IN THE EUROPEAN COURT OF HUMAN RIGHTS **App. No. 58170/13**

Big Brother Watch, Open Rights Group, English PEN and Dr Constanze Kurz
v
United Kingdom

TIMELINE OF EVENTS

Covering the period June 2013 to 28 February 2015

To select a document to read, please click on the date of the document, which is a hyperlink to the document on the internet.

Date (Hyperlink to article)	Summary	Relevant Application Paragraph
June '13		
7.06.13	NSA Prism programme revealed	[20]
17.06.13	GCHQ intercepted foreign politicians' communications	[23], [31]-[38]
19.06.13	Skype communications accessed via PRISM since 2009	[20]-[23]
21.06.13	Series of Guardian articles regarding GCHQ activities and TEMPORA programme. See also: 1, 2 and 3.	[31] - [35]
27.06.13	Revelations regarding continued metadata harvesting and GCHQ sharing with NSA See also: 1.	[20] - [23]
30.06.13	Disclosures that NSA spying on EU allies and foreign embassies	[23], [176]-[178]
July '13		
6.7.13	Australia aids in US data collection. Further information regarding 'Tempora'	[37] - [38]
10.7.13	NSA UPSTREAM programme revealed	[24]-[25]
11.07.13	UN High Commissioner for Human Rights, Navi Pillay, urges respect for right to privacy and protection of individuals revealing human rights violations	[176]-[178]
16.07.13	GCHQ intercepted foreign leaders and diplomats' communications.	[31]-[38]
17.07.13	Intelligence and Security Committee of Parliament "*Statement on GCHQ's Alleged Interception of Communications under the US*	[47]-[52]

	Prism Program"	
17.07.13	The Terrorism Acts in 2012: report of the Independent Reviewer published, noting the breadth of the definition of "*terrorism*"	[105]-[112], [147]
18.07.13	2012 Annual Report of the Intelligence Services Commissioner. In the foreword, the Commissioner set out his conclusion that: "*This report is being finalised at a time of considerable media comment about the legality of GCHQ's activities. The Intelligence and Security Committee are, quite properly, investigating and it is for them to comment further if they wish to do so. In so far as matters related to my area of oversight, which is the only area where it is appropriate for me to comment, I have discussed matters fully with senior officials within GCHQ and I am satisfied that they are not circumventing the legal framework under which they operate… I remain convinced that, because of the layers of checks, assurances and oversight, it would take an enormous conspiracy at all levels to undertake unlawful activity.*"	[77.2]-[80]
31.07.13	Detail of NSA program 'X-Keyscore', consisting of a network of 500 servers across the globe by which intercepted communications are accessed and searched	[18],[20], [25]
August '13		
1.08.13	NSA provides GCHQ funding of over £100 Million and exerts influence. In documents disclosed, GCHQ describes Britain's surveillance laws and regulatory regime as a "selling point" for the Americans. In return for funds, "*GCHQ must pull its weight and be seen to pull its weight*," a GCHQ strategy briefing said. The leaked papers reveal that the UK's biggest fear is that "*US perceptions of the … partnership diminish, leading to loss of access*". See also: 1.	[37]-[38]
2.08.13	Telecoms corporations providing GCHQ direct access to communications	[31], [36]
9.08.2013	Amendment to FISA Act permits warrantless searches by NSA	[23]
15.08.13	NSA breaks US law and own policies	[23]
21.08.13	FISA Court Opinions published revealing mass gathering of US-based internet traffic	[24]-[25]
23.08.13	The Independent reveals GCHQ station in Mid-East	[31]-[38]
30.08.13	Reporting of NSA cyber-attacks on foreign governments	[26]-[27]
September '13		
6.09.13	US and UK beat online privacy tools. PRISM funding disclosed, importance of encryption to TEMPORA	[17], [22], [31], [176]-[178]
11.09.13	NSA shares data with Israel	[18], [27], [130], [161]
16.09.13	Dr Spiegel reveals NSA mass spying on financial records	[20]-[25]
20.09.13	Der Spiegel reveals how GCHQ hacked internet communications company, Belgacom	[17], [176]-[178]
20.09.13	Malcolm Rifkind MP (Chairman of Intelligence & Security Committee) claims statutory framework sufficient	[47]-[52]
28.09.13	NSA has been 'mapping' US citizens' social connections since Nov 2010. Notes the importance of metadata, which "*can be very revealing*"	[21]-[22]

