

~~PRIVACY~~
~~PRIVACY~~
~~INTERNATIONAL~~



The Right to Privacy in Denmark

Stakeholder Report
Universal Periodic Review
24th Session - Denmark

**Submitted by Privacy International and IT-Political
Association of Denmark**

June 2015

Introduction

1. This stakeholder report is a submission by Privacy International (PI), and IT-Political Association of Denmark (IT-Pol). PI is a human rights organisation that works to advance and promote the right to privacy and fight surveillance around the world. IT-Pol is a Danish digital rights organisation that works to promote privacy and freedom in the information society.
2. PI and IT-Pol wish to bring concerns about the protection and promotion of the right to privacy in Denmark before the Human Rights Council for consideration in Denmark's upcoming review.

The right to privacy

3. Privacy is a fundamental human right, enshrined in numerous international human rights instruments.¹ It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.
4. Activities that restrict the right to privacy, such as surveillance and censorship, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.²
5. As innovations in information technology have enabled previously unimagined forms of collecting, storing and sharing personal data, the right to privacy has evolved to encapsulate State obligations related to the protection of personal data.³ A number of international instruments enshrine data protection principles,⁴ and many domestic legislatures have incorporated such principles into national law.⁵

Follow up to the previous UPR

6. In the first cycle UPR review of Denmark, the issue of privacy was already raised. In the National Report, Denmark noted "*thorough examination has been made of whether the rules [introduced by the new anti-terror packages]*

¹ Universal Declaration of Human Rights Article 12, United Nations Convention on Migrant Workers Article 14, UN Convention of the Protection of the Child Article 16, International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter on the Rights and Welfare of the Child, Article 11 of the American Convention on Human Rights, Article 4 of the African Union Principles on Freedom of Expression, Article 5 of the American Declaration of the Rights and Duties of Man, Article 21 of the Arab Charter on Human Rights, and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; Johannesburg Principles on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.

² Universal Declaration of Human Rights Article 29; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; see also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/HRC/17/34.

³ Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (art. 17).

⁴ See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General Assembly resolution 45/95 and E/CN.4/1990/72)

⁵ As of December 2013, 101 countries had enacted data protection legislation: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014). Available at SSRN: <http://ssrn.com/abstract=1951416> or <http://dx.doi.org/10.2139/ssrn.1951416>

*comply with Denmark's human rights obligations, including the obligation to guarantee every individual the right to privacy*⁶ and *"found no reason to propose changes on the basis of the legal protection"*.

7. The summary stakeholders' report included concerns raised by Amnesty International on how the counter-terrorism measures in Danish legislation gave rise to human rights violations including the right to privacy,⁷ and recommended that *"Denmark ensure the right to privacy including by strengthening judicial oversight of requests to intercept electronic or telephonic communications"*.⁸
8. The Working Group report included concerns expressed by the Netherlands on the same issue in view of Denmark's increased police powers, since 2011, to investigate and prevent terrorism.⁹ It thus recommended Denmark to *"carry out an inclusive evidence-based evaluation of the Danish antiterrorism legislation"*.¹⁰ Denmark did not accept this recommendation but merely noted it.

Domestic laws related to privacy

9. The 1953 Constitution of Denmark protects the right to privacy under Section 72: *"The dwelling shall be inviolable. House searching, seizure, and examination of letters and other papers as well as any breach of the secrecy to be observed in postal, telegraph, and telephone matters shall take place only under a judicial order unless particular exception is warranted by Statute."*
10. Other legislation including provisions relating to the protection of privacy and data protection are the Criminal Code of 1930, the Act on Video Surveillance, the Administrative Procedures Act of 1985, the Data Protection Act of 2000, the Freedom of Information Act of 2013, the Health Care Act of 2005, and the Payment Services Act of 2009.

International obligations relating to privacy

11. Denmark has ratified the International Covenant on Civil and Political Rights ('ICCPR'), which under Article 17 of the ICCPR, which reinforces Article 12 of the UDHR, provides that *"no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation"*.
12. The Human Rights Committee has noted that states parties to the ICCPR have a positive obligation to *"adopt legislative and other measures to give effect to the prohibition against such interferences and attacks as well as to the protection of this right [privacy]."*
13. The European Convention on Human Rights was domesticated into Danish law in 1992, and Article 8 reads:

⁶ A/HRC/WG.6/DNK/1, para 78

⁷ A/HRC/WG.6/11/DNK/3, para 78

⁸ A/HRC/WG.6/11/DNK/3, para 79

⁹ A/HRC/18/4, para 79

¹⁰ A/HRC/18/4, para 106.133

“1. Everyone has the right to respect for his private and family life, his home and his correspondence.

14. 2. There shall be no interference by a public authority with the exercise of this right except such as it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

15. Denmark is bound to the Charter of Fundamental Rights of the European Union, Articles 7 and 8 of which relate to the right to privacy and the protection of personal data respectively.

