Crossroads
The ACM Student Magazine

Security, Privacy, and Anonymity

by ***Thomas Wright***

Introduction

The Internet is an evolving communication system and our society is evolving with it. Like many other technological revolutions before, the Internet is influencing our society to the same extent as we are controlling it. It has made communication, information interchange, commerce, and research much easier, cheaper, and faster. In exchange, more and more parts of our lives are taking place in "cyberspace", and this creates new threats to our rights of privacy, security, and anonymity.

"If we accept the (...) view of the Internet as the 'information superhighway', we can view the personal computer as the vehicle that takes us from one location to another [**11**]." We can learn a lot about a person by searching his car, but personal computers are more than just vehicles we travel the net in. They are our digital homes. Not many people would hand their hard drives to strangers. They hold secrets we do not want to share with the world, and even if they do not, most could allow a pretty accurate profiling of their owners personality. Giving someone access to your system is becoming more and more like giving someone access to your home. We all own information we simply do not want to share with the world, therefore an important concept protecting our rights is local system security.

The other side of the story is that it does not take someone breaking in to a system to invade privacy. When communicating via the Internet, we do not know who could be spying because connections can be observed by anyone who has access to any of the points the connection spans. In our usual face-to-face communication, we are used to knowing who is taking part in a discussion within the blink of an eye, registering who is listening and deciding which information we wish to share based on the knowledge we have about any of the people present. But on the Internet we do not know who is present, and even if we do, we usually have little or no information about them.

After shortly discussing the main notions used in this paper, I will discuss problems that arise from the information revolution of the past decade. Section 3 will then take a look at the means of information espionage before Section 4 presents precautions that can be taken to protect privacy. This document is neither an anonymity HowTo, nor an introduction to the technical basics of e-privacy. It focuses on the changing nature of privacy and security in the information age. For further technical and instructive information, please check the references given in the text.

Human Rights in the Information Age

Because of the widespread confusion concerning the main terms this paper deals with, this section will first try to separate the entwined meanings of privacy, security, and anonymity. On this basis I will discover the increasing need for human rights enforcement in the information age and investigate the technological, individual, and societal causes of the dilemma revealed. Finally, I will discuss why our rights can ultimately only be enforced by means of technology and user awareness

Privacy, security, and anonymity are three terms with very similar meanings and are often even used synonymously. This makes it important to identify the significance of each of these three notions. This section will take a look at the differences between their common use and their meanings in the field of computer science.

Security

Security is generally understood as the prevention of spying, attacks, or theft. It means that whatever anyone is planning to do with something that belongs to an individual, it can only be done with the owners explicit approval. The instance being secured can basically be anything, for example, money, life itself, or, as in the case of this paper, any kind of information, such as data on a hard drive, information being

transmitted, or even information being published on the Internet.

Figure 1: The components of security.

In terms of computer science, security has gained a stronger meaning: "One generally-accepted view of information systems security breaks down its goals into the trio of confidentiality, integrity, and availability (...) - CIA [**19**]."

1. **Confidentiality** basically refers to the enclosure of data so it can only be read by an authenticated recipient. In the real world this can mean putting the information in a guarded safe, but when information is transmitted across an open network, this always involves cryptography.
2. **Integrity** is the assurance of the origin and "originality" of information. Originality means correctness in the sense of the author, not ultimate correctness. In other words it means that the original information has not been manipulated.
3. **Availability** is an issue which means the information is accessible when requested, which is of no significance for our discussion.

In the view taken by this paper, it will prove very useful to divide security into local or system security on the one hand, and communication security on the other. Local security is a prerequisite for communication security, because every communication starts or ends on our local machine. If anyone can read the data on your hard drive, you need no longer worry about the data your browser might be sharing with the world (of course it *could* be the browser sharing your hard drive).

Public awareness of data security issues is without doubt far greater than the awareness of privacy or anonymity issues. This is one of the reasons why a stronger focus has been placed upon the importance of privacy and anonymity. Security gains

its great significance as a precondition for privacy and anonymity. After all, if anyone can read your "sent mail" folder, then securing the mail transmission is ultimately useless.

