Communications Privacy and Surveillance:
References

Winter Semester 2013-14 / Summer Semester 2014
Version 13 2014-03-04

New in this Version:

- New material 1st February - 4rd March
- Reason for a new version: important policy statement by UK Deputy PM

New in the 11th & 12th Versions

- New material 16th January – 3rd March 2014

This document constitutes a commented list of some articles, mainly from the Guardian and the New York Times, about the NSA and GCHQ surveillance of digital communications revealed by Edward Snowden, as well as some original source documents and other material. I am assembling it for the Communications Privacy and Surveillance seminar I am holding at the University of Bielefeld.

Bruce Schneier's Crypto-Gram newsletter has a more complete list of articles from all over, although all of the Guardian articles he lists appear here. Bruce has worked with the journlaist Glenn Greenwald and the Guardian; he has seen substantial amounts of the material from Edward Snowden's document cache. As far as I know, he is the only digital-security professional not associated with the NSA or GCHQ who has seen the Snowden material.

The material Bruce Schneier has published on the matter in his monthly newsletter is substantial and takes some time to read and I do recommend that readers of this document also read Schneier. Crypto-Gram contains many technical articles atttempting to assess the exact functioning and the likely effects of various named NSA and GCHQ programs. Its links offer a more diverse commentary that this document; however, there are references here which do not appear there, although I do not claim to be anywhere near complete on the stories.

In September, Glenn Greenwald's partner David Miranda was detained by the London Metropolitan Police for nine hours while attempting to transit through London Heathrow airport. Miranda was said to have been couriering materials between Laura Poitras in Berlin and Greenwald in Rio de Janeiro. His detention caused considerable consternation, indeed furore, because he was detained under an English law which was expressly introduced to allow police to ascertain at ports whether a person of interest is a terrorist or not. Most people, including myself, seem to think it inconceivable in the extreme that Miranda could count as any kind of terrorist. One of the authors of the law in question (referenced below) said that its use in this case is clearly inappropriate. Miranda sued in London court. There is a rumor that Miranda had a written-down password with him that decrypted some of the material, and amongst that material were names one would not wish to distribute (says the UK government in its submission to the court). We do not know yet whether this is considered to be proved. There were claims by the Prime Minister and by the Daily Mail, as well as intelligence chiefs appearing before the Intelligence and Security Committee, that the Guardian's operations have endangered UK security (See Cryto-Gram 15 Sep). As of writing, I know of no public evidence, let alone proof, of this claim. The court which decided whether Miranda's detention was legal did not test this claim, as far as I understand (but I am not a lawyer).

12 May 2012: Landwehr et al., Privacy and Cybersecurity: The Next 100 years. Proc. IEEE Vol.

100, May 12, 2012. A view from a year before the Snowden revelations http://ieeexplore.ieee.org/ielx5/5/6259910/06182691.pdf?tp=&arnumber=6182691&isnumber=6259910

6 June 2013: Glenn Greenwald on the order to Verizon to give the NSA phone records of all its calls on an "ongoing, daily basis" http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

6 June 2013: James Ball explaining what is being collected: metadata, and what it means http://www.theguardian.com/world/2013/jun/06/phone-call-metadata-information-authorities

7 June 2013: The original Greenwald et al article on PRISM http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

8 June 2013: James Ball on details of the PRISM program http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

12 June 2013: Sir David Omand, former director of GCHQ, permanent secretary of the Home Office and UK security and intelligence coordinator, lays down some principles for guiding surveillance http://www.theguardian.com/commentisfree/2013/jun/11/make-surveillance-ethical-and-effective

13 June 2013: Paddy Ashdown said raised the question of how good the oversight is or can be http://gu.com/p/3ggtx

15 June 2013: Schneier's Crypto-Gram https://www.schneier.com/crypto-gram-1306.html

20 June 2013: A document setting out the proceduures by means of which NSA is authorised by a FISA court to gain information about phone calls with non-citizen participation http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document and another setting out procedures to minimise such data collected about US citizens http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document followed by an analysis by Greenwald and Ball http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant

June 2013: Susan Landau comments perceptively in IEEE Computer on the spying and the revelations http://www.computer.org/cms/Computer.org/ComputingNow/pdfs/MakingSenseFromSnowden-IEEESecurityAndPrivacy.pdf

20 June 2013: Barrister Anja Proops raises questions on whether anything resembling the Prism collection can ever be lawful http://gu.com/p/3gkb3

20 June 2013: Ross Anderson on problems the extensive surveillance raises for the legal and medical professions http://www.theguardian.com/commentisfree/2013/jun/20/nsa-surveillance-doctors-lawyers-clients-snooped

21 June 2013: John Naughton, digital-technology columnist for The Observer newspaper, explains the important of "metadata" and how powerful a source of information it can be http://www.theguardian.com/technology/2013/jun/21/nsa-surveillance-metadata-content-obama

24 June 2013: Law Professor Douwe Korff suggests how the UK surveillance may contravene the

Human Rights Act (the UK legislation embodying the European Declaration on Human Rights) http://gu.com/p/3gny6

27 June 2013: Greenwald and Spencer Ackerman on Operation STELLARWIND, ended in 2011, to collect without explicit warrant metadata on emails and other Internet interactions http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama but the collection is ongoing – material about EVILOLIVE and SHELLTRUMPET http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

29 June 2013: Laura Poitras and others, for the German journal der Spiegel, on the NSA spying on EU officials http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html

02 July 2013: Leo Hickmann has a very odd take on the notion of "algorithm" http://gu.com/p/3h223

03 July 2013: Jürgen Trittin recommending Germany offer asylum to Snowden. The problem, as with other countries, is how one would bring him from Moscow to Germany without giving a chance for him to be legally intercepted on the way http://gu.com/p/3h2yf

07 July 2013: Henry Porter on a new book on US counterinsurgency by Douglas Porch http://gu.com/p/3h5f3

07 July 2013: John Naughton is appropriately cynical about NSA "reassurances" that they have "only" been going traffic analysis ("gathering metadata") and not content. Traffic analysis is sometimes more revealing than content! http://gu.com/p/3h4c8

07 July 2013: The technical news service from the Hannover technical publisher Heise reports on data collected by the Deutsche Post, a german postal service, and sent on to surveillance agencies http://www.heise.de/newsticker/meldung/Deutsche-Post-schickt-Daten-an-US-Behoerden-1912542.html (Thanks to Alexander Stiebing for the reference.)

09 July 2013: Cryptome on Snowden and Spiegel: http://cryptome.org/2013/07/snowden-spiegel-13-0707-en.htm

12 July 2013: Greenwald, Ewen MacAskill, Poitras, Ackerman and Dominic Rushe on Microsoft sharing encrypted material with the NSA under order http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data

15 July 2013: Schneier's Crypto-Gram https://www.schneier.com/crypto-gram-1307.html

16 July 2013: Former Taoiseach John Bruton on US spying on the EU (Spiegel, 29 June) http://www.project-syndicate.org/commentary/nsa-surveillance-and-us-violation-of-international-law-by-john-bruton He says it violates the 1961 Vienna Convention and signatories should stick to what they agreed.

