

Privacy, Technology and the Rule of Law

Richard Peck, QC

Vancouver, June 25, 2019

Seventy years ago, George Orwell's dystopian novel, *Nineteen Eighty-Four*, went to the printers. Satirical in form, it is a grim and depressing tale set in a futuristic totalitarian state where truth is banished, love is punished, and privacy is not possible under the omnipresent eye of Big Brother.

The story begins with the rebellious protagonist, Winston Smith, returning to his flat after a numbing day of work in his cubicle at the Ministry of Truth:

Behind Winston's back the voice from the telescreen was still babbling away... the telescreen received and transmitted simultaneously. Any sound that Winston made, above the level of a very low whisper, would be picked up by it; moreover, so long as he remained within the field of vision... he could be seen as well as heard. There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time.

We will return to Winston's plight in due course.

In 1949 when the book was published, Orwell's reference to a TV screen that could both listen to and watch the viewer would have been seen as more fanciful than prescient – like Buck Rogers's jet propelled backpack or Dick Tracy's two-way radio watch – the stuff of comic books.

Comparatively few households had a TV set. Even in 1984, when TVs had become ubiquitous, few would put much stock in the idea that a TV set could ever become a household spy.

Now, in 2019, matters have changed.

In an article published in the *Globe and Mail* earlier this month, the author Ziya Tong sets out a disturbing description of the ways in which technology is being used in the 21st century.

Tong notes that in England today there are 20 towns “where Big Brother doesn't just watch over you, he barks out orders and literally tells you what to do.” One such town is Middlesbrough, which has a network of 144 “speaking cameras.”

Here is an example: “To the lady in the brown dress, blonde hair, with the male in the black suit, could you please pick that cup up and put it in the bin.”

In North London similar cameras are installed at public housing developments and are seen to be oppressive when people standing outside their own homes are told that they are loitering.

In Romford, a town in east London, the Metropolitan Police recently tested controversial facial recognition cameras. Signs had been put up warning members of the public that automatic facial recognition cameras would film them from a parked police van.

The Independent reports that a man named John saw the signs, pulled the top of his jumper over the bottom of his face, put his head down and walked past these cameras. Moments later, a group of police officers stopped John, demanded to see his identification and became “accusatory and aggressive.” John, perhaps understandably, told them to go away, albeit in more profane language. They responded by issuing a penalty notice – a 90 pound fine – for public disorder, akin to our criminal code offence of causing a disturbance by swearing in a public place.

Tong notes, “Britain, home of George Orwell, has more than 6 million CCTVs... about one for every 10 people.”

In San Francisco and a number of other American cities, public buses are equipped with sophisticated audio surveillance systems to listen in on the conversations of passengers.

In Las Vegas, Detroit and Chicago there is what is euphemistically described as the “Intelli-streets” system, installed in streetlights and lampposts with microphones and cameras capable of secretly recording pedestrians' conversations.

Whether “intelli” refers to intelligent or intelligence gathering is something we may never know.

An even more pernicious use of technology involves so-called “stalkerware” apps. These apps use GPS to locate friends or wandering children. But they are also marketed towards jealous partners who want to monitor their spouses' whereabouts. As Elizabeth Renzetti, a journalist with the *Globe and Mail*, observed, while technology did not create stalkers, it certainly “provides a new, faster, stealthier pathway for [them] to travel.”

All of these, of course, come under the comforting heading of “safety measures.”

In 2014, Edward Snowden revealed that Britain's Government Communications Headquarters (the GCHQ) had been tapping into the home webcams of British citizens under a program called Optic Nerve.

It was noted that, in 2008, more than 1.8 million Yahoo! chat accounts were compromised as agents siphoned up millions of images through home laptop and desktop computer cameras. As Tong notes:

And while our fears tend to be directed to hackers spying through baby monitors, or peeping Toms peering through our windows, the biggest window into our private worlds stares right at us every day: the black pinhole of our webcams.

Much of this may seem like an excellent application of modern technology to detect and suppress crime until one recalls the cautionary words of President Franklin Roosevelt in his speech to Congress in 1941: “Those who would give up essential liberty to purchase a little temporary safety deserve neither liberty nor safety.”