30.09.13	Guardian reveals NSA stores metadata of millions of web users for up to one year	[21]-[22]
30.09.13	*BBW & ors v. UK* Application lodged with the Court	
October '13		
2.10.13	Council of Europe Parliamentary Assembly Resolution 1954 (2013): "*National security and access to information*" "*10. The neutrality of the Internet requires that public authorities, Internet service providers and others abstain from using invasive wiretapping technologies, such as deep packet inspection, or from otherwise interfering with the data traffic of Internet users…* *…13. The Assembly is worried about recent disclosures on large-scale surveillance of communications by secret services and resolves to follow up this important issue in due course.*"	[176]-[178]
02.10.13	NY Times reveals NSA tracked cell-phone location of Americans for up to two years	[21]-[22]
4.10.13	NSA cracks encryption standards	[17], [22], [176]-[178]
9.10.13	MI5 chief attacks leaks and defends need for surveillance programmes	[176]-[177]
11.10.13	Nick Bickford (former undersecretary of state and legal director of the Security and intelligence agencies MI5 and MI6): Leave surveillance to the judges	[167]-[168], [177.7]
14.10.13	Prof Scheinin, former Special Rapporteur on human rights and counter terrorism, issues statement on illegality of PRISM in international law, submitted to the European Parliament's LIBE Inquiry.	[119]-[164]
16.10.13	NSA data collection programme used in targeted killing programme. The CIA's drone strike programme reported to be heavily reliant upon NSA targeted communication surveillance. See also 10.02.14 entry.	[21]-[22], [177]
22.10.13	*R v Gul* [2014] A.C. 1260 - Judgment of the Supreme Court of the UK on the breadth of the definition of "*terrorism*" Analysis by David Anderson QC, UK Independent Reviewer of Terrorism Legislation: 1.	[147]
25.10.13	Disclosure that NSA monitored the phone conversations of 35 world leaders including allied heads of state	[23], [176]-[178]
25.10.13	Leaked GCHQ legal memos show fear of legal challenge	[117]-[118], [176]-[178]
October 2013	A series of revelations that US intelligence agencies, and primarily the NSA, have been spying on European and Latin American government ministers. Other stories: Germany, Mexico and Brazil, Spain, The Pope	[23], [176]-[178]
29.10.13	Disclosure of "*arrangements*" allowing UK intelligence agencies to obtain "unselected" – meaning unanalysed, or raw intelligence – information from overseas partners without a warrant, in the IPT proceedings.	[121], [123], [131], [133], [136]
30.10.13	NSA and GCHQ reported to be intercepting metadata pursuant to MUSCULAR program from Google and Yahoo! Both companies deny giving NSA access to their systems. Other stories: 1	[20], [22], [31], [39], [174], [176]-[178]
November '13		

