



PRIVACY FIRST

your choice in a free society

ANNUAL REPORT 2014

Privacy First Foundation
Amsterdam

30 June, 2015

Table of contents

1.	Introduction	1
2.	Policy pillars	2
2.1	Privacy First Passport Trial.....	2
2.2	‘Citizens against Plasterk’ case	4
2.3	Interim injunction proceedings against Data Retention Act	5
2.4	Number plate parking	6
2.5	Highway section controls	7
2.6	Automatic Number Plate Recognition (ANPR)	7
2.7	Campaign SpecifiekeToestemming.nl	9
3.	Privacy First Solutions	10
4.	Political lobbying	11
4.1	Locally	11
4.2	Nationally	11
4.3	Internationally and in Europe.....	11
5.	Communication	11
5.1	Mass media	11
5.2	Individual citizens	14
5.3	Internet.....	15
6.	Events	15
7.	Organization	17
8.	Finances	18

1. Introduction

2014 was an eventful year for Privacy First. In a number of fields of interest the privacy violations followed the same pattern, i.e. the compulsory use of centrally-based technology – without the involvement of Parliament or through defective legislation without an impact assessment focusing on fundamental rights – which, subsequently, is poorly organized and implemented. Instead, starting from the principles of our democratic constitutional State, ensuring the right implementation of such technology and examining how and which technological means can be applied in a privacy-friendly manner, should be the way to go. Privacy First advocates for the application of technologies that serve citizens instead of the other way around, and whereby citizens always stay in control of their own data.

Due to privacy violations, the basic principles of our constitutional State are being increasingly affected. A distrustful and unequal government, which acts as a supervisory body instead of a service provider and guarantor of our constitutional State, will lead to disruption in society in the future. The democratic accomplishments that may be compromised are, among others, the right to anonymity and freedom of movement in the public domain, the presumption of innocence, the legal privilege of lawyers and journalists, medical confidentiality and the use of cash money.

Since 2001, Privacy First has witnessed no new civil liberties, only an increasing number of restrictions. It's like a spy network that slowly but steadily is keeping citizens in a complete stranglehold. This constitutes a threat to the basis of our free society. After the revelations by Edward Snowden, the attention to privacy among the public is growing, yet it's remarkable that this isn't so among the authorities and a few monopolistic ICT companies.

The main focus of Privacy First is that the Netherlands becomes a global pioneer in the field of privacy and thereby gives a positive example compared to the total surveillance-oriented way of thinking of the US, China and other States that are fearful and distrustful of their own citizens. Privacy First is convinced that we are on the eve of an information revolution and that this is the time to build sustainable IT infrastructures that support and reinforce the constitutional State while maintaining everyone's privacy and security. For the year 2015, I see many opportunities to raise privacy awareness when it comes to the following topics:

- Number plates and public transport chip cards as if they were ankle bracelets;
- The new Electronic Health Record and the breakdown of medical confidentiality;
- The criminalization of cash money and anonymous forms of payment;
- Cyber criminality and hacking by the government;
- Big Data and profiling of citizens by authorities and companies;

- Social media and privacy safeguards;
- Infiltration into our homes with ‘smart meters’ of utility corporations.

In 2015 we will launch a new platform on the website of Privacy First in order to refer to privacy-friendly services and products in every possible area. In this way, Privacy First stimulates the growth of a privacy-friendly ICT industry with privacy solutions as its export product!

Bas Filippini

Privacy First Foundation chairman

2. Policy pillars

It's Privacy First's established policy to focus its attention primarily on (impending) privacy violations that (can) hit large groups of people at once. Selecting our themes, we are guided by 1) the scale, 2) the seriousness and 3) the possible impact and consequences of a certain violation. Privacy First prioritizes and publicly identifies mass violations of a grave nature. It then tries to make an end to the violation by means of quiet diplomacy and political lobbying, a public campaign, legal action or – as a last resort – a lawsuit. Since its founding and in line with these criteria, Privacy First has primarily focused on biometrics: the ability to recognize people on the basis of their physical characteristics by making use of, for example, fingerprints and facial scans. Other areas Privacy First has structurally been focusing on over the past few years are camera surveillance, public transport chip cards, medical confidentiality and profiling. The themes ‘privacy and secret services’ and ‘privacy and mobility’ – which relates for example to number plate parking, Automatic Number Plate Recognition (ANPR) and speed controls – were added to the list in 2013 and 2014 respectively. The main policy pillars are listed here below.

