Is it too late to protect privacy? Pessimism reigns over big data and the law

September 17 2014, by Amy Coopes

Society may have already reached a point where protecting privacy has become impossible, and many legal experts are "united in pessimism" about the collection and use of big data, according to a communications surveillance-themed edition of the UNSW Law Journal.

UNSW Professor of Law and Information Systems, Graham Greenleaf, says the strengthening of privacy laws across the world is being overshadowed by "the ability (legal or not) of US-based companies to 'hoover up' the personal data of people in the rest of the world, and to

process and use it with few restrictions".

Noting that "big data only seems to be allowed to flow in one direction", Professor Greenleaf – co-founder and co-director of the AustLII free-access legal database – questions whether society has reached the point where the protection of privacy is now "impossible". However, he argues that although pessimism is justified, fatalism is not: human agency can still turn the situation around. The future is not a matter of technological determinism.

"The prevailing US model of an internet where the user is the product is not necessarily permanent. However, to stop it becoming so, it will take either a second internet bubble to burst, or a concerted effort by the rest of the world to reject privacy-invasive business practices," he writes in the Foreword.

"Neither is impossible, nor likely to occur rapidly."

Professor Greenleaf describes the Journal's authors as united in "pessimism" about big data, with "little enthusiasm for [its] promises … many concerns about its dangers and shared dismay at the inadequacy of privacy laws to deal with the problems raised by it, or by surveillance practices."

UNSW constitutional law expert Professor George Williams and research associate Keiran Hardy examine offences and penalties under Australian anti-terrorist law for whistleblowers and others who disclose national security information, finding "few protections" and significant inconsistencies.

A journalist could receive the same penalty as a source who passed them the national security information, even if they haven't published it or contemplated doing so.

In another "curious" hypothetical, someone who threatened to release sensitive information with the aim of intimidating the government into changing its policy on big data could be jailed for life, while passing the same information directly to a terrorist organisation to aid in an attack on Australian soil has only a maximum 25-year sentence.

"Prosecution for a serious criminal offence may simply be the price that an intelligence officer must pay for revealing improper and immoral conduct in good conscience," Williams and Hardy write.

"Given the sympathy of many for the actions of (Chelsea) Manning, (Julian) Assange and (Edward) Snowden, these limited protections would appear inadequate to a significant section of the community."

Dr Lyria Bennett Moses and Professor Janet Chan consider the benefits and challenges of the big data era for policing and the judiciary.

Though using big data in sentencing, or granting parole or bail could enhance judicial decision-making, they argue that such tools also pose transparency concerns and "may run afoul of well-established legal norms".

"Faith in the apparent rationality and objectivity of big data is often misplaced," they write.

"Ineffectiveness in the context of big data does not only mean that decisions will be 'wrong', it also means that decisions may be unfair. If a person's liberty, for example, is taken away based on inaccurate statistical correlations, then that is both unhelpful and unjust."

Provided by University of New South Wales