Privacy

Privacy is very hard to define; it is commonly used for anything from the state of being alone or undisturbed, our freedom from interference or public attention, up to the right of anonymity. In terms of law "there are three elements in privacy: secrecy, anonymity, and solitude" [**13**]. Secrecy of communication is a security issue, anonymity is to be discussed separately, and solitude is our right to be "unwatchable" by other people. But while digital privacy involves security as a prerequisite, privacy can also be seen as a part of security. A nice division of the aspects of privacy is given by [**23**]:

1. **Information privacy** or data protection, covering the collection and handling of personal information, such as medical, credit, residential information, but also government records, etc.
2. **Bodily privacy**, the protection against invasive procedures such as genetic tests, drug testing, and cavity searches
3. **Privacy of communication**, which covers the security of mail, telephones, e-mail, and other forms of communication
4. **Territorial privacy** which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance, and ID checks

Bodily privacy and territorial privacy are classical "real world problems" and are therefore beyond the scope of this paper. Privacy of communication is a concern of communication security as it was defined in the former section. Information privacy or data protection however is the remaining concept of privacy not covered otherwise. Its implementation effectively means that we have total control of our personal data. As the enclosure of personal data stored on local systems is again an issue of local system security, the term privacy will be used as the protection of personal data while communicating on the Internet. Privacy therefore always involves the secrecy of our real identity. No matter how much information we wish to share with the world, it must remain the user's decision if this information can be tracked back to his personal identity, real name, or home address.

Anonymity

When discussing anonymity we must distinguish between total anonymity and pseudonymity:

1. **Total anonymity** means that the origin of communication is made totally untraceable, for example an unsigned letter without a return address.
2. **Pseudonymity** is concealing a real identity by the use of an alias. Pseudonyms allow answers without the possibility of linking the origin of communication to a person or link several acts of communication to a single, yet unknown identity. Examples are the usage of nicknames in a chat room or pen names.

Total anonymity is very difficult in the Internet because most of the Internet's infrastructure has to do with identification.

Electronic Rights

The introduction to this paper states that "more and more of our lives is taking place in cyberspace," and although a discussion of this proposition could easily lead in a rather philosophical direction, this aim of this paper cannot be achieved without consideration of the implications made. Therefore I will now take a look at the changing nature of privacy and examine the reasons for these changes.

From a social point of view, the Internet is anonymous, and this has resulted in many discussions about risks the Internet may carry. The lack of "real life interaction" has even been seen as a threat to society itself. However, this social anonymity must not be confused with real anonymity. In cyberspace most people fall for the wrong sensation of being anonymous and are not worried about the possibility of being identified, although public discussions, for example about cookies, have improved the situation. We feel safe in the Internet because anonymity is a natural state. When shopping in the real world nobody asks us for identification. When meeting strangers we do not first assure them of who we are and while identification in the real world usually requires a persons active agreement, in cyberspace we can be identified without knowing about it, although the nature of identification can be different. In addition to an identity represented by a name, home address, social security number, etc., there are many ways of linking actions in the Internet, and this is done by the means of "electronic identities."

Basically the term "identity" describes a collection of information that *uniquely* resembles an instance. Examples of identification can be a name and home address identifying a postal reachability, DNA uniquely resembling a physical body, or an account number resembling a bank account. What we would most probably call our own personal identity is the sum of such information referring to *our* name and address, *our* account number, and *our* DNA. When linked to one another, they multiply the possibility of identifying a person, and this linking of personal information is exactly what many businesses on the Internet do. An electronic identity can theoretically link a persons activities on any site anywhere on the web to one another. Once a user is identified, businesses can start to collect all sorts of information, for example, his interests and his financial situation. The primary means of user identification and the collection of such data will be discussed later.

Information has become an asset, a currency, sometimes even power. For many businesses, personal data is the only product deliverable. "People have become targets of surveillance at just about every turn of their lives. In transactions with retailers, mail order companies, medical care givers, daycare providers, and even beauty parlors, information about them is collected, stored, analyzed, and sometimes shared. Their presence on the planet, their notable features, and all their momentous milestones are dutifully recorded [**21**]."

As more and more of personal belongings and personal being is stored on persistent media, the right of informational self-control is merging with the right of self-determination to a new meaning of freedom. The crux of the matter is that the decision whether we would like to share personal information with others should be ours. If we do not want to reveal personal data, we should not have to. If we wish to remain anonymous, we should be capable of doing so. We should also be able to be absolutely sure that we are not being observed if we have the desire to be. Taking the rising amount of network-computing into account, we need to realize that we all have to take measures to enforce our human rights in the information age. To go a step further, for those of us who share a vision of ubiquitous computing, the vision of a zero-privacy society is practically interchangeable.