2.1 Privacy First Passport Trial

Over the past few years, Privacy First and 19 co-plaintiffs (citizens) have been involved in a large scale civil lawsuit against one of the most serious privacy violations in Dutch history: the storage of everyone's fingerprints under the new Dutch Passport Act. Such storage had mainly been intended to prevent small-scale identity fraud with Dutch passports (look-alike fraud), but was also to be used for criminal investigation purposes, counter-terrorism, disaster control, intelligence gathering, etc. This formed a flagrant breach of everyone's right to privacy. In a so-called ‘action of general interest’ (art. 3:305a of the Dutch Civil Code), in May 2010, Privacy First issued a subpoena against the Dutch government in order to let the judges declare the storage of fingerprints under the Passport Act unlawful on account of incompatibility with European privacy law.

In February 2011 however, the Hague district court (unjustly) declared our Passport Trial inadmissible. Therefore the judges didn't address the merits of the case. Privacy First immediately appealed the inadmissibility. Partly due to the pressure exerted by this lawsuit, the Dutch House of Representatives and the Dutch minister of Home Affairs Piet-Hein Donner changed their minds and the central storage of fingerprints was almost entirely brought to a halt in the summer of 2011.

Three years later (our appeal was still pending), the provisions in the Passport Act that were being challenged were partially repealed. Moreover, in January 2014, the compulsory taking of fingerprints for Dutch ID cards was abolished. A month later the Hague Court of Appeal finally came with its judgement in our Passport Trial: it ultimately declared Privacy First admissible and judged that the (previous) central storage of fingerprints was unlawful because it was contrary to the right to privacy.

The judgment by the Hague Court of Appeal paved the way for Privacy First (and other civil society organizations) to continue to be able to *litigate in the general interest* in order to preserve and promote the right to privacy as well as other human rights. A few months later, the minister of Home Affairs Ronald Plasterk announced that the Dutch government would appeal the judgment before the Dutch Supreme Court.

Despite the strong defense by Privacy First (represented by Alt Kam Boer Attorneys in The Hague), on 22 May 2015 both Privacy First as well as all co-plaintiffs were declared inadmissible by the Supreme Court after all. This new landmark ruling by the Supreme Court may have negative consequences for the Dutch legal protection against unlawful (privacy violating) legislation. The Supreme Court basically refers the case to the Dutch Council of State (*Raad van State*), where, in recent years, multiple similar administrative cases of individual citizens against the Passport Act were pending.

Following the inadmissibility before the Supreme Court, Privacy First has submitted the entire Passport Trial case-file to the Council of State in order to strengthen the pending cases there. Ever since, Privacy First et al. have anxiously awaited the judgement by the Council of State.

Meanwhile, Privacy First et al. are preparing to submit a complaint to the European Court of Human Rights on account of violation of the right to privacy (art. 8 European Convention on Human Rights, ECHR), as well as the right of access to justice and an effective legal remedy (art. 6 and 13 ECHR). Consequently, despite the Kafkaesque anticlimax before the Dutch Supreme Court, a European conviction of the Netherlands is on the cards.



© Guus Schoonewille

Passport Trial by Privacy First et al., Palace of Justice, The Hague

2.2 'Citizens against Plasterk' case

Judging by the revelations of Edward Snowden it appears that the spy practices of intelligence services such as the American NSA almost recognize no borders. Instead of calling the Americans to order, secret services in other countries appear to have made avid use of the intelligence that has been collected illegally by their foreign allies. That's why the privacy legislation that should protect citizens against such practices is being infringed in two ways: by foreign secret services like the NSA that collect intelligence illegally, and by domestic secret services that subsequently use this intelligence. In order to call a halt to these practices a national coalition of Dutch citizens and organizations (among which Privacy First) decided at the end of 2013 to take the Dutch government to court and demand an immediate stop to the receipt and the use of illegal foreign intelligence on Dutch citizens. Furthermore, every citizen about whom intelligence has been collected, should be notified about this and the data in question should be deleted.



Apart from Privacy First, the coalition of plaintiff parties consists of, among other organizations, the Dutch Association of Journalists (*Nederlandse Vereniging van Journalisten*, NVJ), the Dutch Association of Criminal Defence Lawyers (*Nederlandse Vereniging van Strafrechtadvocaten*, NVSA) and the Dutch chapter of the Internet

Society (ISOC.nl). These legal proceedings by Privacy First primarily serve the general interest and aim to restore the right to privacy of every citizen in the Netherlands. The lawsuit is conducted by bureau Brandeis; this law firm also successfully represented Privacy First in its Passport Trial against the Dutch government. However, on 23 July 2014, the district court of The Hague issued a disappointing judgement: even though all plaintiff parties (organizations and citizens) were deemed admissible, the judges rejected all claims. In so doing, the judges were so wide off the mark on many aspects that the ruling is very unlikely to be upheld on appeal. Therefore, Privacy First is confident about the outcome of the appeal before the Hague Court of Appeal. Moreover, this case could also be won extrajudicially (in the political arena) by way of a critical review of the 2002 Dutch Act on the Intelligence and Security Services (Wiv).

