, information disclosure strategies should be designed to establish mechanisms for discovering risks; ensure the reliability of the information; publicize or share the information with stakeholders; and act on the information (Jarvis, 2005). Voluntary information disclosure operates at lower cost and may be easier to manage than mandatory disclosure regimes (Jarvis, 2005). However, there are questions about the quality of the information, as well as the decision to disclose, and consistency and comparability of the information is essential; this is critical to formulating effective policy initiatives in response (Jarvis, 2005).

Underlying the voluntary information disclosure movement is the idea that responsible management, in terms of firms being open about the environmental impacts of their business practices, can increase profits and social standing (Schot & Wing, 2006). As discussed above, voluntary memberships through industry associations, such as the Chemical Producers, is a way for firms to demonstrate compliance with industry standards, including pollution control (Schot & Wing, 2006). Indeed, membership may be premised on maintaining a certain level of environmental performance as well as sharing information. So, these organizations can be helpful for sharing information; assuring the harmonized implementation of innovative methodologies and business practices, and fostering cooperation between firms; avoiding free riding; improving the image of the industry; and forestalling regulation, as long as the industry association is making progress toward successful self-regulation (Schot & Wing, 2006). Significant monitoring and enforcement costs can be saved because firms have an incentive to comply and improve

their reputation (Schot & Wing, 2006). The information can also be useful to inform other affected stakeholders, or to pressure specific companies or industries to change.

Voluntary disclosure lacks rigid conditions in which the government dictates the outcome and rules of engagement (Schot & Wing, 2006). However, it is not apparent to what extent improvements can be attributed to the success of industry associations and to what extent they are simply ongoing productivity enhancements, including technological innovation (Jaccard, 2006). We don't have a clear picture of what we can anticipate from voluntary codes and industry initiatives and what should be required through more stringent regulatory measures (Tietenberg, 1998). However, a number of studies have found that the severity of regulations is one of the key factors in accounting for facilities' reduction of toxic emissions (Harrison & Antweiler, 2003). Others have argued that in the environmental arena, even the threat of mandatory regulation can motivate firms to reduce their emissions levels; however, a recent Canadian study found that the highest levels of emissions reduction were achieved through stringent regulations, whereas Canadian facilities responded far less to the mere threat of regulation (Harrison & Antweiler, 2003).

It is also relevant that firms have financial and reputational incentives to deceive the public either by downplaying the harms at stake, or by exaggerating their accomplishments in the area of stewardship (Tietenberg, 1998). Indeed, within the risk disclosure literature, a number of research studies have looked at risk reporting in an international context and found that the lack of transparency in risk disclosure and reporting is primarily due to the lack of standards and uniform measurements for different risk factors nationally and internationally (Lajili & Zeghal, 2005). Information can be made more reliable through the application of set of internationally recognized management standards, such as the ISO 14000 process, discussed above, or by having domestic regulators specify the method of collection and categorization, and penalizing false reporting (Tietenberg, 1998). In this way, transparency and accountability are increased.

Government information disclosure programs can take a variety of forms – they can be mandatory and ranked (i.e. where the government publishes a ranking of firms), or non-ranked, or even voluntary (Schot & Wing, 2006). These strategies are intended to draw attention to the performance of firms, and to inspire peer pressure and public response (Schot & Wing, 2006). In fact, Canada already has a history of incorporating disclosure requirements into environmental legislation. For example, EMS standards have been mandated by provincial governments, such as with respect to Nova Scotia and New Brunswick, in the case of the gas pipeline industry and Alberta's LEAD Program (Wood, 2002). Canadian judges have also used them as sentencing orders. Canadian courts have further used voluntary standards (and other evidence of industry norm) as benchmarks for determining liability (Wood, 2002). Also, statutes and regulations can specify a voluntary disclosure and performance standard as a requirement for achieving certification or operating permits (Wood, 2002).

Yet, if the government simply establishes a set of guidelines or best practices to be followed, including voluntary information disclosure, there is no assurance that firms will abide by them, since no penalty attaches to those who fail to comply, and, thus, the rates of compliance are also likely to be inconsistent (Anand, 2006). On the other hand, compliance may increase over time, through peer pressure, as increasing numbers of firms comply and non-compliant entities fear that they will lose customers or be outmatched by

their competitors (Anand, 2006). These compliance techniques will generally work best if there is a heterogeneity of firms (in terms of the amount of harm, production processes, costs of reducing the threat impact, and susceptibility to market pressure and incentives) and there is considerable public pressure (Schot & Wing, 2006). The reputational loss to the firm must be significant because firms will generally only increase their compliance if there are tangible incentives (such as financial subsidies, or reputational gains, including avoiding public recrimination that may also bring about private legal action, protests and boycotts)(Schot & Wing, 2006).

Conversely, mandatory obligations achieve their intended outcomes much more simply because if the regulator sets out a requirement, and attaches a stringent penalty to it, it stands to reason that it will be obeyed (Schot & Wing, 2006). Of course, some firms may still choose to flout the law and treat the penalty as a mere cost of doing business. It is also significant that mandatory disclosure programs are expensive to run because regulators need to ensure that every firm obligated to disclose actually does so, thereby incurring substantial surveillance and enforcement costs (Schot & Wing, 2006).