24 July 2013: Geoffrey Robertson QC on why Snowden chose wisely to remain where he was http://gu.com/p/3hg5y namely, the US track record in forcing down aircraft. We recall that the Presidential jet of Evo Morales, president of Bolivia, was refused permission to fly through French and Portuguese airspace, and was boarded and searched in Vienna on a refueling stop.

28 July 2013: Naughton on how revelations affect the Internet

http://www.theguardian.com/technology/2013/jul/28/edward-snowden-death-of-internet namely, they herald the "death" of the internet as a global network, and render US cloud-service providers all but useless for business use elsewhere

29 July 2013: Greenwald on public opinion in the US
http://www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew For the first time, more respondents think that anti-terror measures (better said, liberty-restricting measures justified as being for anti-terror purposes) go too far (47%) than think they do not go far enough (35%).

31 July 2013: The UK Parliament's Home Affairs Committee report on internet crime that Britain is "losing the war" http://www.theguardian.com/technology/2013/jul/30/britain-losing-war-against-internet-crime Bruce Scheier has comments in a recent Cryto-Gram about overuse of the "war" epithet and the consequent militarisation of police forces in the US

31 July 2013: Greenwald on XKeyScore, the program to collect data in almost-real-time from specific targeted user devices http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

7 August 2013: CUNY journalism Professor Jeff Jarvis opines that we need the help of the tech companies to protect us from government surveillance
http://www.theguardian.com/commentisfree/2013/aug/07/big-tech-protect-big-brother
It is not clear to me how they could do this, given that those in the US, where many of them are centered, are required to comply with FISA decisions. Interesting in the light of November's revelations is Vint Cerf's comment that Google needs to transfer data unencrypted internally in order to offer improved service (such as, for example, correlation of other user data with user's calendar).

9 August 2013: Ackerman on the secure E-Mail service Lavabit shutting down and being unable to explain why http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden It is moderately certain it is because of a legal order to deliver some materials or otherwise cooperate with the NSA under court order. It is illegal to say so. Lavabit was used by Snowden.

13 August 2013: An extensive NYT article about Laura Poitras and her work
http://nyti.ms/1d0mkQu

15 August 2013: Schneier's Crypto-Gram https://www.schneier.com/crypto-gram-1308.html

17 August 2013: Guardian on Germans' views. The government says initial concerns have been resolved; the public by and large doesn't necessarily believe the government http://gu.com/p/3t4hg

19 August 2013: Greenwald's partner David Miranda detained at Heathrow airport
http://www.theguardian.com/world/2013/aug/18/glenn-greenwald-guardian-partner-detained-heathrow Jonathan Watts interviews him in Rio upon his release and return
http://www.theguardian.com/world/2013/aug/19/david-miranda-interview-detention-heathrow
The Guardian Editor Alan Rusbridger explains what there is to worry about, namely intimidation, and tells about the intimidation from the government leading to the physical destruction on Guardian premisses of computers and storage media containing documents derived from Snowden
http://www.theguardian.com/commentisfree/2013/aug/19/david-miranda-schedule7-danger-reporters as well as a video from 20 August
http://www.theguardian.com/world/video/2013/aug/20/alan-rusbridger-miranda-snowden-nsa-gchq-

video

19 August 2013: Greenwald says this is an obvious attempt at intimidation and it will not work on him http://www.theguardian.com/commentisfree/2013/aug/18/david-miranda-detained-uk-nsa

20 August 2013: The Politics Blog of the Guardian “as it happened” by Andrew Sparrow, Adam Gabbatt and Ben Quinn http://www.theguardian.com/politics/blog/2013/aug/19/glenn-greenwald-partner-detained-live-reaction

20 August 2013: Sir Simon Jenkins, former editor of The Times and now columnist for the Guardian, and one of the best short-article writers in English, is appalled at the Miranda detention and says what it means http://www.theguardian.com/commentisfree/2013/aug/20/innocent-fear-david-miranda

21 August 2013: Greenwald comments on other newspapers' reactions to the Miranda detention and what he said subsequent to it http://www.theguardian.com/commentisfree/2013/aug/21/sending-message-miranda-gchq-nsa In summary: not all the press in the free world is on the side of press freedom; some of it is on the side of government repression.

24 August 2013: An open letter to British Prime Minister David Cameron from editors of newspapers in Nordic countries on press freedom and the Miranda detention http://www.theguardian.com/theobserver/2013/aug/24/cameron-press-freedom-security-miranda and Jamie Doward's report on this http://www.theguardian.com/world/2013/aug/24/david-miranda-detention-greenwald-press-editors

27 August 2013: Schneier on Miranda's detention http://www.theatlantic.com/international/archive/2013/08/the-real-terrifying-reason-why-british-authorities-detained-david-miranda/278952/ Schneier thinks that obtaining his material for analysis should only take a short while, and detaining him for the full 9 hours permitted under the law which was questionably used is clearly an attempt at intimidation.

2 September 2013: The Economist on the NSA breaking encryption http://www.economist.com/blogs/babbage/2013/09/breaking-cryptography

5-6 September 2013: Ball, Julian Borger and Greenwald report that the NSA can access material encrrypted with standard techniques http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security The New York Times is reporting this jointly http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html by Nicole Perlroth, Jeff Larson and Scott Shane.

5 September 2013: Schneier proposes that engineers must "take back" the Internet http://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

5 September 2013: The NSA's classification system for cryptanalysis: what they do and how it's ranked when they do it: http://www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis

5 September 2013: A blog article by Matthew Green, recommended by Schneier, speculating on how that NSA may be defeating encryption. As Schneier says, the math is solid, but the code not necessarily. http://blog.cryptographyengineering.com/2013/09/on-nsa.html Green is also an associate of the Barr Group, newly famous for dissecting Toyota's throttle-control code for the 2005 Camry and showing the possible of uncommanded acceleration.

9 September 2013: Princeton Professor Ed Felten on how the subversion of standards is destroying trust, and what the consequences will be https://freedom-to-tinker.com/blog/felten/nsa-apparently-undermining-standards-security-confidence/

9 September 2013: NYT reports on the NSA subverting encryption techniques and methods http://nyti.ms/1dV982u

9 September 2013: Watts reports that the NSA is said to have spied on Brazilian company Petrobras. The suggestion is that this is for economic rather than for security reasons http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

12 September 2013: Sir Stephen Sedley, a judge of the Court of Appeal from 1999 to 2011, in the London Review of Books 35(17), 12 September 2013 considers government surveillance http://www.lrb.co.uk/v35/n17/stephen-sedley/beware-kite-flyers In the guise of a review of a book on the constitution of Great Britain, Sir Stephen considers what is constitutionally acceptable and what not.