As a society, we have become habituated not only to intrusion but also to an equally troublesome problem: self-divulgence.

We regularly, and of our own volition, give over personal information to non-state actors in the form of corporations such as Facebook, Google and Apple, usually through what is enticingly known as the “online experience.”

Jennifer Senior, a *New York Times* journalist, refers to this as the “privacy paradox,” the contradiction between our contempt for companies that engage in surveillance of our lives versus the willing consignment of our personal information for the convenience of online services.

These services are held out as being free of charge but the old adage holds: nothing is free in this life. We simply pay with a different form of currency, namely, our personal data.

Surveys going back decades show that Canadians place a high premium on personal privacy. So, what is going on here?

It would seem that the apparently benign experience of being online numbs our alertness to the dangers the Internet poses. We become lost in the experience, as if mesmerized. Any sense that we are under surveillance is rendered figmental. Yet when the intrusive nature of what is happening is brought to light, we become momentarily indignant and then fall back into the same pattern. This cycle has a familiar ring to it: a compulsive pattern of behaviour that is extremely difficult to break. In other words, we are addicts.

We have also become slaves to convenience. We now have the disembodied presence of Alexa in our homes. On verbal command, Alexa will turn on the lights, set the temperature and start the coffee. This saves us the trouble of having to flip a switch or two. But at what cost? We forget that Alexa responds to our commands by listening.

As we come to enjoy the ever-increasing benefits of our technologically mediated lives, the digital devices we engage with not only reshape our ideas about privacy, but also influence our behaviours at a subliminal level.

As Brett Frischmann and Evan Selinger explain in “Re-Engineering Humanity”:

We begin to “outsource” responsibility for intimate, self-defining assessments and judgments to programmers and the companies that employ them. Already, many people have learned to defer to algorithms when choosing which film to watch, which meal to

cook, which news to follow, and even which person to date.... Given that the design and workings of algorithms are almost always hidden from us, it can be difficult if not impossible to know whether the choices being made on our behalf reflect our own best interests or those of corporations, governments, or other outside parties.

As much as we want to believe that technology strengthens our control over our lives, in the words of Frischmann and Selinger, “The goal of designing programmable worlds goes hand in hand with engineering predictable and programmable people.”

In the digital age, our right to be left alone is silently depleting to a point of no return.

As privacy recedes, so does autonomy, and autonomy is the essential building block of a liberal democracy.

In an essay on privacy written in 1980, Arthur Schafer stated:

The ideal of privacy is clearly one of the fundamental values of our culture. There is a close relation between the availability of a protected zone of privacy and the individual's ability freely to develop individuality and creativity. In a society which is frequently intolerant of, or hostile to, nonconformity, freedom from constant surveillance is an important precondition for the development of independent and critically-minded individuals.

The provenance of privacy lends itself to debate. Here is a brief lineage.

In 1604, in England, Semayne's Case established that we have the right to privacy in our homes, with the oft-quoted words, “the house of everyone is to him as his castle and fortress.”

In 1765, *Entick v. Carrington*, recognized that privacy interests extend beyond the sanctity of the home to personal effects.

In 1849 in *Prince Albert v. Strange*, the Solicitor General Romilly, one of the great law reformers of his day, referred to the principle

that this Court will protect every person in the free and innocent use of his own property, and will prevent anyone from interfering with that use to the injury of the owner. A man has the right of property in the production of his mind, and incident to that right is the right of making the same public.

In the U.S. in 1888, Judge Cooley, in his text on Torts, had coined the phrase “the right to be left alone,” which was adopted two years later by Brandeis and Warren in their historic *Harvard Law Review* article “The Right to Privacy.”

Then in *Olmstead v. U.S.* in 1928, Brandeis J., dissenting, described privacy as “the right to be let alone – the most comprehensive of rights and the right most valued by civilized men.”

In 1967, the United States Supreme Court, in its landmark privacy decision, *US v. Katz*, found that our right to privacy protects “people, not places.”