16. Denmark is a member of the Council of Europe. It has signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108).

Areas of concern

COMMUNICATIONS SURVEILLANCE

17. In a response submitted by the Danish Human Rights Institute to the consultation process of the OHCHR regarding the General Assembly Resolution 68/167¹¹, it was noted that besides the Data Protection Act, there are no specific national measures to ensure human rights compliance of procedures, practices and legislation regarding the surveillance of communications, apart from the general privacy and data protection provisions in the Constitution and the data protection framework.¹²

I. Law enforcement

18. The police and the Danish Security and Intelligence Service (PET), which is in charge of domestic intelligence operations and is part of the Danish police, must request a court order in order to obtain warrants to intercept private communication.

19.

20. The PET “is responsible for identifying, preventing and countering threats to freedom, democracy and safety in Danish society. This applies to threats in Denmark as well as threats directed at Danish nationals and Danish interests abroad.”¹³

21. In the current legislative framework regulating interception in Denmark, signal intelligence and real-time access can only be requested by presenting the telecommunication providers with a court order. The criminal proceedings requirement applicable for the police to abide by are regulated by Chapter 71

¹¹ “The Right to Privacy In the Digital Age”

¹² Response from the Danish Institute for Human Rights to the consultation process of the OHCHR regarding General Assembly Resolution 68.167 “The Right to Privacy in the Digital Age”, 7 March 2014, pp. 3
<http://www.ohchr.org/Documents/Issues/Privacy/DanishHR.pdf>

¹³ Danish Security and Intelligence Service, *About PET*. Available at:
<https://www.pet.dk/English/About%20PET.aspx>

of Act No. 1139 of 24 November 2013 (the Administration of Justice Act). The only exception is the Center For Cybersecurity which may initiate lawful interception without a court order as enshrined by Chapter 4 of the Act No. 713 of 26 June 2014, but only with regards to information security.¹⁴

22. With regards to encrypted data, if a telecommunication provider has an integrated encrypted system, it must be sure to provide the police access to the data in a non-encrypted form, as required by Section 10 of the Telecommunications Act No. 169 of 3 March 2011. If the data is encrypted by the customer's own systems, the telecommunication provider is not required to decrypt the data, as the comments of the Telecommunication Act note that this will be technically impossible. There is no key disclosure law requiring a suspect in a criminal case to release encryption keys or decrypt data.¹⁵
23. The Ministry of Justice has the authority to investigate police's non-compliance with the procedures established by law to conduct communications surveillance.
24. The data reading provision introduced in 2002 as Section 791 b of the Administration of Justice Act¹⁶ allows the police to access non-publicly available information in a computer system using trojan software or other equipment. This practice amounts to computer network exploitation (CNE), commonly known as hacking, which is an extremely intrusive form of surveillance. It can yield information sufficient to build a total profile of a person, from their daily movements to their most intimate thoughts. There is no restriction on the type of information that the police may obtain through this system.
25. There is very little publicly available information about the use of this power, and there has been little public or Parliamentary scrutiny since this provision was adopted in 2002. The statistics on wire-tapping do not include the activities of the PET. The only public information about the use of data reading is a report on anti-terror packages from 2002 to 2006 where it is noted that the PET has used this authority an unspecified number of times.¹⁷ In January 2012, the Minister of Justice refused to answer a parliamentary question about how often the data reading provision was used by the police and the PET.¹⁸

II. Intelligence agencies

26. The Danish Defence Intelligence Services (DDIS) is in charge of foreign intelligence, and also military intelligence service.

¹⁴ See: Chapter 4: Cyber-security, Interception, Encryption and Data Retention, para 4.1. Available at: <http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms.-media-and-internet-laws-and-regulations/denmark>

¹⁵ Chapter 4: Cyber-security, Interception, Encryption and Data Retention, para 4.4. Available at: <http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms.-media-and-internet-laws-and-regulations/denmark>

¹⁶ Act amending . Available at: <https://www.retsinformation.dk/forms/r0710.aspx?id=1344>

¹⁷ Review of anti-terror package I (2002) and II (2006), Ministry of Justice, 9 September 2010, section 3.2.5 Available at: <http://www.ft.dk/samling/20091/almindel/reu/bilag/699/889250.pdf>

¹⁸ Minister of Justice, Answer to question no . 254 (General . Part) submitted by the Parliamentary Legal Affairs Committee to the Minister of Justice 30 November 2011, 17 January 2012, Available at: <http://www.ft.dk/samling/20111/almindel/reu/spm/254/svar/849995/1067480.pdf>

27. They “analyse, and disseminate information concerning conditions abroad which are of importance to Denmark’s security, and to the security of Danish military units deployed on international missions. Intelligence activities include collection of information of political, financial, scientific, and military interest. It also includes international terrorism, extremists, international arms trafficking, and the proliferation of weapons of mass destruction.”¹⁹
28. The DDIS is regulated by Act No. 602 of 12 June 2013 on the Defence Intelligence Service, as amended by Section 3 of the Act No. 1624 of 16 December 2013.²⁰
29. Under this Act, DDIS can collect any type of information as long as the operation is directed at conditions abroad which are important to Danish security interests. Targeted electronic surveillance against Danish citizens is currently now allowed. In many cases, raw data from mass surveillance activities will include information about Danish persons²¹. Under Section 3(2) of the DDIS law, DDIS is allowed to process information about Danish citizens if it is discovered by chance in connection with operations directed against conditions abroad. The safeguards for Danish citizens in the DDIS law only apply when raw data is analysed, not when it is collected or shared with foreign intelligence agencies.

