# 4 Your footprints in cyberspace

Happily feeling secure and private behind our screens – regardless of the device used, it is easy to forget that every action in cyberspace is recorded somewhere by someone for various reasons, all of which imply knowing more about you and what you do in cyberspace. Recent media reports have confirmed what information professionals have known for years: monitoring it is possible and we have the technology to do it. Every technology has the potential to be misused and abused.

The sections that follow present the "what" and the "how" of the potential watchers with a few hints of "why".

**Figure 9**: Footprints – have you looked for yours?
CC BY Andy_3255, SA (flickr)

For the sake of an example, on August 4, 2013, there were media reports about a family from New York State, USA, who were detained and interrogated under suspicion of terrorist activity. The story revolves around "Mother" searching for pressure cookers, "Father" searching for backpacks and "Junior" wanting more information on the Boston Marathon bombings of 2013. The monitoring computers correlated these searches and reported a potential terrorist threat.

Download free eBooks at bookboon.com

## 4.1 Who is watching your online activities?

### What is this?

Given the massive flows of data across the Internet and the global telephone networks it would be impossible for "people" to watch all of it. But what is too much for humans is digestible for computers which can therefore monitor all or parts of all this traffic and be programmed to produce appropriate reports.

Some of the parties that know what you are up to with your devices are the obvious ones like your Internet Service Provider and your mobile communications provider. But there are many others. If you are using your employer's networks and/or devices your activities may be tracked by your employer. Legislation about this varies from country to country.

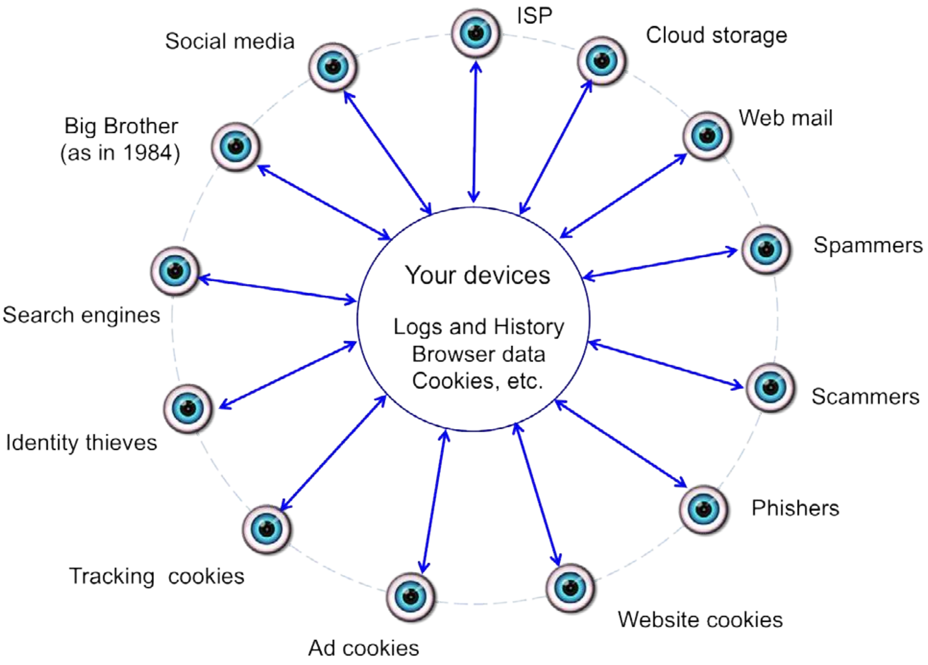


**Figure 10:** Big Brother (and his family) are watching you
© E. Gelbstein, All rights reserved

### Why is this an issue?

It really depends on how each individual feels about "privacy" and the extent to which each society applies the concept of "freedom of speech". While the latter is the subject of Article 19 of the United Nations Declaration of Human Rights of 1948, the Article recognizes that such freedom has limitations.

The most common limitations include items such as: slander, libel and defamation, the disclosure of confidential information, obscenity, etc. The World Summit on the Information Society of 2003 made a statement on the importance of the freedom of expression for the Information Society. Details can be found with a search engine.

Governments around the world are dealing with the challenge of maintaining a suitable balance between privacy, freedom of speech and national security. What elements of these strategies are communicated to the general public and the legal provisions around them vary from country to country and may change in a relatively short time.