Reputational loss is the focal point of many of the data breach notification schemes that have been implemented throughout the United States and the European Union, and which have recently been proposed in Canada and Australia (Smyth, 2014). Mandatory data breach notification refers to a legal obligation imposed upon specific entities to provide notice to affected persons and/or the appropriate regulator when certain types of personal information are accessed, obtained, used, disclosed or modified by unauthorized persons (Australian Government, 2012). Here, the term 'mandatory', means legally required (Schwartz & Janger, 2006); however, many of these statutes also contain 'voluntary' or 'enabling' provisions in that they allow the firm to decide whether to notify a particular individual or entity, depending upon the seriousness of the breach. And, as discussed above, there are powerful deterrents that hinder voluntary disclosure of information that the market considers negative (Anand, 2006). In addition, there are two other major difficulties with these regimes.

The first problem is that the information disclosure 'triggers' are either too narrow or too broad. In the case of the U.S. regime, the disclosure trigger is too broad. To illustrate, *The Californian Civil Code* §1798.29(a) requires any Californian business that suffers a data breach of unencrypted and computerised personal information (where that information is, or is thought to have been, acquired by another person) to notify affected Californian residents about it within a reasonable time, without delay. The incident that triggers the duty to provide notice is a "breach of the security of the system," which is broadly defined as the "unauthorised acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency." The California law thus has a low 'triggering threshold' which means that notification is required by an organisation *whenever* unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorised person, without the requirement that the information was actually misused (Burdon, Lane & Von Nessen, 2010). Note as well that the U.S. mandatory data breach disclosure regime is a state-based model whereby twenty-three states have enacted data breach notification laws modelled after the California law (Burdon, Lane & Von Nessen, 2010).

The problem with this regime is that the requirement for consumer notice is so lax that it produces an overabundance of data breach disclosure letters, leading people to ignore them, even in situations of real risk. As well, this system encourages organisations to cover

up their mistakes and refuse to notify customers, or to inadequately respond to breaches for fear of triggering their disclosure obligation. This is particularly true given that there are few market incentives to disclose negative information, due to the threat of economic and reputational sanctions, especially if the firm's competitors are not also disclosing similar data.

Conversely, there are other examples where the notification trigger is too narrow, although the negative outcome is virtually identical, for the very same reasons already discussed. For example, some U.S. states require that in order for the notification requirement to be 'triggered,' there must be a reasonable likelihood of harm or material harm, or a reasonable likelihood of substantial economic loss, or injury, arising from the breach. This so-called 'risk-based trigger' limits notification to situations where a risk assessment determines that a risk of identity theft or fraud exists for those whose records were breached; and, currently eighteen states have imposed the additional requisite of harm (Tom, 2010).

Another example of the 'risk-based trigger' is found in the E.U. Directive 2002/58/EC, also known as the '*ePrivacy Directive*,' which was amended and supplemented in December 2009 by the so-called '*Citizens' Rights Directive*.' It only requires breached firms to notify individuals in cases where the breach "is likely to adversely affect the personal data or privacy of a subscriber or individual (von Quathem, 2010)." Similarly, the threshold for notification under the proposed Bill put forward by the Australian Parliament at the end of May, 2013 in the *Privacy Amendment (Privacy Alerts) Bill 2013 No. , 2013*, was based on a reasonable belief by the breached firm that the data breach is a "*serious* data breach" which means that it is significant enough to pose a *real risk of serious harm* to affected individuals. This bill was not enacted as the government was defeated in an election a month later.

Furthermore, in Canada, in late May, 2010, Bill C-29 was introduced by Parliament to amend *PIPEDA* and a establish data breach notification scheme at the national level, which would have required organizations to report to the Privacy Commissioner any "material breach of security safeguards involving personal information under their control." Notification was to be made "as soon as feasible" to affected individuals if it was reasonable in the circumstances to believe that the breach created a "real risk of significant harm" which was defined as including bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on a credit record and damage to or loss of property. There were no penalty provisions included in the proposed legislation.

Bill C-29 was not enacted into law, and Bill S-4, the *Digital Privacy Act*, was introduced earlier this year by Industry Minister James Moore and, as of June 17, 2014, it is undergoing Second Reading in the House of Commons (Chung, 2014). Like its predecessor, Bill S-4 proposes changes to *PIPEDA* to deal with online threats and it would require businesses to report data security breaches to consumers and the federal privacy commissioner if they pose "a real risk of significant harm to an individual." The penalty for non-compliance is a fine of up to $10,000. However, given that disclosure is discretionary upon the firm's decision that the breach poses "a real risk of significant harm," in light of the arguments previously raised, it is likely that at least some firms will not choose to disclose because they have a prevailing incentive to withhold negative information from the marketplace. And, what is more, they will not have to provide a credible explanation to anyone of their decision not to disclose. If they are found to be in

non-compliance with the law, they can simply choose to absorb the fine as a cost of doing business (particularly if the costs of compliance exceed the penalty), or skirt around it by arguing that the low triggering threshold wasn't met. In either case, this would appear to render the penalty all but meaningless.

The second problem concerns the fact that disclosure to a regulatory body is not always required. In circumstances where this occurs, we can say that the model is inadequate because it provides no mechanism for regulators, and other organisations, to gain valuable knowledge of data security failures, and thereby learn from those experiences (Schwartz & Janger, 2006). Such is the case with respect to the California mandatory data breach notification statute, discussed above. In the proposed Canadian Bill, disclosure to the federal privacy commissioner is only made in cases where the firm elects to self-trigger its notification requirement. The fact that disclosure to a public body is largely discretionary will only serve to perpetuate the information asymmetries that the proposed legislation intends to prevent. Furthermore, rates of compliance are likely to be extremely inconsistent, and there is a lack of transparency, accountability and predictability in the proposed system, which will make it very difficult to generate reliable data about the frequency and cost of cyber crime incidents across the country. This is especially true when it comes to smaller firms, who may disproportionately shoulder the cost of compliance (Anand, 2006), and may thus fail to self-trigger their disclosure requirement.