Concerns on the respect and protection of the right to privacy in the current Act

30. Problematic provisions in the existing Law 602/2013²² include:
- Chapter 3 'Internal Data Processing',
 - Section 4 (3) mandates the Minister of Defence in laying down new rules on the treatment of Danish intelligence data. This provision gives the Ministry of Defence wide discretion in setting up the conditions of state surveillance (of foreigners abroad) resulting in the risk of unlawful interference with the right to privacy;
 - Section 6 permits the DDIS to store raw data, unprocessed primary data collected from the source, for a period of up to 15 years unless requested by another law (Para 2) and deletion may be omitted for essential reasons relating to defence intelligence tasks in accordance with Section 1.1.
 - Chapter 6 'Rules of access, etc.'
 - Section 9 denies a natural or legal person the right to access information held by the DDIS;
 - Section 11 exempts defence intelligence activities from freedom of information requests and provisions of the Public Administration Act and the data protection legislation.
 - Lower protection for foreigners
 - Section 6(1) requires data about Danish persons to be deleted after 15 years, but there is not deletion limit for foreigners;

¹⁹ Danish Defence Intelligence Service, *About DDIS*. Available at: <http://fe-ddis.dk/eng/About-DDIS/Pages/About-DDIS.aspx>

²⁰ Act 602 of 12 June 2013. Available at: <https://www.retsinformation.dk/Forms/R0710.aspx?id=152195&exp=1>

²¹ This refers to Danish citizens, according “Comments regarding specific provisions” the definition being applied is as follows: 1) Danish nationals, 2) Nordic citizens and other foreign nationals who live in Denmark and are registered with the authorities, and 3) asylum seekers with (known) stay in Denmark for more than 6 months.

²² Law 602/2013 on Defence Intelligence Service, <https://www.retsinformation.dk/Forms/R0710.aspx?id=152195&exp=1>

- Section 7(2) requires an assessment to be made prior to sharing information about Danes with foreign intelligence agencies, but such a requirement does not exist for data shared about foreigners;
- Section 10 allows a Danish citizens and residents to call on the Oversight authority of the DDIs, the TET, to investigate whether information about themselves is being unlawfully processed, but this right is not extended to foreigners
- Ineffective oversight
 - Chapter 9 established an oversight mechanism for the DDIS but it has very little powers.²³

New anti-terrorism package and relevant legal reform

31. On 19 February 2015, the Danish Government presented a new 12-point 'anti-terror initiative'²⁴. This announcement came in the aftermath of the Charlie Hebdo attacks on 7 January 2015 in Paris²⁵, and then the shooting in Copenhagen on 14 February 2015²⁶.
32. As part of these anti-terrorism measures, on 5 May 2015, the law L 200 for the amendment of Act No. 602 (2013) on the Danish Defence Intelligence Services, was proposed in Parliament.²⁷
33. This new anti-terror package is the third since 2001, and will focus on expanding surveillance measures in Denmark through increased budgets and new technologies, but also new powers for the intelligence services including the DDIS and the PET.²⁸
34. The draft bill focuses on conducting surveillance of Danes abroad (very broad definition – see comment below) engaging in or facilitating activities that may involve or increase terror threats against Denmark and Danish interests.
35. Some members of Parliament, as well as members of civil society have strongly criticised the proposed bill arguing that the new provisions introduce inherently disproportionate and indiscriminate measures amounting to mass surveillance of communications of Danish citizens particularly, thereby violating Article 17 of the ICCPR. \
36. The main concerns with the bill proposed on 5 May 2015, include:

²³ Response from the Danish Institute for Human Rights to the consultation process of the OHCHR regarding General Assembly Resolution 68.167 "The Right to Privacy in the Digital Age", 7 March 2014, pp. 3
<http://www.ohchr.org/Documents/Issues/Privacy/DanishIHR.pdf>

²⁴ Ministry of Justice of Denmark, Et stærkt værn mod terror 12 nye tiltag mod terror, February 2015. Available at: <http://www.justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2015/Et%20st%C3%A6rkt%20v%C3%A6rn%20mod%20terror.pdf>

