TECHNOLOGY AND PERSONAL FREEDOM

C. Ian Kyer*

In 1949 George Orwell published his famous *1984*, a book in which he warned of the dangers of technology.[1] He envisioned a world in which Big Brother was able to use technology to monitor and shape people's thoughts and actions, enabling societal control and the suppression of personal freedom. In January 1984 Apple Computer ran its famous commercial introducing the Macintosh computer: A series of drone-like people were seen marching into a hall where Big Brother exhorted them on a large computer screen. Suddenly, a young woman in a tank top and shorts ran into the room, twirling and throwing a large sledgehammer as if in an athletic competition, and destroyed the image of Big Brother. The voice-over told people that the introduction of the "Mac" would be why 1984 would not be *1984*.[2] Clearly Apple saw its technology and the personal computer as liberating. This may be a case of moving from the sublime to the ridiculous, but Orwell's book and Apple's advertisement reflect a long time debate – is technology liberating or enslaving? This debate arises periodically with the introduction of new technology. For example, in 1811 English textile workers known as the Luddites protested the changes brought about by the Industrial Revolution, which they felt threatened to enslave them.

The question of whether the Internet promotes democracy is an aspect of that debate. Many see the Internet as promoting freedom of expression and giving individuals a powerful and easily accessible means of reciprocal communication. The Internet is viewed as having been created as a protection mechanism – difficult to shut down in a nuclear attack – and a hallmark of government inability to suppress Internet communication. Others, however, point out that while suppression may be difficult the tracking of individual postings is relatively easy. This counter-argument notes that people communicate with their personal computers much more candidly than how they otherwise would, failing to acknowledge that the tools for tracking postings on the Internet are numerous, powerful and easily accessible. Monitoring of individual expression has never been easier.

The reality is that the Internet – like all technology – is neither inherently liberating nor enslaving. It is a tool that is capable of either or both, depending on how it is used by individuals and governments, and how it is regulated. Again, there are parallels in history. In the 17th century, the relatively new proliferation of printing presses allowed people the ability to produce pamphlets that criticized the government. The response was often seizure of the presses and subsequent government censorship. Over time, this came to be seen in our society as

* Fasken Martineau DuMoulin LLP

[1] George Orwell, *1984* (London: Penguin, 1949).

[2] The advertisement can be seen online: Uriahcarpenter <www.uriahcarpenter.info/1984.html>.

inappropriate government action and freedom of the press became a cornerstone of democracy.

Let us look at how our society deals with freedom of speech on the Internet. Freedom of speech is, of course, a core value of our society and it is enshrined in the *Canadian Charter of Rights and Freedoms* as "freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication".[3] As a society, we encourage people to share their views on the Internet. However, we have many laws that impose reasonable restrictions on that freedom. We do not allow people to use the *Charter* as a shield if they are promoting racial hatred or terrorism, or if they are seeking to lure children into sexual traps. Yet it is no secret that all of these activities are carried out daily on the Internet and that our governments wish to halt these practices. They point out that the people who seek to carry out these activities without prosecution have developed techniques to maintain their anonymity and disseminate their ideas. As a result, our governments have developed many tools to track what a person says and/or does on the Internet. These tools are continually being developed to track down perpetrators of hate crimes, pedophiles and terrorists.[4] It is unlikely that citizens will object to our government developing and using these tools and techniques for these socially beneficial purposes. However, these same tools and techniques are also capable of being used by governments to monitor and suppress political dissent. Clearly this is an instance where there is need for a balancing of interests.

Traditionally there are two important mechanisms to achieve this balancing of interests – Parliament and our legal system. In the past, when we feared misuse of government or police powers, Parliament adopted laws which imposed checks and balances. Laws were developed to limit wiretapping and other intrusive government

---

[3] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K., 1982, c. 11, s. 2 [*Charter*].

