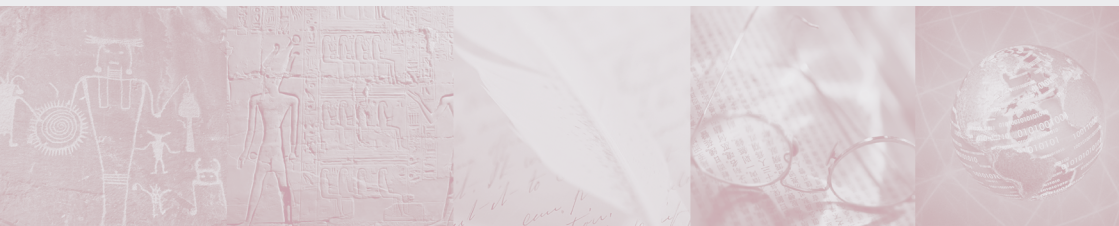


The Information Society Library  
GETTING THE BEST OUT OF CYBERSPACE

# APPROPRIATE USE

GUIDELINES AND BEST PRACTICES FOR  
E-MAIL AND OTHER INTERNET SERVICES

*Stefano Baldi • Eduardo Gelbstein • Jovan Kurbalija*



# P R E F A C E

There is no shortage of books on all matters relating to information management and information technology. This booklet adds to this large collection and attempts to do a number of things:

- offer non-technical readers an insight into the few principles that are important and reasonably stable;
- present the material in a context relevant to the work of those involved in international relations;
- awaken the curiosity of readers enough that they will progress beyond this booklet and investigate and experiment and thus develop knowledge and take actions that will meet their particular needs.

The format of these booklets and their contents evolved from courses given by the authors over the last few years in various environments and the feedback of the attendees. Readers' feedback on these booklets would be greatly appreciated by the authors so that future editions can be improved. The coordinates of the authors are given at the end of this booklet.

## **Acknowledgement**

The authors wish to express their appreciation to Jason Bellone, Information Security Coordinator at the United Nations in New York, for his insightful comments and suggestions during the preparation of this booklet.

ISBN 99932-53-01-4

Published by DiploFoundation

Malta: 4<sup>th</sup> Floor, Regional Building  
Regional Rd.  
Msida, MSD 13, Malta

Switzerland: c/o Graduate Institute of International Studies  
rue de Lausanne 132  
CH-1211 Genève 21, Switzerland

E-mail: [diplo@diplomacy.edu](mailto:diplo@diplomacy.edu)  
Website: <http://www.diplomacy.edu>

Edited by Hannah Slavik and Dejan Konstantinović  
Cover Design by Nenad Došen  
Layout & prepress by Rudi Tušek

© Copyright 2003, Stefano Baldi, Eduardo Gelbstein and Jovan Kurbalija

Any reference to a particular product in this booklet serves merely as an example and should not be considered an endorsement or recommendation of the product itself.

# C O N T E N T S

Introduction .....	5
E-mail and human communication .....	7
Introduction: electronic mail: working for you or against you? .....	9
Appropriate use of official electronic mail .....	14
Good practices to follow. ....	17
Appropriate use of your personal e-mail account .....	27
Accessing the Internet (and other systems) .....	29
Appropriate use of Internet access in the workplace. . .	31
Appropriate use of Internet access in the home. ....	36
Prohibited behaviour .....	37
Privacy, freedom of speech, human rights and other issues concerning the individual .....	39
Introduction. ....	41
Complex social information flows .....	41
About the authors .....	51



## INTRODUCTION

From the very beginning of the Internet – even before it was known by this name – the community sharing the Defense Advanced Research Projects network (DARPAnet) considered electronic mail to be an extremely valuable service.

In the last few years, e-mail has become extremely popular with a worldwide population counted in the hundreds of millions (in July 2003, Hotmail, just one of the free browser-based e-mail services, had 118 million subscribers). E-mail has changed the way we communicate and has also had a major impact on the way we work.

The World Wide Web is a related development that has also dramatically changed the way we think about information, entertainment, shopping and many other activities.

Good and useful as these services are when sensibly used, they can nevertheless raise potential problems in the workplace. This booklet will attempt to help clarify the boundaries between the official and private uses of computer systems, particularly for individuals working in international affairs.

This booklet will focus on the principles of appropriate use. We will present some practices to help readers achieve the following objectives:

- strengthen their air of professionalism;
- avoid being seen as a nuisance by others;
- avoid “importing” problems from the outside world;
- avoid wasting their time as well as that of others;
- prevent Career Limiting Moves.

Growing concerns about information security and office productivity have resulted in a number of new products designed to monitor “electronic activity”, which in turn has led to complex implications concerning the balance between security and personal privacy.

The ISL series includes three booklets devoted to information security issues: *Good Hygiene for Data and Personal Computers*, *Information Security and Organisations*, and *Hactivism, Cyber-terrorism and Cyber-war*.





SECTION



1

# E-mail and human communication

*I know that's what it says but you should've  
known that wasn't what I mean.*

*A genuine statement directed to one of the authors.*





## INTRODUCTION: Electronic mail: working for you or against you?

**E**-mail has become an enormously popular communication mechanism due to a number of positive qualities. Among the most common reasons given for its popularity are that it:

- is very suited for simple, fast communication;
- forces individuals to be concise;
- avoids causing interruptions, i.e. it can be dealt with at an individual's convenience (it is asynchronous);
- overcomes the problems associated with long distances and different time zones;
- provides the option of a message reaching a group of individuals simultaneously;
- enables every individual on a mailing list to get exactly the same version of the information;
- allows the easy management, storage and retrieval of files sent as attachments;
- facilitates individuals' participation in discussions regardless of their personalities and other potential inhibitors;
- is faster than arranging and holding a meeting;
- is vastly superior to voice mail as it avoids the unproductive activity of "phone tag".

However, new technology requires the adoption of new social and cultural protocols for effective use, and these need to be learned.

A face-to-face conversation consists of immediate verbal feedback (with its own risks of miscommunication) as well as many non-verbal signals, ranging from moving the head from side to side to indicate disagree-



Language reflects fundamental changes in society. The adoption of "to e-mail" as a verb confirms e-mail's ubiquitous use today. This phenomenon is not limited to English: for example, the word *courriel* is increasingly used in French.

ment to more specific body movements (many of which are culture dependent).

Immediate verbal feedback also occurs during a phone call. The tone and inflection of the voice can provide important signals in communication.

Neither verbal nor non-verbal signals are available with e-mail messages. E-mail messages are essentially lifeless and it is therefore important to compose them carefully in order to reduce the risk of misinterpretation.

### THE SPECIAL LANGUAGE OF ELECTRONIC MAIL

As e-mail became ubiquitous, many practices were introduced by the younger generation growing up with the technology. Three of these practices will be covered next: Internet Language, Emoticons and Netiquette.

