

**FEBRUARY 2010**

---

# **ONLINE PRIVACY**

---

**DOLAN CUMMINGS**

**MOTION:**

**“WE SHOULD NOT  
EXPECT OUR ONLINE  
ACTIVITIES TO REMAIN  
PRIVATE”**

*Produced by*



**GLOBAL UNCERTAINTIES  
SCHOOLS' RESOURCE**

# CONTENTS

**Introduction**

**Key terms**

**The online privacy debate in context**

**Essential reading**

**Backgrounders**

**Organisations**

**In the news**

## KEY TERMS

[Cyber security](#)

[Data sharing](#)

[Privacy](#)

[Privacy policies](#)

# INTRODUCTION

1 of 7

# NOTES

1  
1  
2  
4  
6  
6  
7

We use the internet for an increasing variety of purposes: for reading news, paying bills, sharing photos, even watching television, and much more. And not only do our own computers record information about all of these activities, but we leave a trail on other computers too. Much of the time we don't even think about this and imagine that what we do online is our own business. But this information trail can have a number of important consequences [Ref: [Wikipedia](#)]. First of all, if we are careless with sensitive information like credit card numbers, we can suffer fraud or even identity theft [Ref: [Identity Theft](#)]. Similarly, any pictures or comments we post on social networking sites like MySpace and Facebook can all too easily end up being seen by people we'd rather not see them [Ref: [Tech Radar](#)]. Even if we are careful with our privacy settings [Ref: [Allfacebook.com](#)], however, and deal only with reputable websites and companies, information about our activities is out of our control. Social networking sites actually own the information posted by users, while internet service providers and search engines too routinely gather information for commercial purposes. If we use the internet at work or school, the management is generally entitled to monitor what we look at [Ref: [Privacy Rights](#)]. And governments can require internet service providers to hand over information about individuals' internet use if they believe they are involved in crime, not least terrorism. The UK government recently created a new unit, the Communications Capabilities Directorate, to implement the controversial Interception Modernisation Programme, maintaining huge databases of people's online activity [Ref: [The Register](#)]. Many internet users are therefore concerned that both private companies and governments gather far too much information about our online activities. Privacy advocates and campaigners argue that we should not give up lightly on the idea that we retain control of who knows what about our online activities [Ref: [Privacy International](#)].

### What are the arguments in the online privacy debate?

Secure software systems mean it is now generally safe to make financial transactions online, whether buying books or selling shares, while encryption and other security software is available for those with particular privacy concerns [Ref: [Wikipedia](#)]. But the question of whether we should expect privacy is not merely a technical one. Those who argue that online privacy is unrealistic believe that the very nature of how we use the internet today makes old-fashioned privacy concerns irrelevant or even undesirable [Ref: [Guardian](#)]. Irrelevant because the internet is all about sharing, not concealing – and if we are really concerned about keeping something private, we shouldn't put it online in the first place [Ref: [WebTechLaw](#)]. It is also considered undesirable because the benefits of privacy are outweighed by those of convenience [Ref: [Visual Revenue](#)] and security [Ref: [CNET.com](#)] if we trust internet companies and government agencies with our information. Privacy advocates counter that whatever the technical difficulties, people are entitled to use the internet without surrendering personal information to private companies or governments, however benign [Ref: [Wired](#)]. Controversies about whether internet companies should collaborate with the authoritarian regime in China, meanwhile, remind us that there can be a dark side to state supervision [Ref: [Asia News](#)].

### Trading privacy for convenience?

There are undoubtedly benefits to surrendering a degree of privacy online, for example, by accepting tracking 'cookies' from websites we visit [Ref: [Visual Revenue](#)]. If we trust internet companies with our address and credit card details, we can pay

for books, flights and other services at the click of a mouse. Users of social networking sites get to use these sophisticated applications free of charge, and can use them to stay in touch with friends, share articles and pictures and chat online [Ref: [Social Networking](#)]. While some people object to companies retaining information about things they read and buy online, others like the fact that web applications can then tailor adverts to their interests rather than annoying them with a scattergun approach [Ref: [eWeb Marketing](#)]. There is also the potential for greater speed and efficiency in everything from paying tax to accessing health services if we allow the relevant agencies to store and share information about us. More generally, some argue that the general culture is simply changing, and that, in the words of Facebook's Mark Zuckerberg, 'privacy is no longer a social norm' [Ref: [Guardian](#)], especially for younger people who have grown up with the internet and are much more comfortable sharing pictures and so on [Ref: [Wired](#)]. On the downside, the more personal information we share online, the greater the chance it will be abused by criminals or unscrupulous companies. Critics argue that any move away from valuing privacy is a worrying cultural trend, since a degree of privacy is essential both to civil liberties and personal well-being, and that young people do value privacy in their own terms even if they behave differently from older generations [Ref: [NPR](#)].