We have seen that an essential component of data breach notification laws is the requirement to inform consumers. From an economic perspective, it is rational to impose an information disclosure requirement upon entities that have a commercial, or contractual, relationship; and this also applies in the environmental setting where we see disclosure obligations imposed upon firms in relation to individual users of dangerous products, workers who are exposed to harmful chemicals in the workplace, and community members who are threatened by toxic emissions from a neighbouring industrial facility (Tietenberg, 1998). In each of these cases, notification will provide affected individuals with an opportunity to take steps to reduce their environmental risks (Tietenberg, 1998). Similarly, an important argument in favour of mandatory data breach notification is that it can give people the incentive to reduce the impact of data security breaches, such as by cancelling credit cards or changing account passwords, and it can increase public confidence in the handling of consumer information.

The other central purpose of these laws, as we have already seen, is to impose a "reputational sanction" upon organisations by ensuring that there is a maelstrom of publicity surrounding an entity that suffers a breach (Schwartz & Janger, 2006). The assumption is that consumers will rely on this information to punish those entities with poor security practices by taking their business elsewhere. Critics of these laws argue that data breach notification laws negatively impact businesses; and, it's true that an exposed data breach will almost certainly have a negative impact upon consumer confidence in the firm, as well as its brand and bottom line. Yet the assumptions about consumer behaviour that underlie the arguments in favour of imposing reputational sanctions upon businesses in this context are largely erroneous (Ponemon, 2005). There is also substantial effort involved in switching services providers and a lack of data that would enable a consumer to evaluate the data security practices of institutions within the same industry sector, such as determining whether better information security is being offered at bank A or bank B. Furthermore, if the target of the breach is an outsourcing entity, a consumer cannot

choose to stop doing business with the company that handles payments, provides insurance, stores, or transports data for a third party (Schwartz & Janger, 2006).

The problem is that if the law relies primarily upon notice to consumers translating into reputational sanctions (such that consumers are prepared to vote with their feet and take their business elsewhere), and this is not occurring much of the time, then the law is not achieving its intended results. And this is problematic because if this method is going to be used as a policy instrument, shouldn't it *affect the decisions* and the behaviour of the firms to motivate them to take action and change their behaviour (Schot & Wing, 2006)? Moreover, in many cases, such as in the Canadian example, it provides no consistent mechanism for regulators, and other organisations, to gain valuable knowledge of data security failures, and thereby learn from those experiences because either the data is not reported to anyone other than the consumer-victim, and/or there are no methods for collecting and using this data at a national level (Schwartz & Janger, 2006).

It is also short-sighted to rely on notice mechanisms alone to protect against the harms that flow from data security breaches. The real concern is not with notification, by itself, but with poor data security practices within organisations. From this perspective, data breach notification laws that don't incorporate risk assessment and risk management procedures are not likely to achieve long-term success (Winn, 2009). Moreover, the traditional model of data breach notification laws, discussed above, fails to distinguish between companies that implement good information security practices in the long-term, and those that demonstrate a wonton and reckless disregard for the personal information they are responsible for protecting (Winn, 2009).

Mandatory disclosure is needed because it increases compliance by imposing penalties against a firm's choice not to reveal negative information (Anand, 2006). Further, in looking to ways of improving the recording and measurement of cyber crime in Canada, the appropriate response is to establish a National Reporting Centre to which Canadian businesses and individuals could report breaches (Smyth & Carleton, 2011). It would also be helpful for the government to embrace a set of standards for firms to meet in the area of preventing and responding to cyber-threats, in terms of the EMSs discussed above. This proposed policy objective is discussed in the next section below.

2. Standard Setting as a Policy Instrument

Earlier, this Article discussed how ISO standards have been used in the environmental law context in Canada to help businesses to operate more efficiently, increase productivity and access new business markets. The voluntary criteria contained in ISO guidelines and standards represent an international agreement as to what constitutes the best practice in dealing with a particular type of hazard or threat (ISO, 2015). Indeed, conformity with these standards can improve business processes and provide consumers and other stakeholders with assurances that environmental benchmarks are being met (ISO, 2015).

It is notable that the ISO has also developed an international set of standards which set out the requirements for establishing, implementing, operating, monitoring, reviewing, and improving, an information security management system within an organization (Susanto, Almunawar & Tuan, 2011). Like the ISO 1400 standards, the ISO 2700 standards can be applied by any organization, regardless of size and product/service, and they can help to foster the more efficient use of resources, improved security and risk management, as well as increased stakeholder confidence/satisfaction.

It is noteworthy that in October 2013, the Canadian Telecommunications Service Providers (TSPs) industry members developed a series of voluntary measures designed to provide guidance to service providers in implementing the optimal level of network security (Industry Canada - CSTAC, 2014). The best practices apply to 'wireline' communications, as well as to TSPs' wireless networks, such as CDMA, HSPA, and future generation phone networks. They do not apply to Wi-Fi or other ad hoc networks (Industry Canada - CSTAC, 2014).

These best practices, which are largely based on the ISO 2700-series, are a benchmark against which TSPs can evaluate their network security policies (Industry Canada - CSTAC, 2014). They are voluntary measures which, along with other benchmarks, are put forward by Industry Canada, on its Website, to give guidance to TSPs that supply and support Canada's telecommunications critical infrastructure on how best to secure and manage their networks (Industry Canada - CSTAC, 2014). The recommendations incorporate all of the following standards: International Organization for Standardization (ISO) 27001, 27002, 27011, 27032, and 27035; Communications Security Establishment Canada's (CSEC) Technology Supply Chain Guidelines for Telecommunication Equipment and Services; Australia's Internet Service Providers' Voluntary Code of Practice; and Internet Engineering Task Force Request For Comment (RFCs) as appropriate (such as Security RFCs, Security Considerations, Ingress Filtering for Multihomed Networks) (Industry Canada - CSTAC, 2014).