### Internet language

Internet language consists of abbreviations or acronyms for commonly used phrases. The emergence of the Short Message Service (SMS) capability for cellular phones has accelerated the development of Internet language. For example, in English, the following are in common use:

afaik	As Far As I Know	rotf	Rolling On The Floor
b4	Before	rtfm	Read The F*cking Manual
cm	Call Me	rtm	Read The Manual [politer, cleaner version]
dur?	Do You Remember?	T+	Think Positive
fyi	For Your Information	tttt	To Tell The Truth
fwiw	For What It's Worth	tx	Thanks
gal	Get A Life	X!	Typical Man!
gmta	Great Minds Think Alike	Y!	Typical Woman!
icwum	I See What You Mean	2bcntd	To Be Continued
imho	In My Humble Opinion	2g4u	Too Good For You
btw	By The Way		

A more complete list can be found on many websites, for example:

<http://www.techdictionary.com/chat.html>

## Emoticons

The smiley, ☺, originally represented by the characters colon, dash, and close parenthesis, :-), is an old and important part of the online social culture. It was extensively used on bulletin boards and subsequently in chat rooms. Today, it is also used to make e-mail communication more “human” by allowing emotions to be represented in plain text.

The smiley has been in widespread use since the early ‘80s, when it was first introduced by Scott Fahlman in a bulletin board posting (shown below):

```
19-Sep-82 11:44 Scott E Fahlman :-)
From: Scott E Fahlman <Fahlman at Cmu-20c>
I propose the following character sequence for joke markers:
:-)
Read it sideways. Actually, it is probably more economical to
mark things that are NOT jokes, given current trends. For
this, use
:-(
```



Much creative effort has gone into creating a large family of emoticons since then:

☺ or ☻ Windows now automatically creates both emoticons whenever the appropriate sequence of characters is typed.

(:O:) a Band-Aid – used when offering help or support.

;-) a winking eye – used to say: “I’m just kidding”.

:o used to indicate surprise.

:@ used to indicate screaming.

A more complete list can be found on many websites, for example:

<http://www.windweaver.com/emoticon.htm>

## Netiquette

Netiquette also first originated on bulletin boards and in chat rooms. Many, if not all, of its features have also been adopted by the online community as good manners.

Many websites and books deal with Netiquette. The fundamental elements of Netiquette are essentially common sense (which maybe is not that common anymore) and good manners, even when operating anonymously. These two principles will be discussed further in the sections that follow.

### ETHICAL AND LEGAL ISSUES

Is e-mail a private form of communication? Not always and not everywhere.

Ethically speaking, electronic mail should have the same degree of privacy protection as telephone conversations. These cannot be tapped without formal authority being granted. The many businesses and organisations that record all phone calls as a matter of course must inform all of their employees of this on the first day of employment.

Depending on the legislation that applies in each situation, monitoring e-mail could be an infringement of an individual's basic rights, such as the freedom of speech. However, many countries consider intercepted e-mail messages to be admissible as evidence in a court of law.

The result is that even the most innocently composed e-mail could lead to major problems for an organisation. For this reason, a growing number of business e-mail systems automatically include a disclaimer in every message sent to an outside party.

These disclaimers are added for several reasons including:

- eliminating a company's liability for the acts of its employees (vicarious liability);
- ensuring that the e-mail cannot be considered a binding contract;
- reminding the recipient that the content of the message is "confidential";
- putting responsibility for an action (checking for viruses) on the recipient;
- indicating that the e-mail is for the specific attention of the intended recipient only, implying that it should not be forwarded without the company's prior consent.



Most lawyers concede that such disclaimers may create a false sense of security and moreover may be of dubious legal value. Such disclaimers cannot be used to impose an obligation on the recipient, who may choose to forward the message to a third party anyway.

In any case, an e-mail on a serious and confidential topic can always be encrypted and/or given an electronic signature, so a disclaimer be-

comes meaningless: if an unencrypted message is sent it cannot be argued that the sender has exercised due diligence in trying to protect it. The subject of encryption is discussed in some detail in the booklet *Good Hygiene for Data and Personal Computers*.

In some cases, the disclaimer is longer than the message itself and can be actually quite amusing as it may appear to assume that the recipient of the message is an absolute cretin.



**An example of a disclaimer approved by a legal department:**

This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail. Please notify the sender immediately by e-mail if you have received this e-mail by mistake and delete this e-mail from your system. E-mail transmission cannot be guaranteed to be secure or error-free as information could be intercepted, corrupted, lost, destroyed, arrive late or incomplete, or contain viruses. The sender therefore does not accept liability for any errors or omissions in the contents of this message, which arise as a result of e-mail transmission. If verification is required please request a hard-copy version. Company X, Suite# 1, Street, City, Country, [www.company.com](http://www.company.com).

Conversely though, do not let this section or any other discussions in this booklet discourage you from using such a useful resource. What is important is to use it sensibly and to be aware of the measures that should be taken in order to limit any risks.



**Global E-mail Statistics:**

Number of e-mail messages sent per day: 32 billion (projected to rise to 60 billion by 2006)

Average time spent on each message (to download, read and reply to/forward it): 2-5 minutes (depending on user's experience)

Lost productivity due to spam: US\$1 per minute

**Spam Statistics:**

- The September 2003 issue of *Wired* magazine has projected that by September 2004 spam will account for more than 50 percent of all e-mail.
- According to Ferris Research Inc., a San Francisco-based consulting group, spam will cost US companies more than US\$10 billion this year.
- If current trends continue it is estimated that by 2005 the average user will receive 1600 spam messages per day compared to 40 messages per day in 1999.

## APPROPRIATE USE OF OFFICIAL ELECTRONIC MAIL

It is important to begin with the realities of e-mail. In the previous section we warned that misusing e-mail could have serious consequences both for the organisation and the individual concerned.

Press reports frequently appear of cases where e-mail was used to harass individuals or to disclose personal and confidential information. Many of these cases end up in a court of law or with the dismissal of the individual concerned.



The anti-trust case against Microsoft was triggered by an internal e-mail sent by Bill Gates spelling out Microsoft's strategy in the "Browser War" against Netscape. The Department of Justice found sufficient grounds for an anti-trust case in this e-mail. This case should serve as a warning to companies and organisations alike about the prospective legal consequences of e-mail communication.

Once a message has been sent, there is no UNSEND function. In addition, many copies of the message will remain in existence: on the sender's personal computer, on the organisation's servers and related data backups, on the Internet service provider (ISP) servers, and the same in reverse order at the recipient's end. Furthermore, this does not take into account any additional copies that may have been created, circulated or forwarded by either party.

Given that using e-mail for official purposes is now a reality, the archival and legal status of e-mail messages has become an important topic for organisations. Electronic records management will become a formal discipline in many organisations.

One of the authors of this booklet, intrigued by many of the messages he received which could have benefited from an UNSEND function, created two folders, called Stupidgrams and Nastygrams, to collect them. Over a period of several years numerous examples of misuse were collected, which have supported the research on which this booklet is based. However, none of these e-mails will ever be published or disseminated to other parties.

An unencrypted e-mail message can be considered the equivalent of a machine-readable postcard – it could be intercepted and read by any number of people – including systems and network administrators as

well as hackers and industrial spies. The contents of an unencrypted message can also easily be modified.



#### Machine readable postcards in the diplomatic world

In early 2002 a suspected hacker intercepted an e-mail message sent by the EU representative in Ankara and leaked it to the press. The content of this message could have, at that time, seriously worsened the already tense relations between the EU and Turkey. The EU demanded action from the Turkish authorities in order to protect the correspondence of its representative. Is this obligation of a host country, as set out in the Vienna Convention on Diplomatic Relations, likely to change in the Information Age?

If malicious code infects your e-mail directory - a common way that such code distributes itself - e-mails containing copies of the code will be sent to all of the individuals in your directory and will appear to come from you. If you are unlucky, the messages could also contain a subject line such as “I Love You” or “Approved” as happened with two e-mail worms in the year 2000.