[4] A number of tools exist to intercept and analyze transmission on the Internet. See Ahmet C Amtepe, Mukkai S. Krishnamoorthy & Bülent Yener, "A Tool for Internet Chatroom Surveillance" online: Rootsecure <http://www.rootsecure.net/content/downloads/pdf/internet_chatroom_surveillance.pdf>. See also <http://www.justice.gc.ca/en/cons/la_al/summary/faq.html> where the Canadian Department of Justice states:

> Under the current laws, not all telecommunications service providers are required to design intercept capabilities into their networks. When a new technology or communication service is introduced, law enforcement and national security agencies often have to research and develop new methods to gain lawful access to those networks. The lack of a technical solution, or a delay in the ability to use it, hampers investigations and the prevention of serious crimes or threats to national security. To address this issue, the government is proposing that service providers in Canada be required to ensure their networks or infrastructures have the technical capability to enable lawful access by law enforcement and national security agencies when the agencies are legally authorized to intercept a communication or search and seize data.

investigative techniques.[5] Use of these techniques required a warrant and the people intending to use these measures were required to convince an independent person (such as a judge) that their intended use was justified in the circumstances. In the rush to deal with such threats as terrorism and pedophilia, the U.S. Congress, and to a lesser extent our Parliament, has too often recently decided that such traditional checks and balances are a hindrance to effective policing and anti-terrorism. It is a sad truth that our Parliament's track record as a body to debate such issues and to subsequently determine where the proper balance lies has been lacking in instances where national security or public safety is seen to be at stake.[6] At the time of the First World War, Parliament expanded the *Official Secrets Act*[7] to make it easier to successfully prosecute perceived spies using cameras. This broad and ambiguous statute – with virtually no safeguards against police or governmental abuse – was passed without debate in 30 minutes.

We as a society need to insist on laws that limit governmental use of invasive tools on the Internet in order to safeguard the privacy of its citizens. Broad, discretionary powers should be avoided in favour of limited, focussed powers authorized by warrants and supervised by the courts. If this is to happen, we need to make civil liberties the sort of legislative priority that we as a society have made environmental issues and global warming. We also need to encourage our courts to monitor the government's use of these tools and techniques, and to narrowly interpret what are reasonable restraints on our fundamental values. To do otherwise is to put our society on the road to Orwell's *1984*.

We as a society also need to be concerned about civil law and defamation. It was said in 1994 that the Internet was a modern frontier with no laws or regulation applying to it – borderless and outside the reach of territorial laws. Many of us doubted this at the time and some maintained that the international reach of the Internet would make it subject to many legal regimes rather than none. Over time this opinion has come to appear prophetic. We are now seeing defamation cases

---

[5] For a discussion of "lawful access" see online: Department of Justice <http://www.justice.gc.ca/en/cons/la_al/summary/faq.html> where it states that:

> Lawful access can only be used with legal authority, i.e. a warrant or an authorization to intercept private communications, issued by a judge under specific circumstances. For example, authorizations to intercept private communications can only be used to target particular communications and can only be carried out for a specific period of time. In order to obtain a warrant to search for and seize data, there must be reasonable grounds to believe that an offence has been committed. For the Canadian Security Intelligence Service (CSIS), both the Solicitor General and a Federal Court judge must approve each warrant application... Lawful access is provided for in legislation such as the Criminal Code, the Canadian Security Intelligence Service (CSIS) Act, the Competition Act and other acts. This legislation is subject to privacy laws and the *Canadian Charter of Rights and Freedoms*.

[6] Martin. L. Friedland, *National Security: the Legal Dimensions*, study prepared for the Royal Commission of Inquiry Concerning Certain Activities of the RCMP (Ottawa: 1979) 31-36.

[7] The *Official Secrets Act*, S.C. 1939, c. 49, revised the relevant provisions which had previously been codified under the *Criminal Code*, R.S.C. 1919.

being brought in those jurisdictions that have laws favouring plaintiffs.[8] If we allow our courts to take jurisdiction in cases where the jurisdictional connection is limited, we will discourage the dissemination of ideas on the Internet and construct barriers to free speech. Although we should start with our own jurisdiction, to be truly effective we should push for international treaties that seek to maintain the Internet as an avenue for free speech and the sharing of ideas.

Only collectively shall we decide whether the Internet and its related technology will be liberating or enslaving. We need to recognize that the answer to this question depends on how it is used by individuals and governments as well as how this technology is regulated and its applicable rules enforced.

[8] On the Australian case of *Gutnick v. Dow Jones* (2003), 210 C.L.R. 575 (H.C.A.), online: Wikipedia <http://en.wikipedia.org /wiki/Gutnick_v_Dow_Jones> and on the Canadian case of *Bangoura v. Washington Post* (2005), 258 D.L.R. (4th) 341 (O.A.C.), online: The Canadian Internet Policy and Public Interest Clinic <http://www.cippic.ca/en/faqs-resources /defamation>. Also see Michael Geist, "Libel case Key for Internet Free Speech" *The Toronto Star* (31 July 2006) online: Michael Geist <http://www.michaelgeist.ca/content/view/1343/159/>.