

Towards un-personal security

Michael Sonntag

In current politics, security is paramount and mostly improved by reducing privacy. But do those two always have to be diametrically opposed? Are technical solutions to provide security while maintaining privacy, perhaps with an option for disclosure in certain cases, e.g. when a crime occurred, possible? This paper discusses un-personal security, i.e. security measures where it is not necessary to identify the person or only to a very limited amount. When this is possible and what such measures are is described together with a categorization of security approaches in the light of privacy.

1. Security and identification

Security and privacy are generally seen as diametrically opposed: You can only have one of the two. If security is improved, privacy must be reduced by the same amount. Similarly any increased amount of anonymity brings about a matching decrease of security. But is this really correct for all kinds of security and privacy as Schneier discusses in [1]? For instance, a fence increases physical security, but does not affect privacy as it can be seen through easily and keeps out all persons without identifying them. Contrarily a curtain will improve privacy, but not keep out burglars; but less visibility of valuables might render this house a less desirable object of attacks. Similarly, a completely anonymous "whistleblowing hotline/E-Mail account" improves privacy and does not reduce security at all. It even increases it through the possibility to communicate misuse, lax security, or active circumvention without fear of retribution. These are examples of the independence of security and privacy in the physical area. Whether such an approach is viable in the Internet or for computer systems this paper will discuss.

Just amassing data on persons through surveillance in the hope of increasing security thereby leads to even larger danger: Break-ins with consecutive disclosure, identity theft, extortion, employee

misuse etc. become more likely the more interesting and tempting the target is. While the fact that a certain person is an employee of a specific company is not very interesting (can be deduced in other ways quite easily), the fingerprint, voice patterns, exact ways through the building including their timing, log-on and –off times etc. are much more desirable, not only as direct information, but also as preparation for then much more dangerous attacks.

2. Categorizing security in the light of privacy

Security is not always the direct opposite of privacy. Therefore security can be classified according to its implications for privacy.

2.1. Personal security

Security will impact privacy only, if it is tied to individual persons or groups with a known membership: Like in the fence example a lock on the door of the server room does not detract from privacy in itself as it affects all persons alike in not being able to open the door. However, the key to this lock is personally attributable: Only a single person can own it (physical key) or, at least should, know it (password, PIN etc.). The latter we call "personal" security, as it is tied to a person and will not fulfil its security purpose without this association. Note, that this does not mean that the person must be *fully* identified ("personal data" according to privacy laws), just that this is possible ("*indirectly personal data*").

What person(s) are actually (or potentially) identifiable results in a second level of distinction: Whether it is "positive", "neutral" or "negative" personal security. Positive personal security means, only those who may get access, in whatever sense, must be identified and all other persons remain completely anonymous, while neutral personal security results in everyone being personally identified in some way. Negative personal security identifies attackers only.

2.1.1. Examples for positive personal security

Personal security measures are those, where the person to be granted access is identified, while attackers and other persons remain anonymous.

- Keys, passwords, tokens for authentication: Through using the token the presence of the person owning or carrying it is detected. Depending on the "key", this is a unique identification or as a

member of the limited group of "carriers". Persons forcing the lock are not identified (by the act itself, other remaining traces like fingerprints might enable this).

- Automatic locking: When users frequently leave their computer unattended, automatic locking is a useful measure: The system is secured without the need to identify any other person. Only idle time or the absence (but not the presence!) of a token/person/... is measured in some way. This must be distinguished from the unlocking method (see keys or tokens above).
- Encryption: Encryption prevents access by anyone without a need for their identification. Similar to passwords, only the person successfully decrypting the data is identified in the process through knowledge of the key. This especially applies to backups, where a lot of personal information is contained in a condensed form. Related to this are cryptographic checksums, where modifications can be detected through some shared secret, identifying both sender and recipient, but nobody on the transmission path or any external person.
- Sandbox (signed code): When executing signed code in a secured compartment, only the identity of the signer must be known. Users of the program remain completely anonymous.