E-mail remains the most powerful mechanism for the distribution of malicious code. In August 2003, the Sobig.F worm affected a considerable number of the world’s computers. The enormous volume of spurious e-mail caused many corporate e-mail systems to be shut down despite the concentrated efforts of information security experts and law enforcement agencies around the world to contain its spread.



#### When using e-mail it is wise to assume all of the following:

- Every e-mail message you send containing your employer’s domain name is the property of your employer.
- Your employer has the right to monitor your usage of electronic mail, access your account and read any messages that you send or receive, even if he or she does not have a published and acknowledged policy concerning the use, misuse and abuse of e-mail.
- All the e-mail messages sent from and received at your employer’s domain are stored on a server and regularly backed up. These backups may be kept for several years and searched if circumstances should warrant it.
- It may be necessary that your official e-mail account be accessed by others (for example in the case of your prolonged absence or in an emergency).

Many organisations and companies have developed fairly detailed policies on all the matters under discussion in this booklet. However, many have not, so a brief discussion of policies is appropriate at this stage.

## Policies

Policies are formal statements of how an organisation manages specific activities. In the case of e-mail and Internet access they cover both appropriate use and security issues.

A well designed and implemented set of policies should have five components:

1. Scope
2. Documentation
3. Dissemination
4. Maintenance
5. Compliance

The first, *scope*, lists all the topics and activities covered by the policies. The typical scope of appropriate use policies would include the following:

- acceptable personal use of corporate resources;
- e-mail policies for corporate and personal use;
- system and resource access;
- physical access and remote access;
- use of encryption;
- software installation;
- mobile communications and computing;
- database administration;
- employers' monitoring rights;
- employee background checks (before and during employment).

The second, *documentation*, describes how these policies are structured and fashioned. Today it can be expected that these policies are an integral part of the employee manual and available on the corporate intranet.

Any amendment or addition to a policy must be included in all versions of the policy documentation, both paper and electronic. A formal method of version control would also be part of the documentation.



The third component, *dissemination*, is the process of ensuring that employees are properly informed on a need-to-know basis. This includes permanent staff as well as temporary workers and other individuals who need access to systems and facilities.

The dissemination process should be good enough to prevent use of the excuse “nobody told me”. Normal practice involves requiring all employees with access to systems and facilities to sign an acknowledgment form, kept by the personnel department, to indicate that: 1) they have received and read the policies; 2) they agree to abide by them; and 3) they accept that non-compliance with the policies may lead to disciplinary action against them.

The fourth component, *maintenance*, recognises that cyberspace is a rapidly changing environment and that policies need to reflect this fact as well as the experiences gained with older versions of these policies.

Finally, the fifth component, *compliance*, is critical as it defines what happens when the policies are not followed and when organisational problems arise as a result. Policies that are not accompanied by effective compliance measures are as good as useless.

## GOOD PRACTICES TO FOLLOW

The following sections suggest several useful e-mail practices.

### 1. E-MAIL OR SNAIL MAIL?

There is no single correct answer to what is the most appropriate communication method. Choice of method is influenced by many factors including:

- the relationship between the communicating parties;
- the sensitivity of the matter being discussed;
- the urgency of the communication;
- whether a need exists for a formal record of the communication.

In many cases all four points have to be factored in, leading to a decision to use several modes of communication. For example, you could send an e-mail to make an appointment for a phone call (to

avoid playing “tag”), follow this by telephoning to discuss the matter at hand, and finally sending a formal letter (or another e-mail) to document the outcome. In other cases the sequence may be reversed – you might phone to provide the context to an e-mail message that will follow, and perhaps send a formal letter as confirmation.

Electronic mail should not be used to replace other forms of communication, but should instead complement them.

Before deciding to write an e-mail, you should be aware of the features of a formal letter:

- letterhead and signature;
- greater thought and editorial care;
- possibility of archiving with other important documents;
- difficulty in copying and forwarding.

In some cases a formal letter sent as an attachment may be acceptable if confidentiality is not a great concern.

## 2. WHY AM I WRITING THIS E-MAIL?

Over the years, the authors have seen many e-mails which did not appear to have been written with a clear purpose or idea.

Here are some useful questions you can ask yourself before you start writing:

- Is the purpose of the message to inform the recipient about something?
- Is this “something” good news or bad news?
- Will this “something” need some action from the recipient - and if so, how soon?

Or is the purpose of the message to:

- ask a specific question?
- ask for an opinion – and is the request formal or informal?
- arrange a meeting or a date and time for a phone call?
- discuss purchases or contracts?
- share your views on a complex subject?

If the purpose for writing a message is not clear, is writing it really necessary?

Clearly, each context may require its own approach. Also, every approach will need to reflect the relationship between the sender and the recipient. Relationships may range from ones between total strangers to ones between individuals who have worked together for many years.

In the case of communicating with a total stranger, it is unwise to assume that the context of the communication will be obvious to him or her, while in the case of communicating with individuals you know well, many assumptions and details will not need to be explicitly spelled out.



#### A Lesson from Diplomatic History:

Greater communication does not necessarily lead to greater understanding and less conflict. Many historians attribute the outbreak of the First World War to a failure of diplomacy. A detailed analysis shows that prior to the outbreak of the First World War the telegraph replaced regular summit meetings of the European leaders as the foremost diplomatic instrument. Such regular high-level summits were the cornerstone of the Concert of Europe security system, established at the Congress of Vienna in 1814, providing a venue for solving problems and disputes. Although the telegraph was a great technological innovation, it did not automatically lead to diplomatic progress. Instead of meeting each other face to face, heads of state started exchanging telegraph messages. This brought about more confusion than understanding and contributed considerably to the outbreak of the First World War.

### 3. GOOD RULES FOR COMPOSITION

Most of the techniques used to render communications more effective involve a combination of style, consistency and common sense.

#### *The subject line*

The subject line should be used to briefly and clearly indicate the context of the message to the recipient. Most e-mail software packages notify the recipient that a message has arrived by showing the sender's name and the subject line. Many of them can also show you the first few lines of the message.

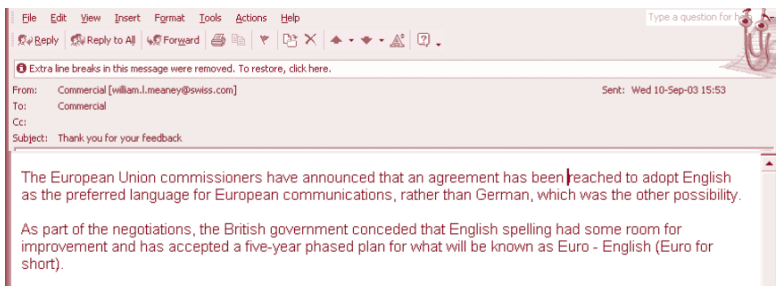
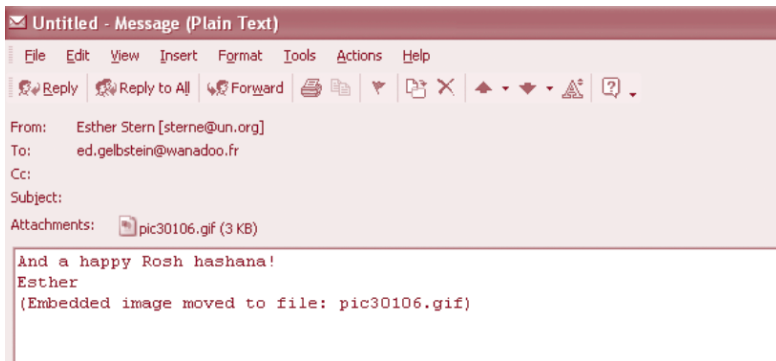
Since most e-mail users receive many e-mail messages during the day you should always try to construct subject lines that clearly convey both the subject of the message (which should also indicate its importance) and its urgency.