Origin

The problems arising in human rights enforcement in the Internet have many causes. The characteristics shown by the Internet today are the result of the permanent historical, political, judicial, and commercial influences on the Internet.

The Internet used to be a network used by professionals who knew the technology they were using. Today the scenario has changed dramatically. Nearly everyone who knows how to use a scroll-wheel and can type 35 characters per minute using two fingers is online. The missing technological background makes it difficult for today's users to judge the risks of Internet communication. Sending unencrypted e-mail, for example, is essentially the same as sending letters via regular mail without an envelope. On the one hand, anyone who happens to cross the letters way can read the letter, on the other hand anyone who can read the letter can also change it, writing or deleting paragraphs as he wishes. Anyone sending personal stories, love-letters, etc. by simply stamping loose sheets of paper and throwing them in a letterbox would certainly be labeled insane, and still such a behavior is part of the daily insanity on the Internet. Many users simply lack knowledge of the way the Internet works. An important yet often underestimated aspect is that special care has to be taken when children come in contact with the Internet. 'Never talk to strangers' is a well-known and well-taught principle that still needs its analogy on the Internet. Children could enter personal data such as home addresses or telephone numbers if requested without realizing the consequences.

The Internet was designed to be a simple but reliable communication platform by military and scientific institutions in the USA and Great Britain. The basic design principle in the late 60s was robustness in the case of nuclear attacks. The original idea was to have as many autonomous nodes (hosts, bridges, routers) as possible communicating equally, with strong interconnection resulting in thousands of possible routes a packet could take from one place to another. In this model, each node is as much the network itself as part of it, and each node decides what to do with passing packets autonomously [**31**]. The Internet we know today is a slight modification of the initial model, mainly for performance reasons. To put it simply, routing packets has been made more intelligent and there are less possible routes a packet can take.

This node-to-node design is the reason why information being sent over the net can be subject to infiltration of many kinds. Any node between sender and recipient can read the packet, forward it, drop it, send it back, or manipulate it in any way it wants. Such practice is the way firewalls do their daily work and the same principle can be used to forge packets to make them look like they are coming from a different machine. A good reference of the technological design of the Internet is given by [**34**].

An often understated source of the dilemma addressed by this paper is the commercial funding shaping the Internet. Businesses learned quickly that customer data can easily be gathered in the Internet and started to invest in technologies to assist data harvesting. By simply watching user actions on a web site, customer reactions and preferences can be distilled. In addition people will fill out questionnaires, assured that they are doing so totally anonymously. Businesses rely on their collected personal data to offer customers individual service and on demographic and statistical data to plan future services and products. But users have the right and desire to stay anonymous and this contradiction has led to "businesses secretly gathering information about customers, and customers who systematically make up personal information. User Databases are full of Donald Ducks and John Does [**4**]," a situation which is of course unsatisfactory for both the businesses and the customers.But commercial data harvesting goes much further. User preferences, buying patterns, interests, financial and family situation, etc. can be linked to electronic identities, and electronic identities can often be linked to real identities.

The strongest opposition of Internet privacy and anonymity, however, are criminal activities. The abuse of the Internet is providing arguments for total observability and traceability of Internet communication. And of course, the Internet does provide criminals a nice platform for organizing and carrying out their activities and also for communication with like-minded. Internet crime is the sole reason there is a discussion about sense and non-sense of anonymity on the Internet, and the reason why, for example, the anonymity project of the TU Dresden [**1**] is having such a hard time with the German department for Internet crime, a section of the Bundeskriminalamt (BKA - the German FBI). A step in the direction of total observability was the European Convention on Cybercrime [**8**], and discussions about restricting the use of cryptography keep coming up. Public security and private anonymity contradict each other in this respect. The possibility of tracking criminal activities simply requires means of observation and lately government reactions to international terrorism have again shown that "privacy is the first thing thrown over board in case of a crisis [**25**, p. 64]."

A great amount of public debate is necessary to clarify how how a balance between security needs and privacy can be found and which foundations such a balance can be set upon.