However, there is nothing which prohibits other entities from implementing these same requirements. Indeed, the federal government could, through Industry Canada, promote the implementation of these standards within the industry sectors that are known to be the most frequently targeted by cyber criminals. According to Symantec, this includes the following industry sectors (in order of threat likelihood): mining; government; manufacturing; wholesale; transportation/communications/electric, gas and sanitary services; finance/insurance and real estate.

Following is a proposed model for effective information security management in Canadian firms which is based on the ISO standards for establishing an information security management system within an organization:

Step 1. System Characterization & Identification of Corporate Information Assets

- Identify and characterize/classify the following:
    - Hardware (including employee devices, such as laptop computers, Smart phones, etc.);
    - Software, including network intrusion identification, encryption, firewalls, and the like;
    - System interfaces;
    - Data and Web-based information - take into account the differing privacy concerns as they relate to internal and external networks and explain what can be monitored and addressed, without violating customer privacy; and
    - People (identify existing knowledge/expertise and lack thereof; seek out knowledgeable experts inside or outside the organization to identify/manage risk).

Step 2. Risk Identification

- Document the history of system compromise (including data from internal and external intelligence; mass media); and
- Consider reports from prior risk assessments, including audits and security tests.

Step 3. Determine Likelihood and Impact of Risk

- Determine the likelihood of risks and the consequences of not taking action (which can be critical to gaining support from staff, who may otherwise not see this process as necessary) including the following (Gilles, 2011):
  - Assess data criticality and sensitivity;
  - Rate the impact of the loss of integrity, availability and confidentiality;
  - Assess the likelihood of threats, including their magnitude; and
  - Identify an authoritative intelligence sources on malicious traffic.
- Assess the adequacy of current or planned controls, including:
  - the viability of system and device hardening mechanisms and learn about other such types of systems and devices;
  - network security monitoring and detection capabilities, including the ability to backup data; conduct timely patch management; restrict access to approved services and devices; log critical network events and identify the source of malicious events; block or blacklist malicious or inappropriate traffic and/or track malicious traffic to originating source or point of entry into the firm network;
  - the integrity of data leaving firm's network and avoid harm to other networks;
  - the ability to monitor DNS activity to detect and respond to abuse; and
  - the ability to respond to external complaints about cases of abuse that have not been prevented.

Step 4. Develop a Risk Management Policy and Set Targets/Goals

- Manage cyber security incidents through a defined, tested, and repeatable program:
  - Modify the business's objectives and company strategy (by senior management) in order to ensure ongoing success and future progress;
  - Control access to particular types of workers, or certain kinds of data;
  - Employ system/device hardening according to industry-recognized standards and develop in-house standards that mandate their use;
  - Mandate hardening requirements for third party service providers through contractual obligations;
    - Require third parties to test and verify all equipment, systems, and software in accordance with well-known best practices;
  - Identify technical processes and tools to scan systems and network equipment for vulnerabilities and detect when new equipment has been added to networks;
  - Establish employee monitoring and detection mechanisms, such as background checks, and controls to prevent unauthorized access, particularly after the termination of employment;

- Determine what categories of malicious traffic the company is willing to filter or block, and ensure the capability to take these actions;
- Establish and enforce an acceptable use policy and/or terms of service policies for customers and employees, especially for abuse management;
- Develop policies and procedures around employee password creation and protection; using personal devices at work; and taking digital and hard-copy workplace documents/data off the company's premises;
- Define processes for breach containment and preliminary investigation of the cause/extent of the breach;
    - Specify measures for defining the risks associated with the breach, including the type of data, the nature and quality of the compromised information, the number of affected individuals, and the potential risk of harm; and
- Develop processes for training/educating employees in all these respects.

Step 5. Develop Ongoing Compliance, Monitoring and Audit Procedures

- Maintain an ongoing system of performance monitoring and target-setting in order to document future action needed to achieve long-term success;
- Undertake independent audits of physical and technical security, both internally and by independent third-party professionals, where applicable;
- Identify items to be audited, measures to address audited items, and measurements which can be used to demonstrate compliance, such as:
    - Document processes and procedures for addressing vulnerabilities;
    - Test devices against hardening security standards employed;
    - Utilize active, ongoing security monitoring (including incident detection);
    - Perform regular risk assessments to identify and respond to risks (including audits and management review processes);
    - Ensure that changes are approved by management with direct responsibility for the operations of the components/systems/procedures being changed;
    - Establish processes for keeping up to date with evolving industry standards and procedures in the area of information technology security; and
    - Set up education and training programs for all employees (including management) to learn about information security goals and procedures, as well as creating incentives for targets to be achieved by employees.

Step 6. Establish Response Procedures for Issues Affecting Customers

- Develop an effective operational security incident-response plan, in the event that a security breach is suspected:
    - Define processes for tracking, defining, validating and responding to third party information;
    - Define strategies for reporting abusive behaviour, which is monitored and responded to appropriately;
    - Establish mechanisms to respond during normal and off-hour times; and

  - Implement data backup/recovery plans and containment procedures, as well as where third-party contractors are involved, or where cloud-storage is used; and
- Establish a method for communicating incident or breach of information with stakeholders and regulatory bodies in the most expeditious manner possible:
  - Define notification procedures that can be implemented in a short period of time in order to protect their customers and partners;
  - Document and communicate internally who is responsible for contact with customers, partners and the general public;
  - Define process for customer notifications;
  - Track customer notifications, including methods and frequency of notifications issued; and
  - Protect the information source in customer notifications; and
  - Establish security mechanisms to ensure that customers and partners can authenticate communications coming from the firm.

