

**SEPTEMBER 2014**

# **SECURITY VS PRIVACY**

**DOLAN CUMMINGS**



**MOTION:**

**“WE SHOULD BE WILLING  
TO COMPROMISE OUR  
PRIVACY IN THE INTERESTS  
OF NATIONAL AND  
INTERNATIONAL SECURITY”**

**DEBATING MATTERS  
TOPIC  
GUIDES**

[www.debatingmatters.com](http://www.debatingmatters.com)

**Institute of Ideas**



**wellcome**trust  
Strategic Award



# CONTENTS

**Introduction**

**Key terms**

**The security vs privacy debate in context**

**Essential reading**

**Backgrounders**

**Organisations**

**Audio/Visual**

**In the news**

## KEY TERMS

[Central Monitoring System](#)

[DRIP](#)

[PRISM](#)

[Privacy](#)

[RIP](#)

[Security](#)

[Tempora](#)

[The Patriot Act](#)

# INTRODUCTION

1 of 6

# NOTES

1  
1  
2  
4  
5  
6  
6  
6

In June 2013, former CIA contractor Edward Snowden leaked information revealing that the US government had an extensive surveillance programme known as PRISM, which monitored communications on a global scale [Ref: [Guardian](#)]. It also emerged that GCHQ, the UK's intelligence and security agency, was intercepting and processing billions of communications every day and sharing the information with the US. That project, known as Tempora, had been in existence since the beginning of 2012 and included recordings of phone calls, the content of email messages, entries on social media sites like Facebook and the history of an internet user's access to websites [Ref: [Guardian](#)]. It later emerged that India's new Central Monitoring System (CMS) gives the Indian state similarly all-encompassing surveillance capabilities [Ref: [The Hindu](#)]. In each case, these revelations caused great concern among civil liberties campaigners, who argue that such state surveillance threatens the privacy of ordinary citizens. Responding to the controversy in the US, President Obama said, 'You can't have 100 percent security and also have 100 percent privacy' [Ref: [NBC News](#)]. In fact, while the specific details of PRISM were new to the public, it is no secret that all states have security services that monitor potential threats to national security, as well as keeping tabs on known criminals in a bid to prevent and solve crimes. And in the context of the global 'war on terror', governments worldwide have stepped up efforts to identify potential threats. Many experts are concerned that the current conflict in Iraq and Syria is a breeding ground for extremists, and insist the security services must closely monitor anyone involved [Ref: [Huffington Post](#)]. The latest controversy in the UK concerns the Data Retention and Investigatory Powers Bill (DRIP), which gives security services access to an unprecedented amount of information about communications between citizens. While civil liberties campaigners see the bill as yet another unjustified attack on privacy, its advocates insist it is a measured response to security concerns and represents a reasonable compromise between privacy and security. The key question is whether privacy can indeed be compromised without betraying one of the core values of a free society.



## SECURITY VS PRIVACY:

**"We should be willing to compromise our privacy in the interests of national and international security"**



© ACADEMY OF IDEAS LTD 2014

**DEBATING MATTERS**

**WWW.DEBATINGMATTERS.COM**

## What is privacy?

Privacy is widely regarded as an important right in free and democratic societies. Article 17 of the United Nations International Covenant on Civil and Political Rights states that: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation” and “Everyone has the right to the protection of the law against such interference or attacks” [Ref: [Human Rights Web](#)]. Most people value the ability to keep their private lives private, to protect information about their finances, for example, and indeed to keep secrets. In politics, the practice of secret ballots enshrines the principle that how people vote is ultimately their own private decision - even if they choose to publicly back a particular candidate, nobody is allowed to scrutinise their actual vote. This protects people from being pressured or coerced into voting against their private wishes. Similarly, when we speak on the phone or send letters or emails, we generally do so in the expectation that the contents of these conversations and correspondences remain private. The idea of the state monitoring citizens’ private interactions is associated with authoritarian regimes and is a key feature of George Orwell’s dystopian novel 1984, in which privacy is all but eliminated.

## Limits to privacy

Despite a general consensus on the value of privacy, it certainly has limits. For example, even before the CMS, India’s Information Technology (Amendment) Act, 2008, allowed the government to ‘intercept, monitor, or decrypt’ any information ‘generated,

transmitted, received, or stored in any computer resource’ in the interest of ‘sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States, or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence’ [Ref: [Human Rights Watch](#)]. Similarly expansive powers are enjoyed by other governments. Indeed, supporters of the UK’s DRIP bill argue that it actually increases privacy by being more specific than previous legislation about which agencies have access to data; it still requires citizens to compromise on privacy, but with less sweeping powers for the state. So, former director of public prosecutions, Ken MacDonald, argues that DRIP makes the right balance between enabling the authorities to keep tabs in communications without giving them carte blanche to snoop on citizens [Ref: [Guardian](#)]. Specifically, the bill backs up earlier legislation that requires service providers like phone companies to retain information about their customers’ activity for up to a year, in case the security services need to investigate them. While some see this as a sinister intrusion into private activity, advocates of the bill emphasise that it mainly concerns ‘metadata’ like the time, date, and originating and terminating points of phone calls, emails and social media activity, rather than specific content. Defending similar legislation in Australia Anthony Bergin, deputy director of the Australian Strategic Policy Institute, insists such data is akin to the ‘material on the front of the envelope’, with the contents of the letter remaining private [Ref: [Sydney Morning Herald](#)]. For those in favour of compromising on privacy, the key point is that such surveillance is no big deal given the rationale behind it. US policy analyst