### What you can do about it

Recognise that it is hard to be totally anonymous in cyberspace. It is prudent to be aware of the extent to which you (and your devices) collect and disseminate information about yourself and your activities in cyberspace.

On this basis, individuals should take steps to maintain the level of privacy they consider appropriate and use their right to express themselves within the bounds of what is sensible and legal. Failure to do so may lead to unpleasant experiences.

The pages that follow explore how your devices commit indiscretions, how you are making disclosures to others – not all of whom may be known to you – and being aware of what others may be saying about you in cyberspace.

What do you want to do?
VOLVO
AB Volvo (publ)
www.volvogroup.com
Volvo Trucks | Renault Trucks | Mack Trucks | Volvo Buses | Volvo Construction Equipment | Volvo Penta | Volvo Aero | Volvo IT
Volvo Financial Services | Volvo 3P | Volvo Powertrain | Volvo Parts | Volvo Technology | Volvo Logistics | Business Area Asia

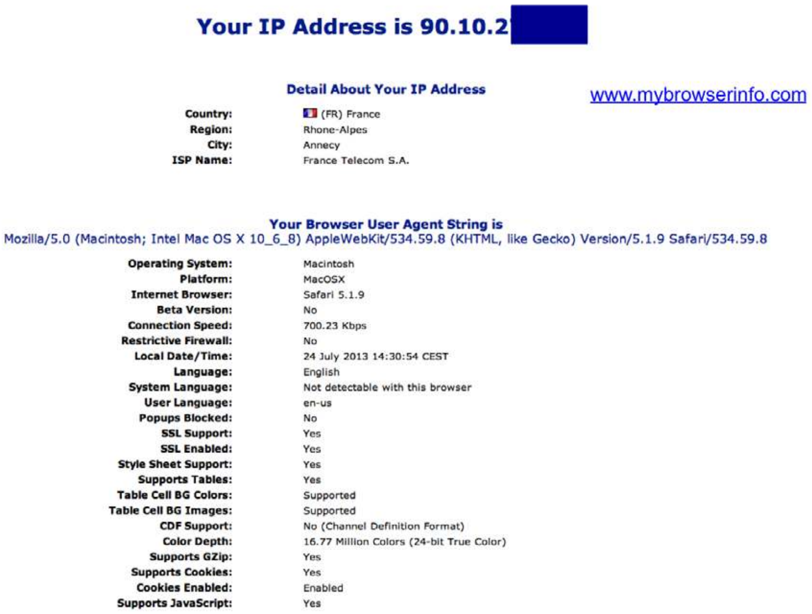
No matter what you want out of your future career, an employer with a broad range of operations in a load of countries will always be the ticket. Working within the Volvo Group means more than 100,000 friends and colleagues in more than 185 countries all over the world. We offer graduates great career opportunities – check out the Career section at our web site www.volvogroup.com. We look forward to getting to know you!

Click on the ad to read more

## 4.2 Your browser disclosures

### What is this?

Every time you connect to the Internet, the browser (part of your device's software) is designed to provide information to whatever you are connecting to.



**Your IP Address is 90.10.2[redacted]**

**Detail About Your IP Address**

www.mybrowserinfo.com

| | |
|---|---|
| Country: | (FR) France |
| Region: | Rhone-Alpes |
| City: | Annecy |
| ISP Name: | France Telecom S.A. |

**Your Browser User Agent String is**

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.59.8 (KHTML, like Gecko) Version/5.1.9 Safari/534.59.8

| | |
|---|---|
| Operating System: | Macintosh |
| Platform: | MacOSX |
| Internet Browser: | Safari 5.1.9 |
| Beta Version: | No |
| Connection Speed: | 700.23 Kbps |
| Restrictive Firewall: | No |
| Local Date/Time: | 24 July 2013 14:30:54 CEST |
| Language: | English |
| System Language: | Not detectable with this browser |
| User Language: | en-us |
| Popups Blocked: | No |
| SSL Support: | Yes |
| SSL Enabled: | Yes |
| Style Sheet Support: | Yes |
| Supports Tables: | Yes |
| Table Cell BG Colors: | Supported |
| Table Cell BG Images: | Supported |
| CDF Support: | No (Channel Definition Format) |
| Color Depth: | 16.77 Million Colors (24-bit True Color) |
| Supports GZip: | Yes |
| Supports Cookies: | Yes |
| Cookies Enabled: | Enabled |
| Supports JavaScript: | Yes |