Step 7. Information Sharing and Reporting

  - Establish and enforce internal policies on classification, privacy and distribution of information, which include requirements for the collection, use, disclosure, retention, and disposal of information;
  - Institute and enforce policies regarding sharing results of auditing/management review of information security practices and processes;
  - Establish policies and enforce compliance with government-mandated information sharing requirements;
  - Create procedures to share cyber security threat information with other firms – ensure that information is limited to threat characteristics and response information, and does not include personal information about individuals;
  - Ensure that applicable privacy legislation is adhered to and ensure that they deal with privacy concerns promptly and transparently; and
  - Evaluate any actions that they take to protect the security of their network against the privacy trade-offs to their customers.

These factors are general enough to overcome differences in firm size, technical complexity and ability, scope of operations, level of internal training and education, as well as the number of customers and the presence (or absence) of shareholders on the part of the company (Brouhle and Harrington, 2009). Moreover, although they are characterized as 'steps,' they should merely be seen as objectives, or priorities, and there is not necessarily a requirement that they be carried out in any particular order.

What are the challenges that a firm faces in implementing a system such as this? A recent Canadian study drew together forty Canadian experts on EMSs to discuss the difficulties with implementing ISO 14001 (Searcy, et. al., 2012). They found that the most common issues included the following: increased costs associated with documentation, employee training and information gathering; lack of administration expertise and lack of guidance in the standard of implementation; lack of management and employee participation; and disclosure of confidential information to third parties (Searcy, et. al.,

2012). However, the authors note that these problems may be more pronounced in smaller firms with limited resources (Searcy, et. al., 2012).

To address these issues, senior management must be committed to the process, and must continually communicate its importance to employees throughout the organization (Searcy, et. al., 2012). As well, the organization must not set out too many objectives to achieve all at once because there is a risk of employee burnout and fatigue. Ideally, the programs to implement them must be tied to existing business plans, strategies, and budgets within the organization in order to reduce employee weariness and confusion, as well as superfluous business practices and processes (Searcy, et. al., 2012).

This flexible approach is likely to be welcome to industry, particularly given that "risk" is highly context-specific, and plays out differently across a range of industry sectors. Thus, the choice of security and technology implemented should depend upon the type of organisation, in terms of its size, its sophistication, complexity, the type and scope of its business activities, as well as the nature of the information protected. In this sense, industry has a great deal of input in developing practical and workable benchmarks and performance goals, or strategies, as well as in determining how to meet the stated goals, than is traditionally the case with respect to command-and-control policy requirements (Hirsch, 2007). There is also much more likelihood that the agreement is going to be reasonable, and workable, within the firm's normal business cycles (Hirsch, 2007).

Yet this still leaves the question of why private companies would comply with these measures which are likely to be expensive to implement. In the environmental pollution sphere, there are examples of how governments were able to change the behaviour of industry emitters, and even get them to embrace costly alternatives, such as renewable electricity generation technologies, through the use of various market-based incentives, including subsidies for research and development; subsidies for renewable technology investments (including grants, low-interest loans and tax credits) (Jaccard, 2006). In the case of information security, we can expect that many firms might initially pass on the costs to their consumers, which might be onerous for smaller firms, if the government were to offer market-based incentives such as grants or tax credits, firms would be able to reimburse their customers, who would stand to be the hardest hit. This approach also puts continuous pressure on firms to find lower-cost ways of meeting the target, and, over time, the result should be ongoing cost reductions through reduced impact from breaches.

Conclusion

The overarching theme of this Article is that cyber-law scholars and policy makers have much to learn from regulators in the field of environmental law. We have witnessed how environmental law transitioned from command-and-control style regulations to market-based approaches, including tradable permits and deposit-refunds, which provided more flexibility and cost-effectiveness for regulated entities. Nevertheless, regulators were unsuccessful at dealing with the enormous problem of environmental law, particularly those issues affecting everyone on a global scale, such as climate change.

Despite environmental law's poor track record in dealing with major problems of global significance, we can point to the fact that the number of unilateral agreements has been growing, and many companies have initiated and established their own multi-stakeholder consultation procedures, on the basis that they can gain respite from existing regulations and circumvent future regulatory pressure, increase their cost-efficiency, improve relationships with shareholders and the public, and increase their standing in the

marketplace (Henriques & Sadorsky, 2008). This strongly suggests that Canadian firms are motivated more than just the threat of regulatory sanctions, and the drive to maximize profits, and that they may be inspired to take action as a result of a myriad of other factors, including the public's concern for environmental degradation (Henriques & Sadorsky, 2008).

The goal for policy-makers in establishing a strategy to combat data breach security problems should be to set flexible, performance-based standards for information security and leave it up to the regulated firms to develop their own security processes, rather than specifying the measures that must be adopted, or the outcomes that must be reached. This would also enable firms to revise their own risk-reduction objectives over time, particularly as technology progresses. At the same time, though, there must be effective measures in place for compliance monitoring and penalties for non-compliance.

References

Abad, C. (2006). The Economy of Phishing. Retrieved on 16th December, 2014 from https://www.cloudmark.com/en/s/resources/whitepapers.

Akerman, B. A. & Stewart, R. B. (1987) Reforming Environmental Law: The Democratic Case for Market Incentives. *Columbia Journal of Environmental Law, 13*, 171-199.

Anand, A. I. (2006). An Analysis of Enabling vs. Mandatory Corporate Governance Structures Post Sarbanes-Oxley. *Del. J. Corporate Law, 31*, 229-252.