## THE SECURITY VS PRIVACY DEBATE IN CONTEXT CONTINUED...

3 of 6

NOTES

Loren Thompson argues: "...compared with the threat posed by terrorists bent upon destroying America, PRISM presents at worst only modest danger to our liberties. Its main purpose is to protect those liberties, not subvert them" [Ref: [Forbes](#)]. And defence policy analyst John Arquilla asks critics to: "...think about the world as it might be without such a sustained effort to find the hidden - to detect, track, and disrupt the terrorists" [Ref: [Foreign Policy](#)]. In other words, privacy might be important, but is it so important that we should risk national and international security rather than compromise a little?

### A sensible compromise?

Internet privacy is especially controversial, as the very thing so many people value about the internet - the ability to communicate with relative anonymity - also makes it useful for terrorists. A paper by the US government's Intelligence Advanced Research Projects Activity group argued that: "...what started out as a benign environment where people would congregate to share information or explore fantasy worlds is now offering the opportunity for religious/political extremists to recruit, rehearse, transfer money, and ultimately engage in information warfare or worse with impunity" [Ref: [Washington Post](#)]. In this context, it is argued that we should all be willing to give up a little privacy so that security agencies can keep an eye on suspicious online behaviour. Long before the latest controversies over PRISM, Tempora, DRIP and the CMS, the controversial Regulation of Investigatory Powers (RIP) Act (2000) in the UK [Ref: [Guardian](#)], and the Patriot Act (2001) in the USA, gave the state much wider surveillance powers, with considerable implications for online privacy [Ref: [Electronic Privacy Information Centre](#)]. Many citizens remain instinctively hostile to state surveillance

of activities, whether online or off. Privacy advocates protest that governments have not convinced them of the need to compromise privacy for national security [Ref: [Salon](#)] and that the debate about 'privacy versus security' represents a false dichotomy [Ref: [NBC News](#)]. Indeed, a 2012 US Congressional report found anti-terror programmes were undermining privacy while gathering no useful information [Ref: [New York Times](#)]. An while the age-old argument against privacy is that 'if we have nothing to hide we have nothing to fear', critics like law professor John Fitzpatrick argue that in a free society we all have the right to keep secrets [Ref: [Institute of Ideas](#)]. Just as the privacy of the voting booth is essential to democratic elections, a wider private sphere within which to think, debate and reflect beyond prying eyes is essential to democracy more generally. Like other civil libertarians, security technologist Bruce Schneier argues that: "Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control", because if we are constantly under surveillance, he argues, we are constantly fearful and self-conscious, and not able to act freely [Ref: [Wired](#)]. So while it might be difficult to maintain an expectation of privacy in a wired world, some believe we must do everything in our power not to abandon it [Ref: [Liberty](#)].



Snooper's charter or justified safeguard? The security bill explained

Alan Travis *Guardian* 10 July 2014

Q&A: NSA's Prism internet surveillance scheme

Leo Kelion *BBC News* 1 July 2013

India's surveillance project may be as lethal as PRISM

Shalini Singh *The Hindu* 21 June 2013

## FOR

Terrorist risk means privacy must take back seat to security

Anthony Bergin *Sydney Morning Herald* 14 August 2014

How the Drip bill will help us convict criminals

Ken MacDonald *Guardian* 25 July 2014

Why NSA's PRISM Program Makes Sense

Loren Thompson *Forbes* 7 June 2013

In defense of PRISM

John Arquilla *Foreign Policy* 7 June 2013

## AGAINST

Drip, drip, drip – the emergency surveillance law erodes our civil liberties

David Allen Green *Financial Times* 11 July 2014

Privacy vs. Security: A False Dichotomy

Robin Koerner *Huffington Post* 3 February 2014

Privacy vs. security: 'False choice' poisons debate on NSA leaks

Bob Sullivan *NBC News* 6 July 2013

The Eternal Value of Privacy

Bruce Schneier *Wired* 18 May 2006

## IN DEPTH

The death of privacy

Alex Preston *Observer* 3 August 2014

In defence of privacy

Frank Furedi *spiked* 30 September 2013

Spies' Battleground Turns Virtual

*Washington Post* 6 February 2008

What Our Top Spy Doesn't Get: Security and Privacy Aren't

Opposites

Bruce Schneier *Wired* 24 January 2008



## BACKGROUNDEERS

Central Monitoring System - A legal viewpoint  
Pavan Duggal *Deccan Herald* 19 August 2014