**Figure11:** Beginning of the list of your browser's indiscretions (screen capture)
© Eduardo Gelbstein, All Rights Reserved

Many website owners collect this information as it tells them many items of interest: what software you are using, where you are connecting from (your home, a hotel, an airplane, etc.), the language you use, the speed of your connection, and a lot more. Browsers also indicate to each web page the link used to reach it (the referral link). To find out what your browser has to say about your arrangements, visit www.mybrowserinfo.com

### Why is this an issue?

Your browser's information is essentially geographic. This means that a multinational company will direct you to their national website – in e-commerce this may result in substantially different prices. Other entities may use this information to block access to copyrighted material (try accessing the BBC iPlayer from outside the UK). When tied together with cookies, privacy becomes an issue to consider.

### What you should do about it

Subscribe to an anonymiser service (there are several commercial providers). This implies connecting to the anonymiser's website which acts as a switch, removing your IP address. While not particularly expensive anonymous browsing may raise concerns to observers (everything is recorded these days) along the lines of "does this person have something to hide?"

## 4.3 Your cookies

### What is this?

Cookies came about with the World Wide Web and graphical user interface browsers. Essentially a small amount of data placed in your device by a web server whenever you visit a web page. The purpose of cookies is to personalise the web pages you visit (advertisements, automatically log you in "welcome back Eduardo" or prefilling a data field with your data. They do so by collecting data of what you do on the particularly website and other information stored for your convenience such as login and passwords, account numbers by clicking on a box "Remember me". So far, so good, because websites can only read the cookies they plant.

There are several kinds of "foreign" cookies placed by other parties – advertisers, collectors of statistical data. Tracking cookies are placed by a third-party website, often advertising. These cookies may contain information fed to it from the webpage visited such as the name of the site, particular items viewed, pages visited, etc.

When you later visit another site containing an embedded advert from the same third-party site, the advertiser will be able to read the cookie and use it to know more about your browsing history. This allows them to place adverts specific to you.

### Why is this an issue?

Many people see tracking cookies as an invasion of privacy since they allow an advertiser to build up profiles without the consent or knowledge of the individual concerned. This highlights the differences in legal systems concerning the protection of personally identifiable information. In Europe there is a European Directive that has been adopted into national law.

In Europe, each website must state that it will be using cookies and that by agreeing you have given the site implied consent. If such consent is not given some of the website functionality will not work.

Elsewhere there is widespread use of privacy policies often written by lawyers. These are complex and detailed statements of how an entity collects, uses, discloses and manages personally identifiable information. Many, but not all websites have a privacy policy. Most people cannot be bothered to look at them in the belief that they have nothing to hide.

Download free eBooks at bookboon.com

While smartphones do not use cookies, there are products for mobile marketers to track users across devices whenever you synchronise your mobile device and your computer's cookies.

### What you should do about it

Verify that the website you visit has an explicit Privacy Policy and read it (or at least try to), then find answers to the following questions:

- Does the website have privacy settings? If so use them and be ungenerous – some websites frequently change their privacy practices.
- Do you know who has planted cookies in your machine and how many there are?
- Would you be surprised if the majority are from places you never heard of?
- Do you know how to delete the cookies in your devices?
- Do you know that you can block and delete cookies in your browser – but it is prudent to find out what the consequences might be before doing so. The author does both regularly without adverse effects – useful cookies are retained.

Click on the ad to read more

## 4.4 Your disclosures

### What is this?

The Internet and other innovations in Information Technology have fundamentally changed the way in which we interact with organisations, with each other and, in turn, these changes have had a major impact on how we understand "privacy".