Arnold, C. A. (2011). Fourth Generation Environmental Law: Integrationist and Multimodal. *William & Mary Environmental Law & Policy Review, 35*, 771-886.

Australian Government, Office of the Australian Information Commissioner. (2012). Discussion Paper: Australian Privacy Breach Notification. Retrieved from 16th December, 2014 from http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/discussion-paper-australian-privacy-breach-notification.

Baros, H. & Hejazi, W. (2014). 2014 TELUS-Rotman IT Security Study. Retrieved 16th December, 2014 from http://forum.telus.com/t5/TELUS-Talks-Business-Blog/2014-TELUS-Rotman-Security-Study-released-today/ba-p/35654.

Bill S-4, An Act to Amend the Criminal Code (Identity Theft and Related Misconduct) (S.C. 2009, c.28).

Boyd, D. R. (2003). *Unnatural Law: Rethinking Canadian Environmental Law and Policy*. Vancouver: UBC Press.

Boyle, J. (1997). A Politics of Intellectual Property: Environmentalism for the Net? *Duke Law Journal, 47*, 87-116.

Brickey, K. F. (1996). Environmental Crime at the Crossroads: The Intersection of Environmental and Criminal Law Theory. *Tulane Law Review*, *71*(2), 487-528.

Brouhle, K. & Harrington. (2009) D.R. Firm Strategy and the Canadian Voluntary Climate Challenge and Registry (VCR). *Business Strategy and the Environment, 18*(6), 360-379.

Burdon, M., Lane, B. & von Nessen, P. (2010) The Mandatory Notification of Data Breaches: Issues Arising for Australian and EU Legal Developments. *Computer Law & Security Review, 26*(2), 115-129.

Cal. Civ. Code §1798.29.

Canadian Anti-Fraud Centre Criminal Intelligence Unit. (2013). Annual Statistical Report 2013 - Mass Marketing Fraud and ID Theft Activities. Retrieved on 16th December, 2014 from http://www.antifraudcentre-centreantifraude.ca/english/statistics-statistics.html#Annual.

Cardenas, A., Radosavac, S., Grossklags, J., Chuang J. & Hoofnagle, C. (2009). An Economic Map of Cyber crime. Paper presented at the 37th Research Conference on Communication, Information and Internet Policy (TPRC), Arlington, VA. Retrieved on 16th December, 2014 from http://www.svetlanaradosavac.com/publications.html.

Carson, R. (1962) *Silent Spring*. Boston, Houghton Mifflin.

Chandler, J. A. (2006). Liability for Botnet Attacks. *Canadian Journal for Law and Technology*, *3*(1), 13-25.

Chung, E. (2014, April 10). New Privacy Rules Target Data Breaches, Fraud. CBC News. Retrieved on 16th December, 2014 from http://www.cbc.ca/m/touch/news/story/1.2604552.

Cisco Systems. (2008). Data Leakage Worldwide: The High Cost of Insider Threats. Retrieved on 16th December, 2014 from http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf.

Criminal Code (R.S.C., 1985, c. C-46).

Darnall, N., Henriques, I. & Sadorsky, P. (2008) Do Environmental Management Systems Improve Business Performance in an International Setting? *Journal of International Management*, *14*(4), 364-376.

Davis, E. S. (2003). A World Wide Problem on the World Wide Web: International Responses to Transnational Identity Theft. *Washington University Journal of Law and Policy*, *12*, 201-227.

Deibert, R. J. & Rohozinski, R. (2010). Risking Security: The Policies and Paradoxes of Cyberspace Security. *International Political Sociology*, *4*(1), 15-32.

Deloitte, Centre for Security & Privacy Solutions. (2010). Cyber Crime: A Clear and Present Danger: Combating the Fastest Growing Cyber Security Threat. Retrieved on 16th December, 2014 from http://www.techrepublic.com/resource-library/whitepapers/cyber-crime-a-clear-and-present-danger.

Doern, G. B. (1982). Spending Priorities: The Liberal View. In Doern, G. B. (Ed.), *How Ottawa Spends Your Tax Dollars: Federal Priorities 1981* (pp.1-55). (Toronto: James Lorimer and Company).

Doern, G. B. (1992) Johnny-Green-Laitlies: The Mulroney Environmental Record. In Abele, F. (Ed.), *How Ottawa Spends, 1992-1993: The Politics of Competitiveness* (pp. 353-376). Ottawa: Carleton University Press.

Elmer-DeWitt, P. & Jackson, D. S. (1993, December 6). First Nation in Cyberspace. *Time*, *142*(2), 62.

Esty, D.C. (1996) Revitalizing Environmental Federalism. *Michigan Law Review*, *95*, 507-653.

Esty, D.C. (2001) Next Generation Environmental Law: A Response to Richard Stewart. *Capital University Law Review*, *29*, 183-204.

Fiorino, D. J. (1996). Toward a New System of Environmental Regulation: The Case for an Industry Sector Approach. *Environmental Law*, *26*, 457-488.

Gillies, A. (2011) Improving the Quality of Information Security Management Systems with ISO 2700. *The TQM Journal,* 23(4), 367-376.

Gunningham, N. (2009) Environmental Law, Regulation and Governance: Shifting Architectures. *Journal of Environmental Law*, 21(2), 179-212.

Hafner, K. (1998). *Where Wizards Stay Up Late – The Origins of the Internet* (New York: Simon and Schuster).

Hardin, G. (1968). The Tragedy of the Commons. *Science*, *162*, 1243-1248.