2.1.2. Examples for neutral personal security

In these measures everyone is identified or becomes identifiable with additional data: Users as well as attackers, but innocent bystanders too.

- Mandatory ID cards: Everyone needs to advertise her/his identity continuously, perhaps even electronically readable (RFID-Tags; see [3] for an example of their use as implants to identify patients), regardless whether currently in a place where identification or even constant locating is necessary.
- Video surveillance: Every person in the area monitored is affected and can potentially be traced and identified through the recording, regardless whether the object to secure has been manipulated or not (see [4] for a vivid description of video surveillance in London, compared to now surely significantly less invasive, and [5] for an assessment of its consequences for security).
- Automatic unlocking: When a computer is unlocked because of detecting the presence of the/an authorized person in a unique way this means, that everyone generally matching the description, like wearing a token of a certain kind, needs to be checked (whether they are the person to look out for or not).

- **Data retention:** Information on all users is collected just in case, regardless whether there is something suspicious going on or not. Like video surveillance it provides a look into the past to identify attacks, but simultaneously on all other activities as well.
- **Intrusion Detection Systems:** They continuously monitor all network traffic (and perhaps computers) for their actions, like running processes (perhaps including the window title, which often includes the filename or title of the document), data sent/received, Although not all data they see is personally identifiable and stored, it is nevertheless a point of all-encompassing surveillance of all users without exception.

2.1.3. Examples for negative personal security

Such approaches will only identify attackers, but not affect normal users or others. Such measures are rare, but an example are Honeypots: systems specifically designed for and intended to be attacked. As they are not in normal use but pose only as closely supervised targets, ordinary users will not be identified or affected at all, except in rare cases of errors, like mistyping URLs or IP/E-Mail addresses.

Another example is the "quick-freeze" procedure as required by the Convention on Cybercrime [2]: If a crime occurs, information necessary to track back the perpetrator can be frozen: It will not be deleted, but is not disclosed either. This helps to ensure data is available for a later proceeding where everything is checked in detail and only afterwards the information retained is disclosed. Negative personal security comes closest to anonymous security.

2.1.4. Comparison of the three personal security classes

These three variations of personal security can be ordered according to their detractive influence on privacy: Negative personal security is most desirable, as everyone remains completely anonymous except the bad guys, which is generally seen as appropriate and a necessity for law enforcement. Next in the hierarchy is positive personal security, where only persons coming into successful direct contact with the system are affected. Here privacy is less of a problem as such activities will be archived without a regular inspection or much interest in this. Additionally there usually exists a contract between the persons affected and the one identifying them. Only in case of misuse the information will be analyzed. Still it is worse, as the definition of "misuse" can be set rather arbitrar-

ily and might include "being suspicious" for whatever reason¹. The worst security measures are the neutral ones, where everyone is affected, even if intending neither legitimate use nor illegal access. Although in many cases no specific search will take place like in positive personal security, regular inspections will happen and accidentally noticing facts and misuse becomes much more likely. Additionally, this information is "tainted" in its view, as these are not "positive" actions taken, but at least "perhaps suspicious" ones. As the security measure incurred costs, incentive exists to make this data pay off in some way, providing further motivation for investigation and usage.

2.2. The role of identification in security

In the common approach, "security" means_

1. Identification of the person requesting access
2. Checking whether this person is allowed access

Obviously, this is a non-anonymous process. It should be noted, however, that in many cases there is a slight difference: The second part must be formulated "checking whether this person should *not* be allowed access" (white- vs. blacklist). While this seems to be the equivalent, there is an important distinction: It assumes that a possibility exists to identify the "criminals". That this is not a very valid assumption airline security exemplifies. Numerous persons are not allowed to fly because of a name which is similar or identical to someone *suspected* of terrorism, and many terrorists are allowed to board planes as they have not yet been unmasked. A computer science equivalent are blacklists for computers sending out spam ([9]; but see also the controversy about the power of these organizations and its possible misuse [11], [10]): Although most servers employ one or several of them, spam is still a huge problem. The opposite, whitelists for computers intended to send mails (see SPF, Sender-ID and the newest one DKIM), have not been successful yet.

