

Surveillance and a Right to Privacy in the Digital Age

By Josephine Langbien

In the digital age, governments can monitor not only our communications, but also our entire electronic existence. And, as a result of Edward Snowden's revelations, we know that they are eager to exploit this possibility. In April, a capacity audience welcomed Kenneth Roth, Executive Director of Human Rights Watch, to discuss the impact of mass surveillance on the right to privacy and freedom of expression.

As a former federal prosecutor, Roth is no stranger to surveillance. He was quick to point out that not all surveillance is necessarily bad. There is a valuable role for targeted surveillance, but it is the mass collection of metadata (the information *about* our communication, rather than its contents) which he finds concerning. Metadata reveals who we call, who we email, what we search for online and even, with the help of GPS tracking on mobile phones, where we physically go. From this information, a government is able to reconstruct our lives with a few clicks of the mouse.

Roth discussed three legal fictions employed by the United States government to justify its mass surveillance activities. Given Australia's participation in the 'Five Eyes' intelligence-sharing program with the US, United Kingdom, New Zealand and Canada, the arguments may also relate to our own privacy as well. First, the US government relies on a 35-year old Supreme Court ruling which held that, by disclosing the phone numbers we dial to telephone companies, we waive our privacy interests in that data. This 'sharing' rationale allows the government to claim that individuals have no privacy rights in any metadata communicated to third parties.

Recently, the US Supreme Court has suggested that it may revisit this interpretation of privacy to assess whether it is still appropriate. Roth noted that the 'because terrorism' argument is also wearing thin among the American public, and US President Barack Obama has accordingly indicated an intention to get out of the business of mass telephone data collection. While undoubtedly a positive step, the US President stopped short of expressly acknowledging a right to privacy. His statement was also limited only to telephone data, leaving the situation regarding online data (including email and banking details) unclear.

The second legal fiction promoted by the US government is that the storing of data does not infringe privacy - it is only when the data is actually examined, according to this argument, that privacy is breached. The US government claims that large amounts of metadata are collected because it 'needs a haystack in order to find a needle'. Yet as Roth pointed out, this argument has never been tested in open court, and was instead considered by a secret intelligence court which only heard submissions from a government lawyer.

Third, mass surveillance is said to be 'legal' according to a restrictively narrow reading of international human rights law, which interprets a State's obligations as limited to its own citizens and territory. The US government therefore does not recognise the privacy of individuals who are not US citizens and are not within US borders. This interpretation of international obligations is pursued despite explicit criticism from the UN Human Rights Committee. The disturbing consequence for Australians is that, under the



Ken Roth addresses a packed room

'Five Eyes' program, our federal government could easily obtain information about Australia citizens 'legally' collected by US agencies.

It is clear that these three grounds do not stand up to closer scrutiny. Snowden's revelations have allowed us to openly question practices that were previously only suspected. For Roth, mass surveillance not only infringes privacy rights, but also affects freedom of expression. If we are unable to communicate in private, then our ability to express secret or sensitive matters is hindered. He does not believe these limitations are justifiable. When Roth questioned a member of White House counsel, they were unable to name a single terror plot foiled on account of metadata collection.

Yet what can be done about the issue of mass surveillance? Roth believes that the answer lies in a deeper understanding of human rights law, and a strengthening of the international right to privacy.

Roth argued that we must instead focus on understanding privacy standards in a digital age. Relevantly, Brazil and Germany have commenced a process at the UN Human Rights Council seeking to update these standards in light of modern communications. In the discussion following his address, an audience member asked Roth how we might deal with Australian politicians who are less concerned about surveillance and privacy rights. Roth wryly suggested we ask our politicians if they have ever visited a porn site, or a psychologist, and whether they would be happy for the world to know about it.

The invasions of privacy Snowden brought to light were only possible because they were approved behind closed doors, without the knowledge or consent of the affected public. The surveillance debate must be moved to the public sphere because, as Roth asserted, the best way to protect our privacy, is publicly.