2.3 Interim injunction proceedings against Data Retention Act

Privacy First was more successful in crucial interim injunction proceedings against the Dutch Data Retention Act. Under this 2009 Act, the telecommunications data (telephony and internet traffic) of everyone in the Netherlands used to be retained for 12 months and 6 months, respectively, for criminal investigation purposes. As a result, every citizen became a potential suspect. In [interim injunction proceedings](#) against the Dutch government, a broad coalition of civil society organizations demanded the Act to be rendered inoperative as it violated the right to privacy. The claimant organizations were Privacy First, the Dutch Association of Criminal Defence Lawyers (NVSA), the Dutch Association of Journalists (NVJ), the Netherlands Committee of Jurists for Human Rights (NJCM), Internet provider BIT and telecommunications providers VOYS and SpeakUp. Boekx Attorneys in Amsterdam took care of the proceedings.

According to the claimant parties, the Dutch Data Retention Act constituted a violation of fundamental rights that protect private life, communications and personal data. This was also the view of the European Court of Justice in April last year, and subsequently that of the Dutch Council of State, the Dutch Data Protection Authority and the Dutch Senate. However, the former minister of Security and Justice, Ivo Opstelten, refused to withdraw the Act. Opstelten wanted to uphold the Act until a legislative change was implemented, which could have taken years. Rather uniquely (laws are seldomly rendered inoperative by a judge, let alone in interim injunction proceedings), the judge made short shrift of the entire Act by repealing it immediately as it was in breach of the right to privacy.



© Lisa S. / Shutterstock.com

The Dutch government decided not to appeal the ruling, which has been final since then. Privacy First considers this to be an historic victory. In the event that another data retention Act will be introduced sometime in the future, Privacy First and others shall not hesitate to contest this before the appropriate courts again.

2.4 Number plate parking

In a growing number of Dutch municipalities, number plate parking is being introduced: when you park your car, you have to enter your number plate in a ticket machine and often payment is only still possible by card or with a parking app. All parking data is stored in municipal databases or in the national database of the so-called Service House for Parking and Residential Rights (Servicehuis Parkeer-en Verblijfsrechten, SHPV). However, as a free citizen you have the right to travel anonymously within your own country. Hence, this also means having the right to park your car anonymously. You also have the right to use any legal tender that offers anonymity, for example cash money. After a large scale protest action in 2013 by Privacy First against number plate parking in Amsterdam, this municipality decided to delete all the parking data and henceforth to only temporarily save data of those guilty of illegal parking, with the view of possible objection and appeal. However, for Privacy First these concessions are insufficient: as long as number plate parking isn't replaced by a privacy-friendly alternative (for example the introduction of parking space numbers), Privacy First will continue to resist it. In 2014, Privacy First did so in court through an objection and appeal procedure initiated by its chairman Bas Filippini. The cause of this case was a fine he received after having refused in principle to enter his number plate for a parking space (which he had paid for). Our attorney Benito Boer (Alt Kam Boer Attorneys, The Hague), brought forward numerous privacy objections against number plate parking. And successfully so: on 30 January 2015, the district court of Amsterdam upheld the appeal against the parking fine of our chairman.



Since then people in the Netherlands are no longer obliged to enter their number plate when parking their car, as long as they're able to demonstrate that they have paid for their parking space (for example with a receipt or parking ticket). Citizens who, despite this ruling, still receive fines for not having entered their number plate, can easily object and appeal this with the [model complaint letter](#) (in Dutch) by Privacy First. For Privacy First, this legal victory is only the first step on the way to privacy-friendly parking: for 2015 we're already preparing new lawsuits against number plate parking, and specifically, against the obligation to pay electronically (and thus traceably). Apart from that, Privacy First supports citizens in individual complaint and appeal procedures.

2.5 Highway section controls

Together with number plate parking, Dutch highway section controls (“*trajectcontrole*”) have for years been a thorn in Privacy First’s side: all motorists are under camera surveillance on a stretch of highway and depending on their average speed they might get a fine for speeding. Up until this day, for this system there is no legal basis with specific privacy guarantees put in place. The lack of such a legal basis is in breach of art. 10 of the Dutch Constitution and the European right to privacy (art. 8 ECHR).

Moreover, all the data which are gathered, are stored in police databases for at least three days; this includes data of the majority of motorists who do not exceed the speed limit. As a result, the police has access to information about the movements of all motorists in the Netherlands. These data could be shared with other authorities, such as the General Intelligence and Security Service, legal authorities and the tax authorities. Every motorist thus becomes a potential suspect. Back in 2012 already, this led the chairman of Privacy First to lodge a complaint and appeal procedure against a fine he received on the basis of a highway section control.