Classifying persons according to their security level also means that there is always a path less secure than others. So a very important attack vector is to achieve a high permission level, to be subsequently allowed to do everything without further checks. If, on the other hand, security is inde-

¹ In the sense of "driving while black": Being investigated out of prejudice because of a completely unrelated property. See for instance the recent privacy scandal of a German supermarket chain investigating private aspects of their employees to detect possible misbehaviour, which incidentally included the videotaping of customers entering their PIN code when paying ([6], [7], [8]).

pendent of the person, everyone is always subject to the same precautions and no less-secure alternative is available to try to get into. Take the x-ray scanning on airports to prevent weapons brought on planes as an example: No identification is necessary and smuggling them onboard becomes very difficult. But if an alternative exists, e.g. persons pre-screened and identified by their fingerprint are allowed a fast-boarding lane without scanning, security actually deteriorates. Evading the all-person scanning is difficult, but it is quite possible to circumvent a fingerprint scanner unobtrusively (or bribe someone) and carry onboard whatever desired.

In this classic way security depends on two difficult and indirect aspects: The identification of the person and the classification. But if the dangerous element itself is checked for anonymity remains, no indirection step is necessary, and security hinges only on the functioning of the scanning system. Speaking metaphorically, un-personal security is looking for the wolf instead of checking all the sheep whether they are really sheep.

It must be conceded, however, that such approaches of directly looking for "problems" are only possible when the problem can be diagnosed directly: It is e.g. comparatively simple to identify a prohibited weapon, but quite difficult to detect the mindset and intentions of persons. In computer science it is quite "trivial" to identify viruses or trojans, but hard to decide whether an advertisement E-Mail is wanted and expected by a person (→ ham) or not (→ spam).

Therefore in practice a combined approach will be necessary: Security without identification should be used whenever the "danger" can be identified directly, and identity-based measures only as a secondary approach when solely "normal" behaviour is recognizable.

2.3. Un-personal security

"Un-personal" or "anonymous" security are security measures which never affect privacy, i.e. working without identification of the person attempting access, regardless whether this should be allowed or not. This means that only proactive security is possible here: As any misbehaving entity cannot be identified later (the difference to negative personal security), logging plays no role whatsoever. However, it does not follow from this that the fact of a breach of security cannot be detected, only that the culprit cannot be identified by such measures alone.

As can be seen from the examples below, un-personal security is not suitable for every aspect of security, but still for a numerous list of very useful approaches, such as:

- Firewalls: Any undesirable connection is just blocked without logging (possible, but then it would be personal security), keeping out all potential intruders. This works extremely well on the packet level and resembles the example from above: A fence with some holes of a very specific shape. Important to note is that the decision whether to pass a packet or not is taken independently of the person it refers to (sender or destination), i.e. solely on the port, the IP address or not personally attributable content data (with the latter coming closer to personal security).
- Application gateways: These exist on a router and check certain traffic, for instance web pages, against a list of known exploits or classes/methods of attack. They are in general independent of the requesting person and the server and only inspect the content according to technical properties. Usually suspicious content is just blocked, but logging or notification to administrators are possible as well, but these would then no longer be classified as un-personal but rather as negative personal security.
- Anti-virus/-spyware programs: Similar to application gateways but checking for viruses, trojans, spyware, rootkits etc. in E-Mails, network traffic, and files. As the sender E-Mail and IP addresses are usually forged, no person is involved at all.
- Write protection: Physical or logical write inhibitions protect against modifications and deletion without the need for any identification. It should be noted however, that this is un-personal security only if *nobody* is allowed write access.
- Sandbox (unsigned code): Applets are executed in web browsers in a so-called sandbox: They cannot access the local file system, connect to servers other than they were loaded from, or call operating system routines and are therefore limited in their abilities to do harm. Similar measures are taken for JavaScript. Both seem to work very well in practice as signed code for which these restrictions are lifted (and where the author is always identified, although not necessarily with his/her real name or only as an organisation → personal security) is very rare.
- Code verification: Checking that some program will only do what it is allowed/is legal to do. This applies especially to checking for exploits or bugs. As only the code is inspected and the "quality" of its author (or publisher) is ignored, no connection to any person is present. If the source of the code is known, it could be classified as positive personal security instead.
- Checksums: They protect against transmission errors. However, they are not that useful as any attacker can easily recalculate them. Countermeasures like cryptographic checksums will usually not be un-personal security any more, as the fact of shared knowledge of the key involved