Of course labelling all messages “Urgent” when they are not will greatly reduce your credibility as the sender. Here are a few examples of *good* subject lines:

- Meeting 17 February: change of time
- Need your comments on the minutes by tomorrow
- Monthly performance report attached

And here are a few examples of *bad* subject lines (all real):

- Hello!
- fwd fwd fwd: airline jokes
- (no subject)



### *Message length*

A typical e-mail user receives somewhere between 20 and 100 e-mails a day – if he or she spends just one minute on each, this could mean nearly two hours simply going through e-mail.

E-mail messages should be short and should focus on just one subject. Ideally they should not exceed 20 lines of text (one full screen). Anything longer should be sent as an attachment instead. Attachments are discussed in a later section of this booklet.

### *Message style*

The composition of an e-mail should be business-like for all official matters. In official e-mail, your address “john.doe@xxxx.org” is the equivalent of your organisation’s letterhead. The message should read like a memorandum and not a holiday postcard, even though the medium accepts informality.

Be careful with the use of irony, jargon, humour, Internet language and emoticons. Not everyone likes them and you would not normally use them in a formal letter that is printed and mailed. Also bear in mind that the recipient may decide to forward your message to others.

Typographical errors should be avoided to the same degree as they are in printed correspondence. In official exchanges they demonstrate carelessness and a lack of respect for the recipient. The text should employ uppercase and lowercase in the same way as formal printed correspondence.

### *Netiquette basics*

Like all other forms of etiquette, netiquette is the way you show consideration for another individual. The most common rules of netiquette are:

- Check your e-mail at least once a day and try to respond to messages quickly. If you cannot respond quickly at least acknowledge receipt and indicate when you will be able to deal with the matter.

- Do not forward private e-mail without the permission of the original sender.
- Do not create or forward chain e-mail letters.
- Do not spam (spam is the process of sending the same message to hundreds or thousands of e-mail addresses for any number of reasons).
- Do not use ALL CAPITALS in your text. This indicates that you are shouting.
- Be careful when using “cc:” and “bcc:” (discussed further below).

*How to fill in the “to:”, “cc:” and “bcc:” fields: To forward or not to forward?*

In official correspondence, the use of carbon copies may be required in order to respect a particular organisation’s practices, its management style and hierarchy as well as its internal politics. Always remember that any copies will add to the already large volume of correspondence that organisations generate and that purposeless copying will only reflect poorly on the sender.

We recommend you not use blind carbon copies (bcc’s) and that you forward the message to any interested party separately from the original distribution list.

Forwarding an e-mail to another individual is a better practice than sending them a bcc. However, forwarding implies considerable trust in the recipient, as the sender has no control over how much further a particular message will circulate and the degree to which such circulation could come back to haunt him or her.

Using a bcc may be justified if a message or an attachment needs to be distributed to a group of recipients and you desire those recipients to remain unknown to each other.

*Auto-forward and auto-reply: two useful out-of-office e-mail features*

Many e-mail packages allow the user to set up a number of functions. The two most relevant to this discussion are:

- auto-forward: the automatic forwarding of messages to another individual or address (for example when a long period of absence without access to e-mail has been planned, such as a holiday in a remote place or a stay in a hospital); and
- auto-reply: an automatic reply to all incoming messages indicating that the recipient is absent from the office or otherwise unable to reply at this time.

Both of these are useful features. The advantage of automatic forwarding is that it enables a colleague or assistant to deal with the matter at hand in your place, if need be.

The automatic out-of-office reply is less helpful because it basically informs the sender that the matter contained in his or her e-mail will not be dealt with for some time. It is a good idea to add to your auto-reply message the name and e-mail address (or telephone number) of an individual who can assist with urgent matters before your return.

### *Mailing lists*

Most e-mail packages allow the creation of e-mail lists, containing the names and addresses of individuals who operate together as a team and who should therefore all receive the same messages.

While this is a very useful feature, it does not really lend itself to a moderated discussion. The “Reply to All” function generates an amount of traffic that quickly becomes unmanageable when the number of individuals in the list exceeds five or six and it should, therefore, be used thoughtfully and sparingly.



Some e-mail packages allow the creation of lists of “undisclosed recipients”. If they do not, the use of bcc can overcome this limitation.

If frequent group discussions by electronic means are necessary, for example when team members are in different geographical locations, it is better to invest in one or more of the tools designed for this specific purpose, ranging from simple bulletin board systems to more sophisticated products such as listservs, whiteboards and team support tools.

### *Attachments*

Any content in electronic form (document, image, audio/video file) can be sent as an attachment to an e-mail message. However, you should take a number of considerations into account when doing so.

**Format:** The recipient must have the necessary software to be able to read the attachment (or in technical terms, to “open the file”). Additionally, such software may need to be of the same type and version number as the one used to create the document if the recipient needs to edit or change it in any way. Alternatively, if all that is required is for the recipient to see and/or make use of the attachment as it is, a simple image viewer may suffice, such as the many available free of charge on the Internet.

You can read a discussion on file formats in section 5 of another booklet in this series entitled *Internet Basics*.

For text documents which the recipient should NOT be able to modify, we recommend you use a product that can convert files into the portable document format (pdf). Adobe Acrobat is one such product and more details about it as well as the Adobe Reader can be obtained free of charge from <http://www.adobe.com>.

**Size:** Large attachments may be inconvenient for a recipient who has a dial-up connection typically operating between 33 and 48 kilobits per second (the nominal speed for a dial-up connection is 56 kbps) and whose Internet charges are calculated on the basis of time spent online. Anything larger than two megabytes should not be sent to such a user without prior warning and agreement.

Free e-mail service providers such as Yahoo! and Hotmail place restrictions on the size of attachments you can send and receive. Most Internet service providers also have limitations on the total volume of e-mail you can receive.

### *Encryption and digital signatures*

The use of encryption and/or digital signatures strengthens the integrity of a message and reduces the risk of another party being able to repudiate it.



Both of these are good mechanisms for improving the confidentiality of electronic communications. Official messages should be encrypted only if this is the policy of the organisation.

A situation where every individual uses his or her own choice of encryption software and digital signatures with their concomitant private and public keys can only be described as anarchic and must be avoided.

Information about encryption practices and products is highly sensitive and should be treated accordingly.

### *Filing, backing up, archiving and managing e-mail messages*

New policies on the indexing and filing structures of electronic mail are constantly being developed. Without such policies the functioning of the organisation's registry would in effect be delegated to the owners of each individual e-mail account.

It is prudent to create an electronic filing system for e-mail that has a rational structure appropriate for the organisation where it is to be used. The folders in this filing system should also be named logically.

Here are some important questions to consider:

- Are all e-mail folders included in the regular data backups of the organisation's servers?
- What steps does the organisation take to manage the voluminous storage of e-mail (for example, is it periodically transferred to an electronic archive)?
- Who has the right to delete electronic mail messages - and under what circumstances?

## **4. DISTINCTLY BAD IDEAS**

Having discussed a set of good practices, it is now time to mention a few that would detract from your image and could, in a worst case scenario, have serious consequences for your career.

*Using your official account for personal correspondence unless authorised to do so by your employer.*

*Sending poorly composed messages* not only creates a poor impression of you as an individual but also, in official correspondence, risks embarrassing your employer.



*Including poorly thought out, offensive or tasteless content in your correspondence* could lead to legal action against you and/or your dismissal. Even if you are lucky and avoid such serious consequences, someone might choose to circulate your poorly composed or thought out messages to a wider audience, which could be potentially embarrassing for you. Instances where personal and highly indiscreet messages about someone were forwarded to many individuals and ultimately leaked to the press have, unfortunately, occurred. The contents under discussion here include attachments.

*Forwarding e-mails that should not be forwarded* may be an indication of poor judgement on your part which, if discovered, could become a career limiting action.

*Granting access to your official e-mail account to a third party.* This would constitute a serious breach of information security as you would be granting access to facilities behind the organisation's security perimeter and consequently invalidating all provisions set



Hackers with malicious intent frequently use the ruse known as "social engineering" to gain access to an organisation's computer systems. This involves various techniques devised to take advantage of most individuals' natural inclination to be polite and helpful.

For example, a well dressed, very polite visitor asks an employee to use their computer for a couple of minutes, to urgently check his e-mail. Most individuals, trying to be helpful, will grant such a request. At this point, the stranger will have circumvented all the firewalls and gained access to the network, a legitimate user logon and, if knowledgeable, can cause havoc in less than a minute.

Another example is when an individual arrives at the reception desk of an organisation claiming to be a maintenance engineer who has to deliver a spare part to the computer room. If he actually looks the part and behaves politely, there is a good chance that access will be granted. Needless to say, this would be a very bad idea.

In the case of a trusted friend, it may be OK to let him or her use your computer. But even a friend may wish to play a practical joke on you and write an inappropriate e-mail from your account to someone else.

up to maintain information security. It is better to have a separate computer with very limited functions, essentially access to the Internet, and point third parties to this machine.

## APPROPRIATE USE OF YOUR PERSONAL E-MAIL ACCOUNT

The good practices we discussed for official e-mail use apply equally well to your personal e-mail accounts.

There are two kinds of personal accounts:

- Those provided by an Internet Service Provider (ISP), which are designed to be used with an e-mail package. Most of these can also be accessed through a browser from any location with an Internet connection.
- Those provided by a number of Internet companies, which are designed to work with a browser and can be accessed from any location with an Internet connection. At present these are still free of charge.

Services such as Yahoo! mail and Hotmail are quite satisfactory for most individuals but lack some of the functionality of ISP e-mail packages and can be considerably slower because actions such as “Delete” or “Move to Folder” cannot be performed locally on your machine. Web-based accounts also appear to attract considerably more spam and junk mail than those of ISPs.



Never forget that certain jobs come with responsibilities that extend beyond traditional office hours and impose a code of conduct on employees covering what they can publish, say to the press (even anonymously) or express in public.

This means that the use of personal e-mail accounts, participation in chat rooms, creation of personal websites and other Internet related activities must always be commensurate with the exercise of your official functions.





SECTION



2

# Accessing the Internet (and other systems)

*The Internet is so big, so powerful and pointless that for  
some people it is a complete substitute for life.*

*Andrew Brown (author and journalist)*



## APPROPRIATE USE OF INTERNET ACCESS IN THE WORKPLACE

**T**he World Wide Web, FTP, user groups, chat rooms and blogs are all wonderful items and can be of great use and benefit. However, they are also all potential time consuming devices that, if not used appropriately, risk wasting not only your own time but also that of your employer as well as the resources (computers, networks, software, bandwidth and security administrators) of the organisation where you are employed.

A formal policy should define the rules of conduct for access to the Internet by employees. The tools to monitor employees' activities are easily available and in extensive use. They can produce very specific reports listing, for example, the "Top Ten" consumers of online time or the "Top Ten" websites visited. These tools can also produce ad hoc reports to identify particular types of "inappropriate" websites that employees visit, such as music download and online gaming sites.

Even if your organisation does not have a formal policy on Internet access, using a measure of common sense in that area is advisable.

Perhaps the most useful thing you can do is learn about how to make the best use of the various features of the Internet, in particular:

- searching for and finding information on the World Wide Web;
- assessing the quality and suitability of any information found;
- knowing the essentials of information security and how to apply them systematically;
- using the functionality of the browser to best advantage: managing cookies and favourites (also known as bookmarks);
- downloading documents and filing them on your computer.

For more details you can consult other booklets in this collection, in particular: *Finding Information in Cyberspace*, *Internet Basics*, *Appropriate Use*, *Good Hygiene for Data and Personal Computers* and *Information Security and Organisations*.

## EXAMPLES OF APPROPRIATE OFFICIAL USE

The list below is not comprehensive:

### *Conducting work related research*

This is the most likely use of the Internet by a knowledge worker. Over 20 million websites are available. Most publishers also provide access to their publications through the World Wide Web, in many cases through a subscription service.

It is important to respect the copyright restrictions of any information found. These vary from site to site and some sites require payment for the right to use the material.

### *Online learning*

A vast choice of courses and training is now available online. Online learning is an activity that demands considerable time and effort and should be undertaken only with the explicit approval of the organisation where you work, particularly if this is to take place during working hours.

More information on this topic can be found in the booklet *Online Learning: Opportunities and Choices*.

### *Electronic meetings*

These can occur in a variety of forms – not including e-mail discussions, which have already been covered in this booklet. The most common forms are:

#### Chat rooms (including private ones)

These have the disadvantage of requiring all the participants to be online at the same time. As a business tool they are probably the least useful.

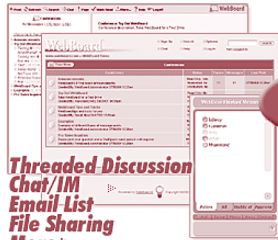
#### Collaboration tools

These have progressed a great deal since the days of bulletin boards and today many commercial products are available.



# WebBoard

## Conferencing 6.1



Get both  
and save  
15%

## Meeting 2.0



### Product Info

[WebBoard Meeting](#)[Basic Edition](#)[Standard Edition](#)[Education Edition](#)[Premium Edition](#)[Blackboard Edition](#)[Product Tour](#)[New Features](#)[Features List](#)[System Requirements](#)

### Support

[Online Demo](#)[Showcase](#)[Downloads](#)

### Purchase

With 30-day  
Money Back  
Guarantee



### Schedule a Live Demo

"Your product stood out from the other vendors not only in product vision and feature-set but also in quality of sales and technical support staff."

- Robert Maxwell, CTO, Triton Systems Holding LLC



### Download a Trial Version

The above web page illustrates one of the many products designed for this purpose.

Many real-time collaboration products are available that support the interaction of two or more individuals over a network. The interaction can be either asynchronous or mimic real meetings with audio interaction between the participants.

Tools focused primarily on general business interaction include: Microsoft's NetMeeting, Lotus' Sametime, Oracle's Collaboration Suite, Latitude's Meeting Place as well as other products from Genesys and Raindance.

Other tools such as Centra, WebEx, PlaceWare and Interwise offer solutions that support both general business activities and services needed for online learning.

### Online Negotiations

The Internet can be a most effective negotiating tool. It provides all the essential elements for conducting negotiations – the means for: ex-

changing messages, drafting text online, and accessing information. The following advantages of online negotiations over face-to-face ones can be highlighted:

- **Decreased emotion:** Internet-based communication is less emotionally charged than face-to-face communication. The distance and space offered by Internet communication, allowing for reduced 'emotional noise' may in some cases actually be an advantage, when emotions might otherwise disrupt proceedings. In Dayton and Rambouillet, proximity negotiations (without direct contact) were used to prevent the delegations from coming into direct contact with each other.
- **Easier drafting of and focusing on the text:** Much of the time and energy spent in the negotiating process involves the drafting of agreements and discussing their details. In negotiations that are strongly focused on producing a final text, much of the preliminary work and many of the details can be completed over the Internet. Through the use of hypertext tools with group editing functions, the negotiating parties can specifically concentrate on the text of the agreement.
- **Managing more meetings with fewer resources:** While the number of international meetings (committees, technical meetings, regime secretariats, etc.) is currently increasing, in many countries the financial and human resources available for such meetings is decreasing. By using the Internet such countries will be able participate without physically sending their experts abroad. Participation via the Internet would reduce expenses, improve diplomatic processes and ensure global participation in decision-making, which is essential for the effective implementation of various international agreements and decisions.



DiploFoundation has been conducting online negotiation exercises for the last six years as part of its postgraduate diploma course. Experience from these exercises and research has helped in the development of the Online Negotiation Assistant (see screen capture below), which consists of various drafting and negotiating tools (e.g. hypertext, voting, knowledge management, as well as language and procedural assistants).

## DISTINCTLY BAD IDEAS

As in the case of e-mail, there are a number of activities that no employer will consider appropriate use of the organisation's resources unless you perform them outside working hours and have formal permission to do so. Activities such as checking the news or your personal financial matters or perhaps downloading a few large files for copying onto a CD-ROM and taking home are usually tolerated, but not much beyond this.



The dividing lines between appropriate use, misuse and abuse are not clearly drawn. Therefore, common sense must prevail. You should not indulge in websites dealing with money laundering, gambling, pornography and so on from an employer's premises or from home using an employer's equipment and/or Internet access services.

Any form of hacking, spoofing, hacktivism or disclosure of confidential information may be considered sufficient cause for immediate dismissal or, if you are lucky, an indirect request for a posting to one of the world's most remote locations!



However careful you think you are being, for example, by deleting cookies, temporary and cache files, etc. all your Internet activities will still leave "footprints" in monitoring systems, proxy servers and many other systems that can be discovered through digital forensics.

## APPROPRIATE USE OF INTERNET ACCESS IN THE HOME

In principle, your home is your castle and you should be able to do as you please there. Right? Well, in fact, maybe not. In the diplomatic world the phrase "activities incompatible with his/her status" is regularly used to send a diplomat back home. There are many other examples involving police officers, university professors, and other professionals whose activities on the World Wide Web from their homes were made public and judged to be unacceptable by their employers.

In the specific case where the equipment and software used at home belong to the employer, security issues must also be considered. In particular, the user may inadvertently download malicious code, or other family members may decide to engage in hacking activities, increasing the risk that the use of a privileged connection to the organisation's systems will compromise the security of the whole network.

Even if you use your own equipment and software and have your own account with an ISP, certain actions exist that can only be described as distinctly bad ideas:

- acting in any way that may be incompatible with your work responsibilities;
- installing unlicensed (pirated) versions of software;
- illegally downloading copyrighted material from websites infringing copyright legislation;
- expressing controversial views in chat rooms (even anonymously);
- performing any form of hacking, spoofing or hacktivism.

## PROHIBITED BEHAVIOUR

Always assume that the following actions are career limiting moves, regardless of whether you have been specifically warned, or whether you use the Internet to perform them.

- *Illegal Access.* Intentionally attempting to access any computer system or facility on which you are not an authorised user.
- *Illegal Interception.* Intentionally intercepting non-public data transmissions.
- *Systems and Data Interference.* Intentionally hindering the functioning of a computer system by interfering with data.
- *Forgery.* Intentionally falsifying data that results in inauthentic data being passed off as authentic.
- *Fraud.* Intentionally causing property loss by interfering with the proper functioning of a computer system with the dishonest intent of procuring economic benefit for yourself.
- *Pornography.* Producing and distributing pornography through electronic means. Procuring pornography in electronic form for yourself or another individual. Possessing pornographic material in electronic form.
- *Abuse of Rights.* Creating, transmitting or distributing threatening, abusive, harassing, defamatory, libellous, deceptive or fraudulent information, or information that is invasive to an individual's privacy.





SECTION



3

Privacy, freedom of  
speech, human  
rights and other  
issues concerning  
the individual

*Liberty means responsibility.  
That is why most men dread it.*

*George Bernard Shaw*





## INTRODUCTION

We know that anybody can become a publisher on the World Wide Web. It is possible to create a website with relative ease and without any editorial or publishing controls, peer reviews or any of the other processes that are considered common practice in the publishing industry.

This may be one of the reasons why out of the over 42 million websites registered in mid-2003, so many are considered to have doubtful or downright offensive content.

Sites with doubtful content include those of quacks and charlatans who offer bizarre explanations for world problems or “magicures” for serious illnesses.

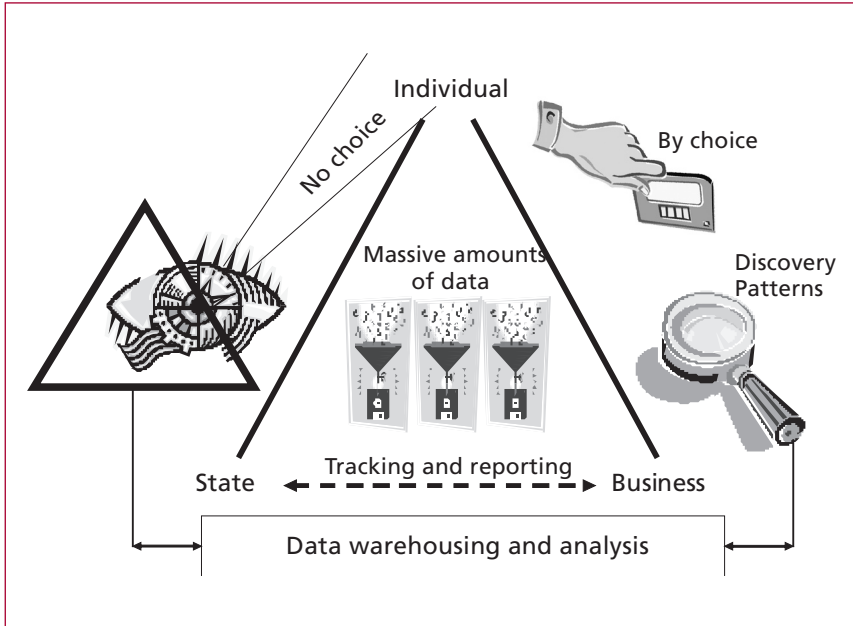
Sites with offensive content include those that wage wars of words on topics such as hate and racism as well as those aimed at causing social upheaval by providing instructions on how to construct bombs or create computer viruses.

All this implies that there is unlimited democracy and freedom of speech on the Web. On the other hand, the preceding sections make it clear that even in the most democratic countries, this is not quite the case since individuals employed by governments, companies, non-profit and international organisations have to accept, as part of their contracts of employment, certain limits to what they can do both at work and even at home.