The hearing in this case took place before the court of Utrecht in April 2015. However, the magistrate was hardly prepared to verify important aspects of the speed checks against higher privacy law and rejected the case. The magistrate considered the section controls to be a ‘minor privacy violation’ and deemed the general Police Act and the warning signs along the highways as sufficient privacy guarantees.

For Privacy First this is incomprehensible. We will therefore submit this matter to the European Court of Human Rights in Strasbourg. Moreover, Privacy First is preparing further legal steps against section controls at a national level. As is the case in the lawsuit against number plate parking, Privacy First is being represented by its attorney Benito Boer (Alt Kam Boer Attorneys, The Hague).



2.6 Automatic Number Plate Recognition (ANPR)

It’s Privacy First’s constant policy to challenge mass privacy violations before court and have them declared unlawful. A current legislative proposal that lends itself very well to this, is the proposal by the Dutch minister of Security and Justice (Ard van der Steur) relating to Automatic Number Plate Recognition (ANPR). The minister wants to store the number plates of all motorists (in other words all travel

movements) on Dutch highways for four weeks through camera surveillance for criminal investigation purposes. Every motorist becomes a potential suspect because of this. Privacy First deems this a wholly disproportionate measure. The proposal was submitted to the House of Representatives by former minister Ivo Opstelten in February 2013 already. Before that, in 2010, minister Hirsch Ballin had the intention to submit a similar proposal, albeit with a storage period of only 10 days. However, back then the House of Representatives declared this subject to be controversial. Opstelten and Van der Steur have thus taken things a few steps further.

According to the current rules, ANPR data of innocent citizens should be erased within 24 hours. In the eyes of the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*, CBP), all number plates that are not suspect (so-called 'no-hits') are to be removed from relevant databases immediately. Van der Steur's plan to also store the number plates of unsuspected citizens for four weeks directly flies in the face of this. It constitutes a blatant violation of the right to privacy of every motorist. In case Parliament accepts this legislative proposal, Privacy First (in coalition with other civil society organizations) will summon the Dutch government and have the law declared invalid on account of being in violation of the right to privacy. In case necessary, Privacy First and individual co-plaintiffs will be prepared to continue this lawsuit all the way up to the European Court of Human Rights in Strasbourg.

What's more, in 2014 it became known that through secret agreements with the police, the tax authorities continuously receive ANPR data on all Dutch motorists on a massive scale. The tax authorities may store these data for many years and they could be requested for by the police, legal authorities, secret services, etc. Privacy First considers this non-statutory exchange of data and U-turn scheme completely illegal. As long as the CBP and the House of Representatives don't take measures, then Privacy First reserves the right to lay this matter before the court as well.



Photo: Chris Zwolle, Flickr

ANPR and section controls on highway A12 near Utrecht

2.7 Campaign SpecifiekeToestemming.nl

On the initiative of Privacy First and the Platform for the Protection of Civil Rights (*Platform Bescherming Burgerrechten*), a large scale internet campaign revolving around the right to medical confidentiality was launched in April 2014: www.SpecifiekeToestemming.nl. Since then, this campaign has been supported by many civil society organizations, health care providers and scholars. The essence of the campaign is that specific consent should (again) become the leading principle when it comes to the exchange of medical data. This is in contrast to the generic consent that applies to the private successor of the Dutch Electronic Health Record (*Elektronisch Patiëntendossier*, EPD): the National Switch Point (*Landelijk Schakelpunt*, LSP). In the case of generic consent, it's unforeseeable who can access, use and exchange someone's medical data. In this respect, generic consent is in contravention of two classic principles: the purpose limitation principle and the right to free, prior and fully informed consent for the processing of personal data. However, in 2014 the legislative proposal '*Clients' rights relating to the electronic processing of data*' of the Dutch minister of Health Edith Schippers threatened to enshrine such generic (broad, unspecified) consent in law at the expense of the existing right to specific (targeted, well-determined) consent. In case of specific consent, prior to sharing medical data, clients have to be able to decide whether or not, and if so, which data to share with which healthcare providers and for which purposes. This minimizes risks and enables patients to control the exchange of their medical data. Partly due to the pressure of our campaign, in July 2014, generic consent was scrapped from the legislative proposal by the House of Representatives and thus specific consent remains: this will have to be implemented in all existing and future systems for the exchange of medical data, including the current National Switch Point. Meanwhile, the Senate is inclined to repeal the legislative proposal as long as it insufficiently guarantees the existing right to specific consent. Moreover, there are several ongoing market developments that indicate that specific consent is and remains the norm within new systems and that privacy by design becomes the new standard. In light of this, the campaign by Privacy First can already be called a success.