Canada's Supreme Court followed suit in 1984, formally enshrining our right to be left alone into our common law in *Hunter v. Southam*.

Four years later, in *R. v. Dymnt*, Justice La Forest observed that:

[S]ociety has come to realize that privacy is at the heart of liberty in a modern state.... Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of the democratic state.

Following that, in *R. v. Duarte* [1990] La Forest J., echoed the language of Romilly, and defined the right to privacy as “the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself.”

So there is a short history of privacy – brief but sufficient for our purposes.

Now to the rule of law.

The phrase “the Rule of Law” trips readily off our tongues. We commonly refer to it as a pillar of democracy. The adjectives we use to describe it include “fundamental,” “foundational,” “indispensable.”

It is expressly referenced in our Constitution as a founding principle of our country.

It is explicit in the very oath we take when we are called to the bar – an oath which requires us to “uphold the rule of law and the rights and freedoms of all persons.”

In 2005, the Supreme Court of Canada said “The rule of law is a fundamental postulate of our constitutional structure that lies at the root of our system of government.”

The late Tom Bingham devoted a whole book to it.

Indeed, the phrase has been repeated so often, in so many circumstances, that it has almost acquired the qualities of a faith – in the sense of a belief in a divine truth. As Hutchison and Monahan said in their book, *Rule of Law*, it is the “will-o'-the-wisp” of constitutional history, calling up the image of an elusive ball of fire that repeatedly appears and then vanishes.

How do we capture and express its meaning?

Bingham aptly identified its essential core which he said was that “all persons and authorities within the state, whether public or private, should be bound by and entitled to benefit of laws publicly made and publicly administered in the courts.”

Former Chief Justice Dickson of the Supreme Court of Canada added to this by saying, “The law must stand supreme as the source and fabric of all social organization.”

That certainly adds to our understanding, but is that enough?

Robert Bolt's great play, *A Man for all Seasons*, provides another answer. There is a memorable scene in which Sir Thomas More is speaking with his son in law, Roper. Roper says that he would set aside every law in England to get at the Devil. More's reply is apt and descriptive:

And when the last law was down, and the Devil turned around on you where would you hide, Roper, the laws all being flat? This country's planted thick with laws – man's laws, not God's – and if you cut them down do you really think you could stand upright in the winds that would blow then? Yes, I'd give the Devil benefit of law for my own safety's sake.

The depth of those words was not lost on the American jurist, Felix Frankfurter, who saw the play late in life. When he heard More's reply, Frankfurter exclaimed, “That's it! That's it!”

Frankfurter immediately grasped that More's words went to the heart of our system of justice. He saw that the words express the need for the existence of law to ensure order and fairness in society.

He saw that the words express the necessity of everyone being equally subject to the law while, at the same time, having equal benefit of the law.

He saw that the words express that the laws are crafted by us. We decide – they are not imposed on us. They are the product of our will, our thinking, our creativity.

If we accept the premise that privacy is an essential value worth protecting, we must not remain complacent.

The fundamental problem is that the law has not kept pace with the development of technology. One wonders if it ever can given the increasing pace at which technology advances.

Decades ago, scholars and writers prophesized a dire state of affairs; few were inclined to listen.

In his famous work, *Discipline and Punish*, Michel Foucault paints a picture of contemporary society that resembles George Orwell's 1984. He spoke of Bentham's panopticon, a circular building designed with a tower at its center, surrounded by prison cells facing inward. The

inmates stationed in the cells cannot see inside the tower, but the watchmen in the tower can always see inside the cells. The prisoners must assume they are always under observation and act accordingly, policing their own behaviour.

For Foucault, the panopticon operates as a metaphor for modern society: as surveillance creeps into ever more private aspects of our lives, in time, citizens too internalize the fear of being watched and, as a consequence, begin to regulate themselves. In his words:

He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power; he makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his own subjection.

We have now come full circle. Back to Winston, our protagonist in 1984. The final paragraph of Winston's story sounds Orwell's cautionary bell:

Two gin-scented tears trickled down the sides of his nose. But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother.

We can only hope that Winston's story remains fiction.