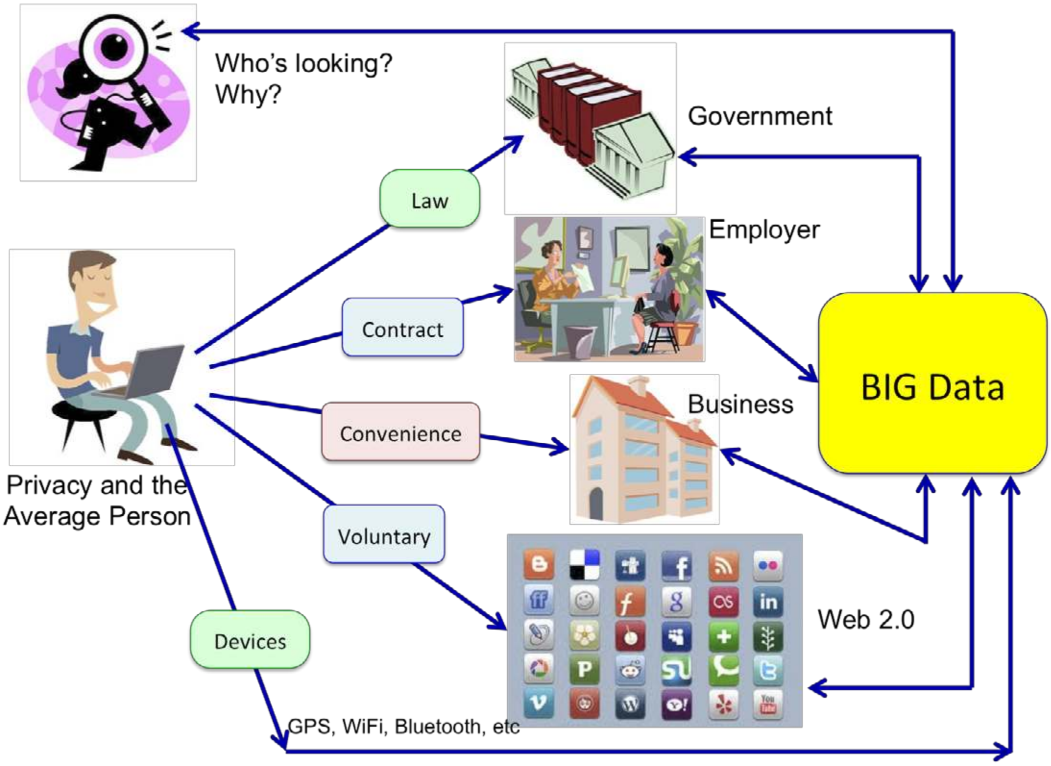


**Figure 12:** Scope of individual disclosures
© E. Gelbstein, 2013, All rights reserved

The figure illustrates the many information exchanges that begin with us as individuals. This first section on disclosures examines those we do because we are required by law and/or contract.

Disclosures required by law tend to be government requirements. These include civil status (births, marriages, divorces, deaths), property records, taxes, social security, driving licenses, etc. Historically done on paper, the adoption of e-government around the world is moving us into an environment where information about individuals is in electronic form and therefore easier to search (no need to dig into a dusty archive in a dark basement).

Disclosures required by contract include those related to employment, where an individual needs to provide details such as address and contact numbers, dependents, bank accounts, diplomas and certificates, etc. They are also required by banks, insurance companies, airlines and other businesses.

Disclosures for convenience are commonplace as well as optional. In exchange for a Frequent Flyer card and the opportunity to earn miles or points, or a supermarket Loyalty Card that may give you discounts and special offers, people willingly agree to provide a considerable amount of personal information, including a personal profile, address, income and more. Each time any such service is used, the party managing the scheme acquires information about the individual and how it uses the scheme.

Voluntary contributions cover all those things we do because we want to. These may include hotel and restaurant reviews, online comments on news items, blogs and other Freedom Of Speech actions as well as more intimate disclosures on social media – feelings, opinions, photographs and more.

Finally, there are the disclosures made by your mobile devices, particularly those that have networking capabilities (Bluetooth, WiFi, contactless protocols, etc.) and also GPS.

### Why is this an issue?

Perhaps it is less of an issue for the two first mandated activities, except that as individuals, we may want some assurances that the information will be used appropriately, be adequately protected and that these processes comply with any relevant legislation. The European Union for example has issued (and is currently updating) a Data Protection Directive that has been implemented by the member countries in ways that reflect their national culture and other related legislation.