1.11.13	Government Response to the Independent Reviewer of Terrorism Report in 2012. See p.7: "*There is no universally agreed definition [of terrorism]. Indeed, as you point out, the UK approach has influenced formulations adopted in other jurisdictions. The UK definition is necessarily broad to tackle the ever changing nature of the terrorist threat, both in the UK and overseas*."	[147]
01.11.13	NSA reliance on 'corporate partners' for data gathering. The purpose of NSA's 'Corporate Partner Access' summarised in leaked document: "*Leverage unique key corporate partnerships to gain access to high-capacity international fiber-optic cables, switches and/or routes throughout the world.*"Notable "corporate partners" include Google, Microsoft and Yahoo; companies respond by stating that their co-operation is compelled by warrant, and limited to compliance with lawful requests, not (as stated in one leaked document) direct access to their servers.	[20]
01.11.13	Close working relationship reported between British, German, French, Spanish and Swedish intelligence agencies – with GCHQ leading. GCHQ reported to play a leading role in advising European counterparts on circumvention or reform of surveillance laws.	[31]-[38], [131]
05.11.13	Judgment of the Court of Appeal of England & Wales in *AJA & ors v Met Police Cmmr & ors* [2013] EWCA Civ 1342 notes the limitations of proceedings before the IPT	[138], [171], [173], [179], [190]
06.11.13	Report commissioned by EU Parliament JHA Committee – mass surveillance a violation of European law: "*in general legal frameworks are characterised by ambiguity or loopholes as regards large-scale communications surveillance, while national oversight bodies lack the capacity to effectively monitor the lawfulness of intelligence services' large-scale interception of data*". See also 1.	[140], [178]
07.11.13	UK Intelligence chiefs appear before ISC. See also 1.	[137. 2], [175]
07.11.13	Submission of Nick Bickford to EU Parliament LIBE Inquiry suggesting that judicial oversight is needed	[165], [175]
08.11.13	Council of Europe Conference of Ministers responsible for Media and Information Society. Political Declaration and Resolutions identified concerns about data privacy and the need to provide effective guarantees against abuse of data collection and surveillance for national security purposes. Resolution No 1, §13(v) invited the Council of Europe to "*examine closely, in the light of the requirements of the European Convention on Human Rights, the question of gathering vast amounts of electronic communications data on individuals by security agencies, the deliberate building of flaws and 'backdoors' in the security system of the Internet or otherwise deliberately weakening encryption systems*".	[128], [139], [176], [178]
18.11.13	Declassification by ODNI of documents revealing that the NSA collected internet metadata from American internet service providers in bulk from 2001 until 2009. The bulk metadata collection was done under the Pen Register/Trap and Trace provisions of FISA. The program was discontinued in 2011 after a series of serious compliance issues were discovered.	[20], [23], [30]
19.11.13	NSA publish documents showing repeated violations of surveillance rules. Foreign Intelligence Surveillance Court reported to have "provided inconsistent oversight that often failed to stop many of the spy agency's transgressions."	[23], [30]
20.11.13	NSA – GCHQ 2007 deal on retention and analysis of UK citizens' metadata by NSA	[20], [23],

		[145]
21.11.13	The Intelligence and Security Committee demand an explanation from GCHQ on the 20.11.13 revelations.	[20], [23], [145]
27.11.13	Report on the Findings of the ad hoc EU-US Working Group on Data Protection setting out factual information re. US programmes.	[20]-[25]
December '13		
04.12.13	The NSA is reported to be gathering nearly 5 billion records a day on the whereabouts of cellphones around the world	[26]-[30], [176]-[178
12.12.13	Opinion of Advocate-General Cruz Villalón in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others* re. data retention by telecoms providers (ECLI:EU:C:2013:845). See also: 1.	[21], [176]-[178]
17.12.13	Former GCHQ chief defends practices, implicitly acknowledges 'backdoor access' to internet companies.	[36]
18.12.13	UN General Assembly passes resolution A/Res/68/167 (*The right to privacy in the digital age*) expressing deep concern at the impact of mass surveillance and the interception of data, including personal data, on human rights, and reaffirming the right to privacy. The resolution called upon states to review procedures, practices and legislation governing interception of communications to ensure full and effective protection of obligations under international human rights law.	[119]-[178]
20.12.13	GCHQ reported to have targeted NGOs, EU officials and heads of state. Former Israeli PM, high ranking EU officials, Médecins du Monde and UNICEF amongst those reported to be targeted.	[10]-[17], [113], [116]
January '14		
9.01.14	*BBW v UK Application communicated to the UK government*	
9.01.14	EU Parliament LIBE Inquiry draft report declares NSA & GCHQ activities appear to be illegal	[176]-[178]
16.01.14	NSA's "*Dishfire*" programme reported to be indiscriminately gathering SMS metadata from text messages globally. Information collected includes location, contact networks, financial transactions and travel plans. Untargeted and indiscriminate, the programme is reported to collect an average of 194 million text messages a day. GCHQ given access to the database. See also: 1.	[26]-[30], [176]-[178]
17.01.14	US President announces reforms: a review of signals intelligence activities, declassification of additional materials including in relation to the s702 foreign surveillance and s215 telephone metadata programs, and an annual review of FISA court opinions for declassification. Also announces intend to end the s215 bulk metadata program as it currently exists. Slow implementation.	[23], [30]
23.01.14	US Government Privacy Board says NSA bulk collection of phone data illegal. See also report here: 1.	[26]-[30], [176]-[178]
27.01.14	GCHQ tapped into fibre-optic cables to spy on Youtube users	[31], [176]-[178]