Legislation is gradually emerging to address the need to protect the most vulnerable members of society – for example children – from unsuitable content and also from fraudulent schemes and unsolicited e-mail such as spam.

## COMPLEX SOCIAL INFORMATION FLOWS

This section discusses the relationships and information flows that raise privacy issues between three sets of players: the State, represented by government departments and related agencies, the business community and individuals.



### INDIVIDUALS AND THE STATE

Privacy, interpreted as the “right to be left alone,” is assumed to be a fundamental right of modern society. Since the publication of George Orwell’s *1984*, the threat to privacy has often been publicised with the phrase “Big Brother is Watching You”, where “Big Brother” is assumed to mean the government.

For many years, many States have had the constitutional right to oversee the territories and populations within their national boundaries. Information gathering has always been an essential tool in exercising this oversight as demonstrated by the oldest written records, most of which deal with State functions.

Information technologies have provided powerful tools for gathering and analysing enormous amounts of information. All government departments use them (tax, social security, health, property, criminal records) as do companies licensed by governments to provide essential services (electricity, water, telecommunications).

All of this information is collected with the implicit but involuntary consent of the citizenry as there is no possibility for a citizen to opt out of these schemes, short of emigrating.

Technologies such as data warehousing are used to aggregate and relate data from many different systems (for example taxation, housing records, and car ownership) in order to conduct sophisticated analyses that search for inconsistencies, unusual patterns and other discoveries that could have a dramatic impact on society. In most cases such analyses remain within the scope of the Universal Declaration of Human Rights.

Terrorism, espionage and other activities against the State have given rise to increased surveillance of suspected individuals (be they nationals of the State or not) in order to achieve an appropriate level of national security. The technologies used to conduct such surveillance have been around for some time, starting with telephone line taps and video cameras, and today extending to the tracking of mobile phone conversations and the interception of potentially subversive electronic mail messages.

As previous sections have shown, such monitoring can also be conducted by an employer with or without involvement by the State.

Civil liberties campaigners see national security concerns as leading to an ever greater invasion of personal privacy. A few years ago considerable public debate ensued over a proposal to equip personal computers with a special chip (the so-called “Clipper” chip) to give each computer a unique identity, which coincidentally could have also been used to provide a back-door for government surveillance.

The Clipper chip battle was won by the libertarians, but today the pendulum is swinging back towards strengthened national security. The US “Patriot Act” – and comparable legislation in other countries – introduced a framework for the stricter control of electronic communications, including a provision for “lawful interception”. The concept of lawful interception to support the gathering of information is also included in the Council of Europe’s Convention on Cybercrime of 2001 (Articles 20 and 21).

We must not forget that as technology evolves it provides better tools to support surveillance. For example, cell phone operators have the abili-

ty to track the position of a caller down to a few tens of meters. The anticipated next generations of cell phones may have Global Positioning by Satellite (GPS) capabilities and help to increase the accuracy of this tracking.

Most of the legal framework on privacy is based on the “Guidelines for Privacy Protection” developed and published in 1980 by the Organisation for Economic Cooperation and Development (OECD) – (<http://www.oecd.org>).

These guidelines were not legally binding documents but they did have a major influence on Western European legislation and practices, which resulted in the drafting of several legally binding documents, including the Council of Europe Conventions, European Union Directives, and much national legislation.



#### The Safe Harbour Agreement

**Background:** The EU’s “Data Protection Directive” which entered into force in 1995 prohibits the export of personal data to countries which do not have adequate privacy protection. The USA was among those countries because it leaves it to the business sector to safeguard privacy protection. This led to a number of problems because many US companies (e.g. Microsoft, Amazon, etc.) had computer systems that integrated huge amounts of data about their clients across the world including the EU.

**Positions:** The EU demanded a change in US legislation on privacy protection. As this would have required significant legal changes, it was not acceptable to the US.

**Solution:** The way out of this negotiating deadlock was found in the “Safe Harbour Agreement” which specifies that US companies handling EU citizens’ data could agree to voluntarily observe the EU’s privacy protection requirements. Once a company signed, the formal enforcement mechanisms agreed upon between the EU and the US would apply.

**Comment:** The conflicting views on e-privacy protection between the EU and the US confirmed that increasing interdependence created by electronic commerce could challenge some basic principles embedded in the respective social and cultural histories of different countries. Globalisation will cause this issue to reappear as other societies begin to participate. The “Safe Harbour Agreement” should be seen as a valuable precedent.

### *The protection of the most vulnerable members of society*

If surveillance represents one side of the coin, the protection of vulnerable members of society represents the other.

Cyberspace, and in particular the Internet, enables various individuals and groups to publish and disseminate information as well as to participate in wide ranging debates. The misuse of these facilities (see also the booklet in this series entitled *Hactivism, Cyber-terrorism and Cyberwar*) by disseminating content which is subversive or against the national and global values of civil society, presents a major challenge: what are the correct mechanisms to achieve the proper balance between what is right and proper and what is seen to be against the public interest?

Here are some examples of content that could be seen to be against the public interest and values:

- Libel and defamation: This is an area where legislation is well developed and can be applied without modification to the Internet.
- Hate speech (advocating murder, genocide, racism, torture, and similar actions): This is a controversial topic simply because of the differences that exist among countries as to what constitutes “hate speech”.
- Subversive organisations (including organised crime and terrorism).
- Child pornography (either the content distributed through the Internet or the production and ownership of such material): The subject of adult pornography that could be accessed by children is more of a grey area.

National legislation is basically designed to apply to all citizens equally and this is one of the cornerstones of modern legal systems. Applying this criterion to the Internet can cause difficulties, however.

For example, the US Congress proposed the Communications Decency Act (CDA) in order to protect children from pornography on the Internet. However, the US Supreme Court reacted by indicating that, “CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to each other.”

In Europe, some cases relating to the control of Internet content have arisen, most notably the ruling made by a French court in the year 2000 against Yahoo! for hosting the sale of Nazi memorabilia on its US website. The court requested Yahoo! to deny access to this material to users accessing its website from France. This case opened many dilemmas in the field of content control. One of the obvious conclusions is that a global regime for content control would be the only viable option as national authorities do not have jurisdiction over websites hosted in other countries.

### **Businesses, e-commerce and individuals**

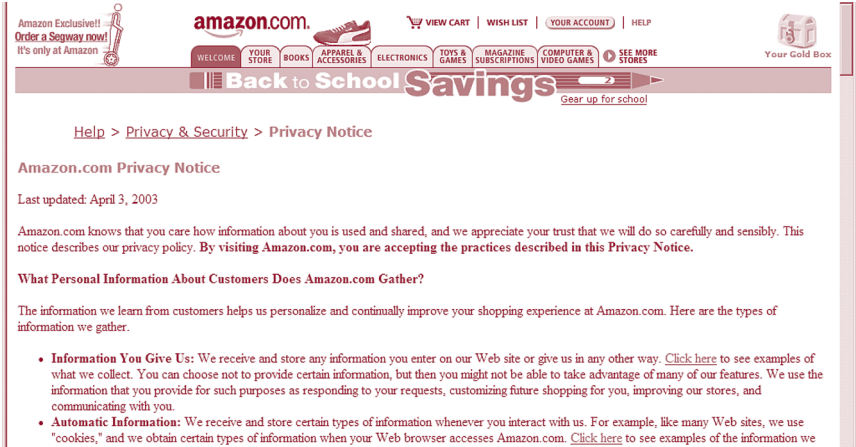
A different kind of “surveillance” exists between individuals and businesses. This is very much the case in electronic commerce.