### Trading privacy for security?

There have long been concerns that the internet can be used by terrorist groups to recruit new members, raise money and plan attacks, and some argue this means we must be prepared to sacrifice some privacy [Ref: [Daily Mail](#)]. Security agencies

have even been monitoring applications like Second Life for signs of terrorist activity. A recent 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. Critics counter that the scope for terrorist activity online is overblown, and little more than an excuse for governments to snoop on ordinary citizens. Juan Cole argues in Salon that, 'Any monitoring by law enforcement of innocuous activity and communication in a virtual world, conducted broadly and without oversight, would be unconstitutional and could invade the privacy of millions of persons. I found no evidence based on my own observations that a virtual world is suitable for planning a terror operation' [Ref: [Salon](#)].

### So does privacy still matter?

Despite the purported benefits of giving up a degree of privacy, many internet users remain instinctively hostile to the idea that companies and government agencies can track their online activities. They point out that just because the internet makes it easier to store and share data, that doesn't mean we have to go along with it. If we do accept it, it should be because we are convinced of the benefits. Telecoms expert Norman Lewis suggests what really matters is trust: if we genuinely trust

companies with our data, that is very different from if they just assume we do [Ref: [Battle of Ideas](#)]. An important question, then, is whether we are asked to opt into a system in which our data will be stored or shared so we can reap benefits, or whether companies simply go ahead and do it for their own benefit. Similarly, privacy advocates protest that governments have not convinced them of the need to compromise privacy for national security [Ref: [Salon](#)]. Even if surrendering it would help the security services, they argue privacy remains an important consideration in its own terms. 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: [Archive.org](#)]. 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 [Ref: [Liberty](#)], security technologist Bruce Schneier argues the real choice is not between privacy and security but liberty versus control, because if we are constantly under surveillance, 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.

F.T.C.: Has Internet Gone Beyond Privacy Policies?

*Media Decoder blog, New York Times* 11 January 2010

Rethinking privacy and trust

Norman Lewis *Battles in Print* 20 September 2009

Spying on your email

Henry Porter *Guardian Liberty Central blog* 3 August 2009

Spies' Battleground Turns Virtual

*Washington Post* 6 February 2008

Who's afraid of Facebook?

Nathalie Rothschild *spiked* 15 August 2007

Terror laws 'eat away at privacy'

*BBC News* 6 September 2002

Terrorist threat shifts priorities in online rights debate

*CNET News.com* 17 September 2001

## For

Privacy no longer a social norm, says Facebook founder

*Guardian* 11 January 2010

Limiting online anonymity - and why that's a good thing

Sarah Warn *sarahwarn.com* 26 October 2009

Fight against terror must mean the end of ordinary people's privacy, says ex-security chief

*Daily Mail* 25 February 2009

The privacy myth

Paul Jacobson *Web.Tech.Law* 2 February 2009

## Against

Other people's privacy

Nicholas Carr *Rough Type* 17 January 2010

Why Facebook is Wrong: Privacy Is Still Important

Marshall Kirkpatrick *ReadWriteWeb* 11 January 2010

Does more snooping strike the right balance between privacy and security?

*Daily Telegraph* 27 April 2009

The Eternal Value of Privacy

Bruce Schneier *Wired* 18 May 2006

## In Depth

'You Have Zero Privacy Anyway—Get Over It'

David Adams *OS News* 11 December 2009

Why Facebook and Google hate privacy

Gary Marshall *TechRadar* 10 December 2009

Danah Boyd: 'People looked at me like I was an alien'

*Guardian* 9 December 2009

Is Online Privacy a Generational Issue?

