GlobalResearch
Center for Research on Globalization

“Violent Voyeurism”: Surveillance, Spyware and Human Rights

By Dr. Binoy Kampmark
Global Research, June 24, 2019

Theme: Intelligence, Police State & Civil Rights

Surveillance is merely a variant of violent voyeurism, the human behind the camera or visual apparatus observing behaviour in a setting, often private. Its premise is privacy’s violation; its working assumption is privacy’s irrelevance; officially tolerated such a concept is unofficially repudiated. Studies on surveillance do as much to reveal its problems as accommodate them: the great, all seeing commissar of email, letters and conversations remains persuasive.

Those who have put pen to paper on this have not always been very sympathetic. Judith Jarvis Thomson tended to see matters of privacy as a secondary interest: privacy rights are bundled up, as it were, with others, a second order of concern. The violation of privacy comes after more salient breaches. But mass market surveillance, much of it manufactured in the private sector, the ubiquity of spyware, and the ease with which such material can be acquired, has eclipsed such quibbles.

The innovations on the market have proven to be devastatingly effective. Canadian privacy research group Citizen Lab’s work in this field has shed light on a range of manufacturers pushing such products as FinFisher, the Remote Control System (RCS) of Hacking Team, and Israel’s own NSO Group’s Pegasus. As Sarah McKune and Ron Deibert observed in 2017,

> “business is booming for a specialized market to facilitate the digital attacks, monitoring, and intelligence-cum-evidence-gathered conducted by government entities and their proxies.”

Pegasus spyware remains one of the NSO Group’s most damnably and dangerously effective products, used to target individuals in 45 countries with impunity. Human rights activists such as Ahmed Mansoor can testify to its spear-phishing qualities, having been a target of various SMS messages with links intended to infect his iPhone. Had he actually clicked on those links instead of passing them on to experts at Citizen Lab and the cybersecurity firm Lookout for examination, surveillance software would have been installed.

An even more high profile instance where Pegasus is alleged to have been deployed is the case of slain journalist and occasional Riyadh critic Jamal Khashoggi, who was brutally dismembered in the Saudi Arabian consulate in Istanbul on October 2, 2018. A suit against NSO was subsequently filed in Tel Aviv by fellow dissident critic Omar Abdulaziz, claiming that communications between him and Khashoggi had been monitored by Saudi authorities deploying NSO software.

Much of this is shrugged off as exceptional: the NSO Group, for instance, argues that such

technology has been used to legitimately target terrorist groups and criminals; besides, their sale is premised on ethical restrictions. "It is not a tool to be weaponized against human rights activists or political dissidents," explains the NSO Group in an email. Such ethical considerations were little bar in the cases of Khashoggi, at least initially. But the concern, and publicity, was sufficient to prompt some mild action on the part of NSO Group. While the firm concluded that its technology did not "directly contribute" to tracking Khashoggi prior to his killing, new requests from Saudi Arabia were frozen over concerns of misuse.

David Kaye, the UN Special Rapporteur on freedom of expression, has made the latest effort to remind citizens that spyware, commercially and readily available, can be a very dangerous thing. A good deal of matters in life take place behind the screen of safe privacy. Dissidents and contrarians need their space to survive; journalists need their room to document abuses and make the powerful account. In the face of modern surveillance, expansive, beefed up, and developed by global corporations, the task had gotten that much more challenging.

Kaye's gloomy report, published to the UN Human Rights Council, supplies the disturbing stuffing the world of surveillance provides. It leaves little room for the fence sitters: surveillance harms and impairs. It is axiomatic that trust is denuded in that pursuit, and its very nature and intrusive activity eliminates the consensual bridge between citizen and state, and, as by-product, citizen and citizen.

It is, furthermore, generally unsupervised.

> "Digital surveillance is no longer the preserve of countries that enjoy the resources to conduct mass and targeted surveillance based on in-house tools. Private industry has stepped in, unsupervised and with something close to impunity."

The market itself was "shrouded in secrecy; indeed, our knowledge of the problem exists mainly because of the digital-forensic framework of non-governmental researchers and tenacious reporting by civil society organizations and the media".

As a function, such spyware is directed against specific individuals, "often journalists, activists, opposition figures, critics". This has led to unmistakable consequences: arbitrary detention, torture and extrajudicial killings. This suggests two parts of the equation: to see, at one end; to then order, at the other, the suppression if not elimination of the individual.

Kaye suggests a reasoned brake on the industry.

> "States should impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights-compliant safeguards regime is in place."

This may be sadly ambitious, given the security establishment's various addictions to technology in this field. Such suggestions are the equivalent of banning space technology that might be deployed in weaponry. Spyware is as much a product as a vision, the equivalent of arms manufacturing and efforts to produce the most lethal and insidious creation. To mention human rights in the same breath is the equivalent of seeking a more

honed form of killing, a decent form of surveillance. Seen in its amoral context, such products are neither wicked nor good, a mere mechanism to monitor and police. But behind the eye of spyware are its unscrupulous users. Behind the gazing software is a state or corporate employee, the voyeur of the national security state ever keen to peer into the lives of citizenry.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com

---