International Cyber Developments Review (INCYDER)

2014 Q2

In this issue:

Contact:
NATO Cooperative Cyber Defence Centre of Excellence
Filtri tee 12, Tallinn 10132, Estonia
publications@ccdcoe.org
www.ccdcoe.org

We are glad to announce that in order to make the project and its database more accessible, we are currently preparing a website for the INCYDER project. The new website is to be launched this autumn and will allow for more frequent news updates and include a comprehensive and fully searchable database with a collection of cyber security related legal and policy documents from major international organisations.

About

Given the cross-border nature of cyberspace, cyber security has become a relevant issue for everyone, whether they have an international, regional or domestic perspective. In addition to nation states, numerous international and regional organisations and other international entities have launched initiatives related to cyber security. Documents on cyber security have been issued, both in the form of non-binding instruments such as declarations, recommendations, policies and strategies, and also in binding documents such as conventions, directives, regulations and action plans. One way or another, all of these developments feed into national and international organisations' and other stakeholders' planning, strategy and capability development, as well as their cyber security investment analysis and decision making. For the wider audience they reflect overall trends and the nature of national interests regarding cyber security.

Due to the growing number of entities active in cyber security, orientation within the flow of legal and policy documents can be challenging. Therefore, NATO CCD COE's International Cyber Developments Review (INCYDER) project, formerly known as Cyber Security Status Watch, focuses on the work of international organisations and brings together knowledge of all the relevant legal and policy instruments in order to improve overall awareness of international developments and, most importantly, to serve as a central hub for easy access to the wide range of different legal and policy instruments that make up the contemporary domain of cyber security.

The current Quarterly Report sheds light on NATO's enhanced cyber defence policy, elaborates on the European Court of Justice's cases regarding the "right to be forgotten" and the invalidation of the Data Retention Directive, and highlights the African Union's successful adoption of a cyber security convention. It also lists some interesting reads in the area of cyber security.

NATO Summit to Update Cyber Defence Policy

NATO defence ministers have approved a new and enhanced NATO cyber defence policy which is to be endorsed at the NATO Summit in Wales in September.

The defence ministers of NATO member countries met in Brussels on 3 - 4 June 2014. One of the items agreed on was a "new and enhanced" cyber defence policy, which is to be endorsed at the NATO Summit in Wales in September 2014.[1]

As NATO recognises that cyber defence is part of NATO's core task of collective defence, the new policy confirms that NATO member states are able to invoke Article 5 of the North Atlantic Treaty on collective self-defence in case of a cyber attack with effects comparable to those of a traditional armed attack.[2] According to Jamie Shea, Deputy Assistant Secretary General for Emerging Security Challenges at NATO Headquarters, the policy does not set any detailed criteria for the activation of Article 5 which would have to be decided by the Allies on a case-by-case basis.[3]

NATO is continuing to underline its fundamental responsibility for defending its own systems, while nations are expected to defend theirs. The new policy will also "help enhance information sharing and mutual assistance between Allies, improve NATO's cyber defence training and exercises, and boost cooperation with industry."[4] It will also confirm the applicability of international law to cyberspace.

The Summit is likely to discuss the development of a NATO cyber range capability. An earlier Estonian Defence Forces proposal to use its cyber range as the Alliance's main cyber defence training field[5] was approved in June by NATO's Supreme Allied Commander Transformation, General Jean Paul Paloméros.[6]

[1] NATO, Press conference by NATO Secretary General Anders Fogh Rasmussen following the first day of meetings of NATO Defence Ministers, 3 June 2014, http://www.nato.int/cps/en/natolive/opinions_110618.htm

[2] Steve Jordan, 'NATO updates cyber defence policy as digital attacks become a standard part of conflict', *ZDNet*, 30 June 2014, http://www.zdnet.com/nato-updates-cyber-defence-policy-as-digital-attacks-become-a-standard-part-of-conflict-7000031064/

[3] Ibid.

[4] NATO, 'NATO steps up collective defence, support for reforms in Ukraine', 3 June 2014, http://www.nato.int/cps/en/natolive/news_110609.htm

[5] Estonian Ministry of Defence, 'NATO Secretary General thanks Estonia for offer of cyber range', 16 February 2014, http://www.kaitseministeerium.ee/en/nato-secretary-general-thanks-estonia-for-offer-of-cyber-range

[6] Bruce Jones, 'NATO approves new military cyber warfare training centre in Estonia', *HIS Jane's 360*, 18 June 2014, http://www.janes.com/article/39677/nato-approves-new-military-cyber-warfare-training-centre-in-estonia

EU Data Retention Directive Invalid

In April 2014 the Court of Justice of the European Union declared the European Union Data Retention Directive[7] invalid. The Court ruled that, despite the Directive's legitimate purpose of fighting against serious crime and the protection of public security, it does not meet the principle of proportionality and should provide more safeguards regarding the protection of fundamental rights such as respect for private life and the protection of personal data.