²⁵ The Guardian, *Charlie Hebdo magazine attack: vigils held as French hunt suspects – as it happened*, 8 January 2015, Available at: <http://www.theguardian.com/world/live/2015/jan/07/shooting-paris-satirical-magazine-charlie-hebdo>

²⁶ Johnston, C., *One dead and three injured in Copenhagen 'terrorist attack'*, The Guardian, 14 February 2014. Available at: <http://www.theguardian.com/world/2015/feb/14/copenhagen-blasphemy-lars-vilks-prophet-muhammad-krudttonden-cafe>

²⁷ Bill No. 200, Motion to Law amending the Law on Defence Intelligence Service (FE) (Strengthened efforts towards activities abroad, which may pose a terrorist threat against Denmark and Danish interests), para. 1. Available at: http://www.ft.dk/Rlpdf/samling/20141/lovforslag/L200/20141_L200_som_fremsat.pdf

²⁸ Ibid, para. 1

- The power given to the DDIS to conduct targeted surveillance of Danes abroad, which it was previously not permitted to do so as noted above;²⁹
- The suspicion standards has been lowered to a standard of “specific reasons to believe” instead of “presumed suspect” (as defined in the Administration of Justice Act), The comments of the proposed Section 3(3) in the DDIS law state that targeted surveillance of Danes abroad can be done solely for intelligence gathering at an early stage before there is grounds for a criminal investigation in co-operation with PET and does not require that the PET have a case opened against the Dane being targeted, as previously required for DDIS to be able to intervene;³⁰
- The proportionality test is very weak. The court cannot consider the specific methods for targeted acquisition, which in many situations will affect the degree of interference with the right to privacy. Even though the court is formally required to consider the proportionality of the targeted surveillance, the comments of the law specifically state that the proportionality requirement capabilities including including electronic retrieval (Signals Intelligence/
- SIGINT), including network retrieval (Computer Network Exploitation /CNE), physical collection (person sources), partners, and by contacting third parties (*foreign intelligence sharing*) in general;³¹
- The collection methods are completely unregulated by the proposed Section 3(3) and are entirely at the discretion of DDIS. This authorises targeted searches on Danes in previously collected raw data, either by DDIS or its foreign partners.³² There is no requirement that the information relates to activities of Danes abroad, and it could even be communication for a target in Denmark collected illegally (under Danish law) by DDIS' foreign partners.
- Unlike police wiretapping under the Administration of Justice Act, there is no requirement that DDIS notifies a person that have been subject to targeted surveillance. PET can use the information collected by DDIS in a subsequent criminal case, and the suspect will be unaware of how the state prosecutor obtained this part of the evidence.³³
- The lawyer appointed in the court case for targeted DDIS surveillance will have limited options under the proposed Section 3a for representing his/her client. The evidence presented by DDIS can only be reviewed at the offices of the court, and DDIS will not be required to inform the lawyer of the source of the evidence presented. The hearing will be held in camera i.e. not be public.³⁴

37. Other provisions in the '12 *point plan*' that have been addressed through other reforms, include *the establishment of a national PNR system*. Under

²⁹ It is important to note that this provision would apply to : 1) Danish nationals, 2) Nordic citizens and other foreign nationals who live in Denmark and are registered with the authorities, and 3) asylum seekers with (known) stay in Denmark for more than 6 months.

³⁰ Bill No. 200, Motion to Law amending the Law on Defence Intelligence Service (FE) (Strengthened efforts towards activities abroad, which may pose a terrorist threat against Denmark and Danish interests), *Comments regarding specific provisions*, pp 12-13. Available at: http://www.ft.dk/R1pdf/samling/20141/lovforslag/L200/20141_L200_som_fremsat.pdf

³¹ Ibid, pp. 13. Also see: See 3.1.2 “On Internal treatment of information under the DDIS Law §4 and 5” <http://www.tet.dk/wp-content/uploads/2014/11/%C3%85rsrede%C3%B8relse-om-kontrol-af-PET-i-2014.pdf>

³² Ibid, page 13; Ministry of Defence comments on the consultation responses for the draft bill of 10 April 2015, pp 7-8. Available at: <http://www.ft.dk/samling/20141/lovforslag/l200/bilag/1/1527071.pdf>

³³ Ministry of Defence comments on the consultation response for the draft bill of 10 April 2015, pp 6-7. Available at: <http://www.ft.dk/samling/20141/lovforslag/l200/bilag/1/1527071.pdf>

³⁴ Comments regarding specific provisions in the bill of 5 May 2015, pp 14-15. Available at: http://www.ft.dk/R1pdf/samling/20141/lovforslag/L200/20141_L200_som_fremsat.pdf

Section 4 of the plan, the government will establish its own national system for passenger name record (PNR) starting with providing with the PET with access to all relevant information provided by airlines on their passengers. The document notes, that it will align itself as far as possible with the future European PNR system, which has been discussed since 2007³⁵, but as result of legality and data protections concerns has yet to be finalised. Such a decision is concerning as PRN systems raise concerns around reliability, deduction of sensitive data, profiling, discrimination and long data retention periods.