February '14		
04.02.14; 07.02.14	GCHQ's Joint Threat Research Intelligence Group exposed. Targets included 'hacktivists' and online campaign & protest groups.	[10]-[17], [116], [176]-[178]
10.02.14	Reports that U.S. program of targeted killings relies largely on the NSA's analysis of cell phone metadata and geolocation rather than human intelligence	[21], [176]-[178]
11.02.14	The Interception of Communications Commissioner gives evidence to Home Affairs Committee, notes that RIPA "*is an extremely difficult act of parliament to get your mind round*" and that over 560,000 requests for use of metadata were made by law enforcement authorities in a year. See Transcript of evidence.	[128]-[129], [143]-[164]
19.02.14	*R. (on the application of Miranda) v Secretary of State for the Home Department* [2014] 1 W.L.R. 3140 – judgment of the Divisional Court taking a wide definition of terrorism	[147]
21.02.14	European Parliament report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)).	[128]-[129], [143]-[164]
28.02.14	GCHQ's 'Optic Nerve' programme reported to intercept millions of Yahoo! webcam images, prompting US criticisms. See also: 1.	[31], [176]-[178]
March '14		
5.03.14	Disclosure that IPT located in the Home Office's premises	[171]-[173]
12.03.14	Sir Tim Berners-Lee – credited as the founder of the Internet - calls for web bill of rights	[176]-[178]
12.03.14	European Parliament resolution of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)) criticizes mass surveillance and calls for a prohibition on its use. The Parliament found "*compelling evidence of the existence of far-reaching, complex and highly technologically advanced systems designed by US and some Member States' intelligence services to collect, store and analyse communication data, including content data, location data and metadata of all citizens around the world, on an unprecedented scale and in an indiscriminate and non-suspicion-based manner*". It also stressed its strong belief that "*that the fight against terrorism can never be a justification for untargeted, secret, or even illegal mass surveillance programmes; takes the view that such programmes are incompatible with the principles of necessity and proportionality in a democratic society*". The Resolution also "[c]*all*[ed]] *on the United Kingdom, in particular, given the extensive media reports referring to mass surveillance by the intelligence service GCHQ, to revise its current legal framework, which is made up of a 'complex interaction' between three separate pieces of legislation – the Human Rights Act 1998, the Intelligence Services Act 1994 and the Regulation of Investigatory Powers*	[18]-[52], [119]-[178]