Campaign banner *SpecifiekeToestemming.nl*

3. Privacy First Solutions

Privacy First is of the opinion that it's high time to actively engage companies in a privacy-friendly Netherlands of the future. To this end, Privacy First - with its new initiative called Privacy First Solutions – wants to dismantle the barriers in order to apply privacy-friendly solutions. Interacting with partners from various fields, Privacy First aims to stimulate industry to develop and implement innovative privacy solutions. The little dot on the horizon we're trying to get near to is the Netherlands as a global pioneer in the field of privacy. In order to achieve this, at this stage Privacy First Solutions focuses on three goals:

1. Examine continuously, through discussions and knowledge transfer, how the right to privacy relates to modern technological developments.
2. Stimulate companies to apply privacy by design and to make privacy a unique selling point.
3. Offer a platform for companies that operate and innovate in a privacy-friendly way so that they can take on a leading role on a national and an international level.

Privacy First believes that privacy offers companies the perfect chance to go about their business in a socially responsible way and to position themselves positively on the market. There are many companies that already want to show that they care about the privacy of their customers. After all, dealing with personal data responsibly is of crucial importance for companies to gain the trust of consumers.

Privacy First Solutions also aims at uniting companies and organizations in the area of privacy. By sharing experiences and thinking about solutions together, we can contribute to a Netherlands of the future wherein doing business in a privacy-friendly way is the norm.

Privacy First Solutions started off with a successful pre-launch event on 2 December 2014. After an introduction on the necessity of the initiative, there was room for sharing a number of best practices and good ideas, like Greenhost, a privacy-friendly internet provider, followed by the *DataWijzer* and *Hack-je-Hokje*, two initiatives by the Dutch National ThinkTank (*Nationale DenkTank*). The former summarizes privacy terms and conditions in simple icons and the latter provides insight into online profiling. In 2015, Privacy First, among other things, will develop a platform that enables organizations to come together to brainstorm about privacy-friendly ways to do business and innovate. Several more events and projects are coming up and Privacy First will advise authorities and companies ever more often on the development of privacy-friendly legislation, policy and technology.

4. Political lobbying

4.1 Locally

In 2014 Privacy First has been contacted by city council members from various Dutch cities for information and advice in order to define local standpoints with regard to (in particular) number plate parking, camera surveillance and municipal Privacy Impact Assessments.

4.2 Nationally

Apart from various emails sent to individual members of Dutch Parliament, in 2014 Privacy First sent the following letters to the Dutch House of Representatives, the Senate and (cc) to relevant Dutch officials:

- Letter dated 8 April 2014 to the House of Representatives (standing committee for Security and Justice) pertaining to the legislative proposal on ANPR;
- Letter dated 6 June 2014 on behalf of SpecifiekeToestemming.nl to the House of Representatives (standing commission for Health, Welfare and Sport) pertaining to the legislative proposal on clients' rights relating to the processing of medical data;
- Email dated 15 October 2014 to the House of Representatives (standing commission for Infrastructure and Environment) pertaining to the public transport chip card.

4.3 Internationally and in Europe

Following our previous lobby against Taser weapons at the United Nations Committee against Torture, at the beginning of 2014, Privacy First was invited by the Organization for Security and Cooperation in Europe (OSCE) to a number of meetings in Vienna on the topics of torture, privacy and the protection of personal data. Furthermore, Privacy First was invited for the Computers, Privacy and Data Protection Conference in Brussels and the ALB Data Protection Conference in Kuala Lumpur. Moreover, Privacy First maintained contacts with various members of the European Parliament. As of 2015, Privacy First wants to become more active on a European level.

5. Communication

5.1 Mass media

In 2014, the national media outreach of Privacy First has widened and has become more diverse relating to its content. Apart from requests for interviews, Privacy First is increasingly called upon by journalists for background information and

research suggestions. Privacy First also appears in foreign media ever more often. Below is a selection of our appearances in the media in 2014:

- Security.nl, 7 January, 2014: 'ID-kaart zonder vingerafdrukken over enkele weken beschikbaar' ('ID card without fingerprints available within weeks')
- AD/Rotterdams Dagblad, 28 January, 2014: 'Gegevens parkeerders blijven toch bewaard' ('Data of parking customers are kept just the same')
- Security.nl, 30 January, 2014: 'Kohnstamm: Europese vuist tegen NSA-surveillance nodig' ('Kohnstamm: Europe should stand up against NSA surveillance')
- NU.nl, 11 February, 2014: 'Commissie EU stemt voor verplicht alarmsysteem in auto's' ('European Commission votes in favor of compulsory alarm system in cars')
- Radio 1, 13 February, 2014: interview with Privacy First about lack of privacy in the Netherlands
- NRC.nl, 18 February, 2014: 'Hof: centrale opslag vingerafdrukken in strijd met recht op privacy' ('Court: central storage of fingerprints in breach of right to privacy')
- NRC Next, 19 February, 2014: 'Vingerafdrukken centraal opslaan is in strijd met de wet' ('Central storage of fingerprints against the law')
- ZDNet, 19 February, 2014: 'No, you can't store people's fingerprints in a central database, Dutch court rules'
- Ravage Webzine, 26 February, 2014: 'Europese auto's krijgen spionagekastje' ('European cars equipped with spy device')
- BNR Nieuwsradio, 10 March, 2014: interview with Privacy First about pilot experiment with customer data by ING
- Leeuwarder Courant, 12 March, 2014: 'Duizenden camera's en zeventien miljoen ogen' ('Thousands of cameras and seventeen million eyes')
- Netzpolitik.org (Germany), 12 March, 2014: 'Militärgeheimdienst der Niederlande der illegalen Datenweitergabe überführt' ('Dutch military secret service illegally transfers data')
- Volkskrant.nl, 2 April, 2014: 'Cameradrones toegestaan - wat betekent dat voor u?' ('Camera equipped drones allowed – what does this mean for you?')
- RTL.nl, 2 April, 2014: 'Kentekens voortaan vier weken opgeslagen' ('Number plates stored for four weeks from now on')
- NU.nl, 3 April, 2014: 'Opslag camerabeelden kentekens door politie stap dichterbij' ('Storage of camera images by police a step closer')
- RTL Nieuws, 3 April, 2014: television interview with chairman of Privacy First about storage of ANPR data
- Radio 1, 9 April, 2014: interview with chairman of Privacy First about legislative proposal on storing ANPR data for four weeks
- NU.nl, 22 April, 2014: 'Geef patiënt regie over medische gegevens' ('Give patients control over medical data')
- TROS Radar & VARA Kassa, 22 April, 2014: 'Geef patiënt regie over medische gegevens' ('Give patients control over medical data')
- SmartHealth.nl, 24 April, 2014: 'Kan iedere zorgverlener bij al je medische gegevens?' ('Do all healthcare providers already have access to your medical data?')

- Zorgvisie, 25 April, 2014: 'Landelijke campagne voor behoud medische privacy' ('National campaign for maintaining medical confidentiality')
- NRC Handelsblad, 30 April, 2014: 'Geef arts en patiënt eigen dossier terug' ('Give doctors and patients their own health records back')
- Radio 1 (NOS), 13 May, 2014: interview with Privacy First about lawsuit 'Citizens against Plasterk'
- Trouw, 14 May, 2014: 'Wirwar van camera's langs de snelweg' ('A tangle of cameras along the highways')
- Omroep Gelderland, 5 June, 2014: television interview with Privacy First about civil drones
- Telegraaf, 8 June, 2014: 'Gevangen in 'datakluwen'; privacyvoorvechters pleiten op Big Brother Dag voor vrijheid' ('Trapped in a 'data maze': privacy advocates promote Big Brother Day for freedom')
- Lexology (United Kingdom), 15 July, 2014: 'Dutch government violated article 8 ECHR by requesting and saving personal data in central register'
- NU.nl, 23 July, 2014: 'Nederland mag gegevens blijven uitwisselen met NSA' ('Netherlands may continue to exchange data with NSA')
- NOS Teletekst, 23 July, 2014: 'AIVD mag gegevens krijgen van VS' ('Dutch intelligence service may receive data from US')
- Security.nl, 24 July, 2014: 'Hoger beroep tegen uitspraak over uitwisseling NSA-data' ('Appeal against court decision about exchange of NSA data')
- Radio 1 (NOS), 7 August, 2014: interview with Privacy First about lack of legislation concerning drones
- Frankfurter Allgemeine Zeitung (Germany), 12 August, 2014: 'Big Brother in Holland'
- AD/Rotterdams Dagblad, 20 August, 2014: 'Stop met bewaren van gegevens parkeerders' ('Stop retaining data of parking customers')
- Advocatenblad, August, 2014: 'Typisch Opstellen' ('Typically Opstellen')
- BNR Nieuwsradio, 11 September, 2014: interview with Privacy First about 'smart cameras' at Schiphol Airport
- Verkeer in Beeld, 20 October, 2014: 'Kritiek op OV-chipkaart blijft aanhouden' ('Ongoing criticism against public transport chip card')
- Personal Computer Magazine, 22 October, 2014: 'Belastingdienst kijkt op grote schaal mee met politiecamera's' ('Tax authorities access police cameras on a large scale')
- EenVandaag, 28 October, 2014: interview with Privacy First about the use of ANPR cameras by the tax authorities
- Metronieuws.nl, 7 November, 2014: 'Amsterdam voor de rechter om kentekenparkeren' ('Amsterdam taken to court due to number plate parking')
- Trouw, 11 November, 2014: 'Is kentekenparkeren een aantasting van de privacy?' ('Is number plate parking a privacy violation?')
- Telegraaf, 11 November, 2014: 'Privacykwestie voor rechtbank; weigeraar kentekenparkeren laat zaak voorkomen' ('Man refusing to enter number plate for parking ticket brings privacy matter to court')
- Radio 1, 11 November, 2014: 'Anoniem parkeren moet kunnen' ('Parking anonymously should be possible')
- RTL Nieuws, 11 November, 2014: report on lawsuit by Privacy First against number plate parking