38. The Danish government has already submitted a legislative proposal³⁶ for increased access PNR to the Danish Security and Intelligence Service (PET).³⁷ This expansion of access to the PET is concerning given that it exempts from the Data Protection Act, and that the conditions for accessing the information are very vague, and would allow the PET to collect any information contained in the PNR as long as it is can justify it is relevant for combatting terrorism. Further, since the PET can share data with the DDIS, and the DDIS can share data about non-Danish citizens with foreign intelligence, it is likely to be shared with allied agencies. Foreign airlines will be required to provide PNR data about their Danish destinations to PET even in situations where their national data protection law does not permit this exchange of information.³⁸
39. The current proposal also does not include³⁹:
- a right to access
 - a right to rectification
 - safeguards or limitations on the use of the PNR data for profiling of citizens not suspected of involvement in terrorist activities

40. Other provisions included in the '12 point plan' that remain of concern but have not yet emerged in proposed legislation, include:

Social media monitoring

41. Under Section 2 of the plan, the government notes that it will invest further funds to obtaining technologies and staff for strategic and tactical data analysis and processing operations, including the analysis of social networks. Such capabilities will be given to the police and the Danish Security and Intelligence Service (PET), The government argues that such operations will enable them to identify potential threatening individuals prior to attacks or other serious crimes being committed. On 19 February 2015, the Danish Passport Act was amended so that passports of suspected foreign fighters can be seized.⁴⁰ The decision to seize a citizen's passport can be based on social media posts. The implications for freedom of expression on social media have not been properly analysed by the Danish government.

³⁵ See: European Commission, Migration and Home Affairs, *Passenger Name Record (PNR)*. Available: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index_en.htm

³⁶ Draft bill on amending Law on Security Intelligence Service and the Customs Act (Police Intelligence access to airline passenger information in terrorism cases and SKAT's handling of airline passenger information in connection with customs control). Available at: <http://hoeringsportalen.dk/Hearing/Details/49480>

³⁷ EDRI, *New Danish PNR system will rival the EU PNR Directive*, 22 April 2015. Available at: <https://edri.org/new-danish-pnr-system-will-rival-the-eu-pnr-directive/>

³⁸ Ministry of Justice comments on the consultation response for the draft PNR bill of 10 April 2015, page 8. Available at: <http://www.ft.dk/samling/20141/lovforslag/1204/bilag/1/1526722.pdf>

³⁹ EDRI, *New Danish PNR system will rival the EU PNR Directive*, 22 April 2015. Available at: <https://edri.org/new-danish-pnr-system-will-rival-the-eu-pnr-directive/>

⁴⁰ Law L 99 to amend the Passport Act. Available at: http://www.ft.dk/samling/20141/lovforslag/L99/som_fremset.htm#dok

Access to pre-paid SIM cards

42. The government will examine the establishment of a mandatory registration system for all SIM cards, including pre-paid cards, which currently allow user not to register. This is of extreme concern as SIM registration, in effect, eradicates the ability of mobile phone users to communicate anonymously. As repeatedly highlighted by the UN Special rapporteur on freedom of expression, (in 2013 and in 2015) any limitations to anonymity further aggravates the vulnerability of users to State surveillance.

Increased capacity for decryption

43. Section 6 of the plan notes the decision of the government to strengthen the DDIS collection of electronic information, including by increasing its capacity to decrypt. As recognised by experts, including the UN Special Rapporteur on freedom of expression (2015 report), encryption is an essential tool available to individuals to maintain and protect their anonymity, that they can use to mitigate interferences with their right to privacy and freedom of expression. The threat of decrypting communications will have a direct chilling effect on individuals to feel secure and safe to communicate online. It is essential that the power to obtain decryption of information be strongly regulated.

Access to communications data and data retention

44. Under the Act on Electronic Communications Network and Services, Act No. 169 of 3 March 2011 (the "Tele Act"), telecommunications providers must ensure that their network and services are set-up as to allow the police to access historic user data and intercept current data.⁴¹
45. A major concern is the continued use of telecommunications data retention policies in contradiction of a recent decision by the European Court of Justice (CJEU). In April 2014, the CJEU struck down the EU-wide data retention policy calling it mandatory data retention "an interference with the fundamental rights of practically the entire European population...without such an interference being precisely circumscribed by provisions to ensure that is actually limited to what is strictly necessary".
46. On 2 June 2014, the Danish government provided a response to the CJEU ruling⁴² noting that, following a legal analysis by the Ministry of Justice, it had concluded that the Danish data retention law, despite being a transposition of the annulled Directive and covering the entire population as the Directive, was not in conflict with the Court's judgement nor the EU Charter of Fundamental Rights.
47. On a positive note, the Minister of Justice repealed the session logging provision in the administrative order for data retention. This was not part of the EU Data Retention Directive 2006/24/EC, but the Danish government had chosen to expand on the communication data the ISP should retain to include session logging information (which refers to source and destination IP

