

Undermining Privacy, Internet Spying: The “Hidden” Security Agenda Behind the “Hidden” Browsing Histories” Issue.

Theresa May and the Snooper’s Charter

By [Dr. Binoy Kampmark](#)

Global Research, December 29, 2015

Region: [Europe](#)

Theme: [Police State & Civil Rights](#)

“Trust Me’ might be just the most manipulative thing a politician can say. It means leave me alone in secret to operate without proper challenge.” Tom Watson, UK Deputy Labour Leader, Dec 18, 2015

Many government policies are advertised as useful for broader safety – till they are reversed to apply to the very officials who create them. The UK Home Secretary is very much of that school. Readers will be aware what Theresa May has done her invaluable bit to undermine privacy on the broader pretext of protecting security.

Central to this is the Home Office’s insistence on the Investigatory Powers Bill that seemingly insists on more intrusion than investigation. The bill, in rather futile fashion, will compel phone and web companies to retain records of every citizen for at least a year, providing a data pool which police and security services could access when required. The legislation goes further, enrolling the relevant service providers in a pseudo-police role that will override encryption if needed.

May has found herself having to sugar coat the bill with some decent premise, and has decided to go the cyber bullying card, a view she outlined to South Suffolk MP James Cartlidge.[1]

The tactic is standard: if people are misbehaving on the internet, those on facilitating its use should be made responsible for moral behaviour. Accordingly, “Internet connection records would update the capability of law enforcement in a criminal investigation to determine the sender and recipient of a communication, for example, a malicious message such as those exchanged in cyberbullying.”

The response by *The Independent* has been an attempt to pull the history of Theresa May’s browsing history for the last week of October, a freedom of information request that purposely excludes any information directly concerned with security matters.

What is good for the goose of inquiry is also grand for the gander placed under the scrutinising eye of the state. In short, if you are going to be equal before the law, then by golly even ministers should have their browsing history on the internet made available for the public gaze.

Not so, according to the Home Office. The FOI request has been dismissed as vexatious. In

other words, the request was dismissed on grounds of an action “brought without sufficient grounds for winning, purely to cause annoyance to the defendant.”

The Home Office’s response, drawing upon section 14(1) of the Act, insisted that the department had “decided that your request is vexatious because it places an unreasonable burden on the department, because it has adopted a scattergun approach and seems solely designed for the purpose of fishing for information without any idea of what might be revealed.”

The response provides a suitable template for critics of the surveillance state, if only because it demonstrates the hopeless rationale for the entire metadata retention regime. If the request by *The Independent* was, by its nature, scattergun, one could hardly assume that the security state’s behaviour in this regard is anything but scattergun.

This legal excuse remains one of the least convincing in the area of information law. It is, however, used repeatedly by states who have freedom of information regimes, providing slivers when asked, but generally withholding the bulk of what is deemed too sensitive for release.

The point is often the same: we will have a regime to allow information for the public precisely because we are intent on disallowing much of it. Regulation, in other words, is constriction, measured in the name of protecting that great, inscrutable fiction known as the public interest. You are kept in the dark because ignorance is necessary bliss.

In the case of the Home Office, there could be few things more fundamentally vexatious than a metadata retention regime premised on the nonsense of combating trolls and bullies on the world wide web.

The efforts on the part of *The Independent* have at least demonstrated to British citizens that this regime has other purposes, managing to get some egg onto the faces of Home Office officials. It is by no means the only quarter targeting the potential consequences of the bill. Labour’s Deputy Leader Tom Watson has argued that the bill’s supposed self-guarding mechanisms and oversight simply do not go far enough in protecting privacy.

In Watson’s mind, there was merely a “very limited review of the Home Secretary’s warrants by a judge appointed by a Commissioner who is appointed by the prime minister.” It was a “false choice to say that these massive extensions of state power must be introduced without checks and balances.”

Apple’s CEO Tim Cook finds its provisions similarly repellent for privacy. “We believe it would be wrong,” went a company statement, “to weaken security for hundreds of millions of law-abiding customers so that it will also be weaker for the very few who pose a threat.”[2] Given this government’s supposed love of the corporate sector, big business and all, David Cameron and his Home Secretary have their work sharply cut out for them.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

Notes

[1] <http://www.theverge.com/2015/12/26/10667222/uk-surveillance-bill-cyberbullying>

[2] <https://diginomica.com/2015/12/28/home-office-refuses-to-reveal-theresa-mays-internet-history-says-request-is-vexatious/#.VoGdsraLTMw>

The original source of this article is Global Research
Copyright © [Dr. Binoy Kampmark](#), Global Research, 2015

[Comment on Global Research Articles on our Facebook page](#)

[Become a Member of Global Research](#)

Articles by: [Dr. Binoy
Kampmark](#)

Disclaimer: The contents of this article are of sole responsibility of the author(s). The Centre for Research on Globalization will not be responsible for any inaccurate or incorrect statement in this article. The Centre of Research on Globalization grants permission to cross-post Global Research articles on community internet sites as long the source and copyright are acknowledged together with a hyperlink to the original Global Research article. For publication of Global Research articles in print or other forms including commercial internet sites, contact: publications@globalresearch.ca

www.globalresearch.ca contains copyrighted material the use of which has not always been specifically authorized by the copyright owner. We are making such material available to our readers under the provisions of "fair use" in an effort to advance a better understanding of political, economic and social issues. The material on this site is distributed without profit to those who have expressed a prior interest in receiving it for research and educational purposes. If you wish to use copyrighted material for purposes other than "fair use" you must request permission from the copyright owner.

For media inquiries: publications@globalresearch.ca