- Volkskrant.nl, 19 November, 2014: 'Privacybeschermers kritisch over 'koevoetcontrole' bouwmarkten' ('Privacy advocates object 'crowbar surveillance' in hardware stores')
- De Gelderlander, 21 November, 2014: 'Wat als je lijkt op een crimineel?' ('What if you look like a criminal?')
- Radio 2, 26 November, 2014: interview with Privacy First about unclear drone regulations
- AT5, 26 November, 2014: discussion with Privacy First about DNA database for detection purposes
- NRC Handelsblad, 6 December, 2014: 'Kort geding tegen staat om opslag van internet- en belgegevens' ('Interim injunction proceedings against the State on account of storage of internet and telephone data')
- NU.nl, 6 December, 2014: 'Kort geding tegen Nederlandse staat vanwege bewaarplicht' ('Interim injunction proceedings against the Dutch State on account of the Data Retention Act')
- NOS Teletekst, 6 December, 2014: 'Kort geding tegen bewaarplicht data' ('Interim injunction proceedings against Data Retention Act')
- Trouw, 8 December, 2014: 'Mag provider gegevens opslaan?' ('May providers store data?')
- Leeuwarder Courant, 13 December, 2014: 'Mag die duimafdruk van mijn paspoort af?' ('Can I have that thumb print removed from my passport, please?')



Dutch television interview with Bas Filippini, 3 April 2014 © RTL Nieuws

5.2 Individual citizens

On a daily basis Privacy First receives questions from citizens on a wide variety of privacy issues. In 2014 the following themes held sway:

- Number plate parking;
- The compulsory taking of fingerprints for passports & ID cards;
- Highway section controls;
- Automatic Number Plate Recognition (ANPR) on highways;

- Municipal camera surveillance;
- Camera system @MIGO-BORAS;
- Medical confidentiality and Electronic Health Record/National Switch Point;
- Public transport chip cards;
- 'Smart' energy meters & 'smart' grid;
- Privacy in the workplace.

In almost all cases Privacy First was able to answer these questions satisfactorily, sometimes after consulting relevant experts within our network. In case of an absence of knowledge or experience relating to the issue at hand, Privacy First redirects people to other NGOs or to specialized government bodies.

5.3 Internet

The Privacy First website is our primary way to share news and voice opinions. Alongside the Dutch website www.privacyfirst.nl, there is also an English one: www.privacyfirst.eu. Since the end of 2013, both websites are sponsored by the privacy-friendly Dutch internet provider Greenhost. Since the start of 2014, the number of visitors on our websites has more than doubled; by now there are around 25,000 visitors each month. Privacy First is particularly active on Twitter and since the end of 2014 it has its own LinkedIn group for everyone who's concerned with privacy issues. Furthermore, Privacy First is active on Facebook and will continue to reserve space for (possibly anonymous) guest columns and articles on its websites. Midway through 2015, Privacy First will launch an entirely new website offering better opportunities for donations, anonymous communications, social media and citizen participation. Would you like to stay up-to-date on the latest developments around Privacy First? Then sign up for our digital newsletter by sending an email to info@privacyfirst.nl!

6. Events

In January 2014, Privacy First was again an official event supporter of the international Computers, Privacy & Data Protection (CPDP) conference in Brussels. Every year this large conference brings together hundreds of European and North-American privacy experts from science, government, business and civil society. Apart from that, in 2014 Privacy First gave guest lectures and presentations at the Amsterdam Platform for Privacy Research (APPR), the Rotterdam University of Applied Sciences and the Rietveld Academy. Symposiums and gatherings Privacy First actively took part in, in 2014, took place at the Platform for the Protection of Civil Rights (*Platform Bescherming Burgerrechten*), the Discussion Platform on Human Rights the Netherlands (*Breed Mensenrechten Overleg Nederland*), the Dutch Dialogue Marketing Association, the Netherlands Committee of Jurists for Human Rights (NJCM), the Study Association for International and European Law (URIOS), the Electronic Commerce Platform (ECP-EPN), the Platform Identity Management Netherlands, the Dutch Association for Media and Communication

law (VMC), the Society for Government Management (VOM), the Royal Netherlands Academy of Arts and Sciences (KNAW), the Ad de Jonge Centre and De Balie.