The principle objective of the European Union (EU) Data Retention Directive 2006/24 is to harmonise Member States' provisions concerning the retention of certain data which are generated or processed by providers of publicly available electronic communications services or of public communications networks with the aim to ensure that the data would be available for the purpose of the prevention, investigation, detection and prosecution of serious crime.[8] According to the Directive, providers must retain traffic and location data as well as related data necessary to identify the subscriber, but not the content of the communication.[9]

The April 2014 ruling reflects the struggle of human rights activists who have fought hard to have the original Europe-wide law re-considered.[10] The representatives of the parties who initiated the cases in Ireland and Austria put forward the argument that the Directive is incompatible with the Charter of Fundamental Rights of the European Union,[11] and that there is still no evidence available of the excessive collection of communication data being a necessary and proportionate measure for combating organised crime or terrorism in the EU.[12] Furthermore, it was argued that the retained data is used for the investigation of crimes not foreseen in the Directive, like theft, drug trafficking and stalking.[13]

The Court's ruling found that the retention of data for the purpose of allowing the competent national authorities to have possible access to the data is satisfying an objective of general interest.[14] However, when assessing the proportionality of the interference, the Court concluded that "Directive 2006/24 does not lay down clear and precise rules governing the extent of the interference with the fundamental rights enshrined in Articles 7 and 8 of the Charter." Therefore the Court held that the Directive "entails a wide-ranging and particularly serious interference with those fundamental

[7] European Union, *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC*, 2006, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1405060274756&uri=CELEX:32006L0024.

[8] Ibid.

[9] Court of Justice of the European Union, *The Court of Justice Declares the Data Retention Directive to Be Invalid*, Press release no 54/14, 8 April 2014, http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.

[10] Electronic Frontier Foundation, 'Data Retention Directive Invalid, Says EU's Highest Court', 8 April 2014, https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court.

[11] European Union, *Charter of Fundamental Rights of the European Union*, 2010, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

[12] EDRI, 'Data Retention: "We Ask the Court to Rule in Favour of Freedom"', 17 July 2013, http://history.edri.org/edrigram/number11.14/data-retention-hearing-ecj-2013.

[13] Ibid.

[14] European Court of Justice, Judgment of the Court (Grand Chamber) of 8 April 2014. Digital Rights Ireland Ltd (C-293/12) v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung (C-594/12) and Others., 44 (2014).

rights in the legal order of the EU, without such an interference being precisely circumscribed by provisions to ensure that it is actually limited to what is strictly necessary."[15] Moreover, the Court found that the Directive "does not provide for sufficient safeguards, as required by Article 8 of the Charter, to ensure effective protection of the data retained against the risk of abuse and against any unlawful access and use of that data",[16] "does not ensure that a particularly high level of protection and security is applied by those providers by means of technical and organisational measures" nor "ensure the irreversible destruction of the data at the end of the data retention period".[17] Furthermore, the "Directive does not require the data in question to be retained within the European Union" and consequently, control over the data cannot be fully ensured.[18]

The consequences of the Directive being held invalid are uncertain. Whereas some states have initiated a review of their national data retention regulation or even ruled national data retention laws invalid,[19] others are looking for alternative measures to keep retaining the data[20] or have not taken any concrete steps. This leaves the local ISPs in a legal vacuum where it is not certain whether national data retention laws need to be adhered to or not, and results in stopping the collection of subscriber data despite the countries' data retention laws remaining in force.[21] The European Commission has assured that it will carefully assess the verdict and its impacts, and take its work forward in light of progress made in relation to the revision of the e-Privacy directive whilst taking into account the negotiations on the data protection framework.[22]

[15] Ibid., l. 65.
[16] Ibid., l. 66.
[17] Ibid., l. 67.
[18] Ibid., l. 68.
[19] Electronic Frontier Foundation, 'Data Retention Directive Invalid, Says EU's Highest Court'; Republic of Slovenia, Information Commissioner, 'Slovenian Constitutional Court Holds Data Retention Unconstitutional, Orders Deletion of Data', 11 July 2014, https://www.ip-rs.si/index.php?id=272&tx_ttnews[tt_news]=1256&cHash=2885f4a56e6ff9d8abc6f94da098f461.
[20] NDTV, 'UK Government Seeks Data Retention Law After European Union Verdict', *NDTV.com*, 10 July 2014, http://www.ndtv.com/article/world/uk-government-seeks-data-retention-law-after-european-union-verdict-556498.
[21] Liam Tung, 'Four of Sweden's Telcos Stop Storing Customer Data after EU Retention Directive Overthrown', *ZDNet*, 11 April 2014, http://www.zdnet.com/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown-7000028341/.
[22] European Commission, *Data Retention Directive: Commissioner Malmström's Statement on Today's Court Judgment*, Press release, 8 July 2014, http://europa.eu/rapid/press-release_STATEMENT-14-113_en.htm.

