University of Wollongong
Research Online

Faculty of Informatics - Papers (Archive)

Faculty of Engineering and Information Sciences

2012

Human rights, regulation, and national security (introduction)

Simon Bronitt
Griffith University

Katina Michael
University of Wollongong, katina@uow.edu.au

Publication Details

Bronitt, S. & Michael, K. (2012). Human rights, regulation, and national security (introduction). IEEE Technology and Society Magazine, 31 (1), 15-16.

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

Human rights, regulation, and national security (introduction)

Abstract
Law disciplines technology, though it does so in a partial and incomplete way. This fact is refl ected in the old adage that technology outstrips the capacity of law to regulate it. The rise of new technologies poses a signifi cant threat to human rights. The pervasive use of closedcircuit television (CCTV), as well as mobile CCTV, telecommunications interception, and low-cost audiovisual recording and tracking devices (some of these discreetly wearable), extend the power of the state and corporations to signifi cantly intrude into the lives of citizens.

Keywords
security, introduction, national, human, regulation, rights

Disciplines
Physical Sciences and Mathematics

Publication Details
Bronitt, S. & Michael, K. (2012). Human rights, regulation, and national security (introduction). IEEE Technology and Society Magazine, 31 (1), 15-16.

This journal article is available at Research Online: http://ro.uow.edu.au/infopapers/2539

This paper originally published as: Bronitt, S. & Michael, K. (2012). Human rights, regulation, and national security. IEEE Technology and Society Magazine, 31 (1), 15-16.

A Note on Human Rights, Regulations and National Security

Simon Bronitt, Katina Michael

Professor Simon Bronitt, Director, ARC Centre of Excellence in Policing and Security (CEPS), Griffith University, Queensland, Australia 4111

Associate Professor Katina Michael, School of Information Systems and Technology, University of Wollongong, NSW, Australia, 2522

Law disciplines technology, though it does so in a partial and incomplete way as reflected in the old adage that technology outstrips the capacity of law to regulate it. The rise of new technologies poses a significant threat to human rights – the pervasive use of CCTV (and now mobile CCTV), telecommunications interception, and low-cost audio-visual recording and tracking devices (some of these discreetly wearable), extend the power of the state and corporations significantly to intrude into the lives of citizens. The regulatory failures in controlling the media's appetite for salacious stories, and the resulting corruption of some senior police, are the subject of a major inquiry into the culture, practices and ethics of the press. The inquiry in the United Kingdom chaired by Lord Justice Levenson, examines phone-hacking and other potentially illegal behavior, and the relationship between the press and police and the extent to which that has operated in the public interest.[1] Recommendations for enhancing the regulation of the press must balance the need for press freedom with the highest ethical standards. While the introduction of the *Human Rights Act* 1998 (UK) has led to a change in the attitude of British police to its role in the protection of human rights, it clearly had negligible impact on the Fourth Estate!

Australia is not immune from similar risks of regulatory failure, and there is a similar, though less wide-ranging review which has been instigated by the federal government. For instance, media organisations have found hacking into email and computer systems runs the risk of prosecution under federal criminal law.[2] Unauthorised interception of communications (telephone, SMS or email), or gaining

[1] Joshua Rozenberg (2011), Phone-hacking inquiry judge is right to investigate behaviour of the media's 'good guys'. guardian.co.uk, Wednesday 21 September 2011. Accessed 17/12/2011 at http://www.guardian.co.uk/law/2011/sep/21/joshua-rozenberg-leveson-inquiry

[2] Jonathan Clough (2010) Principles of Cybercrime, Cambridge University Press, London.

unauthorised access to intercepted material, are federal offences carrying stiff penalties. That being said, there appears to have been no prosecutions for such conduct in Australia. And Australia is certainly not the only country in this quandary.

While misuse of surveillance by corporations may be difficult to detect, Australia exercises continuous oversight over surveillance for law enforcement and national security purposes. The *Telecommunications (Interception and Access) Act 1979* (Cth) (TIA) has numerous oversight mechanisms, including reporting obligations on the law enforcement agencies to the Attorney General and the Commonwealth Ombudsman. Each year, the Attorney-General's Department collates these data and submits a report to Parliament. The annual report tracks the (ever upwards) trend in surveillance, though this barely rates a media mention today– intrusive surveillance technologies, once reserved only for the investigation of serious federal offences, is now universally available to law enforcement officials across Australia to gather evidence and intelligence relating to a wide range of offences. What is clear, is that the line between what is considered intelligence and what is considered evidence is beginning to blur as a result of advancements in social media and more broadly, social computing. In particular, the worrying trend is in the rise of warrants to intercept and access communications relating to terrorism offences, though unlike drugs crime, these warrants are not producing material which is adduced in legal proceedings. The nature of law enforcement surveillance is serving an intelligence rather than evidence-gathering function, supplanting or more likely further extending surveillance performed by the Australian Security Intelligence Organisation (ASIO) for national security. Indeed, the *Telecommunications Interception and Intelligence Services Legislation Amendment Act 2010* (TIISLA) has amended the TIA Act to remove legislative barriers to interoperability between national security and law enforcement agencies and enhanced their ability to share information.