allows identification. Only if the shared secret is known by many entities (but e.g. itself strongly secured on smartcards), anonymity remains.

- Double execution with variance: Targeting the same area as code verification is multiple performance of some action with slight variations and checking whether the results are identical. This can be directly related to code verification (e.g. executing the same program with stacks growing in opposite directions to check for buffer overflows), but is generally applicable (like executing a query twice on different servers, with different sorting, additional elements, ...).
- Tripwires: This approach checks a system for modifications as compared to a "baseline" established at a point in time where it was presumable in perfect order. As only "anonymous" files, or rather their checksum, are compared with a previous version, no personal data is touched. If nothing suspicious is found, no action like logging takes place, and if an alert occurs only the changed files are mentioned (that these belong to certain people is of no consequence here; moreover these are usually executable files with no personal content and the administrator as "owner"!). Who modified a file also plays no role in this check.

2.4. Responsibility for security and privacy

Security is generally not the obligation of the affected person: *Objects* are secured *from* other *persons*, not the person from the object (→ safety). This leads to a "do it for me" attitude, where security is seen as a necessary evil. From this also stems the dislike and the ubiquitous circumvention actions for more intrusive approaches, which's reasons are not connected with privacy ("too complicated", "takes too long", "inconvenient", "hampers work", ...). Security is therefore hard to guarantee as continuous monitoring and training is necessary: Who is affected by the measures has only little interest in their success.

Privacy on the other hand is a "do it yourself" task: Everyone is responsible on his/her own to guard their personal data. Only when passing it on, others become responsible in addition (but only for ensuring that the rules set by the person are fulfilled). E.g. when participating in mail-in competitions, name and address are disclosed and optionally their use for advertising can be prohibited. The company organizing the competition is responsible for guarding the privacy only to the extent defined in law and the scope allowed by the person itself; i.e. those which did not cross out that line.

This dichotomy is mirrored e.g. in Austria in the legal framework as well: Security breaches are often crimes² and therefore prosecuted by the police and the criminal courts. Privacy on the other hand is (with very few exceptions if not breached by a public body) a private matter only and therefore citizens must organize investigations themselves and go to civil courts. From this the comparative importance follows: A security breach is a serious thing, while a privacy infraction is more of a gentlemen's misdemeanour. This is mirrored in the police activities³: There were numerous incidents with child pornography and various kinds of computer fraud in many years, but there was never even a single case connected with privacy to investigate. The reason for this is not because no privacy problems exist or there are so many other crimes, that no resources for investigating them are available: They are just not seen as important and when they occur, which is usually in companies which "loose" personal data of customers or employees, this is nothing to be made public, but rather kept secret if possible at all.

A similar distinction exists in business coverage: Numerous companies sell "security" in various forms. Hardware, software, services, education etc. are readily available in a huge and lucrative economy. Contrastingly, companies specializing on increasing or ensuring privacy are rare⁴ and small, but those dealing in personal data, the opposite of anonymity, are again many and huge.

3. Approaches towards un-personal security

To achieve security without identification, three general approaches are especially important:

1. Fences: General security barriers intended to keep out unwanted entities. They can be general, like bars on a window, when nobody is expected to cross this particular boundary, or specific, i.e. with a kind of door. The latter then usually needs to be combined with identification (not necessarily directly personal one, could also be a kind of token where possession alone is enough) of the entities allowed to pass it.