Here, millions of individuals willingly disclose a considerable amount of personal information to business organisations: credit card numbers, names and addresses, as well as other information which, if used against them could have serious consequences, such as fraud or identity theft.

The legal safeguards for individuals vary in different parts of the world. For example, the European Union (and previously several of its member states) has developed data protection legislation (in particular the 1995 “European Directive on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data”). This directive clearly specifies the limits to which information about individuals can be kept in electronic form, and what constitutes use, misuse and abuse, as well as the situations in which the provisions of the directive do not apply.

Other countries, for example the US, do not have equivalent laws but instead, leave it to up to businesses to decide about the extent of privacy protection they provide and to advise their customers accordingly. Virtually all serious electronic commerce operators have clearly stated privacy policies.

The web page below presents the privacy notice of one of the major business-to-consumer electronic commerce sites.



Amazon Exclusive!!  
Order a Segway now!  
It's only at Amazon

amazon.com

WELCOME | YOUR STORE | BOOKS | APPAREL & ACCESSORIES | ELECTRONICS | TOYS & GAMES | MAGAZINE SUBSCRIPTIONS | COMPUTER & VIDEO GAMES | SEE MORE STORES

VIEW CART | WISH LIST | YOUR ACCOUNT | HELP

Your Gold Box

**Back to School Savings**  
Gear up for school

Help > [Privacy & Security](#) > [Privacy Notice](#)

Amazon.com Privacy Notice

Last updated: April 3, 2003

Amazon.com knows that you care how information about you is used and shared, and we appreciate your trust that we will do so carefully and sensibly. This notice describes our privacy policy. **By visiting Amazon.com, you are accepting the practices described in this Privacy Notice.**

**What Personal Information About Customers Does Amazon.com Gather?**

The information we learn from customers helps us personalize and continually improve your shopping experience at Amazon.com. Here are the types of information we gather.

- **Information You Give Us:** We receive and store any information you enter on our Web site or give us in any other way. [Click here](#) to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future shopping for you, improving our stores, and communicating with you.
- **Automatic Information:** We receive and store certain types of information whenever you interact with us. For example, like many Web sites, we use "cookies," and we obtain certain types of information when your Web browser accesses Amazon.com. [Click here](#) to see examples of the information we

The success and sustainability of electronic commerce, both business-to-consumer and business-to-business, require extensive trust in the businesses' privacy policies and the security measures they employ to protect their clients' confidential information from theft and misuse.

On the other hand, in many countries information about individuals is either part of the public record or can be obtained from accredited as well as from less scrupulous sources for relatively modest sums of money.



James Lee, a spokesperson for the company ChoicePoint (<http://www.choicepoint.net>), which specialises in buying and selling information about individuals, in the context of selling personal information to the US government has been quoted as saying, "Our whole purpose in life is to sell data to make the world a safer place."

Business organisations also exploit data warehousing technologies to gain an insight into the habits and preferences of their clients. Supermarkets that introduce a loyalty card scheme use it to track the buying habits of individuals – what day of the week/time of day they prefer to shop, how much they spend, which products they buy (as the data warehouse is linked to point of sale equipment).

The results of these analyses are subsequently used to create personalised, targeted marketing initiatives for individual households. Where

data protection legislation does not exist or is weak, such information may also be sold to other operators.

### **Government departments and businesses**

Data protection legislation places considerable responsibilities on the corporate and business holders of personal data in electronic form.

Government departments and regulators are also responsible for defining what constitutes unethical and fraudulent business practices. This topic is also of considerable interest to organisations such as the International Chamber of Commerce (website: <http://www.iccwbo.org>).

Many recent developments can provide pointers for the future.

- There is a growing trend towards increasing the responsibilities of Internet Service Providers (ISPs) for the content hosted on their websites.
- The fight against terrorism is increasing the exchange of information about individuals between business operators and government departments.

One example of such exchanges relates to the US Computer Assisted Passenger Pre-Screening (CAPPS) system that requires airlines to provide personal information about passengers to state authorities.

The management of Internet use and other new technologies involves dealing with apparent contradictions and paradoxes. It is not necessarily true that increased national security inevitably leads to reduced personal privacy. The same is true for the balance between protecting the public good and freedom of expression.

Creative and constructive thinking can be used to bring practices outside the zero sum paradigm into reality.

One example of such an approach is the 1999 French national legislation on encryption: The restricted use of encryption was liberalised by allowing individuals to use strong encryption. This step was balanced by the government's agreement to provide more funding for its e-police and security institutions plus requiring individuals to facilitate the decryption of encoded messages if this was ordered by a court of law.



The second example is the “Safe Harbour Agreement”, which was discussed earlier. This agreement provided a win-win arrangement for:

- European citizens, who received the same level of protection regarding the use of their personal information in electronic form as they had in Europe;
- US companies, which could exchange data between Europe and the United States without restrictions;
- The US government, which did not have to modify its existing legislation.



## About the authors

### Stefano Baldi

Stefano Baldi is a career diplomat in the Italian Ministry of Foreign Affairs, Counsellor at the Permanent Mission of Italy to the UN – New York. He has also served at the Permanent Mission of Italy to the International Organisations in Geneva, where he has developed several initiatives for the use of information technologies (IT) in the diplomatic community.

Baldi has an academic background in demography and international social issues. He also lectures on the use of internet for ministries of foreign affairs and missions at DiploFoundation's Postgraduate Diploma Course on Information Technology and Diplomacy. Baldi's most recent research focuses on the impact and future developments of information technology in international affairs.

<http://baldi.diplomacy.edu>

[baldi@diplomacy.edu](mailto:baldi@diplomacy.edu)

### Ed Gelbstein

Eduardo Gelbstein is a Senior Special Fellow of the United Nations Institute for Training and Research (UNITAR) and a contributor to the United Nations Information and Telecommunications (ICT) Task Force and to the preparatory work for the World Summit on the Information Society. He is the former Director of the United Nations International Computing Centre.

In addition to his collaboration with the United Nations, he is a conference speaker and university lecturer reflecting his 40 years experience in the management of information technologies.

He has worked in Argentina, the Netherlands, the UK, Australia and after joining the United Nations in 1993, in Geneva (Switzerland) and New York (USA). He graduated as an electronics engineer from the University of Buenos Aires, Argentina in 1963 and holds a Master's degree from the Netherlands and a PhD from the UK.

[gelbstein@diplomacy.edu](mailto:gelbstein@diplomacy.edu)

### Jovan Kurbalija

Jovan Kurbalija is the founding director of DiploFoundation. He is a former diplomat with a professional and academic background in international law, diplomacy and information technology. Since the late 1980s he has been involved in research on ICT and law. In 1992 he was in charge of establishing the first Unit for IT and Diplomacy at the Mediterranean Academy of Diplomatic Studies in Malta. After more than ten years of successful work in the field of training, research and publishing, in 2003 the Unit evolved into DiploFoundation.

Jovan Kurbalija directs online learning courses on ICT and diplomacy and lectures in academic and training institutions in Switzerland, the United States, Austria, the United Kingdom, the Netherlands, and Malta.

The main areas of his research are: diplomacy and development of the international regime on the Internet, the use of hypertext in diplomacy, online negotiations, and diplomatic law.

[jovank@diplomacy.edu](mailto:jovank@diplomacy.edu)

# NOTES