Apart from that, in 2014 Privacy First was consulted by the Netherlands Institute for Human Rights (privacy and the protection of personal data) and had personal meetings with, among others, the Dutch Data Protection Authority, the General Intelligence and Security Service, members of the House of Parliament belonging to the political parties D66, PvdA, VVD, ChristenUnie and SP, the Confederation of Netherlands Industry and Employers (VNO-NCW), the new Public Interest Litigation Project (PILP), Crowdsuing.nl, NL Confidential, Dime (Data is me) and IT's Privacy. Furthermore, Privacy First was involved in several dissertations and commissioned a legal dissertation on camera surveillance in the workplace.



Vincent Böhre (Privacy First) at the Reuring! Café of the Society for Government Management together with the General Intelligence and Security Service & the National Coordinator for Security and Counterterrorism, 19 January 2015, The Hague

Photo: Rein J., Shutterfly.com

On a regular basis Privacy First organizes networking drinks and theme nights for the public as well as for our volunteers, donors and experts from our network of journalists, scientists, lawyers and people working in ICT. Since 2012 these gatherings take place at the Privacy First office in the former building of the *Volkskrant* newspaper in Amsterdam. Because part of the *Volkskrant* edifice was being turned into a hotel (Volkshotel), Privacy First had decided to temporarily suspend these gatherings until after the summer of 2014, when the new hotel and café-restaurant Canvas opened their doors.

At the end of the year, Privacy First organized a successful pre-launch of its new initiative Privacy First Solutions in Canvas, with inspiring speakers of Greenhost and the National ThinkTank. It's Privacy First's intention to (co-)organize other events like this, both in our own office in the Volkshotel as well as elsewhere in the Netherlands. Would you like to receive an invitation to our forthcoming event? Send us an email and we'll put you on our guest list!



Martijn van der Veen (Privacy First) during the pre-launch of Privacy First Solutions, 2 December 2014, Amsterdam Photo: Maarten Tromp

7. Organization

Privacy First is an independent, ANBI (Institution for General Benefit) certified foundation that largely consists of volunteers. In 2014, the core of the organization of Privacy First consisted of the following persons:

- Mr. Bas Filippini (founder and chairman)
- Mr. Vincent Böhre (director of operations)
- Mr. Martijn van der Veen (advisor Privacy First Solutions).

In 2014, the group of Privacy First volunteers has remained stable and consists largely of professionals who structurally support the foundation, both as far as the actual work at hand is concerned (various privacy themes and translation services) as well as in terms of organization (ICT, fundraising, PR and photography). Apart from that, Privacy First can rely on a large network of experts from all corners of society, varying from scientists and legal experts and people working in ICT to journalists, politicians and public officials.

8. Finances

To carry out its activities, the Privacy First Foundation largely depends on donations. In recent years the number of Privacy First's donors has grown rapidly and in 2014 Privacy First's income has more than doubled. Furthermore, since the start of 2015, Privacy First receives financial support from the Democracy & Media Foundation for the benefit of our multiannual project Privacy First Solutions. It's Privacy First's constant policy to spend as much of its income on content-related issues and to keep the operational costs as low as possible. In principle, travel and lunch expenses are to be paid for on one's own account and internal communication (also by telephone) is done mostly on the internet, while expensive parties and other luxuries are out of the question. In this way every Euro is spent as effectively as possible for the benefit of the privacy of every Dutch citizen.

Annual Overview 2014 (Euro)

2013 (Euro)

Revenues:

Donations	73,933	32,938
Sublease	1,928	1,272
Miscellaneous	3,379*	273

*: Exemption from litigation costs by the Hague Court of Appeals in the Passport Trial by Privacy First et al.

Expenditures:

Personnel costs	42,901	27,956
Legal costs	33,389	348
Housing	3,464	5,089
Campaign costs	2,595	190
Events	1,868	577
Websites	1,156	758
Banking and insurance costs	783	548
Office costs	350	1,094
Travel costs	256	129
PO box and postage costs	252	213
Communications & PR	137	165
Promotional material	61	258
Miscellaneous	51	130

Would you like to support Privacy First? Then please donate on account number NL95ABNA0495527521 (BIC: ABNANL2A) in the name of the Privacy First Foundation in Amsterdam, the Netherlands. The Privacy First Foundation is recognized by the Dutch Tax and Customs Administration as an Institution for General Benefit (ANBI). Therefore your donations are tax-deductible.





PO Box 16799

1001 RG Amsterdam, the Netherlands

Telephone: +31-(0)20-8100279

Email: info@privacyfirst.nl

Website: www.privacyfirst.eu

Privacy First is registered in the Register of Foundations of the Amsterdam Chamber of Commerce under No. 34298157. RSIN/fiscal number: 819211710.