Possible Foundations

Germany traditionally has exemplary laws on the protection of personal data. The tele-services data protection act (Teledienstedatenschutzgesetz TDDSG [**15**]) and the media-services treaty (Mediendienste-Staatsvertrag MDStV [**14**]) govern all service providers to obey the principles of avoiding personal data where possible and to save personal data sparingly where necessary. Personal data is only allowed to be saved with the explicit permission of the user and only data needed for accounting is to be saved. Where possible, access to services should always be provided by aliases. If personal data is intended for commercial reasons such as advertising or marketing, again the explicit permission is needed, and the user has to be informed about which data is being saved and what it is being saved for. But reality is different. National laws are of practically no significance in the Internet, for they are only applicable to companies based in the country the law is enforced by. This means the German laws on the protection of personal data are useless when using services from foreign countries. And moving the office to a different country is obviously of less expense than lengthy law-suits. The role of politics therefore cannot be a legislative or regulatory, but an educating and advising one, a role already spotted by the German data protection institutions, which are creating informational web sites [**9**].

The USA has taken a different stand in the fight for human rights in the Internet and reacted to the 1998 European 'Directive on Data Protection' with a set of guidelines: "In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the Directive, the U.S. Department of Commerce in consultation with the European Commission developed a 'safe harbor' framework. The safe harbor - approved by the EU in July of 2000 - is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU or facing prosecution by European authorities under European privacy laws. Certifying to the safe harbor will assure that EU organizations know that your company provides 'adequate' privacy protection, as defined by the Directive [**32**]." Since the commercialization of the Internet, supply and demand have become the driving motors of Internet innovation. Hence the self-regulating mechanisms of free markets should work in the Internet as well. These of course need well-educated customers with the possibility to compare products, which means that further education is necessary for a great amount of users. In this scenario, the state again must play the already discussed role of an advisor. Unfortunately, user education is still far from satisfactory and the safe harbor principles have become a mere workaround for US companies, the exact stated 'streamlined means for U.S. organizations to comply with the Directive'.

"While laws always have a territorial reference (...), technology is universal. The question, which technical options the browsers Netscape Navigator and Internet Explorer offer, is the same all over the world [**5**]." The problem is, that most users rely on technology offered by businesses. This means that informational rights will be regarded unimportant until the customers demand for right-enforcing technologies is strong enough to justify a good supply of such tools. Open source and freeware projects on the other hand, are often technological pioneers, aiming at 'doing it right' instead of making money no matter what. Of course, ultimately the users interest is the commercial interest, but this rule only has an effect when a large amount of users know and point out what they want. Since the public privacy discussion regarding cookies, all commercial browsers have mechanisms to control them. Here it lies in the hands of the users to show software businesses that there is a strong demand for data protection. If users had the choice, and realized the meaning of such a technology, they would surely decide to use it.

As national legislation or regulation cannot protect privacy on an international basis, the only support left at the moment is technological. Bruce Schneier once wrote in a slightly different context: "It is insufficient to protect ourselves with laws; we need to protect ourselves with mathematics [**25**]." The same seems applicable for the protection of privacy in the Internet. For this self-regulation to work, the Internet communities awareness for privacy concerns must be strengthened. Users must exhibit their interest in such technology one the one hand, and their reluctance towards privacy infiltration on the other.

Means of Infiltration

To gain an understanding of the threat posed today it is necessary to take a look at the means of information espionage used. The discussion presented here focuses on the not so obvious means of information espionage, and not issues such as trojans or hacking, as most people are aware of such threats and many good resources regarding them can be found. Every act of Internet communication leaves some traces behind, but in this section I will mainly discuss the possibilities of privacy infringement while browsing. There are several places where such traces can emerge [**18**]:

1. on your local system
2. on your local service provider's system
3. on your content provider's system
4. on any system between the other three

Here I will concentrate on the way content providers can collect data because local system security and encryption can stop systems in between from doing so.

User profiling cannot start without a correlation between several communication acts being possible, thus the first step must always be stamping communication acts with an identity. If the user is unknown a new profile can be created and henceforth this user's actions can be associated with one another.

User Identification

The first instance of identification in the Internet is the IP address resembling the reachability of a computer. In the early days of the Internet each computer needed a static IP address to be able to take part in Internet communication, but because the majority of users today use dial-in networks and are assigned dynamic IP addresses, a unique identification by a computers IP address is only possible for the length of a connection.