What are Drip and Ripa - is the UK's 'emergency' new snooping law legal?  
James Temperton *Expert Reviews* 11 July 2014

Security and freedom in the internet age  
Norman Baker *Liberal Democrats* 10 July 2014

India: Digital freedom under threat? Surveillance, privacy and government's access to individuals' online data  
Melody Patry *Index on Censorship* 21 November 2013

Lethal surveillance versus privacy  
Shalini Singh *The Hindu* 22 June 2013

India: New Monitoring System Threatens Rights  
*Human Rights Watch* 7 June 2013

India's 'Big Brother': The Central Monitoring System (CMS)  
Maria Xynou *CIS India* 8 April 2013

Digital young citizens: unlocking the privacy versus security debate  
Michel Nienhuis *Open Democracy* 13 June 2011

Privacy, Human Rights and the Law  
Professor John Fitzpatrick *Institute of Ideas* 2009

Osama bin Laden's "Second Life"  
Juan Cole *Salon* 25 February 2008

No Snoopers' Charter  
*Liberty*

Privacy  
*Liberty*

The United Nations International Covenant on Civil and Political Rights  
*Human Rights Web*

Radicalisation Research

## ORGANISATIONS

Central Bureau of Investigation (India)

Liberty

Mi5

5 of 6

NOTES



## IN THE NEWS

Your smartphone, apps reveal more than you know  
*Livemint* 12 August 2014

Wikipedia swears to fight 'censorship' of 'right to be forgotten' ruling  
*Guardian* 6 August 2014

Would you trade privacy for national security?  
*Market Watch* 6 August 2014

UK government proposes public sector data sharing  
*S C Magazine* 4 August 2014

Drip surveillance law faces legal challenge by MPs  
*Guardian* 22 July 2014

Asio spy chief defends surveillance network and argues for broader powers  
*Guardian* 21 July 2014

Parliament passes emergency Data Retention Bill  
*BBC News* 17 July 2014

Commons passes emergency data laws despite criticism  
*BBC News* 15 July 2014

DRIP filter: Controversial data retention bill forced through UK parliament  
*Russia Today* 15 July 2014

Liam Fox Says ISIS Terrorism Threat Means UK Intelligence Surveillance Should Increase  
*Huffington Post* 22 June 2014

Govt. violates privacy safeguards to secretly monitor Internet traffic  
*The Hindu* 9 September 2013

India introduces Central Monitoring System  
*The Register* 8 May 2013

Inquiry Cites Flaws in Counterterrorism Offices  
*New York Times* 2 October 2012

6 of 6

NOTES

## AUDIO/VISUAL

Privacy, Human Rights and the Law  
Professor John Fitzpatrick *Institute of Ideas* 2009



## ABOUT DEBATING MATTERS

Debating Matters because ideas matter. This is the premise of the Institute of Ideas Debating Matters Competition for sixth form students which emphasises substance, not just style, and the importance of taking ideas seriously. Debating Matters presents schools with an innovative and engaging approach to debating, where the real-world debates and a challenging format, including panel judges who engage with the students, appeal to students from a wide range of backgrounds, including schools with a long tradition of debating and those with none.



## FIND OUT MORE:

Debating Matters engages a wide range of individuals, from the students who take part in the debates, the diverse group of professionals who judge for us, the teachers who train and support their debaters, and the young people who go on to become Debating Matters Alumni after school and help us to continue to expand and develop the competition. If you enjoyed using this Topic Guide, and are interested in finding out more about Debating Matters and how you can be involved, please complete this form and return it to us at the address below.

Debating Matters Competition  
Academy of Ideas Ltd  
Signet House  
49-51 Farringdon Road  
London  
EC1M 3JP

- Yes, I'd like to know more. Please send me further information about the Debating Matters Competition:
- I am a teacher and would like further details about events in my area and how to enter a team
- I am a sixth form student and would like further details about events in my area
- I am interested in becoming a Debating Matters judge
- I am interested in sponsoring/supporting Debating Matters
- Other (please specify)

First name

Surname

School/company/  
organisation

Professional role  
(if applicable)

Address

Postcode

Email address

School/work phone

Mobile phone



**“A COMPLEX  
WORLD REQUIRES  
THE CAPACITY  
TO MARSHALL  
CHALLENGING IDEAS  
AND ARGUMENTS”**

**LORD BOATENG, FORMER BRITISH HIGH  
COMMISSIONER TO SOUTH AFRICA**

**DEBATING MATTERS  
TOPIC  
GUIDES**

[www.debatingmatters.com](http://www.debatingmatters.com)