"Right to be forgotten" or "right to know"?

While the European Union is struggling with the comprehensive reform of the EU's 1995 data protection framework[23] the Court of Justice rules on a landmark case reinforcing the European Union citizens' right to be forgotten by search engines.

In a case of a Spanish citizen lodging a complaint against a Spanish newspaper, Google Spain and Google Inc. the citizen complained that an auction notice of his repossessed home that appeared on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant.[24] The citizen requested, *inter alia,* that Google Spain or Google Inc. should remove the personal data relating to him, so that it no longer appeared in the search results.[25] The request triggered debates on the applicability and interpretation of the "right to be forgotten", a principle of the EU Data Protection Directive that allows a person to ask for personal data to be deleted once that data is no longer complete or accurate.[26]

Accordingly, the Court of Justice firstly analysed the applicability of the EU law, namely the 1995 Data Protection Directive[27] to the search engine Google Spain, especially given that the company's data processing server is located in the United States. The Court found that search engines are "processing" personal data and should be viewed as "controllers" in respect of that processing.[28] Regarding the territorial scope of the EU rules, the Court affirmed that even in the case where the physical server of a company that is processing data is located outside Europe, EU rules still apply to search engine operators if they have a branch or a subsidiary in a Member State which is "intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State".[29]

Secondly, the Court scrutinized whether an individual has the right to request that his or her personal data be ceased to be accessible via a search engine, the so-called "right to be forgotten". The Court confirmed that in order to comply with the Data Protection Directive, the operator of a search engine is "obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is

[23] European Union, 'Commission Proposes a Comprehensive Reform of the Data Protection Rules', 25 January 2012, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm.
[24] European Commission, *Factsheet on the 'Right to Be Forgotten' Ruling C-131/12*, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.
[25] Ibid.
[26] European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*, 1995, para. 12, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1405077292706&uri=CELEX:31995L0046.
[27] European Union, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data*.
[28] Judgment of the Court (Grand Chamber) of 13 May 2014. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 41 (n.d.).
[29] Ibid., l. 60.

lawful".[30] This underlines that "even initially lawful processing of accurate data may, in the course of time, become incompatible with the directive where those data are no longer necessary in the light of the purposes for which they were collected or processed" and therefore "appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed."[31] It was also highlighted that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media, and that therefore it cannot be ruled out that in certain circumstances the data subject is capable of exercising the "right to be forgotten" against that operator but not against the publisher of the web page.[32]

Challenges in implementing the decision

The Court's ruling has raised many questions regarding the practical applicability of the right to be forgotten for search engines. According to the judgement, a search engine will have to delete information when it receives a specific request from a person affected, thus affecting any company or website that holds European customers' digital information. The search engine will then have to assess the deletion request on a case-by-case basis and apply the criteria determined in the EU law and the Court's judgment. Should the search engine decline the request, the person can still turn to national data protection supervisory authorities or to national courts.[33]

The burden of fulfilling the judgement will fall largely on Google, which is by far the dominant search engine in Europe, having more than 90 percent of the search business in France and Germany.[34] In order to follow the Court's guidance, Google has opened an initial online system handling the requests that assesses each individual request and attempts to balance the privacy rights of the individual with the public's right to know and distribute information.[35] As of July 2014, more than 70,000 requests have been made through that online form.[36]

However, the Court's decision gives only very vague direction on which data should be removed and on what bases, and thus the criteria to be applied by Google or any other search engine in deciding which data will be removed are opaque.[37] Google has reported that each application is reviewed individually, in most cases with limited information and almost no context,[38] and that Google cannot be specific about why certain information is removed because that could violate an individual's privacy rights under the court's decision.[39] Since the reporting system is still in

[30] Ibid., l. 88.
[31] Ibid., l. 93.
[32] Ibid., l. 85.
[33] European Commission, *Factsheet on the 'Right to Be Forgotten' Ruling C-131/12*.

[34] David Streitfeld, 'European Court Lets Users Erase Records on Web', *The New York Times*, 13 May 2014, http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html.
[35] Google, 'Legal Help', n.d., https://support.google.com/legal/contact/lr_eudpa?product=websearch.
[36] Mark Scott, 'European Companies See Opportunity in the "Right to Be Forgotten"', *The New York Times*, 8 July 2014, http://www.nytimes.com/2014/07/09/technology/european-companies-see-opportunity-in-the-right-to-be-forgotten.html.
[37] Ibid.
[38] Jim Edwards, 'It's Becoming Clear Just How Vast The Censorship Of Google Is Going To Be', *Business Insider*, 11 July 2014, http://www.businessinsider.com/google-right-to-be-forgotten-censorship-2014-7.
[39] David Drummond, 'We Need to Talk about the Right to Be Forgotten', *The Guardian*, 10 July 2014, sec. Comment is free, http://www.theguardian.com/commentisfree/2014/jul/

its initial phase, mechanisms for reversing a search engine's decision about certain data are yet to be developed.[40] Given these challenges, it should not be the role of a search engine company to decide what information is relevant.[41] Importantly, some claim that the ruling "opens the door to large-scale private censorship in Europe"[42] and even that it can be used by individuals trying to hide information not flattering to them but which is publicly available.[43]