13 September 2013: Harvard Law Professor and Director of the Berkman Center for Internet and Society Yochai Benkler says that the NSA must be reformed, and from outside http://www.theguardian.com/commentisfree/2013/sep/13/nsa-behemoth-trampling-rights

15 September 2013: Naughton substantiates his view on (not) trusting US Cloud computing providers http://gu.com/p/3tyn3

15 September 2013: Schneier's Crypto-Gram https://www.schneier.com/crypto-gram-1309.html Includes the link to the Miranda opsec blunder http://joshuafoust.com/extraordinary-court-statement/

16 September 2013: UK academics complain about undermining the infrastructure of the Internet http://www.theguardian.com/technology/2013/sep/16/nsa-gchq-undermine-internet-security Here is their letter on the Bristol Cryptography Blog http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html

18 September 2013: Matthew Green's technical explanation of the concerns about DUAL_EC_DRBG http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html

19 September 2013: Sir Simon Jenkins' outrage at the extent of the surveillance. http://www.theguardian.com/commentisfree/2013/sep/19/gchq-we-monster-we-cant-control

20 September 2013: Sir Malcolm Rifkind's reply to Jenkins http://gu.com/p/3jvca Rifkind is a former Foreign Secretary and Defence Secretary of the UK Government and chairs the Intelligence and Security Committee of the UK Parliament. The ISC usually meets in secret and is the oversight body of the intelligence and security agencies. Notably, Rifkind has seen no need to respond to Ross Anderson's and Bruce Schneier's specific technical claims about how these spying techniques have subverted essential social services such as doctor-patient and lawyer-client-expert confidentiality, and commercial transactions over the Internet. It may be because – how shall I put it? - the technical issues aren't well understood by some politicians.

21 September 2013: Computer-security firm RSA warns users that the default random-number generator algorithm in its security software Bsafe is “weak”, and advises users to switch to one of

the other generation algorithms in the software.
http://www.theguardian.com/world/2013/sep/21/rsa-emc-warning-encryption-system-nsa

23 September 2013: Apple's Fingerprint ID hacked by CCC
http://www.theguardian.com/technology/2013/sep/22/apple-iphone-fingerprint-scanner-hacked
Bruce Schneier had a comment in the 15 September Crypto-Gram that the fingerprint-ID was probably a good idea. He suggested that if a thief walks off with your iPhone, you likely have greater problems.

30 September 2013: Ball on the NSA storing metadata on internet use for up to a year
http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents

3 October 2013: Lavabit founder Ladar Levison is able now to talk more about what went on leading to his decision to close the company http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html

4 October 2013: Brilliant article by John Lanchester http://gu.com/p/3j9cj Lanchester writes extensive and very readable articles for the London Review of Books on such matters as the global financial collapse due to the collapse of the market for sub-prime mortgage derivatives in the US

4 October 2013: Schneier explains how the NSA goes after online anonymity, Tor and Firefox users, with two tools QUANTUMINSERT and FOXACID
http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

4 October 2013: Ball, Schneier and Greenwald report in a more general manner on this activity
http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption
Please note that Schneier has said that the URL inside the essay has been corrupted and is now serving malware – so don't click on it

4 October 2013: A document showing how EGOTISTICALGIRAFFE targets Tor users
http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document

4 October 2013: Another document expressing NSA frustration with Tor
http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

4 October 2013: But the NSA thinks that Tor is fundamentally secure, and there are no potential alternatives http://www.theguardian.com/world/interactive/2013/oct/04/tor-high-secure-internet-anonymity

4 October 2013: The US Director of National Intelligence (James Clapper) has set up a Review Group to review the NSA surveillance and has called for comment. The Center for Democracy and Technology along with the Electronic Frontier Foundation have responded. They point out that DUAL_EC_DRBG is insecure. And false X.509 certificates have been deliberately distributed. https://www.cdt.org/files/pdfs/nsa-review-panel-tech-comment.pdf The ACM response to the same call is far more anodine http://usacm.acm.org/images/documents/ReviewGroupUSACM.pdf

4 October 2013: Schneier explains how the publish-and-fix regime of publicising security failures has enhanced Internet security and how the NSA's programs to build in surreptitious backdoors and other mechanisms are subverting it and thereby making the Internet less secure that it might be
http://www.theguardian.com/commentisfree/2013/oct/04/nsa-attacks-internet-bruce-schneier

6 October 2013: Former government minister Chris Huhne says that the UK National Security

Council was never briefed on the surveillance, and should have been http://www.theguardian.com/commentisfree/2013/oct/06/prism-tempora-cabinet-surveillance-state

7 October 2013: The newspaper Die Zeit relates how the German surveillance agency BND surveys Internet communications. Legally, but uncontrolled, says the paper. http://www.zeit.de/digital/datenschutz/2013-10/bnd-internet-ueberwachung-provider (Thanks to Christoph Rüther for the reference.)

9 October 2013: Andrew Parker, current Chief of UK MI5, explains why the current surveillance is necessary. He does not address any of the technical matters concerning the subversion of legitimate Internet transactions raised by Schneier and Anderson. I think I shall start to call it the Schneier-Anderson Test: do you address them (pass) or not (fail)? http://www.theguardian.com/uk-news/2013/oct/09/david-cameron-mi5-chief-edward-snowden-gchq-leaks

10 October 2013: Prominent UK human-rights barrister Clive Stafford Smith suggests that Andrew Parker's "world view" does not hold up in his experience http://www.theguardian.com/commentisfree/2013/oct/10/mi5-andrew-parker-different-world-shaker-aamer

11 October 2013: The British newspaper Daily Mail said that the Guardian's revelations about GCHQ and NSA data collection and analysis is "lethally irresponsible" Guardian editor Alan Rusbridger responds http://gu.com/p/3jfxe

11 October 2013: And the Guardian solicited the views of other editors of major press organs throughout the world on the nature of what it is doing revelations http://gu.com/p/3jfx4

11 October 2013: The Guardian also quotes from many non-press people involved, including Schneier, Anderson and other security informaticians http://gu.com/p/3jfx2

11 October 2013: UK Deputy Prime Minister Clegg announces an inquiry into the appropriateness of GCHQ surveillance http://www.theguardian.com/world/2013/oct/10/guardian-nsa-spies

11 October 2013: The Coalition government is at odds over GCHQ surveillance and the Guardian's revelations http://www.theguardian.com/uk-news/2013/oct/11/coalition-spying-vince-cable-mi5-mi6-gchq

12 October 2013: Hilary Clinton at a Chatham House conference says that a dialog needs to start with as much oversight and citizen participation as possible http://www.theguardian.com/world/2013/oct/11/hillary-clinton-spying

12 October 2013: Shami Chakrabati, Director of the human-rights organisation Liberty and ex-MI6 officer Nigel Inkster debate the rights and wrongs of such surveillance practice http://gu.com/p/3jgv9

14 October 2013: Lord Blencathra is a former Home Office minister, who led the formal inquiry into the data communications bill (the "snoopers' charter"), proposed earlier this year by the government and defeated in parliamentary and ex-parliamentary debate The bill would have legitimised much of what the GCHQ has been found already to have been doing. This suggests that the Parliament cannot legitimately approve of current GCHQ techniques http://gu.com/p/3jh7h

14 October 2013: Prominent UK human-rights barrister Clive Stafford Smith may possibly have

had his communciations with clients monitored
http://www.theguardian.com/uk-news/2013/oct/13/gchq-accused-monitoring-privileged-emails-lawyer-client-libya

14 October 2013: The Law Society has expressed its concern over the threat to privileged legal communications, especially in court cases involving government and government programs
http://www.theguardian.com/law/2013/oct/13/gchq-surveillance-right-challenge-state-law

15 October 2013: Lord (Ken) Macdonald QC, former Director of Public Prosecutions, suggests in response to the comments by the Head of MI5, Andrew Parker, that surveillance must explicitly conform with, and be ruled by, the law of the land http://gu.com/p/3jgzk

15 October 2013: Schneier's Crypto-Gram https://www.schneier.com/crypto-gram-1310.html

16 October 2013: Former Minister Nick Brown criticises surveillance programs and lack of transparency, because the "snoopers' charter" (the data communications bill) was rejected by Parliament http://gu.com/p/3jt4q

17 October 2013: The UK Parliament's Home Affairs Committee is to look in to the Guardian's publication of material from Snowden http://www.theguardian.com/uk-news/2013/oct/16/mps-investigate-guardian-edward-snowden-leaks I take it you couldn't do this without the other investigation into surveillance practices (see next). On the other hand, Committee Chairs are independent of government politics, as they have to be. Vaz is Labor.