A technique for identification is the assignment of a Globally Unique Identifier (GUID) or Universally Unique Identifier (UUID). GUIDs are used in a multitude of ways; Microsoft, for example, inserts GUIDs into documents created by their Office suite, identifying the system and installation a document was created on. GUIDs have been standardized by the Open Software Foundation (OSF) as a 16-byte number (e.g., {3F2504E0-4F89-11D3-9A0C-0305E82C3301}). But GUIDs are not necessarily of this type; the Intel Pentium serial numbers, for example, also identify each computer uniquely.

A GUID has to be saved locally and submitted to its creator to act as an identifier. In the Internet this is done by saving them in so-called cookies, small information containers that can be read and written to in the process of a http request/response pair. By being saved locally and persistently, they can identify a user the next time he visits the same site. Most browsers allow a configuration of cookies, for example to only accept cookies for the server they originate from, but there are many workarounds for such security settings, such as web bugs or redirects, which make it possible to share GUIDs across several domains. GUIDs of course can be deleted or changed locally, and will not track a single user across several machines.

A very obvious method of identifying users is having them identify themselves using

logins and passwords. This always requires registration and is a great opportunity for content providers to request personal information. Providing an e-mail address is mandatory in most cases, and users are often even queried about their real name, home address, telephone number, birthday, etc. Such personal information is sometimes even mandatory even if it is unnecessary for the services being offered. User registration poses an even greater threat than the usage of GUIDs which can be lost, forcing a domain to restart the collection of data. Once a business has a users login and password or even real name and home address, access to services can always be tracked back to the correct user.

Data Harvesting

Once a user is identifiable, the collection of data can begin. The aim of data harvesting is to learn as much about a user as possible. To achieve this goal, users can be asked directly, for example, by the means of questionnaires, or user behavior can be observed to indirectly find out what their interests are.Questionnaires are predominantly used in the process of site registration. In addition to the personal data often mandatory for registration, users are often asked to fill out questionnaires about interests, marital status, financial situation, frequency and type of Internet usage, education, etc.User behavior is observed by analyzing so-called "clicktrails." A great deal of information can be distilled by watching which links a user follows, which products he takes a look at or even buys, which articles he reads, etc. Even queries to search engines can be used to analyze a user's interests. The observation is not necessarily carried out by the server providing the information displayed; third parties can also be involved. DoubleClick and other Internet advertising companies do their daily work by embedding banners on foreign web sites or in HTML e-mails. Requests to such web sites result in the browser requesting the embedded images from the marketer's server, and all information submitted to the original server can also be submitted to them. Sites without banners can also use this method by embedding invisible images - so called web bugs - to catch information [**26**].

"Offline, too, monitoring of people's behavior has increased by leaps and bounds in recent years [**10**]." Credit card, bonus, and discount programs are ways of collecting user information in the real world. As many such programs can also be used in the Internet, for example Payback [**22**], buying patterns can be traced online and offline and electronic identities can be linked to real ones.

Trusted Third Parties

In the 1990s a term called "infomediaries" was used for the idea of trusting a third party to retain ones personal data and provide identification to other companies when necessary [**10**]. Only AOL and Microsoft have developed systems to actually perform such a task, but trusting a third party only shifts the problem to a single and even more mighty counterpart. "The Passport service is intended to give Microsoft and Passport affiliates the ability to send unsolicited commercial email to Internet users and to profile their activities [**20**]."

Threats to Come

Further means of commercial privacy infringement are on their way. GPS and mobile phones allow the physical tracking of users' movements. Location-based services and cell-phone payment systems, video surveillance and face-recognition, biometric identification, and ubiquitous computing are all buzz-words that could one day do rid of privacy altogether.

Privacy Enforcement

This section briefly introduces methods of enforcing the different aspects of privacy in the Internet. A complete discussion of possibilities and their technical implementation is beyond the possible scope of this paper. Therefore the emphasis is placed on references for further reading.

Securing Communication

There are several technologies available for securing communication channels on the Internet with encryption. The three most supported and widespread technologies are SSL/TLS, SSH, and VPNs.