While attempting to comply with the Court's ruling, Google is initiating a public debate[44] about how to balance one person's right to privacy with another's right to know.[45] It is clear that without further guidance from the European Union this complex issue will continue to be fraught with uncertainty regarding the practical implementation of the Court's ruling.

10/right-to-be-forgotten-european-ruling-google-debate.

[40] Mark Scott, 'Google Reinstates European Links to Articles From The Guardian', *The New York Times*, 4 July 2014, http://www.nytimes.com/2014/07/05/business/international/google-to-guardian-forget-about-those-links-right-to-be-forgotten-bbc.html.

[41] Ibid.

[42] Streitfeld, 'European Court Lets Users Erase Records on Web'.

[43] Edwards, 'It's Becoming Clear Just How Vast The Censorship Of Google Is Going To Be'.

[44] For example, by setting up a special advisory council. See, Google, 'The Advisory Council to Google on the Right to Be Forgotten', https://www.google.com/advisorycouncil/.

[45] Drummond, 'We Need to Talk about the Right to Be Forgotten'.

African Union Adopts Convention on Cyber Security

The African Union (AU) has adopted the "African Union Convention on Cyberspace Security and Protection of Personal Data" at its 23rd Ordinary Session in Malabo. Changes made to the previous draft convention are still unclear as the final text is not yet available to the public.[46]

According to an official press release of 30 June 2014, the long-awaited "African Union Convention on Cyberspace Security and Protection of Personal Data" has been adopted among a number of other legal instruments at the 23rd Ordinary Session of the AU.[47] The semi-annual summit was held from 20-27 June in Malabo, Equatorial Guinea and brought together an Assembly comprising the heads of state and government of the African Union.

Based on the latest draft, the convention addresses three main areas: (1) electronic transactions, (2) personal data protection, (3) cyber security and cybercrime.[48] The treaty was first drafted in 2011 and previous versions of the document were criticised mainly by the private sector, civil society organisations, and advocates of privacy who reportedly had limited influence on its development.[49] The convention was expected to be adopted in the 22nd AU summit in January 2014, but the process was postponed as many opposed the treaty claiming that it included provisions which would endanger privacy or limit the freedom of speech.[50] To review the convention in light of the criticism, the AU held a meeting of experts in May 2014.[51]

As the amended text of the treaty has not yet been released to the public, it is not possible to assess whether substantial changes have been made to the draft. It seems that the focus has shifted towards data protection as the latest available version of the draft was called the "African Union Convention on the Confidence and Security in Cyberspace".[52] According to this draft, the Convention will enter into force 30 days after the 15th instrument of ratification or accession is deposited.[53]

[46] This report is written on 14 July 2014

[47] African Union Directorate of Information and Communication, *Press Release №18/23rd AU SUMMIT, The 23rd Ordinary Session of the African Union ends in Malabo,* press release, 30 June 2014, http://summits.au.int/en/sites/default/files/PR%2018%20-%2023rd%20AU%20Assembly%20ends%20in%20Malabo%20(3).pdf

[48] African Union, http://au.int/en/cyberlegislation

[49] Ephram Percy Kenyanito, 'Africa moves towards a common cyber security legal framework', *Acces.org blog,* 2 June 22014, https://www.accessnow.org/blog/2014/06/02/africa-moves-towards-a-common-cyber-security-legal-framework

[50] See NATO CCD COE, *International Cyber Developments Report (INCYDER) 2014 Q1*, April 2014, https://www.ccdcoe.org/publications/articles/INCYDER-2014Q1.pdf

[51] African Press Organisation, 'FIRST SESSION OF THE SPECIALISED TECHNICAL COMMITTEE (STC) ON JUSTICE AND LEGAL AFFAIRS', 7 May 2014, http://appablog.wordpress.com/2014/05/07/first-session-of-the-specialised-technical-committee-stc-on-justice-and-legal-affairs/

[52] African Union, http://au.int/en/cyberlegislation

[53] Ibid.

Interesting reads

European Union Agency for Network and Information Security (ENISA) annual report 2013 is available here: http://www.enisa.europa.eu/publications/programmes-reports/enisa-annual-report-2013

ITU and ABI research launched the Global Security Index (GCI) to measure levels of cybersecurity capabilities in nation states. Read more about the project here: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx