Communications Data and Civil Liberties Under Threat

blogs.lse.ac.uk/mediapolicyproject/2012/04/30/communications-data-and-civil-liberties-under-threat/

Robin Mansell, Professor of New Media and the Internet, at the LSE, warns that government's goals for cybersecurity go too far.

"In cyberspace, the war has begun". The UK Government wants to introduce legislation to make us safe. The hope is that making it easier to use intelligence gleaned from sifting communications data will lead to preventative action or a robust response when threats are real. In my new book, – *Imagining the Internet* and a short paper published today, I argue that these policies go too far.

Discussion about a Government move to supplement its powers under the Regulation of Investigatory Powers Act (RIPA) 2000, produced a flurry of media attention in April 2012. The Government claims that civil liberties will be safeguarded if the reach of communications data collection and analysis is extended to routine monitoring of every move that citizens make online. Why should citizens question this?

The 2010 Government's Strategic Defence and Security Review said that a comprehensive Cyber Operations Memorandum of Understanding is needed to "allow us better to share information, intelligence and capabilities to enable joint planning…". The UK Government could be preparing to be able to share the results of its analysis of large quantities of communications data with other governments such as the US, a country which leads in computer-based modelling to detect potentially bad behavior. It is only through more principled resistance to routine and ubiquitous communications data collection that civil liberties in the UK are likely to be preserved.

That criminals and terrorists will use digital technology to evade authorities is not a new observation. When people know that more data are being collected and stored, even on a decentralized basis, the 'underground web' is likely to grow. Even if authorities in the UK are not to be permitted to monitor real time data, the risk is higher that vast stores of data – including content – will be mined. It is not possible to get communications data from social media websites like FaceBook or Twitter without using techniques that require interception of content, not just information about what web pages have been visited or who texted whom. Government claims that authorities will not be permitted to access content are not persuasive.

Computerized software modelling is supporting augmented intelligence gathering. Governments are becoming captivated by the idea that analysis of communications data will give them more accurate information to protect us. The models have in common the apparent offer of a technical fix that will protect everyone from serious crime and other threats. But the results of data analysis on this scale can be skewed by anyone (authorities or others) who forges information – this is cyber propaganda in the Internet Age.

Governments do need to protect citizens from unwanted intrusions into their private online spaces. They do need to ensure that citizen interests in security are met. But surveillance, privacy intrusion, software agent misbehaviour, and a lack of transparency are becoming more and more prominent features of society. The right to be free from surveillance should not be an unaffordable luxury. More spending on the collection and analysis of communications data by Government without deeper consideration of the means by which civil liberties such as the right to freedom of private correspondence can be protected is not a way forward. The challenge is to start imagining how

Government can be responsive to its citizens' demands for improvements in their lives and livelihoods instead of answering the siren call of accumulating huge quantities of data on the premise that doing so will make citizens safer.