Secure Sockets Layer (SSL) and the newer Transport Layer Security (TLS) are general purpose protocols supported by almost all web browsers and all enterprise web servers. They are mainly used for securely transmitting data between web sites and clients, and use digital certificates for authentication. Sensitive data should never be entered into web-forms without the transmission being secured, and many web browsers display symbols to indicate a secure connection (e.g., closed pad locks in Internet Explorer and Netscape Navigator). Many mail services also offer the possibility of secure mail download via SSL or TLS [**29**], and there is also an open-source SSL library project [**30**].

Secure Shell (SSH) is a suite that allows secure remote logins and file transfers between Unix Systems (although there are also Windows clients available). SSH also has the possibility to tunnel other protocols such as X Windows connections. There are both commercial [28] and open source [27] SSH projects.

Virtual Private Networks (VPN) are a family of protocols for joining remote computers together by tunneling communication data through a secure protocol. To a client, it seems as if it is a direct part of the network the VPN tunnel is connecting to. Many VPN implementations exist. For further information see [33].

An important aspect of securing communication is the assurance of originality. Digital signatures and certificates are technologies that can provide such assurance. For a comprehensive introduction to all aspects of communication security see [24].

Data Protection

Anonymizing Proxies serve as public proxy services with varying extra features such as blocking cookies and potentially hostile JavaScript and Java code, filtering information the browser sends such as referrer URLs, or even automatically generating user aliases. The main function of an anonymizing proxy, though, remains hiding the requester's IP address. Users should be aware of the fact that the connections made are not secure and can thus still be observed by anyone in between themselves and the anonymizing proxy. In addition, the anonymizing proxy services may log connections and could be forced to share the logs, or may even abuse data themselves. Several commercial as well as free anonymizing proxies exist [6]. Another way of enforcing data protection is to filter personal information and the causes of information leaks locally. A great amount of tools for this purpose and further information can be found at [2].

Anonymity Enforcement

If the data being sent between communicating parties is encrypted, nobody can read the information being interchanged. What an observer can do, though, is find out who is communicating with whom. David Chaum introduced the so-called MIX model in [7] which can even conceal who is taking part in communication. There are several slightly different new implementations of the MIX networks. For a comprehensive discussion on MIXes see [17] and [6].

Anonymous or pseudonymous mailing can be achieved by using so-called "anonymous remailers." Two different technical implementations exist, but the principle is the same: an encrypted mail is sent through one or several servers that will remove all information that could lead back to the mails origin. For further information on the topic, take a look at [**3**].

"Freenet is free software which lets you publish and obtain information on the Internet without fear of censorship [**12**]." It uses encryption and mechanisms similar to those of MIX networks to hide the communicating participants. Once published, documents are no longer controllable by even the author. Only the network can decide to remove the least popular documents to make way for new ones.

Conclusion

The right of being anonymous is probably the most difficult to grasp for the inhabitants of western 'civilized' countries these days. In the course of time we have become lethargic in respect of the enforcement of our own rights. Resulting from the sensation of living in a free country, not having to worry about the rights our forefathers still had to fight for, we nowadays take these rights for granted. Freedom of speech for example can be worth less than nothing if a radical opposition will condemn us for what we are saying. Electronic anonymity could one day be the only harbor of our personal security and freedom [**16**].

Luckily we are not alone, there are many organizations and institutions fighting for exactly this cause, but the problem is we all have to take part. The Internet is, as shown, a judicial no man's land, thus legislative regulation can only put up signposts for citizens, who must choose their direction and act independently. The citizens, in return, have the duty to learn about and enforce their rights for generations to come.

The starting point in digital rights enforcement can only be common sense. Do not reveal personal data unless it is absolutely necessary. As long as we willingly share personal information there is no need for businesses to stop requiring it. If commerce realizes that customers no longer wish to be analyzed (unless it is done anonymously), then they will suddenly have a strong interest in developing the technology required. In the enlightening book *Database Nation* Simson Garfinkel wrote "Technology is not privacy neutral. The overwhelming tendency of technology is to out privacy. (...) Technology is intrusive [**35**]." I would argue that technology itself is of course neutral,

but the people financing technology aren't. Money makes the world go round, and invading privacy currently makes more money than respecting privacy. It is the consumers responsibility to direct the development of technology in a society-friendly direction.