17 October 2013: The UK Parliament's Intelligence and Security Committee will hold a formal open inquiry into GCHQ's practices. (I am on the IET Information Technology Policy Panel and we intend to submit evidence.) http://gu.com/p/3jj42

17 October 2013: Richard Norton-Taylor and Ian Cobain give ten examples in which “national security” has been given as a reason for the government to try to stop the press publishing material. All arguably spurious. http://gu.com/p/3jthf

17 October 2013: The EU is drawing up new regulations on data protection in view of the Snowden revelations. http://gu.com/p/3jjh5

17 October 2013: An editorial in the Guardian on recent developments; two articles in the Washington Post; new bills being written in the US Congress, and so on. http://gu.com/p/3jkxm

18 October 2013: Keir Starmer, the Director of Public Prosecutions for England and Wales, says that there is a public-interest defence for some journalistic behavior which would otherwise be against the law, and announces legal guidelines for such protection. http://gu.com/p/3jkt5

18 October 2013: Edward Snowden says he has no documents with him in Russia and disputes that Chinese or Russian spy services had obtained any information from him. http://gu.com/p/3jk48

18 October 2013: Facebook, Google, Microsoft, Yahoo! And Twitter have given joint written evidence to the UK House of Commons Home Affairs Committee asking for a “full public debate” to demonstrate that state powers are not being abused. http://gu.com/p/3jk8k

18 October 2013: The commentator Jonathan Freeland deplores the reaction of the British Parliament to the Snowden revelations and contrasts it with that of the US Congress.
http://gu.com/p/3jkmk

20 October 2013: A news item about former Cabinet Minister Chris Huhne's report that the UK cabinet was not informed about GCHQ's Tempora program. http://gu.com/p/3jybg

20 October 2013: Huhne's article. The cabinet and the National Security Council were not informed about Tempora, and neither was the committee set up to scrutinise the communications data bill, which legitimised much of what Tempora was doing and was decisively rejected by parliamentarians. http://gu.com/p/3jy6b

20 October 2013: Harold Evans, former editor of the Sunday Times and now retired, recounts experiences at the Sunday Times in which "*over 14 years the barriers erected against legitimate inquiry on grounds of national security – reporting, not document dumps – proved spurious or self-serving.*" http://gu.com/p/3jy94

24 October 2013: Frau Merkel disapproves of spying on "friends" after the revelations that the NSA had recorded French telephone calls, and also her phone. http://gu.com/p/3jpvc

25 October 2013: An article by Simon Jenkins on Silicon Valley, technology, surveillance and the future. http://gu.com/p/3jp2v

25 October 2013: Ball with some details of measures taken by GCHQ to keep details of its surveillance program secret. GCHQ was apparently concerned about legal challenge, which is indeed what is now happening in Strasbourg http://gu.com/p/3jpmg

25 October 2013: Guy Verhofstadt, former Prime Minister of Belgium, says that the EU has a duty to protect its citizens from certain forms of surveillance, and that privacy regulations need strengthening. http://gu.com/p/3jpm3

29 October 2013: US Senator Dianne Feinstein, who chairs the Senate's intelligence oversight committee, becomes incensed at finding out that the NSA concealed certain activities from her committee and says reform is needed http://www.theguardian.com/world/2013/oct/28/nsa-surveillance-dianne-feinstein-opposed-allies

1 November 2013: A throughly worthwhile suggestion from Cambridge MP Julian Huppert for better technical oversight of electronic spying, and for a debate to "rebalance" the needs of security and privacy. http://gu.com/p/3kxh2

1 November 2013: The Oxford Professor, noted commentator on Germany and European society, and Guardian columnist Timothy Garton Ash, argues that of the need for and tensions between freedom, security and privacy, it is privacy that is most under threat and needs most attention http://gu.com/p/3k2z2

1 November 2013: The New York Times reports that the revelations on surveillance are undermining the business model of internet firms and that they are starting to take countermeasures http://nyti.ms/Hi6F3o

1 November 2013: Julian Borger reports the extent of cooperation between the British, French, German, Spanish and Italian security services on the collection of information on electronic communications http://gu.com/p/3k3h8

1 November 2013: Matthew Taylor, Nick Hopkins and Jemima Kiss suggest that countries are taking steps towards physically-internal internet domains, as a response to the reports of pervasive spying http://gu.com/p/3k3dt

1 November 2013: Dan Roberts and Spencer Ackerman report that US Secretary of State John Kerry has said that some surveillance activities have gone "too far" http://www.theguardian.com/world/2013/oct/31/john-kerry-some-surveillance-gone-too-far

1 November 2013: In UK parliamentary debate, MPs Dominic Raab and Julian Huppert say it is not the case that Guardian reporting on the surveillance activities of the spy services has gone too far and that a debate on appropriate oversight is needed http://www.theguardian.com/media/2013/oct/31/tory-dominic-raab-defends-guardian-mi5-nsa-gchq

1 November 2013: Ian Brown, Associate Director of Oxford University's Cybersecurity Centre suggests that one consequence of pervasive surveillance will be that the Internet will "balkanised", evolve separate domains, separated along narrow lines of national interest http://gu.com/p/3k3ga

2 November 2013: Jamie Doward reports on the reasons the Metropolitan Police have given in court for the detention of David Miranda, and they seem to be that he is promoting a "political or ideological cause" http://gu.com/p/3k44f Apparently that makes you suspect of terrorism. Gee, one could detain a few Guardian columnists for that – Timothy Garton Ash or Simon Jenkins, for instance.

2 November 2013: MacAskill and Ball provide some background on the history of NSA's surveillance activities http://www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance

4 November 2013: Matthew Taylor and Hopkins report on the letter from seventy human rights organisations to UK Prime Minister David Cameron saying the government's reactions to the spying revelations are endangering the UK's reputation for press freedom http://www.theguardian.com/world/2013/nov/03/uk-reaction-nsa-leaks-human-rights A link to the actual letter is included.