² Like unauthorized computer system access (§ 118a StGB), message interception (§ 93 para 3 TKG), computer fraud (§ 148a StGB) etc. See also the European Convention on Cybercrime [2].

³ Personal account of the head of the unit responsible for computer forensics in a large part of Austria.

⁴ One example are anonymization services like JonDonym (<http://www.jondos.de/>) regarding web browsing and Anonymizer (<http://www.anonymizer.com/>) for E-Mail and other services.

2. Automatic anonymous searches: Detectors for illegal objects like metal (→ weapons) or drug detectors work anonymously, but are usually employed only as negative personal security, i.e. persons detected as positive will be identified in a second step (the testing itself is anonymous!).
3. Seals: They provide authenticity through their complicated design but do not identify their (exact) source, i.e. who placed them there. Examples are security elements on paper money, which ensure its authenticity, but do not identify the source of the money, i.e. through whose hands it passed. A seal only identifies its issuer, which is typically not a single natural person and additionally unrelated to the security check.

According to this distinction, the examples provided above as well as the approaches discussed below in more detail can be classified as shown in Table 1. The last two are examined in more detail below as examples towards un-personal security, but which are not completely anonymous so not actually belonging to that group. The final subsection describes an approach for instances where un-personal security is not possible, but improving privacy is still important.

Security measure	Fence	Anonymous search	Seal
Firewall	X		
Application gateway		X	
Antivirus SW		X	
Write protection	X		
Sandbox	X		
Code verification		X	
Checksum			X
Double execution		X	
Tripwire			X
Automatic anonymisation		X	
Data safe			X

Table 1: Un-Personal (or close to this) security measures vs. the three general approaches

3.1. Automatic anonymisation

Automatic anonymisation refers to the practice of continuous surveillance (which in itself is personal security!), where any suspicious activity is searched for fully automatic and, if none is found, the data is automatically anonymized or deleted completely. Only positive matches will remain, resulting in negative personal security if identification follows. If just access is denied, this method comes very close to un-personal security. It is then comparable to a hole in a fence with a peculiar shape or a fishing net with a minimum size of the netting: Everything matching can pass unnoticed in any direction, frequency, appearance etc. anonymously, but those entities not matching the "ex-

ception" will be stuck. Note that the permission depends solely on the "shape" of the entity passing through: No identification is necessary to pass, i.e. no list of "allowed shapes" exists. In a way, any unwanted entity makes its decision itself: Its own shape is preventing it from getting through, not the decision of some other person whether its shape is acceptable or not. As the shape alone is not always sufficient, especially in IT, any method which is fully automatic and does not require identification, i.e. only looks at one or more properties not allowing identification even together, can be subsumed under this heading. Through this, neutral personal security can be transformed to negative or even un-personal security.

A prime example from the non-IT world is the section control on highways: At a certain place every single car is photographed digitally, the license plate scanned, and the same is done again on a later position. Depending on the time the car required to reach the second place the average speed can be calculated. If it is below the speed limit, all data is immediately and completely deleted: It is impossible to identify any car (and therefore person) afterwards, if the speed limit was obeyed. But if the car drove too fast, the data is stored and transmitted to the police for further processing (and a fine).

An example from the IT area are network intrusion detection systems: Only alerts are stored, and perhaps tried to trace back to the originator. Still, every packet on the whole LAN segment is copied, investigated and stored (so in this configuration it would be neutral personal security, as identification is typically possible within a company). But when all the traffic is not copied but only inspected and generalized to achieve a baseline to compare with, no personal data is stored any more. Still, persons are identified for a short period through investigating the content as well as source and sink of the packets. If the investigation ignores the payload content and only focuses on the flow, i.e. the protocol, and generalizes source and sink ("Computer of user 12" → "Development department"), anonymity has been reached. As these modifications are one-way only and if they are performed immediately, this closely resembles the example of section control above.

