Mass surveillance and the lost art of keeping a secret

Theo Tryfonas[1], Tom Crick[2], Michael Carter[3], and Panagiotis Andriotis[1]

[1] Cryptography Group, University of Bristol, UK etc. etc.
t.tryfonas@bristol.ac.uk, p.andriotis@bristol.ac.uk
[2] Cardiff Metropolitan University, xxx
tcrick@cardiffmet.ac.uk
[3] Canada

Abstract. Global security concerns, acts of terrorism and organised crime activity have motivated nation states to delve into implementing measures of mass surveillance in cyberspace, the breadth of which was partly revealed by the whistleblower Edward Snowden. But are modern nation states fighting a battle in the wrong space? Is mass surveillance of cyberspace effective and are the conventional metaphors of technology control appropriate for it? Can algorithms detect, classify and decide effectively on what constitutes suspicious activity? We argue that as cyberspace is a construct that has only recently been viewed strategically, let alone indoctrinated (the UKs cyber-security strategy is only 4 years old), the societal impact of such bulk measures is yet much unclear as are the assumptions about the fitness of state organisations that are charged with their oversight and the potential for unintended consequences. Recent experiences highlight the role of multiple forms of intelligence inputs, especially human- and community-based, and the need for application of such intrusive measures in a targeted manner. We believe that intrusive measures, where necessary, must be used decoupled from the seductive promises of advanced technology and ought to go hand-in-hand with means that strengthen the affected communities to identify, report and battle extremism and organised crime, in ways that safeguard the fundamental principles of our contemporary democratic Western states.

1 Introduction

xxx