References

1 Anonymität und Privacy (JAP). <http://anon.inf.tu-dresden.de/>.

2 Tools for Protecting Online Privacy. <http://www.epic.org/privacy/tools.html>.

3 Bacard, A. Anonymous Remailer FAQ. <http://www.andrebacard.com/remail.html>.

4 Bäumler, H. *E-Privacy*. "E-Commerce Meets E-Privacy." Vieweg Verlag, 2000.

5 Bäumler, H. *E-Privacy*. "Datenschutz im Internet." Vieweg Verlag, 2000.

6 Bäumler, H. *E-Privacy*. "Privacy Tools." Vieweg Verlag, 2000.

7 Chaum, D. Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. 1981. <http://world.std.com/~franl/crypto/chaum-acm-1981.html>.

8 Convention on Cybercrime. <http://conventions.coe.int/>.

9 Berliner Beauftragter für Datenschutz und Informationsfreiheit. <http://www.datenschutz-berlin.de/home.htm>.

10 The Economist. No Hiding Place: The Protection of Privacy Will Be a Huge Problem for the Internet Society. 2003. <http://www.economist.com/displayStory.cfm?story_id=1534283>.

11 Fasoldt, A. How Did We Cope Without the Internet? A Look Back After 20 Years of 'Technofile'. <http://aroundcny.com/technofile/texts/tec113003.html>.

12

The Free Network Project. <http://www.freenetproject.org/>.

13

Gavison, R. Privacy and the Limits of Law. *Yale Law Journal,* 89, 1980, pp. 421-471.

14

Mediendienste-Staatsvertrag - MDStV. <http://www.datenschutz-berlin.de/recht/de/stv/mdstv.htm>.

15

Teledienstedatenschutzgesetz - TDDSG. <http://www.netlaw.de/gesetze/tddsg.htm>.

16

Goltzsch, P. Anonymität im Internet. *Bundeszentrale für Politische Bildung, Schriftenreihe Bd. 382*. <http://www.bpb.de/publikationen/3DIHPI,0,0,Anonymität_im_Internet.html>.

17

Kesdogan, D. *Privacy im Internet - Vertrauenswürdige Kommunikation in Offenen Umgebungen*. Vieweg Verlag, 2000.

18

Köhntopp, M. and Köhntopp, K. Datenspuren im Internet. *Computer & Recht*, 4, 2000, pp. 248-257.

19

Confidentiality, Integrity, Availability (CIA). <http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm>.

20

Sign Out of Microsoft Passport! <http://www.epic.org/privacy/consumer/microsoft/>.

21

Nissenbaum, H. Protecting Privacy in an Information Age: The Problem of Privacy in Public. *Law and Philosophy*, 17, 1998, pp. 559-596. <http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>.

22

Payback. <http://www.payback.de>.

23

Privacy and Human Rights. <http://www.privacyinternational.org>.

24

Schneier, B. *Angewandte Kryptographie*. Addison-Wesley, 2000.

25

Schneier, B. *Secrets and Lies*. John Wiley & Sons, 2000.

26

Smith, R. M. On Internet Privacy and Profiling. 2000. <**http://www.senate.gov/~commerce/hearings/0613smi.pdf**>.

27

The OpenSSH Project. <**http://www.openssh.org/**>.

28

SSH Communications Security. <**http://www.ssh.com/**>.

29

Introduction to SSL. <**http://developer.netscape.com/docs/manuals/security/sslin/contents.htm**>.

30

The OpenSSL Project. <**http://www.openssl.org/**>.

31

Sterling, B. Short History of the Internet. <**http://w3.aces.uiuc.edu/AIM/scale/nethistory.html**>.

32

US Department of Commerce: Safe Harbor. <**http://www.export.gov/safeharbor/**>.

33

The VPN Consortium. <**http://www.vpnc.org/**>.

34

Washburn, K. *TCP/IP: Running a Successful Network*, 2e. Addison Wesley, 1996.

35

Garfinkel, S. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly & Associates, 2001.

Acknowledgements

The original paper was written as part of the conference seminar "dependable distributed systems" which was organized by the **laboratory of dependable distributed systems** at **RWTH Aachen University** during summer term 2004. Many thanks go to professor Felix Gaertner for pointing me towards the crossroads magazine.

Biography

Thomas Wright, (**thomas.wright@rwth-aachen.de**) is currently studying Computer

Science and Physics at the **RWTH Aachen University** in Germany. He is especially interested in Information Theory, Artificial Intelligence, and the social impact of technology.