Chapter 10
Human Rights Defenders and the Right to Digital Privacy and Security

Tanya Notley
Tactical Technology Collective, Germany

Stephanie Hankey
Tactical Technology Collective, Germany

ABSTRACT

Digital technologies, such as mobile phones and the internet, provide new opportunities for Human Rights Defenders to mobilise people, coordinate activities, uncover and document abuses, publish findings, and engage new audiences. However, with these new opportunities come new risks as well. This chapter examines the right to and need for private digital communication as part of freedom of expression in the context of carrying out human rights work. Drawing on their experiences at Tactical Technology Collective, an international non-government organisation, the authors argue that the most effective means to address the digital privacy needs of people who are defending human rights is to provide a range of support − including awareness raising media, how-to toolkits, and hands-on training − that assist Human Rights Defenders to identify and then address digital risks by changing behaviours in ways most appropriate to their local context.

RIGHT TO PRIVACY WHEN USING DIGITAL TOOLS

In *The History of Human Rights* Micheline Ishay points out that state justifications for using surveillance are not new (Ishay, 2008). The British utilitarian philosopher, Jeremy Bentham (1748-1832), argued that the right act or policy was that which would cause "the greatest good for the greatest number of people." Perhaps most famously, this perspective led him to develop the idea of a 'panopticon' to gaze over the walls of prisons to provide a constant watch on the prisoners kept inside (ibid., p352). While his idea was not taken up by the government of the

DOI: 10.4018/978-1-4666-1918-0.ch010

time, Bentham's argument that the more people believe they are being watched, the more likely they are to decide to not engage in behaviour they believe they may be punished for, is one which remains pervasive among governmental and corporate policies around the world. This same rationale, for example, is applied to justify the use of surveillance cameras – placed in streets, airports, hotels, homes, schools and shops – by governments, citizens and private companies. However, while the widespread use of video surveillance is often controversial in terms of privacy rights, in this chapter we will illustrate that internet and mobile telephony surveillance is something quite different. This is because new methods of internet and mobile telephony surveillance can and are being used to track our behaviour and communication in spaces we often believe are private; this usually happens without our knowledge or consent.

Changes to our right to and ability to control privacy can be understood as part of what Ishay refers to as the rise "of a more bureaucratized, cyber-controlled society" (Ishay 2008, p352). At the root of these changes, she contends, are the expansion of counter-terrorist activities (particularly post September the 2011 terrorist attacks in the United States), paralleled with increases in access to and use of digital technologies. Within this context she asks if we need new human rights laws and mechanisms to protect digitally-mediated spaces that support both freedom of thought and freedom of expression. To debate what changes are needed in order to catch up with technological change, she suggests that we may need to look not only to new human rights treaties, but also toward greater coordination and campaigning among civil society regarding the implications of new forms of control that can be exerted when we use digital technologies to communicate (Ishay, 2008, pp. 354-5).

There are many factors that can be used to explain why we are now seeing increasing levels of and types of digital surveillance activities. Diebert and Rohozinski (2010) contend that the risks to governments posed by what they call 'dark networks' (which they define as networks carrying out or promoting criminal activities which might range from paedophilia networks to copyright infringements to credit card fraud) and also 'resistance networks' (referring to those who legitimately oppose governments or challenge their actions and effectiveness) have contributed to a "massive expansion of electronic surveillance among all countries, a significant portion of it carried out through extra-legal means and / or downloaded to private companies" (ibid. p28). More specifically, the September 2011 attacks, they state, led the United States to quickly implement wide-ranging legislation, in the form of the PATRIOT Act, which expanded the scope for electronic surveillance. Many countries were quick to follow in the footsteps of the U.S., requiring lawful access provisions for law enforcement to the files and records kept by private Internet Service Providers (ISPs) (ibid.).

Today we are seeing significant changes to privacy laws rights in a number of countries alongside changes to media and communication regulatory structures, policies and laws that can also impact on our privacy. For example, in the United States, the proposed 'Commercial Bill of Privacy Rights' would clarify and in some cases significantly extend the rights of governments and companies to obtain, keep and share private digital communications (Electronic Frontier Foundation, 2011; Kerry, 2011; Ramonas, 2011). In India, the government is in the process of drafting a Privacy Bill (Gupta, 2011), while 2011 rules to the IT Act (amended in 2008) increase the ability of companies and states to carry out a range of surveillance activities (Abraham, 2011a, 2011b).

Some countries have a dedicated 'Privacy Ombudsmen' or Commissioner to oversee and protect privacy rights including those in the digital realm. One exceptional example that illustrates the potential for country-level privacy regulations