Technological innovations not only benefit law enforcement. They also enhance the visibility of police misconduct that hitherto has been difficult, if not impossible, to establish. Not only are police watch-houses subject to monitoring, both inside and outside interview rooms, but there is increasing CCTV monitoring in urban inner city precincts which inevitably captures video evidence of police going about their work. In 2010, a Queensland Police officer was sentenced to 9 months imprisonment after

the violent assault on three people in his custody at the time of the offence.[3] A YouTube video had been posted showing the officer punching 23 year old Timothy Steele in the head and forcing a high-powered fire hose into his mouth. The footage also showed the officer slamming Renee Toms, then 21 years of age, to the floor of the watchhouse before pulling her by the hair, lifting her off the ground.[4] In another incident in 2008, unlawful use of police powers against a homeless man was captured on the Brisbane City Council CCTV system, providing critical evidence at the trial of the homeless man for refusing to comply with police directions and resist/assault police.[5] Due to the proliferation of CCTV, these 'captured' incidents showing police misconduct has risen in recent times. Some police are now calling for new video technologies to be worn at all times to increase public confidence and protect officers, as well as gather up-to-the-second intelligence and evidence.[6], [7]

Beyond these CCTV systems, which are not always working or trained on the right spot, youth on the streets who are most likely to encounter police in tense and difficult interactions increasingly resort to self-help surveillance. The incorporation of point-of-view (POV) surveillance devices into mobile devices has enhanced the capability of citizens to exercise what Steve Mann has called 'sousveillance'.[8] Some researchers have considered sousveillance to be surveillance from below (by citizens) rather than from above (by the state). Mann himself has stated that sousveillance is a form of "reflectionism."[9] In essence, sousveillance is the "philosophy and procedures of using

---

[3] Marissa Calligeros, October 12, 2010, "Cop bashing video released", *Brisbane Times*, http://www.brisbanetimes.com.au/queensland/cop-bashing-video-released-20101012-16gyh.html Last Accessed, 17 December 2011.

[4] AAP General News Wire (Sydney). 2010. "Former Qld cop jailed over bashings", http://news.smh.com.au/breaking-news-national/former-qld-cop-jailed-over-bashings-20101011-16f1v.html, 11 October 2010.

[5] ABC News. 2008. "Caught on camera: Qld Police punching homeless man", Last accessed http://www.abc.net.au/news/2008-07-22/caught-on-camera-qld-police-punching-homeless-man/447364

[6] David Murray, (2010). "Police say body cameras will cut down attacks", The Sunday Mail (Qld). http://www.theaustralian.com.au/news/police-say-body-cameras-will-cut-down-attacks/story-e6frg6oo-1225884744609, June 27, 2010.

[7] Mallory Cooke, 2011. Aussie Officer Studies New Technology at Fort Smith P.D., http://www.5newsonline.com/news/rivervalley/kfsm-aussie-officer-studies-new-technology-at-fort-smith-pd-20110512,0,6720541.story, 12 May 2011.

[8] Steve Mann, (2001). "Can Humans Being Clerks make Clerks be Human? - Exploring the Fundamental Difference between UbiComp and WearComp", Informationstechnik und Technische Informatik, 43(2), pp. 97-106.

[9] Mann, S. (1998) 'Reflectionism' and 'diffusionism': new tactics for deconstructing the video surveillance superhighway. *Leonardo*, 31(2): 93-102.

technology to mirror and confront bureaucratic organizations".[10] Police misconduct captured on high-definition recording devices can be immediately uploaded to personal blogs, Facebook, YouTube and other social media sites. This 'new visibility'[11] of policing in the 21st century increases public transparency of officer conduct, and stimulates community and media interest in use of force incidents. Although there is evidence that the new 'less lethal force' options available to police, such as Tasers or Oleoresin Capsicum (OC) spray, help reduce lethal outcomes for citizens and minimise officer injury, recurrent images of incidents of police brutality has intensified community anxiety and demands for enhanced police accountability in recent years.

This special section on the social implications of national security technologies addresses questions of human rights, regulation and legislation, evidence-based policy, and new emerging forms of social modelling and simulation. Many of the cases addressed by the authors are based on the Australian experience but are equally universal in applicability and relevance.

---

[10] Steve Mann, Jason Nolan, Barry Wellman, (2003). Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. Surveillance and Society, 1(3), 331-355. Available at http://www.surveillance-and-society.org/articles1(3)/sousveillance.pdf

[11] See generally Andrew Goldsmith (2010), "Policing's New Visibility", British Journal of Criminology, 50(5), pp. 914-934.