⁴¹ Chapter 4: Cyber-security, Interception, Encryption and Data Retention, para 4.2. Available at: <http://www.iclg.co.uk/practice-areas/telecoms-media-and-internet-laws/telecoms.-media-and-internet-laws-and-regulations/denmark>

⁴² Note on importance of the Court's judgment of 8 April 2014 in Joined Cases C -293/ 12 and C- 594/12 (on logging Directive) for Danish logging rules. Available (in Danish) at: <http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2014/Notat%20om%20logningsdirektivet.pdf>. See English summary available here: <https://edri.org/denmark-data-retention-stay-despite-cjeu-ruling/>

addresses, port numbers, and session types e.g. TCP or UDP).⁴³ Given that the legal basis for data retention in Denmark is Section 786(4) in the Administration of Justice Act, which authorises the Minister of Justice to lay down the precise data retention requirements in an administrative order, the Minister was able to repeal session loggings without having to amend the law.

48. However as the Ministry of Justice plans to revise the data retention law in 2015-16, it will be important to monitor whether they decide to re-introduce the session logging as reported by the Danish newspaper Berlingske in January 2015⁴⁴ Especially as the Retention Order Guidelines have yet to be updated to take into account this amendment. It is important to note that the Danish police has noted that session logging information has not been helpful in criminal investigations but on the contrary, the availability of such data has caused practical problems.⁴⁵
49. The lawfulness of data retention policies under human right standards has been called into question by the CJEU, and Denmark should give serious consideration as to whether the continued requirement for ISPs to retain data on the entire population is in fact a violation of their obligations with respect to the rights to privacy and freedom of expression. Retention must be targeted, justified and subject to prior judicial authorisation and oversight.

Establishment of Center for Cyber Security

50. Act No. 713 of 25 June 2014 on the Centre for Cyber Security⁴⁶ was adopted. The Act establishes a Center for Cyber Security within the Danish Defence Intelligence Service.
51. Chapter 3 notes that the tasks of the Centre are to “*task to detect, analyse and contribute to addressing security incidents*”.
52. Chapter 4 outlines the provisions regulating the powers of the Centre for Cyber Security to conduct the interception of communications. The following provisions are of concern⁴⁷ and pose significant risks to the right to privacy and contradict Denmark's national and international human rights laws and standards.
53. The Centre for Cyber Security can process packet and traffic data generated by networks of affiliated authorities (Section 4), and authorities at the Ministry of Defence, without a court order (Section 5).
54. The law expands the range of public institutions and private companies which can be monitored by the Centre for Cyber Security, Private companies can

⁴³ Lund, J., *Danish government wants more data retention and plans to re-introduce session logging*, T-Politisk Forening, 7 January 2015. Available at: <http://itpol.dk/notater/more-data-retention-in-Denmark-session-logging-coming-back>

⁴⁴ Dahlgaard, M., and Jung, E., *Politiet vil genindføre overvågning af danskere på internettet*, Nationalt, 7 January 2015. Available at: <http://www.b.dk/nationalt/politiet-vil-genindfoere-overvaagning-af-danskere-paa-internetet>

⁴⁵ Masnick, M., *Danish police admit that data retention hasn't helped at all*, TechDirt, 29 May 2013. Available at: <https://www.techdirt.com/articles/20130523/02542423184/danish-police-admit-that-data-retention-hasnt-helped-all.shtml>

⁴⁶ Act No. 713 of 25 June 2014 on Centre Cyber Security, Available: <https://www.retsinformation.dk/Forms/R0710.aspx?id=163853&exp=1>

⁴⁷ Järvinen, H., *Danish government plans to create a Centre for Cybersecurity with privacy-invasive powers*, EDRI, 12 March 2014. Available at: <https://edri.org/danish-government-plans-create-center-cybersecurity-privacy-invasive-powers/>

volunteer to be monitored, and all of this data processing is exempt from the Danish data protection framework.

55. Data retention for 3 years for data related to a security incident, and 13 months for all other (Section 17), this is an expansion of previous cyber crime law which for packets was set as fourteen days
56. The Danish Institute for Human Rights expressed concern that the Centre for Cyber Security, which includes the Danish GovCert, which is the national point of contact for internet related security incidents regarding national services and infrastructure and the military equivalent (MilCert), are exempted from the Act relating to the processing of personal data and thus the oversight of the Data Protection Authority (Section 8).⁴⁸
57. Whilst recognising a State's legitimate security concerns and the need to protect their citizens, it is essential that it does not do so as the expense of the rights of individuals, such as the right to privacy, freedom of expression and association.
58. Any cybersecurity policy must align itself with Denmark's national and international human rights obligations to respect and protect the right to privacy of its citizens.