	Act 2000" (at [23]).	
13.03.14	UN HR Council criticises NSA in question & answer session.	[119]-[164]
18.03.14	Intelligence Services Commissioner gives evidence to Home Committee. See also: 1.	[128]-[129], [143]-[164]
18.03.14	Washington Post reveals the NSA's MYSTIC program: recording all phonecalls within four countries on a 30-day rolling buffer	[26]-[30], [176]-[178]
19.03.14	NSA lawyer says US corporations were aware of surveillance programmes	[20], [24]
28.03.14	Director of National Intelligence Clapper Confirms NSA conducted warrantless searches of information collected under section 702	[23]
29.03.14	GCHQ and NSA targeted private German companies and Angela Merkel, Spiegel Online	[17], [22], [31], [39], [174], [176]-[178]
April '14		
08.04.14	*BBW & ors v. UK* Application stayed pending domestic proceedings in the Investigatory Powers Tribunal	
08.04.14	CJEU decision in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger* (ECLI:EU:C:2014:238) declares Data Retention Directive invalid	[21], [176]-[178]
08.04.14	2013 Annual Report of the Interception of Communications Commissioner finds, *inter alia*, that "*indiscriminate retention for long periods of unselected intercepted material (content) does not occur*". It was noted, amongst other things, that it is "*sometimes appropriate for the interception agencies to apply explicitly by analogy the RIPA 2000 Part I principles of necessity and proportionality to* [the] *receipt* [of information lawfully obtained by interception abroad] *here even though* [that Part] *does not strictly apply*" (§6.8.6)	[77.1], [137.1], [170]
10.04.14	Article 29 Working Party Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes concludes that *secret, massive and indiscriminate surveillance programs are incompatible with our fundamental laws and cannot be justified by the fight against terrorism or other important threats to national security. Restrictions to the fundamental rights of all citizens could only be accepted if the measure is strictly necessary and proportionate in a democratic society.*" (p.2) "*Under no circumstance surveillance programmes based on the indiscriminate, blanket collection of personal data can meet the requirements of necessity and proportionality set out in these data protection principles.*" (p.6)	[21], [176]-[178]
12.04.14	Further disclosures about the extent of mobile phone surveillance carried out by the NSA, as of May 2012 said to include technical information on approximately 70% of mobile phone networks worldwide.	[26]-[30], [176]-[178]
22.04.14	UN Human Rights Committee Concluding Observations on 4th periodic report of the US expresses concerns relating to the mass surveillance programmes and lack of effective remedies for affected persons (at [22]): "*The Committee is concerned about the surveillance of communications in the interest of protecting national security, conducted by the National Security Agency (NSA) both within and outside the United States, through the bulk phone metadata surveillance programme*	[119]-[164]

	(Section 215 of the USA PATRIOT Act) and, in particular, surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendment Act, conducted through PRISM (collection of communications content from United States-based Internet companies) and UPSTREAM (collection of communications metadata and content by tapping fiber-optic cables carrying Internet traffic) and the adverse impact on individuals' right to privacy. […] *The Committee is concerned that the current oversight system of the activities of the NSA fails to effectively protect the rights of the persons affected.* […] *Finally, the Committee is concerned that the persons affected have no access to effective remedies in case of abuse (arts. 2, 5 (1) and 17)*".	
30.04.14	Reports that the GCHQ had sought unrestricted access to NSA data	[26]-[30]
May '14		
09.05.14	Home Affairs Select Committee report on Counter Terrorism concludes that "[w]*e do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability, and to the credibility of Parliament itself […] There are questions about the accuracy of information provided to the House by the security and intelligence agencies in the past, particularly in 2003.* […]. *158.* […] *we recommend that the Commons membership of the Intelligence and Security Committee should be elected like other select committees and that the Chair, who should always be a member of the Commons, ought to be subject to election of the whole House, as is the case for Select Committees. We further recommend that the Chair should always be a member of the largest opposition party.*" The Committee also concluded that RIPA was in need of review (at [177])	[137], [170]-[175]
13.05.14	Greenwald's "No place to hide" further details US and UK surveillance programs. Disclosed NSA and GCHQ documents openly discuss the agencies' desires to "collect it all," "know it all" and "exploit it all."	[176]-[178]
16.05.14	Disclosure of the evidence of Mr Charles Farr to the IPT. See Applicants' Update Submission.	[121], [123], [131], [133], [136], [176]-[178]
19.05.14	Further disclosures concerning the NSA's gathering of the mobile-phone metadata in five countries, and interception of voice data (i.e. content) in two of those countries	[21], [26]-[30], [176]-[178]
31.05.14	Disclosures that the NSA was collecting millions of photographs from online communications	[31]
June '14		
18.06.14	Spying together: Germany's deep cooperation with the NSA. Der Spiegel publishes a large cache of further NSA/GCHQ documents, some of which further described the TEMPORA programme, showing the scale of NSA and GCHQ programmes and the degree of cooperation between the NSA and other third countries. See also: *New NSA Revelations: Inside Snowden's Germany File*, Der Spiegel.	[31]-[40], [176]-[178]
26.06.14	Intelligence Services Commissioner's Annual Report for 2013 finds numbers of individual privacy breaches. However, he dismissed the possibility of "deliberate activity" which was unlawful, noting that "*for unlawful warrants or authorisations to be*	[119]-[178]