Whenever you choose to make disclosures "for convenience", you can expect the party to whom this information has been provided to use it for their benefit, not just yours, and with your explicit consent (sometimes without it) share this information for marketing purposes with what they call "partner organizations". In the worst case you will receive more junk mail in your letterbox or you e-mail in-tray as well as unsolicited phone calls.

Voluntary disclosures require careful thinking because they are irreversible and forever. Various attempts by groups have been made, mostly in Europe, to have "the right to be forgotten" in social media. They remain unresolved and will no doubt be the subject of debate and ethical questioning for years.

The reader may consider (re)-reading George Orwell's book Nineteen Eighty Four (published in 1949) as the book anticipated social developments in society that have become reality. The GPS capability of mobile devices and the ubiquity of video cameras have more than a passing resemblance to "Big Brother is watching you".

Download free eBooks at bookboon.com

### What you should do about it

For the first two sets of disclosures: not much. It is prudent to ascertain that the information held about you is correct, accurate and up to date. It is good to remember than financial institutions rely on such information to assess your credit worthiness before granting a loan.

The convenience category is a matter of personal choice. There are people who, in order to maximize their privacy do not even use credit cards and do not join any loyalty schemes. At the other extreme there are the "junkies" who joined dozens of such schemes.

You can say online almost anything you wish, as most societies guarantee you extensive freedom of speech rights. Many countries have introduced legal restrictions on what they consider appropriate use of freedom of speech. Such restrictions include topics such as incitation to harm, offence and hate. An employer would not take kindly to their employees using social media to disclose sensitive information or even criticism. In September 2013 a low cost airline denied boarding to a passenger who used a social media tool to make adverse comments about the boarding procedure.

Items posted on social media must be assumed to be kept forever and require forethought. The "funny" photograph of 2005 could become a major embarrassment in 2015 and the candid comment made about someone else may result in litigation. The challenge here is that social media features encourage spontaneity, the opposite of careful consideration. In cyberspace there is no UNDO function.

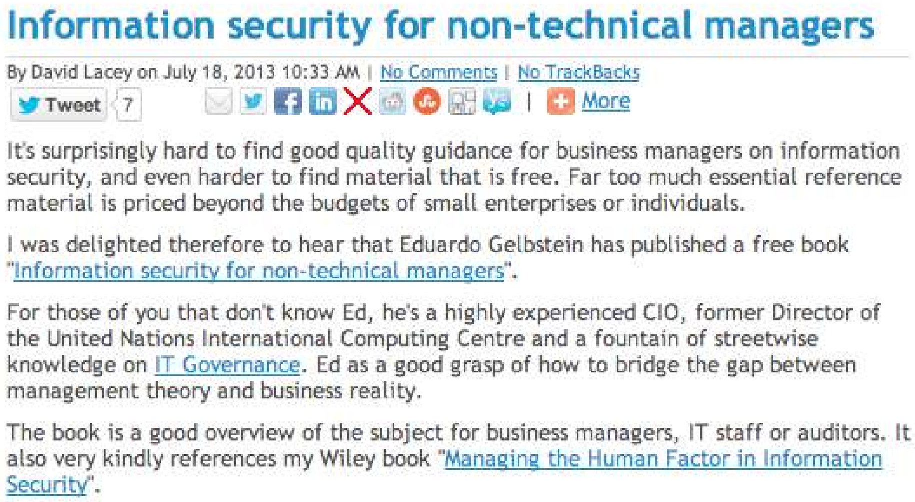
Download free eBooks at bookboon.com

Click on the ad to read more

## 4.5 What others may be saying about you

### What is this?

People who know you (and some who don't) may be "talking" about you in Cyberspace and this may range from the positive and helpful to malicious gossip, posting embarrassing photographs and worse. Social media and blogs are the most common channels for doing this. Unfortunately, some items of information about you may go viral and end up being published in the media.



Information security for non-technical managers

By David Lacey on July 18, 2013 10:33 AM | No Comments | No TrackBacks

It's surprisingly hard to find good quality guidance for business managers on information security, and even harder to find material that is free. Far too much essential reference material is priced beyond the budgets of small enterprises or individuals.

I was delighted therefore to hear that Eduardo Gelbstein has published a free book "Information security for non-technical managers".

For those of you that don't know Ed, he's a highly experienced CIO, former Director of the United Nations International Computing Centre and a fountain of streetwise knowledge on IT Governance. Ed as a good grasp of how to bridge the gap between management theory and business reality.