Harrison, K. & Antweiler, W. (2003) Incentives for Pollution Abatement: Regulation, Regulatory Threats, and Non-Governmental Pressures. *Journal of Policy Analysis and Management, 22*(3), 361-382.

Harrison, K. (1996) *Passing the Buck: Federalism and Canadian Environmental Policy* (Vancouver: UBC Press).

Henriques, I. & Sadorsky, P. (2008). Voluntary Environmental Programs: A Canadian Perspective *Policy Studies Journal,* 36(1), 143-166.

Hirsch, D. D. (2007) Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law," *Georgia Law Review, 41*, 1-64.

Industry Canada - Canadian Security Telecommunications Advisory Committee (CSTAC). (2014). Security Best Practices for Canadian Telecommunications Service Providers (TSPs). Retrieved on 16th December, 2014 from http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf10719.html.

Industry Canada. (2011) Archived — 2. The Sustainability Context for Canadian Industry. Retrieved on 16th December, 2014 from http://www.ic.gc.ca/eic/site/sd-dd.nsf/eng/sd00529.html.

International Organization for Standardization (ISO). (2014) About ISO. Retrieved on 16th December, 2014 from http://www.iso.org/iso/home/about.htm.

Jaccard, M. (2006). Mobilizing Producers toward Environmental Sustainability: The Prospects for Market-Oriented Regulations. In M. Toner, (Ed.), *Sustainable Production: Building Canadian Capacity* (pp. 154-177). Vancouver: UBC Press.

Jarvis, B. (2005). Accounting for the Unaccountable: Valuing the Environment in Energy Policy. In Doern, G. B. (Ed.), *Canadian Energy Policy and the Struggle for Sustainable Development* (pp. 105-127). Toronto: University of Toronto Press.

Lajili, K. & Zeghal, D. (2005). A Content Analysis of Risk Management Disclosures in Canadian Annual Report. *Canadian Journal of Administrative Sciences* 22(2)125-142.

Lazarus, R. J. (1991). The Tragedy of Distrust in the Implementation of Federal Environmental Law. *Law and Contemporary Problems, 54,* 311-374.

Lazarus, R. J. (1995) Meeting the Demands of Integration in the Evolution of Environmental Law: Reforming Environmental Criminal Law. *Georgetown Law Journal, 83*, 2407-2529.

Lazarus, R. J. (2001). The Greening of America and the Graying of United States Environmental Law: Reflections on Environmental Law's First Three Decades in the United States. *Virginia Environmental Law Journal*, *20*, 75-106.

Lazarus, R. J. (2003). A Different Kind of "Republican Moment" in Environmental Law. *Minnesota Law Review,* 87, 999-1035.

Lazarus, R.J. (2013). Environmental Law at the Crossroads: Back 25, Looking Forward 25. *Michigan Journal of Environmental and Administrative Law, 2,* 267-284.

Levin, K., Cashore, B., Bernstein S., & Auld, G. (2012). Overcoming the Tragedy of Super Wicked Problems: Constraining Our Future Selves to Ameliorate Global Climate Change. *Policy Sciences*, *45*(2), 123-152.

Long, B. L. (1997). Environmental Regulation: The Third Generation, *The OECD Observer*, *26, 206*, 14-18.

Martin, P. (2009). Copenhagen Climate Summit Ends in Bitter Disagreements. Retrieved on 16th December, 2014 from http://www.wsws.org/en/articles/2009/12/cope-d19.html.

McKenna, G., Finsterbusch, K. & Baroni-Harris, M. (1996). *Taking Sides: Clashing Views on Controversial Social Issues*. Guilford, CT: Dushkin Publishing Group/McGraw-Hill.

Morgan, D. (2014, 29 August). Hackers Attack Air Traffic Control Tower. *ABC News*. Retrieved on 16th December, 2014 from http://abcnews.go.com/US/story?id=95993.

Morrow, D. and Rondinelli, D. (2002). Adopting Corporate Environmental Management Systems: Motivation and Results of ISO 14001 and EMAS Certification. *European Management Journal*, *20*(2), 159-171.

Munroe, K. B. (2012). *Risk and Advantage in a Changing Climate: Business Preferences for Climate Change Policy Instruments in Canada.* Doctoral Dissertation submitted to the University of British Columbia, Vancouver. Retrieved on 16th December, 2014 from https://circle.ubc.ca/handle/2429/42421.

Paehlke, R. (2000). Environmentalism in One Country: Canadian Environmental Policy in an Era of Globalization. *Policy Studies Journal, 28*(1) 160-176.

Personal Information Protection and Electronic Documents Act (S.C. 2000, c. 5).

Pindyck, R.S. (2013). Pricing Carbon When We Don't Know the Right Price. *Regulation*, *36*(2), 43-46.

Ponemon Institute. (2005) National Survey on Data Security Breach Notification. Retrieved on 16th December, 2014 from http://www.whitecase.com/files/FileControl/863d572d-cde3-4e33-903c-37eaba537060/7483b893-e478-44a4-8fed-f49aa917d8cf/Presentation/File/Security_Breach_Survey%5B1%5D.pdf.

Ponemon Institute. (2012). Global Study on Mobility Risks. Retrieved on 16th December, 2014 from http://www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf.

Ponemon Institute. (2013) *2013 Cost of Cyber crime Study*. Retrieved from 16th December, 2014 from http://media.scmagazine.com/documents/54/2013_us_ccc_report_final_6-1_13455.pdf.

Prislan, K. & Bernik, I. (2010). Risk Management with ISO 2700 Standards in Information Security, *Advances in E-Activities, Information Security and Privacy*. Retrieved on 16th December, 2014 from http://www.wseas.us/e-library/conferences/2010/Merida/ISPACT/ISPACT-07.pdf.