	issued it would require considerable ineptitude or conspiracy on a massive scale". He also found that "*GCHQ do not conduct activities outside the UK legal framework*." In response to the media allegations, the Commissioner concluded that "[t]*he results of* []*his questioning and briefing allowed* [him] *to conclude that GCHQ were not circumventing the law in the UK*". And see here: 1.	
30.06.14	"*The right to privacy in the digital age*": Report of the Office of the United Nations High Commissioner for Human Rights	[119]-[178]
30.06.14	FISA granted extensive warrant to NSA to spy on all but closest allies	[23], [124]
July '14		
01.07.14	*The Terrorism Acts in 2013*: Report of the independent reviewer on the operation of the Terrorism Act 2000 and part 1 of the Terrorism Act 2006	[US/30], [US/31]
02.07.14	US Privacy and Civil Liberties Oversight Board "*Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*". See also here: 1.	[23]
05.07.14	Washington Post analyses a large cache of intercepted communications obtained pursuant s702 FISA warrant (foreign communications). 9 out of 10 individuals whose data is collected are not targets of NSA but caught in dragnet	[20]-[25]
17.07.14	Data Retention & Investigatory Powers Bill receives Royal Assent, following its introduction on an emergency basis 7 days previously.	[149]-[150]
25.07.14	Reports of USA/Saudi Arabian surveillance collaboration	[18], [27], [130], [161]
August '14		
11.08.14	US Government releases previously classified documents related to the NSA electronic metadata program	[22], [26]-[30], [176]-[178]
25.08.14	Intercept reveals ICREACH, NSA's programme that allows searching of metadata by 23 agencies	[22], [26]-[30], [176]-[178]
September '14		
14.09.14	Revelations of GCHQ attacks on German satellite internet companies and NSA programme to 'map' the internet	[113]-[116]
30.09.14	Theresa May MP (Secretary of State for the Home Department) vows that a Conservative government, if elected in May 2015, would extend surveillance and data retention powers. See also here: 1.	[140]-[142], [176]-[178]
October '14		
07.10.14	National Crime Agency director general says UK snooping powers are too weak.	[119]-[127]
07.10.14	Twitter sues U.S. Government over limits on ability to disclose surveillance orders to the public	[20], [24]
12.10.14	Government will amend RIPA to rein in police's use of snooping on journalists	[146], [176]-[178]