3.2. The data safe

A data safe is a personal virtual safe deposit box for electronic documents. It can contain e.g. electronically issued permissions or documents proving rights or status, like an electronic birth certificate. These are stored online safely, i.e. protected through backups from loss and through encryption from unauthorized access.

When requested by someone to prove a fact with a document stored there, three options exist: Firstly the document may be retrieved and passed to the person, or secondly the interested party could be allowed access to the data safe (perhaps not the whole but only relevant documents). Both approaches are not anonymous at all. The third option is that the data safe administrator could be asked by the data owner to confirm to the third party that certain documents exist and are valid. Obviously this depends on the operator, which need to be very reputable (and could for instance be the government itself, then posing no problem in this respect), and the document, which must be identifiable as genuine by the operator. The big advantage of this variant is, that the data itself need *not* be provided to the third person. Only the confirmation by the operator that a certain class of data exists is transmitted, removing the transmission of superfluous data and acting like a seal⁵. Obviously this works best when not the information itself is required, but only whether a certain property exists: A typical case for checking permissions in a distributed system.

One practical instance are public cigarette vending machines: In Austria they can only be operated by persons above the age of 16 years, which is usually proved by first inserting a banking card⁶, and then buying the cigarettes. However, stored on the card there is not the birth date, just a single bit, marking whether the owner is older than 16 years or not. Here the vending machine owner simply trusts the secure (such cards are very hard to counterfeit because of cryptography) seal provided by the banks⁷, which presumable correctly checked the age of the person the card was issued to.

3.3. Four-eyes approaches

Approaches requiring multiple persons for identification are not really un-personal security, as seen comprehensively identification of the affected persons *is* possible, although it becomes much more complicated and both misuse by employees as well as through external persons, e.g. by hacking, increases in difficulty. In effect, in normal operation it is equivalent to un-personal security, but if enough reasons exist, by a special procedure the veil of anonymity can be pierced.

⁵ See for example SET (Secure Electronic Transaction, an Internet credit card payment system), where merchants receive from the payment provider only a confirmation that a valid credit card exists, but not the card data itself.

⁶ "Bankomatkarte", "Maestro-Karte"

⁷ Whether the person holding the card is actually the owner is not verified, but this has been discounted as too complicated to verify and not necessary, as other ways to circumvent the limitation exist as well.

The basic idea is that the personal information is split in two or more parts, which are connected through a unique but non-identifying common element, for instance a random number. These parts must be stored and secured separately. Any person should have access to a single part only. To identify which person is connected to which data (or the reverse), therefore two persons must work together and combine data from separate systems. For each of them the data is either completely anonymous or not available at all.

Example for such approaches are pseudonyms in certificates for electronic signatures. The person owning the certificate remains anonymous to all recipients of signed documents. It is important to note, that this might be even a fully legally valid signatures, like an enforceable contract! However, the certification authority *does* know the real identity of the certificate owner. Through inquiring there, with sufficient reasons and permissions, it can be ascertained who actually electronically signed a document. On the other hand the certification authority has no access to the signed documents and is therefore ignorant of the actual use of the certificate⁸. While this scheme is not that interesting for a normal certificate, it becomes so when the certificate contains special attributes, e.g. age, permissions to sign for other entities etc.

Another application for the four-eyes approach is automatic unlocking in a wide sense. This has been described briefly above, but cannot be subsumed here directly as it is: Unlocking a specific computer requires not an identification as an authorized person only, which could be separated and pseudonymized, but as a single user. However, when the identity of the user is less important than the permission as such, this approach *can* be used. Consider for instance subscriptions to electronic libraries: While a username and a password can be shared easily amongst several persons and be used (almost; depending on other precautions) simultaneously, this is impossible or much more difficult with a physical access token. Regarding the type of security, a password means direct personal identification, but a token, like smartcards or key generators, need not be coupled to an identity (although currently they usually are): Their presence would be sufficient to prove authorization.

4. Conclusions

Un-personal security has been introduced, classified, and explained according to several examples in this paper. Its importance is constantly increasing, as e.g. identity theft, which was for a long

⁸ Inquiries for revocation lists could provide some information, but collecting such data is prohibited.

time a problem mostly occurring in the USA only, has now reached Europe as well. Therefore the desire for privacy becomes stronger, although remaining secondary to security in the view of the general populace (at least as long as they are not affected personally⁹). Approaches to combine both are therefore urgently needed. Security independent of identity, i.e. decisions based on some properties and not the unique identification of a person, must therefore be investigated and have been outlined. The three main avenues for this are fences, anonymous searches, and seals.

Although un-personal security cannot be used to counter all security threats and is not suitable in all circumstances, it deserves a much larger focus. When identification is necessary, a four-eyes approach should be followed: This is better than the typical current usage of full identification in all situations and where all data is stored on a single server, so only a single barrier must be overcome to obtain all information on someone. Negative personal security is another option with comparatively little privacy infraction, which is still able to improve security.

5. References

- [1] SCHNEIER, Bruce: Security vs. Privacy. Blog entry 29.1.2008.
http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html
- [2] Convention on Cybercrime. <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>
- [3] VeriChip: VeriMed Patient Identification. <http://www.verichipcorp.com/content/solutions/verimed>
- [4] McCAHILL, Michael, NORRIS, Clive: CCTV in London. March 2002. http://www.urbaneye.net/results/ue_wp3.pdf
- [5] GILL, Martin, SPRIGGS, Angela: Assessing the impact of CCTV. Home Office Research Study 292. February 2005.
<http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf>
- [6] LANGFELDT, O.: Mitarbeiterüberwachung bei Lidl. <http://www.datenschutz.de/news/detail/?nid=2596>
- [7] HAAS, Sibylle, LANDENBERG, Marcus v.: Lidl-Kunden fühlen sich bespitzelt.
<http://www.sueddeutsche.de/,ra3m1/wirtschaft/artikel/551/167072/>
- [8] MÜHLBAUER, Peter: Lidl und die PINs. <http://www.heise.de/tp/r4/artikel/27/27661/1.html>
- [9] Wikipedia: DNSBL (DNS Blacklist) <http://en.wikipedia.org/wiki/DNSBL>
- [10] Nic.at: Spamhaus.org changes nic.at listing.
http://www.nic.at/en/uebernic/current_issues/nicat_news/news_view/period/1180648800/2591999/archived/article/81/spamhaus-org-aendert-nicat-listing/
- [11] Spamhaus: Report on the criminal "Rock Phish" domains registered at Nic.at.
<http://www.spamhaus.org/organization/statement.lasso?ref=7>
- [12] Bayerische Datenschutzaufsichtsbehörde für den nicht-öffentliche Bereich: Dürfen Schüler ihre Lehrer im Internet benoten?
http://www.regierung.mittelfranken.bayern.de/aufg_abt/abt1/EuropDatenschutztag2008PressekonfVortrag.pdf
- [13] THÜR, Hanspeter: Empfehlung gemäss Art. 29 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG), betreffend die Bearbeitung und Weitergabe von elektronischen Datenspuren durch die Firma X im Auftrag von Urheberrechtsinhabern.
<http://www.edoeb.admin.ch/dokumentation/00445/00508/index.html?lang=de&download=M3wBUQCu/8ulmKDu36WenojQ1NTTjaXZnqWfVpzLhmfhnpmmc7Zi6rZnqCkkIN1fXd+bKbXrZ2lhtTN34al3p6YrY7P1oah162apo3X1cjYh2+hoJVn6w==>

⁹ See e.g. the recent privacy discussion on teacher evaluation in school portals in Germany ([12]), or the desire for anonymity against prosecution for P2P file-sharing of music or films (???)