Privacy Amendment (Privacy Alerts) Act 2013.

Rechtschaffen, C. (1997). Deterrence vs. Cooperation and the Evolving Theory of Environmental Enforcement. *Southern California Law Review*, *71*, 1181-1272.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley Computer Publishing.

Schott, S. & Wing, C. (2006). Information Disclosure as an Environmental Policy Instrument and a Self-Regulatory Tool. In G. B. Doern (Ed.), *Innovation, Science,*

Environment: Canadian Policies and Performance, 2006-2007 (pp. 213-232). Montreal: McGill-Queens University Press.

Schwartz, P. M. & Janger, E. J. (2006). Notification of Data Security Breaches. *Michigan Law Review, 105*, 913-984.

Searcy, C., Morali, O., Karapetrovic, S., Wichuk, K., McCartney, D., McLeod, S. & Fraser, D. (2012). Challenges in Implementing ISO 1400 Environmental Management System. *International Journal of Quality and Reliability Management, 29*(7), 779-796.

Smith, H. A., (2008). Political Parties and Canadian Climate Change Policy. *International Journal, 64*, 47-66.

Smith, R., & Urbas, G. (2001) Controlling Fraud on the Internet: A CAPA Perspective. *A Report for the Confederation of Asian and Pacific Accountants, Research and Public Policy Series No. 39*. Canberra: Australian Institute of Criminology.

Smyth, S. M. (2012). Internet Law and Policy from a Canadian Perspective. In K. Ismaili, J. B. Sprott & K. Varma (Eds.), *Canadian Criminal Justice Policy: Contemporary Perspectives* (pp. 326-360). Oxford University Press: Ontario, Canada.

Smyth, S. M. & Carleton, R. (2011). *Measuring the Extent of Cyber-Fraud: A Discussion Paper on Potential Methods and Data Sources*. Ottawa: Public Safety Canada.

Smyth, S. M. (2013). Does Australia Really Need Mandatory Data Breach Notification Laws – And If So, What Kind? *Journal of Law, Information and Science, 22*(2), 159-182.

Sossin, L. (2014) Runaway Train: Assessing Risk in the Aftermath of Lac Megantic. *The Walrus*, July/August, 2014. Retrieved on 16th December, 2014 from http://thewalrus.ca/runaway-train.

Sparrow, M. (2008). *The Character of Harms*. Cambridge: Cambridge University Press.

Steinzor, R. I. (1998). Reinventing Environmental Regulation: The Dangerous Journey from Command to Self-Control. *Harvard Environmental Law Review*, *22* 103-202.

Susanto, H., Almunawar, M. N. & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical and Computer Sciences*, *11*(5) 23-29.

Symantec (2013). "Internet Security Threat Report" *2013 Trends, 19*, April 2014. Retrieved on 16th December, 2014 from http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf.

The Council of Europe's *Convention on Cyber crime*, Budapest, 23.X1.2001. Retrieved from 16th December, 2014 from http://conventions. Coe.int/Treaty.en.Treaties/HTM/185.htm

Tietenberg, T. (1998). Disclosure Strategies for Pollution Control. *Environmental and Resource Economics,* 11(3-4), 587-602.

Tom, J. M. (2010). A Simpler Compromise: The Need for a Federal Data Breach Notification Law. *St. John's Law Review, 84*(4), 1569-1603.

Toner, G., & Frey, C. (2005) Governance for Sustainable Development: Next Stage Institutional and Policy Innovations (198-221). In G. B. Doern (Ed.), *How Ottawa Spends 2004-2005: Mandate Change and Continuity in the Paul Martin Era.* Montreal: McGill-Queen's University Press.

UK House of Lords, Science and Technology Committee. (August 10, 2007). Personal Internet Security – Volume I: Report. 5th Report of Session 2006-2007. London.

Van Nijnatten, D. L. (1999). Participation and Environmental Policy in Canada and the United States: Trends Over Time. *Policy Studies Journal, 27*(2) 267-287.

Vaughn, S, Carpentier, C. L., Patterson, Z. & Miller, P. (2005) Canada-US Electricity Trade and the Climate Change Agenda (pp.151-173). G. B. Doern (Ed.), *Canadian Energy Policy and the Struggle for Sustainable Development*. Toronto: University of Toronto Press.

von Quathem, K. (2010). Personal Data – Security Breach Notification in the European Union: First Step Taken, More to Come. *World Data Protection Report*. Retrieved on 16th December, 2014 from http://www.cov.com/files/Publication/3c4eadcd-c074-44f8-925f-4a63d5304d70/Presentation/PublicationAttachment/9c8fb8a0-b55a-4464-ac4b-4a7722eda833/Security%20breach%20Notigication%20in%20the%20EU,%20first%20step%20taken,%20more%20to%20come.pdf.

White, M. D. & Fisher, C. (2008). Assessing Our Knowledge of Identity Theft: The Challenges to Effective Prevention and Control Efforts. *Criminal Justice Policy Review*, *19*(1) 3-24.

Winn, J. K. (2009). Are Better Security Breach Notification Laws Possible?" *Berkley Technology Law Journal*, *24*(3), 1133-1166.

Wood, S. (2002). Environmental Management Systems and Public Authority in Canada: Rethinking Environmental Governance. *Buffalo Environmental Law Journal*, *10*, 129-210.

Wood, S., Tanner, G. & Richardson, B. (2010). What Ever Happened To Canadian Environmental Law? *Ecology Law Quarterly, 37*, 981-1040.

Zittrain, J. (2009). *The Future of the Internet and How to Stop It*. New Haven: Yale University Press.