15-23.10.14	Intelligence and Security Committee, 2014 Privacy and Security Inquiry takes oral evidence including from Open Rights Group, Big Brother Watch, Theresa May MP	[137. 2], [175]
21.10.14	Italian Parliament Publishes Draft Internet Bill Of Rights, with a 4-month consultation period. Similar Brazilian law here: 1.	[176]-[178]
23.10.14	UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism presents report on mass surveillance to UN General Assembly. Urges Governments currently engaged on mass surveillance of the internet for counter-terrorism purposes to update their national legislation in line with international human rights law. See: mass internet surveillance threatens international law, UN report claims.	[119]-[178]
27.10.14	Publication of the Initial Assessment (dated 11 July 2014): UK OECD National Contact Point refuses to probe a complaint against telecommunications companies for their alleged role in GCHQ mass surveillance. The NCP concluded that "*the NGO has not been able to substantiate the allegations*", in particular "*the link the complainants make to the specific companies identified*" (at [44]), although it found that a compelling case had been established as to the concerns regarding the legality of mass surveillance (at [47]-[48]).	[36]
29.10.14	Secret policy reveals GCHQ can get warrantless access to bulk NSA data. See also here: 1.	[121], [123], [131], [133]-[136]
November '14		
03.11.14	New GCHQ Director Robert Hannigan says the web is a terrorist's command-and-control network of choice. See also: 1.	[36]
06.11.14	UK Government policies governing interception of legal communications disclosed	[146], [176]-[178]
25.11.14	Intelligence and Security Committee of Parliament publishes Report on the intelligence relating to the murder of Fusilier Lee Rigby. See also: 1 and 2.	[31]-[40]
26.11.14	UN General Assembly (Third Committee – 39 states) passes resolution A/C.3/69/L.26/Rev.1 (*The right to privacy in the digital age*) demanding privacy protection in light of Snowden revelations and new challenges to liberty presented by information age. See also here: 1.	[21]
December '14		
04.12.14	The Intercept discloses the AURORAGOLD program, whereby the NSA and GCHQ obtained technical information on cellphone networks globally, in some cases by subverting encryption standards. 70% of global cellphone networks reportedly hacked.	[26]-[30], [176]-[178]
05.12.14	Investigatory Powers Tribunal rules GCHQ mass surveillance programme TEMPORA is lawful in principle. See also here: 1. See See Applicants' Update Submission generally.	[138], [171]-[173]
05.12.14	Evidence for the Investigatory Powers Review published by the Interception of Communications Commissioner's Office The IOCCO made a number of comments, including in relation to:	[113]-[116], [128]-[139],

	– Discoverability of interception: "*in practice it will be virtually impossible for the aggrieved person to ever be aware of the interception of communications due to the requirement to keep secret matters relating to the existence of a warrant and the exclusion of the product of warranted interception from legal proceedings*" ((§3.1.4, p.15) – The functions of the IPT: "*the Tribunal processes appear to deal with the actions of public authorities and therefore it is not clear if that would include investigating the circumstances when a CSP is at fault concerning the interception of the wrong communications address and / or the disclosure of the wrong communications data*". (§3.1.4, p.15) – The growth of data retention: ""[t]*he volumes and detail contained, especially in traffic data, are at a level not envisaged* [when legislation was introduced] *in 2000*". The capacity of modern mobile devices to access data and materials "*is staggering and so is the volume and detail of the data generated as a result, especially relating to the location of a mobile phone/end user device.*" (§3.2.8, p.19); – The lack of guidance as to use of retained data: "[t]*here is an absence of consolidated guidance as to what may be done with the data outside the boundary of the justifications as to why the data was acquired in the first instance*" (§3.10.4). – "*in practice, an additional and appropriate test as to whether something is, was or continues to be proportionate to the Article 8 interference undertaken can only be obtained by scrutinising the operational conduct carried out, or put another way, the downstream use of the material acquired*" (§3.11.8)	[158]-[162] [171]-[173], [176]-[178]
8.12.14	Issue paper published by the Council of Europe Commissioner for Human Rights: "*The rule of law on the Internet and in the wider digital world*", noting concerns about widespread surveillance and acquisition of digital data. In particular, at pp.16-17:"*…it is becoming increasingly clear that secret, massive and indiscriminate surveillance programmes are not in conformity with European human rights law and cannot be justified by the fight against terrorism or other important threats to national security. Such interferences can only be accepted if they are strictly necessary and proportionate to a legitimate aim.*" The Commissioner's Recommendation 2 stated *inter alia* that "*Suspicionless mass retention of communications data is fundamentally contrary to the rule of law, incompatible with core data-protection principles and ineffective. Member states should not resort to it or impose compulsory retention of data by third parties*". See also: 1, 2 and 3.	[20]-[40], [119]-[178]
09.12.14	2 draft Codes of Practice published for consultation: updated Acquisition and Disclosure of Communications Data Code of Practice; and new Retention of Communications data Code of Practice. A notable addition to the proposed Code is the guidance on "*Communications data involving certain professions*", including the statement that: "*3.72 Communications data is not subject to any form of professional privilege – the fact a communication took place does not disclose what was discussed, considered or advised.*"	[22], [88]
9.12.14	Legal profession heads call for RIPA reform	[146], [176]-[178]
23.12.14	NSA releases over a decades worth of oversight reports	[23]