Foreign spying

59. In its 2014/15 annual report, Amnesty International noted how the Danish authorities had refused investigate allegations of unlawful surveillance by foreign intelligence agencies in Denmark, following the revelations made by US whistleblower Edward Snowden.
60. The request came from Danish members of Parliament and the public, but the Danish government said that it did "not find reason to believe" that US intelligence agencies were carrying out "illegal surveillance activities targeting Denmark or Danish interests."⁴⁹
61. Despite this position taken by the Danish government, follow-up investigative research by the Danish newspaper, Dagbladet Information, in collaboration with the Intercept, revealed documentation pointing towards the involvement of Denmark (amongst others), in a NSA programme called RAMPART-A.⁵⁰ The programme related to the creation of a network of intelligence agencies whereby foreign partners would "provide access to cables and host U.S. equipment" which allowed the NSA to tap into various "congestion points around the world" in order to intercept phone calls, faxes, e-mails, internet chats, data from virtual private networks, and calls made using Voice over IP software like Skype.⁵¹

⁴⁸ Response from the Danish Institute for Human Rights to the consultation process of the OHCHR regarding General Assembly Resolution 68.167 "The Right to Privacy in the Digital Age", 7 March 2014, pp. 3
<http://www.ohchr.org/Documents/Issues/Privacy/DanishHR.pdf>

⁴⁹ Amnesty International, *Amnesty International Report 2014/15: Denmark*. Available at:

<https://www.amnesty.org/en/countries/europe-and-central-asia/denmark/report-denmark/>

⁵⁰ Gallagher, R., How Secret partners expand NSA's surveillance dragnet, *The Intercept*, 19 June 2014. Available at:
<https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>

⁵¹ Ibid

62. Furthermore, a classified presentation revealed information about the NSA's top-secret spying agreements with 33 third-party countries include Denmark as well as 17 other EU Member States.⁵²
63. A report on '*Mass Surveillance*' by the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe⁵³ notes Denmark's close historic collaboration with the US dating back from the late 1990s, noting that it was under "*significant pressure*" to update its wiretapping laws to be able to partner with the NSA and its "9-eyes", and then for a period of two years it provided "technical assistance" to decrypt codes of intercepted communication and to tap internet communications.⁵⁴
64. The Danish Defence Intelligence Service neither confirmed, nor denied the partnership with the NSA.⁵⁵
65. The CoE Parliamentary Assembly report noted ⁵⁶ revelations by the New York Times that the NSA had monitored communications in countries, including the host – Denmark, which were preparing for the climate change talks in view of the Copenhagen Climate Summit in 2009.⁵⁷
66. Such covert surveillance partnerships directly threaten the right to privacy as well as the security of the telecommunication network and infrastructure. The Danish government must ensure it meets its international legal obligations to protect the privacy from external threats and mass, unlawful, disproportionate and unnecessary interference with their privacy.
67. The allegations made above by the various sources, which provide evidence of violations of the right to privacy must be effectively investigated by an independent commission of inquiry. Such independent investigation have been initiated by other Europeans following similar allegations.

DATA PROTECTION

68. Originally governed by two acts, the Private Registers Act of 1978 and Public Authorities's Registers Act of 1978, data protection is now regulated by the Act on processing of Personal Data adopted on 1 July 2000, which implemented the EU Data Protection Directive.
69. Data processing within the police sector is exempted from the act.⁵⁸

⁵² Open Rights Groups, *Data retention in the EU following the CJEU ruling*, updated on April 2015. Available at: https://www.openrightsgroup.org/assets/files/legal/Data_Retention_status_table_updated_April_2015_uploaded_finalwithadditions.pdf

⁵³ Committee on Legal Affairs and Human Rights, *Mass Surveillance*, 26 January 2015, para 28. Available at: <http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf>

⁵⁴ Post Online, *Spying program with NSA goes back years*, 30 June 2014. Available at: <http://cphpost.dk/news/spying-program-with-nsa-goes-back-years.10050.html>

⁵⁵ Geist, A., Gjerding, S., Moltke, H. and Poitras, L., *NSA 'third party partners tap the Internet backbone in global surveillance program*, Information, 19 June 2014. Available at: <http://www.information.dk/501280>

⁵⁶ Committee on Legal Affairs and Human Rights, *Mass Surveillance*, 26 January 2015, para 54. Available at: <http://website-pace.net/documents/19838/1085720/20150126-MassSurveillance-EN.pdf>

⁵⁷ Vidal, J., and Goldenberg, S., *Snowden revelations of NSA spying Copenhagen climate talks spark anger*, The Guardian, 30 January 2014. Available at: <http://www.theguardian.com/environment/2014/jan/30/snowden-nsa-spying-copenhagen-climate-talks>

⁵⁸ Response from the Danish Institute for Human Rights to the consultation process of the OHCHR regarding General Assembly Resolution 68.167 "The Right to Privacy in the Digital Age", 7 March 2014, pp. 6 <http://www.ohchr.org/Documents/Issues/Privacy/DanishIHR.pdf>