Heather West *Wired* 1 October 2009

Two-Thirds of Americans Object to Online Tracking

*New York Times* 29 September 2009

Technology shouldn't give Big Brother a head start

Bruce Schneier *MPR News* 31 July 2009

Teens Take Advantage of Online Privacy Tools

*NPR* 3 April 2008

## ESSENTIAL READING CONTINUED...

5 of 7

NOTES

US seeks terrorists in web worlds

*BBC News* 2 March 2008

Osama bin Laden's "Second Life"

Juan Cole *Salon* 25 February 2008

Virtual terrorists

*The Australian* 31 July 2007

EU Privacy Czar Claims Right to Prohibit US Access to EU Financial

Records

Jonathan Winer *Counterterrorism blog* 1 February 2007

Pentagon sets its sights on social networking websites

*New Scientist* 9 June 2006

Perspective: Net privacy and the myth of self-regulation

Evan Hansen *CNET News.com* 16 October 2001

Facebook’s Mark Zuckerberg on privacy  
8 January 2010

Privacy, human rights and the law  
John Fitzpatrick *Institute of Ideas Christmas Lecture*  
15 December 2009

Google’s Privacy  
Eric Schmidt *CNBC* 3 December 2009

Data matching: a threat to privacy?  
James Welch *Guardian* 23 November 2009

Rethinking Privacy in an age of Disclosure and Sharing  
*Battle of Ideas* 31 October 2009

Facebook should compete on privacy, not hide it away  
Bruce Schneier *Guardian* 15 July 2009

We’re Giving Up Privacy and Getting Little in Return  
Bruce Schneier *Minneapolis Star Tribune* 31 May 2009

Politicians Overreacted To Terrorist ‘Threat’ Online  
*Techdirt* 12 March 2009

The National Security Strategy: Implications for the UK intelligence community  
Sir David Omand *ippr* 9 February 2009

The Horrifying Dangers Of Online “Cartoon-Like Personas”  
Tim Jones *Electronic Frontier Foundation* 6 February 2008

Using Web 2.0 tech in a top secret world, podcast  
Lewis Shepherd, a former senior technology officer at the US Defense Intelligence Agency 14 January 2008

Cookie Survey Results - Convenience outweighs most of the worries

Emer Kirrane *VisualRevenue*

Facebook’s privacy policy

Is Online Privacy at Work a Myth?

*Yahoo Hotjobs*

## ORGANISATIONS

American Library Association’s Office for Intellectual Freedom

Becoming paranoid, a weblog about computer security, privacy and staying safe online

Google Privacy Centre

Privacy International

Shut your Facebook

What is Identity theft?

## IN THE NEWS

7 of 7

## NOTES

Home Office spawns new unit to expand internet surveillance  
*The Register* 28 January 2010

Sun on Privacy: 'Get Over It'  
*Wired* 26 January 1999

Cybercriminals revive old scams to target smartphones  
*BBC News* 17 January 2010

Google Attack Part of Widespread Spying Effort  
*PC World* 13 January 2010

Online health records can save lives  
*Guardian* 13 January 2010

Privacy groups file FTC complaint against Facebook  
*Guardian* 17 December 2009

Facebook Privacy Changes Go Live; Beware of "Everyone"  
*PC World* 9 December 2009

Legislation to access public's texts and emails put on hold  
*Guardian* 10 November 2009

How Facebook tried to put a shine on \$9.5m privacy suit  
*Guardian Technology Blog* 21 September 2009

Internet firms resist ministers' plan to spy on every e-mail  
*The Times* 2 July 2009

Jacqui drops central snooping database  
*The Register* 27 April 2009

Government wants phone and internet providers to track users  
*Guardian* 27 April 2009

Virgin sacks 13 over Facebook 'chav' remarks  
*Guardian* 1 November 2008

US Spies Want to Find Terrorists in World of Warcraft  
*Wired* 22 February 2008

## ABOUT DEBATING MATTERS

Debating Matters because ideas matter. This is the premise of the Institute of Ideas & Pfizer 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

# “TEENAGE CITIZENS THINKING DEEPLY ABOUT...SOCIAL ISSUES”

IAN GRANT, CEO, BRITANNICA

Produced by



**GLOBAL UNCERTAINTIES**  
**SCHOOLS' RESOURCE**