4 November 2013: Here a carefully measured comment from the Marconi Professor of Communications Systems at Cambridge, who is a Fellow of the Royal Society and Fellow of the Royal Academy of Engineering. He seems determined. If anyone is unsure what the acronym "F.U." stands for, please ask :-) http://paravirtualization.blogspot.co.uk/2013/11/fu-nsa.html

4 November 2013: Hopkins and Taylor interview former Home Secretary David Blunkett, who says the law needs to be improved to provide better oversight of electronic-spying activity http://www.theguardian.com/world/2013/nov/04/david-blunkett-review-laws-security-services

5 November 2013: GCHQ is able to tap into internal Google traffic, which travels unencrypted as explained by Vint Cert to Jeff Jarvis in an earlier note referenced here. http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/

6 November 2013: Germany has called in the UK Ambassador to explain about the extent of UK's data gathering in Berlin http://gu.com/p/3k5p3

6 November 2013: A brilliant political cartoon by Steve Bell on the UK spying on Germany http://www.theguardian.com/commentisfree/cartoon/2013/nov/05/steve-bell-germany-spying-

claims

7 November 2013: The inventor of the World Wide Web, Sir Tim Berners-Lee, expresses his disgust at the undermining of the Internet infrastructure, the consequences of that undermining, and that the strengths of the Internet must be reconstituted http://www.theguardian.com/world/2013/nov/06/tim-berners-lee-encryption-spy-agencies

7 November 2013: Nick Hopkins formulates 10 questions which the UK Parliament ISC could usefully put to the chiefs of MI5, MI6 and GCHQ when they appear http://gu.com/p/3k752

7 November 2013: News on the Miranda case. Miranda's lawyers argue that his detention was unlawful. The prosecution says, near the end of the article, why it thinks his detention was legal. http://gu.com/p/3k75h

7 November 2013: John Kampfner opines that the justifications offered for spying by NSA and GCHQ gives weight to the arguments of authoritarian regimes for similar controls over electronic communication of their peoples http://gu.com/p/3k7vz

7 November 2013: Cambridge MP Julian Huppert argues for reform of spying oversight http://www.theguardian.com/commentisfree/2013/nov/07/spy-chiefs-evidence-reform-oversight-intelligence

8 November 2013: Patrick Wintour reports on the appearance of the Heads of MI5, MI6 and GCHQ before the UK Parliament's ISC http://www.theguardian.com/world/2013/nov/07/nsa-leaks-enemies-rubbing-hands-glee-mi6

8 November 2013: The live blog by Paul Owen of developments during the public interview of MI5, MI6 and GCHQ chiefs by the UK Parliament's ISC http://www.theguardian.com/world/2013/nov/08/nsa-files-reaction-spy-chiefs-grilling-live It turns out that the IETF has been meeting in Vancouver. See Owen on Talbot on Farrell's comment at the meeting at 11.14 in the blog.

8 November 2013: Michelle Richardson, ACLU counsel and fellow of Stanford Law School's Center for the Internet and Society, opines that Senator Feinstein, chair of the intelligence oversight committee, doesn't have a clue: http://www.theguardian.com/commentisfree/2013/nov/08/dianne-feinstein-nsa-intelligence-reform-bill

8 November 2013: Jonathan Freeland, a commentator in the Guardian, speculates in the New York Times about why Brits in particular seem to be more concerned about revelations about GCHQ than about what GCHQ is actually doing: http://nyti.ms/17kKIN3
8 November 2013: Bruce Schneier suggests in the Atlantic Monthly that the partnership between Internet companies and surveillance organisations (partly cooperative and partly coerced) is starting to fray http://www.theatlantic.com/technology/archive/2013/11/a-fraying-of-the-public-private-surveillance-partnership/281289/

10 November 2013: The Observer's infotech columnist John Naughton relates how “British and US spies have compromised e-commerce and civil liberties with a series of clever coding stunts”, along with the no-infamous pencil sketch of NSA obtaining access to Google-internal networks with a smiley face: http://www.theguardian.com/world/2013/nov/10/nsa-war-on-terror-neat-hacking-game

11 November 2013: Lord Deben, a former government minister, says that (in the Guardian's words) “spying agencies too easily use terrorism [sic] as an excuse to invade civil liberties.”

http://gu.com/p/3k7f4 Quotation marks are needed around the word “terrorism”, otherwise the sentence doesn't mean what it was intended to mean!

11 November 2013: Kenneth Roth, executive director of Human Rights Watch, argues that current spying laws cannot cope with “the digital era” http://gu.com/p/3k9db

11 November 2013: The Economist reports on the IETF's Vancouver meeting and the discussion of what is to be done pursuant to the revelations about NSA surveillance http://www.economist.com/blogs/babbage/2013/11/internet-after-snowden

12 November 2013: The UK Information Commissioner, Christopher Graham, says that issues of national security cannot be allowed to overshadow concerns of legitimate public interest http://www.theguardian.com/uk-news/2013/nov/11/information-commissioner-very-concerned-online-eavesdropping

12 November 2013: Jim Sensenbrenner, author of the US Patriot Act, has told a committee of the European Parliament, in what is said to be the first ever address by a US lawmaker, that expanding his bill to restrict electronic intelligence gathering to include non-US citizens would be a step too far http://www.theguardian.com/world/2013/nov/11/sensenbrenner-leahy-nsa-reform-european-parliament

13 November 2013: The administration of the University of Bielefeld has circulated a memorandum warning about threats to the confidentiality of research data (by which they also mean draft papers) transmitted both within the university intranet itself and to/from collaborators outside the university. The administration reminds researchers that they have a legal obligation to ensure that confidentiality as far as possible. It announces that technical measures are being developed by the university computing services to assure it in the future. The document is not publicly available as yet.

15 November 2013: Bruce Schneier's Crypto-Gram for November. As usual, packed with information about the surveillance situation, and also what people offering services over the Internet, and the IETF, are beginning to do about it. One significant push appears to be to offer incontrovertible crypto by default for all TCP apps https://www.schneier.com/crypto-gram-1311.html

17 November 2013: The UK's ex-Lord Chancellor, Lord Falconer, says any social threat claimed to be posed by revelations about surveillance has been exaggerated, and defends the reporting by the Guardian http://gu.com/p/3kegc

18 November 2013: Nick Hopkins and Matthew Taylor report on private firms offering Internet surveillance capabilities http://gu.com/p/3kfch

18 November 2013: Indonesia recalls its ambassador to Australia for “consultations” after it is revealed that Australia had overheard communications of the Indonesian President and his wife. Australia said “everybody does it”. Indonesia replied “we don't.” http://gu.com/p/3kf85

18 November 2013: Lord Ashdown, former leader of the UK's Liberal Democratic party, now in coalition government, says that government surveillance activities are out of control and the proper level of surveillance, and to what end, requires a “high-level inquiry” http://gu.com/p/3kfed

19 November 2013: Sir John Stanley, chairman of the UK Parliamentary committee on arms export controls, says according to the article that “governments must review the electronic equipment now

being sold by private companies to ensure that authoritarian regimes were not allowed to acquire technology that could be used for internal repression" (indirect quotation) http://gu.com/p/3kgc8

19 November 2013: Spencer Ackerman reports on the publication of a FISA court order that allowed collection of "Americans' email and internet data", as well as the court's concern that restrictions were being violated http://www.theguardian.com/world/2013/nov/19/court-order-that-allowed-nsa-surveillance-is-revealed-for-first-time

19 November 2013: Spencer Ackerman reports that some of the proceedings of the US FISA court have been made public, and reveal the "extent of NSA disregard for privacy restrictions" http://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy

20 November 2013: The commentator Sir Simon Jenkins says that the days are over of believing spy chiefs when they ask the public to trust them. http://www.theguardian.com/commentisfree/2013/nov/20/days-believing-spy-chiefs-over

20 November 2013: James Ball reports that GCHQ has asked NSA to provide it with details of Britons who were not under specific suspicion, since 2007 http://www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

20 November 2013: Jin Sensenbrenner, an author of the US Patriot Act, says that NSA surveillance practices are hurting business http://www.theguardian.com/commentisfree/2013/nov/20/jim-sensenbrenner-nsa-overreach-hurts-business

21 November 2013: The UK Parliament's intelligence and security committee, the oversight committee of GCHQ and other intelligence services, is to ask for a detailed report on GCHQ's request to the NSA to collect information on Britons not suspected of wrongdoing http://gu.com/p/3khp9

22 November 2013: James Risen and Laura Poitras report on NSA's surveillance "strategy" as contained in a document they have seen http://nyti.ms/18Xx2mp

24 November 2013: Twitter announces it is to join Google and Facebook in using "perfect forward secrecy" to protect the communications of its users from surveillance http://gu.com/p/3kjfg PFS is a way to protect individual session keys from compromise even if a long-term key using in asymmetric cryptography is compromised in the future. Wikipedia suggests that PFS is (yet) another invention of Whit Diffie et al. http://en.wikipedia.org/wiki/Forward_secrecy

26 November 2013: Ian Traynor reports an interview with Justice and Rights Commissioner VivianeReding, who says the EC is considering "freezing" the data-sharing arrangements with the US because of concerns about surveillance activities, that the US will have to adjust their surveillance activities to comply with EU law and to enable legal redress in the US courts for Europeans whose rights may have been infringed, and that European businesses need to compete on a "level playing field" with US rivals. This latter seems to refer to "commercial swaps", the exchange of commercial information in order to inhibit terrorist funding, and sharing information on transatlantic airline passengers http://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing

26 November 2013: US senators Ron Wyden, Mark Udall, and Mark Udall, members of the Senate Intelligence Committee which oversees the work of the NSA, say that the bulk collection of metadata on US phone calls violates the intent of the Fourth Amendment, and the bill now before Congress to limit surveillance activities does not go far enough http://nyti.ms/1evwVD5

26 November 2013: Nicole Perlroth and John Markoff suggest that the NSA was able to obtain internal data from Yahoo! and Google by tapping into HW owned by the companies who provide data-transmission services to them http://nyti.ms/18koED5

27 November 2013: Jaron Lanier laments that the "cool devices", which everyone thought would enhance human potential, are inextricably intertwined with the loss of freedom, the "consumer-surveillance economy", and he cannot separate the two trends http://nyti.ms/1cFq5sI

28 November 2013: Reuters reports that Canada let the NSA spy on the G20 summit in Ottawa in 2010 http://gu.com/p/3knj7

28 November 2013: Journalist Misha Glenny reports in the NYT on the varieties of malfeasance on the Internet, including cybercrime, credit-card fraud, "hacktivism", espionage, malware and deception, and so on http://nyti.ms/1e4WpXQ He notes that credit-card fraud continues to "rise steadily" in the US, which he claims is a result of the "lamentable failure" of US credit-card issuers to adopt chip-and-pin. So an opportunity here for an amusing diversion (if you're not a banker). Chip-and-PIN as it then was was definitively broken by the group around Ross Anderson in Cambridge, announced in http://www.lightbluetouchpaper.org/2010/02/11/chip-and-pin-is-broken/ and the prize-winning technical paper in 2010 http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf Banks dismissed the attack as "theoretical", whereupon Master's student Omar Choudary implemented and demonstrated hardware to perform an attack in real-time http://www.lightbluetouchpaper.org/2010/10/19/the-smart-card-detective-a-hand-held-emv-interceptor/ Some banks then apparently put pressure on Cambridge University to remove Choudary's MPhil thesis from the public domain. Anderson carefully explained the notion of a public university and public research, referenced here http://www.lightbluetouchpaper.org/2010/12/25/a-merry-christmas-to-all-bankers/ The point here is that when Professor Anderson et al. tell you in a public document that X "is broken", then, first, that statement means exactly what it says, and, second, it is correct. That weakness has been fixed, it seems, but stuff about chip-and-PIN is ongoing – here is a paper from 2012 about organisations using weak nonce-generation that allows pre-play attacks http://www.cl.cam.ac.uk/~rja14/Papers/unattack.pdf This all underlines the general point that security protocols and devices are not once-and-for-all things. When we worry that SSL/TLS has been "broken" by surveillance organisations, it is not an all-or-nothing thing that is being worried about; it is a gradual thing.

29 November 2013: Former UK Director of Public Prosecutions Lord McDonald has given a speech in which he said oversight of surveillance organisations must be improved; the intelligence and security committee of Parliament should become a Select Committee with concomitant powers (which it does not currently have); and it should be led by an opposition-party politician who was not formerly associated with the security services in any executive capacity http://gu.com/p/3knkg

2 December 2013: David Anderson QC, the UK's independent reviewer of terrorism legislation, recommends that detention without suspicion at UK ports should last no longer than an hour, with concrete suspicion of involvement in terrorism required for further detention. Also, stronger safeguards on personal electronic data and other sensitive information during such inquiries http://www.theguardian.com/law/2013/dec/01/uk-terror-law-watchdog-detention-borders-schedule-7

2 December 2013: A revelation today that Australia offered to share data with other 5-eyes members, ostensibly to circumvent laws which prevent spying on one's own citizens. Geoffrey Robertson QC on the (il)legality of some of this

http://www.theguardian.com/commentisfree/2013/dec/02/privacy-australians-surveillance-metadata
2 December: Tim Berners-Lee is reported by Ed Pilkington to be "dismayed" by attempts to subvert WWW security, and about the invasions of privacy
http://www.theguardian.com/technology/2013/dec/03/tim-berners-lee-spies-cracking-encryption-web-snowden

2 December 2013: Ross Anderson suggests what it is like to work in various professions in a "post-Snowden" world, as an advertiser, police officer, lawyer, civil servant, doctor, and banker
http://www.theguardian.com/world/2013/dec/02/work-surveillance-snowden-spying-security

3 December 2013: Ben Emmerson QC is the United Nations special rapporteur on counter-terrorism, and the British judge on the international criminal tribunals for Rwanda and the former Yugoslavia. He is starting an investigation for the UN into the surveillance matters revealed in the Snowden documentation, which is due to report in Autumn 2014. He says that a suggestion that the Guardian's reporting can be equated with aiding and abetting terrorism, as has been suggested by some in Britain, should be decisively rejected http://gu.com/p/3kpy2

4 December 2013: Member of the UK parliament's Home Affairs Select Committee Julian Huppert, along with David Winnick one of the two members most concerned about the extent of spying and its consequences, comments on the interview with Guardian editor Alan Rusbridger; inter alia that the focus should more properly be on the nature of surveillance and what surveillance is appropriate, rather than how a newspaper handled the revelations (in fact, somewhat around 1% only of the documents have been published or commented, and care has been taken not to compromise security personnel). It is also surmised that MI5 Chief Andrew Parker will give evidence to the committee – he has been invited for December 17 to explain his claim that the leaks have endangered British national security, but has not agreed to appear. http://gu.com/p/3kqph
Huppert notes