28.12.14	Der Spiegel details NSA efforts to crack encrypted internet communication	[17], [22], [176]-[178]
January '15		
11.01.15	Thatcher and Blair Cabinet Secretary: Intelligence committee has 'helped' public by confirming GCHQ's internet tap 'Tempora' powers. Lord Butler, the former head of the UK's Civil Service for 10 years under three prime ministers identified the disclosures of GCHQ's capabilities in the ISC's Lee Rigby report as confirming the agency's interception powers	[31]-[40]
19.01.15	Study for the LIBE Committee: "*National security and secret evidence in legislation and before the courts: exploring the challenges*" published. The authors noted the breadth of the notion of national security in EU Member State legal systems and the wide range of surveillance operations carried out based upon that: "*the conceptual features attributed to th*[e] *term* ['national security'] *remain 'open-ended' even in those Member States with legal frameworks. There are several concepts which are often used or prescribed in EU Member States, yet there is no commonly held legal definition in any of the countries under examination that meets the legal certainty and "in accordance with the law" test"*	[147]
19.01.15	GCHQ captured emails of journalists from international media. Agency includes investigative journalists on 'threat' list.	[10]-[17], [146], [176]-[178]
26.01.15	Draft Report of the Committee on Legal Affairs and Human Rights of the Parliamentary Assembly of the Council of Europe on Mass Surveillance (Rapporteur, Pieter Omtzigt). See also: 1 and 2.	[20]-[40], [113]-[178]
29.01.15 The report	The US PCLOB calls on President Obama to halt the surveillance programme of domestic telephony data and noted that intelligence agencies had not yet disclosed legal opinions from the FISA Court assessing the legality of the foreign intelligence programmes. The report also noted "imminent" release of internal rules for the FBI, CIA and NSA governing when they can collect, use and disseminate information from the international communications dragnets.	[23]
February '15		
6.02.15	Security Services capable of bypassing encryption, draft code reveals	[17], [31], [176]-[178]
6.02.15	IPT declares UK regime governing receipt of PRISM and UPSTREAM data breached Articles 8 or 10 ECHR, prior to disclosures made in the proceedings.	[119]-[139]
18.02.15	UK admits monitoring legally privileged communications and says that intelligence agencies breached rights	[146], [176]-[178]
19.02.15	The Intercept Discloses That GCHQ and NSA collaborated to steal millions of Cellular Encryption Keys. See also here: 1.	[17], [22], [31], [39], [174], [176]-[178]

Additional documents and materials		
Timelines of relevant events	A helpful timeline with relevant attachments is also available at http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html and (from a US perspective) at https://www.eff.org/nsa-spying/timeline.	
Further map of submarine cables (Undated)	http://lifewinning.com/submarine-cable-taps/ Click on individual cables for name, owner(s), and associated surveillance programmes	