

# Privacy in The Polippix Project

Niels Elgaard Larsen, Ph.D.  
IT-Political Association of Denmark (IT-POL)

May 21, 2008

## **1 Privacy Enhancing Technologies are not enough**

We do not believe that the invasion of privacy is primarily caused by design or implementation errors that can be fixed by performing Privacy Impact Assessments or adding Privacy Enhancing Technologies.

The threat to privacy is mainly caused by centralized gathering of increasingly detailed personal information. Once our personal data is stored and handled by the state our privacy is compromised no matter how the systems are designed and implemented.

To allow citizens more privacy, we have to design systems that are decentralized and require less personal information. For example it should not be necessary to identify yourself when using public libraries (you could still pay a deposit to make sure you would return a book) or medical services (it should be possible to prove that you were covered by health insurance without revealing your identity).

Our personal freedom is threatened by the vast amount of personal information we are forced to hand over to the state just to be citizens, make an income (and pay taxes), receive medical care, get an education, etc. But it is also threatened by leakage of personal information that we are not formally required to release. The latter is the focus of the Polippix project.

Privacy Enhancing Technologies are not enough. We need Privacy Guaranteeing Technologies.

## **2 Trusting the state**

In the view of many actors in the public debate, citizens are too technically challenged to be responsible for their own personal privacy. Therefore the state must do it for them.

## 2.1 Case: Eboks

In Denmark, all citizens can get a free state sponsored Digital Signature.

Public offices, employers, banks, etc want to save money by replacing paper-mail with electronic “mail”. They could just encrypt documents using the public key of the recipient and send it as an email. But the general opinion is that Danes cannot be trusted with receiving encrypted email.

Instead, they use a service called Eboks. Eboks is a centralized database that receives personal electronic mail for 1.5 million Danish citizens. To read the mail, the citizen can log in using a digital signature, find the new message, download it as PDF-file and view the PDF-file.

Eboks is a private company that is partially and indirectly owned by the Danish state. The result is that a state controlled company now distributes and stores personal documents for more than a quarter of all Danes.

## 2.2 Case: Government PC-inspections

A working group at the Danish Board of Technology in April 2008 proposed that in order to access public web-pages, citizens would have to let the state run special software on their computers to let the state verify that the level of security was acceptable.

When IT-Pol pointed out the very obvious implication for the privacy of the citizens, the board argued that citizens already trust vendors of operating systems, middleware (e.g. Java), etc.

## 2.3 Why this is the wrong approach

Many of us are perfectly able to protect our own private data. The members of IT-Pol might be better at doing this than most Danes. But we believe most Danes would prefer to be responsible for their own private data. We do not think that the state is particularly competent in handling personal information.

Many Danes could need some help in handling personal data, but the state is not suited to provide that help for the following reasons.

- It will be a centralized solution. When it fails, it will have very serious consequences.
- Because of the many relations between state and citizen, the state is particularly susceptible to compromise privacy by function creep.

- The state has frequently demonstrated that it has an interest in monitoring its citizens, for example the recent extensive data retention legislation.
- When personal information is handled by the state, it means that we, as citizens, have no choice in who we entrust our personal information to. Therefore, we really loose control of our own data. We might trust Apple, Ubuntu (Canonical), Sun, or Microsoft to run the software on our computers, we might trust Google, Yahoo, Facebook, Wikipedia, etc. with our online activities, but that is our choice and if we feel that they abuse our trust, we can replace any software or service.
- When solutions are being forced on citizens, it can harm the relationship between the state and its citizens.

For citizens that can not, or do not want to, take care of personal data security there is no need to leave it to the state. Citizens should be free to appoint any proxy to do it. It could be their bank, their trade union, church, a family member, Google, etc.

### **3 Anonymity**

We believe that we have the right to communicate with each other in privacy. Anonymity is not an objective in itself and it has some drawbacks.

When engaging in public debates, we present ourself. We want other people to be able to contact us and we get credibility from our past work.

But we also understand that we are privileged. There are people that can not always be expected to let their online statements be linked to their private lives: whistle-blowers, victims of abuse, etc.

Many of us also use the Internet for tasks that are private. As a result of state surveillance and private interests, many tasks that we used to do in our private homes are now done one the Internet. For example, before the Internet it was not a secret which newspapers we were subscribing to, which books we were buying or lending, who we sending letters to, which goods we bought. But it was also not registered in centralized databases.

Now the state mandated data retention registers every website we visit and everyone we email with. Before the Internet, we would take the encyclopedia from the bookcase and look up anything and nobody would know what we were researching. Now we might Google it, and Google will register our search and link it with our Google email correspondence, or we could look it up in an online encyclopedia, in which case the encyclopedia would

log which entries we read; and probably something like Google Analytics or Woopra would also log each individual lookup and link it to other traces we have left on the Internet.

The only realistic way of regaining some of our lost privacy is to use anonymity when we want to protect our privacy.

## 4 Polippix

The Polippix project is an effort to use technology to help people regain some of the rights and possibilities that have eroded either because of technology or by technology. The right to privacy is a very important example. Others, not discussed in this paper, are fair use (copyright) and the right to tinker (restricted by the Infosoc directive).

The primary expression of Polippix is a live-cd, that can be booted on most computers, and gives the user access to technologies used in Polippix.

### 4.1 Polippix Privacy Objectives

Polippix has gotten a lot of coverage as a tool to counter excessive Danish and European surveillance and data retention. This is deserved. The September 15, 2007 introduction of the Danish data retention is an important event, marking the day from which almost every Danish citizen came under daily observation without being under suspicion for any crime.

But there are many other threats to our online privacy, which are not marked by a particular day or year. The objective of the Polippix project is to protect users against all violations of online privacy.

From a technical point of view it does not make much of a difference whether Big Brother is the national police, a search engine company, an employer, a family member, a foreign country, or organized crime. These Big Brother candidates do not act independently. Personal data is traded between private companies, police exchange personal data across borders, national states can force private companies operating locally to release personal data on their citizens. A good example of this is the 2007 Danish data retention laws. Personal data is collected on request by the state, but is collected and stored by ISP's, wireless hotspot owners, hotels, housing communities, etc. This means that it is not just a matter of trusting the national police and intelligence with our private data, we also have to trust the personal integrity and technical competence of hotel owners, ISP's, etc.

It also does not matter why a Polippix user would want to keep Big Brother out of her private life.

- She could be doing something wrong.
- The mere collection of private data could violate her privacy.
- She could fear that her personal data could be abused.
- She could lack trust in legal and technical systems that should keep her private data confidential. I.e. Big Brother could be incompetent.
- She could lack trust in the people handling her data.
- She could have a need to assure others that the information she received from them would remain confidential. For example she could be a journalist communicating with confidential sources.

We therefore need a tool that will protect us against all threats to our private online life.

## 4.2 Privacy Technology in Polippix

Polippix is based on Linux and other free software. It is a live-cd based on the Kubuntu distribution. That allows users to try the Polippix software without installing software on their computers. It also prevents private information from being stored on hard-disks when using Polippix.

Some of the Polippix software relevant for privacy are:

- TOR (The Onion Routing) is a system enabling users to communicate anonymously on the Internet by routing data traffic through a few nodes randomly selected out of hundreds of thousands of TOR nodes. This does put a limit on the bandwidth and latency of the network.
- macchanger is a program that Polippix uses to change all network hardware MAC addresses at boot-time. This makes it impossible to link data traffic on local area networks to the computer on the network. E.g. when a laptop running Polippix is used on an open wireless network, data traffic cannot be linked to the laptop.
- Twinkle, SIP/ZRTP phone. Twinkle is an IP-phone using the SIP protocol. TOR is currently not able to handle very time-critical application like phone conversations, so privacy must be ensured by other means. Twinkle can use the ZRTP protocol for encryption of the conversation. This prevents eavesdropping, but not logging of participants in phone calls. It also does not provide anonymity, although anonymity

is less important for phone calls because recognition of human voice also compromises anonymity.

But when Polippix/Twinkle with macchanger is used on, for example, open WiFi access-points, registration of participants can be prevented.

Even for IP-to-PSTN calls some degree of anonymity can be achieved. In PSTN the tracking of phone calls are based on the billing system. Because the price of phone calls to PSTN land-lines have dropped dramatically, it is possible to sponsor free phone calls for every user. I.e., the originator of every phone call is the sponsor, although the phone call could have been made from any of the distributed or downloaded CD's.

- GnuPG, bcrypt, etc are systems that can be used to encrypt data.
- wipe can securely erase harddisk or files on harddisks. Useful when selling a computer, handing it in for repair or returning it to an employer.
- jhead is a tool that can clean jpeg images from tags identifying the camera. We plan to add tools that can remove unwanted extra information from text documents, such as authors, editing history, older versions, etc.
- Etherape and driftnet: Etherape is a graphical network monitor that dynamically displays Internet connections. driftnet displays all images passing through a computer. We include these programs, because they illustrate how little privacy we have if we do not take measures to protect it.

## **Lessons Learned from the Polippix Project**

The reception of Polippix outside our own environment has been overwhelming. 13,000 physical CD's were distributed to the members of trade union PROSA, more than 35,000 CD images were downloaded from our homepage and mirrors in a week, after that we lost track of downloads. Polippix has been covered on every major TV- and radio channel and all national newspapers.

### **The publics view on privacy and surveillance**

In our contact with politicians, media, and even scientists, we have often encountered talking points that express that the public has accepted the

invasion of privacy, that Big Brother is now a good thing, and that young people do not want privacy.

We disagree. We got in contact with many Danes after the release of Polippix. On September 15, 2007 when the data surveillance was introduced in Denmark, we took to the streets of Copenhagen, asking random people questions that reflected the effect of the introduced surveillance. The question (in english translation) included:

- Do you watch porn on the net? What kind?
- Are you a member of a political party or a religious society? Which?
- Do you eat pork when travelling on airplanes?
- Do you have regular contact with communists, xenophobes, or muslims?
- Who are the last 5 persons you phoned?
- What is your sexual orientation?
- How much do you earn per year?
- Do you consider your answers confidential? On a scale from 1-10, how much do you trust **us** with your answers? The **police**?
- Can we publicize your answers?
- Do you want to give us your name and address to enter a draw for two bottles of wine?

From this we learned which parts of their lives, people wanted to keep private and it led to very interesting discussions about privacy.

- Many people actually do want privacy. That is why so many downloaded Polippix. They did not accept Big Brother. But some had accepted their fate of no privacy, because they did not know they had a way of avoiding it.
- There is an enormous variation in which parts of their lives, people want to keep private. For example, some were very frank about their sexuality, but would not reveal their salary, while others would not tell which organizations and societies, they were a member of.
- Most of the randomly selected people were not at all aware of the extent of the newly introduced surveillance. And after they were made aware of it, most of them did not accept it, or at least did not accept substantial parts of it.

- Younger people did seem more willing to expose themselves on the Internet. But they were also conscious about making the choice about what to expose.
- Even people that were not worried about the decrease in privacy were changing their behaviour because of the surveillance, even if they were not doing anything illegal.

## Community support

There is an overwhelming opposition to the data retention and other surveillance introduced by the state among IT-professionals in Denmark. It is our impression that this is caused by an interest in privacy, but also because most IT-professionals actually know and understand exactly what is going on, realize the enormous implications for privacy, know that the measures will not help fight terrorism, and can seriously cripple the Internet as we know it.

Free Software is particularly well suited for the objectives of the Polippix project, because we need to use software technology to counter the technology of states, private corporations, etc. That can only work if we base it on software that can be used and developed independently. This is guaranteed by the four freedoms of Free Software as defined by the Free Software Foundation. Freedom to:

**run software for any purpose** even to counter government surveillance.

If we had to use non-free software we would have needed permission from every manufacturer of software used on Polippix. Considering that the Danish minister of justice has publicly criticized Polippix and that Polippix is now being used in some countries with a history of less democracy and respect for privacy, we doubt that we would have gotten the necessary permissions.

**study how the program works, and adapt it to your needs** Polippix users need to be able to verify that there are no back-doors.

**redistribute copies so you can help your neighbour** We needed to distribute tens of thousands Polippix CD's and CD images. We want peer-to-peer distribution for anonymity. Any restriction on redistribution would have been fatal to the project.

We want Polippix users to be able to redistribute Polippix. This is the point of the CD/USB-memory replication schemes we are currently

developing. If Polippix users could not freely redistribute Polippix then IT-Pol would be a bottleneck and a single point of failure for Polippix.

**improve the program, and release your improvements to the public**  
so that the whole community benefits

- That makes it possible to develop Polippix using existing Free Software projects.
- This ensures that Polippix cannot be easily stopped.

## **Conclusion**

Polippix has helped create an informed debate about privacy.

Although most of the software on the Polippix CD originates from existing projects, getting a physical CD that circumvents the surveillance has been an eye-opener for many Danish citizens. It demonstrates that we give up privacy for practically nothing.

Although only a small part of the population uses Polippix or similar techniques, getting Polippix out to tens of thousands of Danes demonstrates that protecting your privacy is a very real concern for others than geeks and hard-core criminals.