> *Efforts [during the Rusbridger interview] to explain to committee members about the background, and projects such as those designed to undermine the anonymity software tool Tor, were repeatedly shut down. ....*
> *This was symptomatic of the wider problem: Britain has missed the point. While in America the president has committed himself to a full review of oversight structures, and the UN has launched an investigation into spying practices, in Britain politicians and the press have been distracted by the vehicle, not the content. We should bear in mind that the only real leak has come from the NSA itself, which failed to control what it claims is very sensitive information but was apparently available to hundreds of thousands of people.*

The New York Times has an account of the interview by Ravi Somaiya at http://nyti.ms/1c9w3Ay

9 December 2013: Matthew Taylor and Nick Hopkins report that Amnesty International will take legal action against the UK government over concerns that its communications have been illegally accessed by UK security services http://gu.com/p/3y34g

9 December 2013: Jan Philipp Albrecht, an MEP, has announced that arrangements are being made to have Edward Snowden address the European Parliament by video link http://gu.com/p/3y35x

9 December 2013: 8 of the "world's leading technology companies", meaning Internet companies Apple, Google, Microsoft, Facebook, Yahoo, Twitter, LinkedIn, and AOL, have written an open letter to US President Obama demanding changes in laws and surveillance practices to restore public trust in the Internet http://www.theguardian.com/world/2013/dec/09/nsa-surveillance-tech-companies-demand-sweeping-changes-to-us-laws

9 December 2013: The open letter has its own WWW site at http://reformgovernmentsurveillance.com/

9 December 2013: CUNY Journalism professor and Guardian commentator Jeff Jarvis welcomes the letter as a "critical step in sparking real debate over surveillance and civil rights" but says it does not go far enough http://www.theguardian.com/commentisfree/2013/dec/09/tech-giant-companies-open-letter-white-house

9 December 2013: Mark Mazetti and Justin Elliott report in the NYT on spying agencies' infiltration of on-line games such as World of Warcraft and Second Life http://nyti.ms/1aNPMop

10 December 2013: Matthew Taylor and Nick Hopkins report that some 500 of the world's leading authors, including 5 Nobel Prize winners, have instigated a petition to the UN demanding an "international bill of digital rights" that would "enshrine the protection of civil rights in the Internet age", because the spy agencies are undermining democracy in their current surveillance practices http://gu.com/p/3y43k . The petition is at http://www.change.org/petitions/a-stand-for-democracy-in-the-digital-age-3

10 December 2013: The British playwright Tom Stoppard expresses his view on the conflict between surveillance and open society at http://gu.com/p/3y44z
He asks:

> *What is the society we wish to protect? Is it the society of complete surveillance for the commonwealth? Is this the wealth we seek to have in common - optimal security at the cost of maximal surveillance? Not that anybody asked us. It takes a brave newspaper to have forced the question into the open.*

10 December 2013: Let's not forget that the US and UK aren't the only ones. Nicole Perlroth reports on Chinese infiltration into computers at the foreign ministries of the Czech Republic, Portugal, Bulgaria, Latvia and Hungary, according to security company FireEye http://nyti.ms/18jv70N

10 December 2013: Dan Goodin reports in *ars technica* that the FreeBSD developers do/will not allow users of FreeBSD to make use of the hardware encryption on chips from Intel or Via directly, without an extra SW entropy-adding layer http://arstechnica.com/security/2013/12/we-cannot-trust-intel-and-vias-chip-based-crypto-freebsd-developers-say/ (thanks here to a pointer by Dewayne Hendricks in the Risks Forum 27.65 of 19 December http://catless.ncl.ac.uk/Risks/27.65.html)

11 December 2013: Former UK government minister David Heath is proposing a Member's Bill (a bill introduced by an MP rather than by the government) to eliminate warrantless surveillance in the UK http://gu.com/p/3y5x9

12 December 2013: Patrick Wintour and Alan Travis report that Andrew Parker, head of MI5, will not give evidence after all to the UK parliament's Home Affairs Select Committee, as decided by the Home Secretary Theresa May, who said that such an appearance would "duplicate" his work with the ISC. May will appear at the HASC. Also, the ISC's call for evidence for open hearings has been published http://gu.com/p/3y6vf

12 December 2013: Matthew Taylor and Nick Hopkins report that the organisation Index on Censorship has criticised the EU for not defending the actions of Edward Snowden, and not taking more decisive action pursuant to the revelations http://gu.com/p/3y62h The IoC's report is at http://www.indexoncensorship.org/2013/12/eureport/

12 December 2013: Kim Willsher reports that a new French law passed on 11 December allows French government and intelligence officials to monitor any internet usage, from anyone, in real time, without specific warrant http://gu.com/p/3y5kp France thereby becomes the first explicit internet-surveillance state in the Western world.

12 December 2013: In the NYT, Julia Baird explains from Sydney how electronic eavesdropping hurts diplomacy, using the example of the break in political communications between the two regional powers Australia and Indonesia. (Besides being a journalist, Baird has a PhD in political science) http://nyti.ms/IHjpS2

13 December 2013: David E. Sanger reports in the NYT on the rumors of the White House review committee's report on the NSA electronic surveillance, that broadly it should continue, but under new restraints to increase privacy protections. For U.S. citizens, that is. http://nyti.ms/1j1zNNy

15 December 2013: Bruce Schneier's December Cryto-Gram newsletter has articles about the NSA spying on on-line gamers; about how the NSA tracks people using cookie data; and about how the NSA's QUANTUM packet-injection system works and how to protect oneself from it https://www.schneier.com/crypto-gram-1312.htm

15 December 2013: There is an article in Foreign Policy about the FBI's communications-technology spying efforts, which are essential because the FBI has the "in-land" security mandate, while the NSA the "foreign". It will surprise no one who has been in touch with intelligence efforts (for example, James Bamford's books on the NSA) to learn that they work hand-in-hand. The article spells out how. This is also referenced in December's Crypto-Gram http://www.foreignpolicy.com/articles/2013/11/21/the_obscure_fbi_team_that_does_the_nsa_dirty_work

16 December 2013: Former Labour MP and former chair of the UK parliament's Home Affairs Select Committee Chris Mullin relates the recent history of the accounts of the UK security services given to Parliament and doubts whether current accountability arrangements are adequate http://gu.com/p/3y893

16 December 2013: Spencer Ackerman reports that some NSA officials are reportedly thinking of a possible offer of amnesty for Edward Snowden in exchange for a return of the materials he has given the Guardian and other journalists. The White House is said t o be dead against it. It sounds to me like a "trial balloon" http://www.theguardian.com/world/2013/dec/15/nsa-edward-snowden-amnesty-documents

16 December 2013: The U.S. blogger Marcy Wheeler suggests that the review committee report is a "typical administration whitewash" http://www.theguardian.com/commentisfree/2013/dec/16/obama-nsa-review-group-whitewash

