NATIONAL POST

A massive surveillance network is revealed, America shrugs

By: Jesse Kline – July 18, 2013

"In Soviet society … there was no legal or societal concept of privacy, nor any demarcation between the lives of citizens and the right of the militia to monitor their lives," wrote Louise Shelley in the 1995 book *Policing Soviet Society*. "Autonomy was an alien value in a society that expected state intervention into daily life. Undercover work thus did not challenge central societal values; the use of listening devices, surveillance and hidden cameras were almost taken for granted by the citizenry."
Society's deference to the surveillance state allowed communist authorities to keep tight control over the population — putting fear into the minds of people that any statement that could be perceived as anti-Soviet, even in private, would have serious consequences.

Western society, especially in the United States, has traditionally valued privacy, individual autonomy and a judicial system that respects the rights of the accused. But these values have always been on shaky ground: People have constantly struggled to gain, and maintain, their rights.

Even before the National Security Agency (NSA) existed, FBI director J. Edgar Hoover was setting up a spy ring to gather information about politicians, journalists, dissidents, labour bosses and civil rights leaders, including, perhaps most notably, Martin Luther King, Jr. Hoover would collect information that he could then use to destroy the lives and careers of his enemies through blackmail, or by leaking sensitive information.

As the Cato Institute's Julian Sanchez notes, average citizens were likely not directly affected, but they "lived in a world with an architecture of surveillance that granted chilling and antidemocratic power to a small group of men who operated in secret, feared even by presidents and generals." And "Hoover's surveillance machine had nothing on the architecture of surveillance" the United States has now.
Since Edward Snowden released details of the NSA's massive surveillance program last month, the sheer size and scope of the operation has become increasingly clear. Intestimony before the House Judiciary Committee on Wednesday, the agency's deputy director, Chris Inglis, revealed that analysts look at data up to three hops away from the original source. That means that agents not only gather information on who the target is calling, but also everyone in the suspect's contact list, as well as all the people those contacts associate with.
It is said that everyone in the world can be connected through six degrees of separation, or six hops. Research shows that on the Internet, everyone is connected by less than five hops. Thus, three hops allows authorities to gather personal information on an incredibly large number of people — about a million for each person being investigated for possible links to terrorism, to be exact.

Of course, the NSA says it only collects metadata — information about who is calling whom — and not the contents of calls, but this information can reveal just as much about a person's behaviour.

Say, for example, someone calls an airline and a hotel in Brazil. Or perhaps they call their doctor, insurance company and an HIV hotline. It's easy to figure out what's going on in that person's life without hearing the details of their conversations.

When asked if the NSA's programs could be kept secret indefinitely, ODNI's council replied: 'we tried'

This information can potentially be combined with cellphone location data that can pinpoint where someone lives and works, and where they are at all times of that day and night, as well as the contents of their emails, social networking posts and web searches (much of which is collected by the NSA's Prism program).

There is also the potential that it can be compared with other databases, such as the massive collection of license plate scanners deployed throughout the United States, which store information about where vehicles are going and where they've been in the past.

A report released Wednesday by the American Civil Liberties Union (ACLU) shows that the state of Maryland alone collects approximately 7,000 license plate images every eight hours. Jersey City, N.J., a city of 250,000, has an estimated 10 million images on file, allowing authorities to plot the movement of residents over a five-year period.

For such an egregious violation of privacy, one would hope there would be safeguards in place to prevent abuse; or, at the very least, that these devices were effective in putting kidnappers, bank robbers and other violent offenders behind bars. Neither is the case.

According to the ACLU, only five states have laws governing the use of these devices. In Maryland, out of a total of 29 million license plates scanned within a four-month period, only 0.2% were flagged as being suspicious and 97% of those were for registration or vehicle-emissions violations.

If government agencies start correlating the information contained in these various databases to catch everyone from tax cheats to people who make stupid comments on the Internet, it's likely that the public will never know about it.

When asked whether "a program of this magnitude, gathering information involving a large number of people involved with telephone companies could be indefinitely kept secret from the American people?" the general council for the Office of the Director of National Intelligence told the congressional committee: "we tried."

Even if these systems are only being used as the government says they are, the very existence of such an omnipresent surveillance network creates a disturbing potential for abuse. Yet, when the *National Post* asked readers what they thought about the revelation of the NSA's programs, the general sentiment could be summed up as, "who cares?"

"I don't mind if my emails are read by government spies because I have nothing to hide," wrote one reader. "We must all be subject to scrutiny by the government to promote the welfare and security of the public."

The big worry is that Westerners will look at the erosion of their longstanding rights to privacy, liberty and protection against unreasonable searches, and collectively shrug — as those living in Soviet Russia once did.