The book is a good overview of the subject for business managers, IT staff or auditors. It also very kindly references my Wiley book "Managing the Human Factor in Information Security".

**Figure 13:** Blog posting about the author's other Bookboon book (screen capture)
© Eduardo Gelbstein, All Rights Reserved

### What is this an issue?

While you may have little control over what others say about you, it's better to know than to remain ignorant. There have been so many misuses and abuses of social media – where spontaneity displaces thoughtfulness – that have resulted in people losing their jobs for having created embarrassing situations for their employers.

Knowing your public profile on the World Wide Web allows individuals to explore what actions they may wish to take to protect their reputation and privacy, ranging from gaining a better understanding of legal options to consulting a lawyer with specific knowledge and experience of cyberspace legislation.

### What you should do about it

Use a search engine and be surprised… this also gives you the option of setting up an alert whenever you (or someone with the same name) is mentioned in a website that allows search engines to access its content.

## 4.6 Your IDs and privacy in cyberspace

### What is this?

Identity Theft if a common crime in cyberspace. Using information collected from multiple sources – and much of this information is readily available to the patient searcher, it is possible to become a "copy" of you that is good enough to allow others to pretend they are you.

This may have only minor impact – the Secretary General of Interpol, Roland Noble, was the victim of this when someone pretended to be him in Facebook, created a page and used it to make "friends" with other senior police officers around the world. This happened again in 2012 and the victim was a senior NATO military official.

Identity Theft becomes a serious matter when financial matters are involved and you – the genuine person – starts getting demands for payment for major expenditures.

### Why is this is an issue?

Mainly because of disclosures made in goodwill without thinking of the possible consequences: credit card numbers and other important information sent in an e-mail, personal details revealed in blogs, chats, text messages, web pages and social media can all be used against you and cause you considerable trouble to unravel.

### What you should do about it

Remember the words of the North African proverb: "a closed mouth catches no flies" (original: Dans une bouche fermée, les mouches n'entrent pas). Discretion works well and, to quote Benjamin Franklin, Three can keep a secret if two of them are dead.

## 4.7 Being selective about who is in your network

### What is this?

A young man is proud of having over 500 Facebook friends. Several professionals have over 500 connections in Linkedin, while others have thousands of followers in Twitter. None of them can confirm that they actually know these people, write down a credible list of their names or even remember how and where they had something in common to justify such associations.

### Why is this an issue?

Amazingly, it is possible to buy "Friends" and "Followers" to apparently enhance one's image (any search engine will lead you to places that will sell you such services).

Unknown people wishing to link up with you may therefore not even be real but, by linking, they will have access to all the information you choose to provide and may subsequently use it against you.

Download free eBooks at bookboon.com

### What you should do about it

The answer is simple and difficult to apply, particularly those who like social media and spend considerable time immersed in it. Don't link to anyone you do not know, however good the reasons others may advance for accepting them.

Review your links regularly – you can in fact remove people from your network (a search engine will give you step by step instructions). Some social media sites make it more complicated that it should be.

## 4.8 Social media and Internet Memory

### What is this?

Social networks (and/or social media) are popular and have large numbers of subscribers. Their main purposes include linking up people with shared interests, those who lost contact with old friends, etc., and allow them to express and discuss views, opinions, reviews and feelings.

### Why is this an issue?

From and information security perspective, the main issues are:

- Social networks operate on the assumption that everyone can be trusted.
- There are no guarantees that any Third Party Applications or links posted in these networks are free of malware or are genuine websites
- A hacker could take control of your account and use it to spread disinformation, malware and scams – and you will be blamed
- As stated before, everything posted becomes the property of the Operator and it is hard or impossible to remove such postings – The Internet Memory seems to last forever.

### What you should do about it

Virtually all of the things discussed in this book should be considered and, ideally, applied. In particular:

- Ensure you have the latest updates for your security software, web browser, and operating system
- If there are any privacy and security settings on your social network websites use them to define your comfort level for sharing information. Less is always better than more
- Use strong passwords and have a different one for each social network you use
- Don't hesitate to delete, un-friend or whatever action is required to keep your network free of people you don't actually know or wish to network with
- Don't follow links in email, tweets, posts, and online advertising