70. There are various on-going initiatives which pose a concern regarding the measures taken to protect the personal data of citizens including:

Medical data:

71. Making medical data available for private and public sector research is a priority for the Danish government. It is actively used to attract pharmaceutical companies to Denmark.⁵⁹ All public sector databases in Denmark use the Personal Identification Number (CPR), including medical data, so it is easy to crosslink medical data with socio-economic data. The majority of the medical databases are available to researchers at little or no cost once their research project has been approved.⁶⁰ In many cases, medical data is used for research without consent from the citizens involved. This is possible because of a liberal interpretation of the research exemption in Section 10(1) of the Data Protection Act. Names and addresses of citizens, as well as complete diagnoses, can be shared with private pharmaceutical companies in personally identifiable form, so that the companies can contact the individuals and ask whether they wish to participate in medical trials. In one case, a large number of Danish citizens were contacted by a pharmaceutical company about a diagnosis for a heart condition which several of the citizens were unaware of themselves.⁶¹

Leaked social security data⁶²:

72. In April 2014, it was reported that the 900,000 Danish social security number and/or national identification number (CPR) were inadvertently exposed by the Danish Ministry of Economic Affairs and the Interior and the data was available online for one hour.

Data leak from CSC.⁶³

73. Computer Science Corporation, which handles a large amount of the public-sector data processing in Denmark, was subject to a major hacking incident between April and August 2012, whereby information from several sensitive databases was leaked. This was not discovered until the beginning of 2013. An investigation by the Center for Cybersecurity has revealed several deficiencies in the IT-security practices by CSC. The report from August 2014 is classified, but was obtained by the newspaper Politiken,⁶⁴ The data controllers for the leaked databases are government institutions which have the ultimate responsibility for maintaining adequate data security, a responsibility which they have neglected in the CSC case.

Recommendations

⁵⁹ Ministry of Foreign Affairs, Denmark - *The Heart of Life Sciences for Clinical Trials*, Invest in Denmark, February 2013, Volume 5, Issue 1. Available at:

http://www.investindk.com/~media/Files/Articles/Denmark_The_Heart_of_Life_Sciences_for_Clinical_Trials.ashx

⁶⁰ Ibid

⁶¹ DR, *Firma fik helbredsoplysninger om 84.000 personer*, 10 October 2013. Available at:

<http://www.dr.dk/Nyheder/Indland/2013/10/10/10060546.htm>

⁶² Lewis, D., *900,000 Danish Social Security Numbers Leaked*, 7 April 2014, Forbes, Available at:

<http://www.forbes.com/sites/davelewis/2014/07/04/900000-danish-social-security-numbers-leaked/>

⁶³ Hamill, J., *Pirate Bay Warf accused on hacking international police database*, The Register, 7 June 2013.

Available at:

http://www.theregister.co.uk/2013/06/07/pirate_bay_founder_named_as_suspect_in_paneuropean_police_database_hack/

⁶⁴ Sorgenfri Kjaer, J., *CSC-sagen: En stak papirer, som når fra Jorden op til Månen og tilbage igen*, Politiken, 12

October 2014. Available at: <http://politiken.dk/forbrugogliv/digitalt/internet/ECE2422372/csc-sagen-en-stak-papirer-som-naar-fra-jorden-op-til-maanen-og-tilbage-igen/>

74. We recommend that the government of Denmark:

- Recognise and take steps towards compliance with international human rights law and standards by ensuring the application of the following principles to communication surveillance, namely legality, legitimacy, necessity, adequacy, proportionality and respecting process of authorisation from a competent judicial authority; due process, user notification, transparency, public oversight and respect for the integrity of communications and systems as well as ensuring safeguards against illegitimate access and right to effective remedy;
- Ensure that its communication surveillance laws, policies and practices adhere to international human rights law and standards and respect the right to privacy;
- Ensure, in particular, that all anti-terrorism measures, including those currently proposed, are in respect with human rights and fundamental freedoms enshrined in its Constitution and protected by international human rights law and standards, particularly the right to privacy;
- Make clear the basis and limits of any intelligence sharing arrangements their intelligence agencies have with foreign intelligence agencies in order to ensure that intelligence sharing arrangements are in accordance with national and international human right law and provide to Danish citizen's a clear understanding of the legal nature of the relationships;
- Ensure that any information accessed by the DDIS from data collected by other (foreign) intelligence agencies is subject to the same protection and safeguards as information intercepted by Denmark;
- Effectively investigate the credible allegations of unlawful surveillance by foreign intelligence agencies and the part played by the Danish security services/government;
- Review the data retention framework in order to ensure its compliance with the European and international standards;
- Review the data protection framework in order to ensure its compliance with the European data protection standards;
- Investigate and take necessary measures to address security breaches of personal data which directly threaten the right to privacy of its individuals, and ensure those those responsible are sanctioned and case of recognised violations, victims have access to redress.