16 December 2013: Tanjev Schultz reports in the Süddeutsche Zeitung (SZ) on the appointment in Germany of Klaus-Dieter Fritsche as Secretary of State for Secret-Service Matters, a new position inside the Chancellery. The SZ reports that he is a political heavyweight personally well acquainted with the services, which are the Federal Communications Agency (Bundesnachrichtendienst, BND) and the Federal Department for the Protection of the Constitution (Bundesamt für Verfassungschutz), and also that this new position likely resulted from the revelations and debate surrounding NSA/GCHQ electronic eavesdropping http://www.sueddeutsche.de/politik/klaus-dieter-fritsche-auf-du-und-du-mit-den-geheimdienst-chefs-1.1845214

17 December 2013: Charlie Savage reports in the NYT that Judge Richard J. Leon of the Federal

District Court for the District of Columbia (Washington, D.C.) has ruled that the surveillance of phonecall metadata is probably unconstitutional, and has ordered government surveillance to stop collecting it for two individuals. Execution of the judgement is delayed pending an expected government appeal http://nyti.ms/1cMT4wP Also reported in the Guardian by Spencer Ackerman and Dan Roberts http://www.theguardian.com/world/2013/dec/16/nsa-phone-surveillance-likely-unconstitutional-judge

17 December 2013: David E. Sanger and Alison Smale report in the NYT how the surveillance activities have hindered the political exchanges between Germany and the U.S., and summarise what the view of the German government is said to be on such activities http://nyti.ms/1cNvDDD

17 December 2013: Nick Hopkins reports on Home Secretary Theresa May's appearance before the UK parliament's Home Affairs Select Committee on Monday 16 December. http://www.theguardian.com/politics/2013/dec/16/theresa-may-mps-spy-chiefs-nsa May sees no need for intelligence chiefs to give evidence to the Committee, and claims accountability through the Intelligence and Security Committee (ISC) suffices. HASC members note the different role of the ISC from that of other parliamentary Committees, including that its members are appointed by the Prime Minister rather than being elected through the House of Commons. May reiterates her view that the Guardian's revelations have damaged national security and claims it is "obvious" (see the redacted "live blog", at time 2.40pm=14.40 UTC http://www.theguardian.com/politics/blog/2013/dec/16/nick-cleggs-monthly-press-conference-politics-live-blog). She was repeatedly asked if there was evidence for this, for example a plot that had come to light through electronic surveillance, which was being enacted, and was foiled by police and security forces. There was no concrete answer with such an example, neither was there an unequivocal answer "yes, there are such examples", as noted by member Julian Huppert.

17 December 2013: Paul Owen and Jonathan Watts extend (18 December) an agency-disseminated report that Edward Snowden has offered to help Brazil in measures against U.S. spying if he is granted political asylum. Many transatlantic cables run through Brazil http://gu.com/p/3y9db A translation of Snowden's letter into Portuguese is published by the Folha de S. Paulo http://www1.folha.uol.com.br/mundo/2013/12/1386291-leia-integra-da-carta-de-snowden-ao-brasil.shtml (note that the link given in the Guardian story is not direct).

18 December 2013: Ian Traynor and Paul Lewis report on considerations behind the release today of an interim EU report on what to do about surveillance. Germany is pursuing a bilateral agreement with the US under the basis of no mutual surveillance, but that seems not to be progressing. The US has only agreed not to monitor Chancellor Merkel's communications http://gu.com/p/3ya43 The article refers to yesterday's article in the NYT by David E. Sanger and Alison Smale (referenced above).

18 December 2013: In the NYT, Adam Liptak analyses the Leon ruling from the Federal District court of D.C., bringing in other relavant recent rulings and comments from amongst others the Supreme Court http://nyti.ms/JyZzZb

18 December 2013: Dominic Rushe, Paul Lewis and Spencer Ackerman report on a meeting between President Obama and chiefs and senior executives of internet-technology companies at the White House on 17 December. Apparently there were many issues on the agenda, including the troubled federal healthcare WWW site, but according to the article all people wanted to talk about was the NSA activity. Fifteen companies were represented. Mark Pincus of Zynga and Marissa Mayer of Yahoo were photographed next to the President by Reuters; Tim Cooke of Apple and Eric Schmidt of Google were also present, as was Randall Stephenson, chairman and CEO of AT&T. Senior representatives of Comcast, Facebook, Microsoft, Twitter and Netflix were present. A joint

statement was issued on the companies' behalf: "*We appreciated the opportunity to share directly with the president our principles on government surveillance that we released last week and we urge him to move aggressively on reform.*" http://www.theguardian.com/world/2013/dec/17/tech-companies-call-aggressive-nsa-reforms-white-house

18 December 2013: The NYT has an editorial on the Leon ruling http://nyti.ms/1hXSC2Om

18 December 2013: The ruling on surveillance by the Federal District Court of D.C., Judge Richard Leon, is available at http://legaltimes.typepad.com/files/obamansa.pdf

18 December 2013: A debate was held in the UK parliament building on the evening of Tuesday 17th December, between Sir David Omand, former GCHQ head, Alan Rusbridger, editor of the Guardian, Jimmy Wales, founder of Wikipedia, George Howarth MP, a Labour member of the intelligence and security committee, GCHQ's parliamentary oversight, Diane Johnson MP, shadow home affairs minister, and Katy Clark MP. The debate was blogged live by Paul Owen http://www.theguardian.com/world/2013/dec/17/alan-rusbridger-jimmy-wales-ex-gchq-chief-debate-spying-live

18 December 2013: Glenn Greenwald gave a presentation today to the committee of the European Parliament investigating the NSA/GCHQ surveillance activities that he and the Guardian reported. There is a link to a video of the session on his blog at http://utdocuments.blogspot.com.br/2013/12/the-lie-of-mp-julian-smith.html Apparently he was asked a question about the provenance of his information by a British MEP, did not answer the question because journalists are entitled to protect both their sources and their processes, and a British MP who has called for prosecution of the Guardian for its reporting sent out a tweet which clearly misrepresented what Greenwald said (that is what Greenwald's blog post addresses).

19 December 2013: The Review Group on Intelligence and Communications Technology, convened by U.S. President Obama, has written a 300pp report, a preliminary version of which has been released. The Review Group consists of Richard Clarke, a former cybersecurity adviser to the government and POTUS; Michael Morell, a former deputy CIA director; Geoffrey Stone, a University of Chicago law professor; Peter Swire, a Georgia Institute of Technology business professor and expert on privacy law who served earlier on Obama's national economic council (he is also associated with the Center for Democracy and Technology, which released a technical document in response to Congress's call for evidence, referenced here earlier); and Cass Sunstein, a Harvard law school professor who is married to the US ambassador to the UN (I have a couple of Sunstein's books – on political and legal handling of risk, and on worst-case scenarios). There are 46 recommendations. It is available for reading on-line at http://www.theguardian.com/world/interactive/2013/dec/18/nsa-review-panel-report-document

19 December 2013: A short article by Dan Roberts and Spencer Ackerman on the report. They highlight the recommendations to end direct bulk collection of phone metadata by the NSA (maybe the phone companies could retain records and deliver data to the NSA "on demand", the report suggests); that collecting data on foreigners should have a higher authorisation level (re: President Obama not knowing that Chancellor Merkel's telephone calls were being heard); and that the US government should not "undermine efforts to create encryption standards" and not "subvert, undermine, weaken or make vulnerable" commercial security software. The report http://www.theguardian.com/world/2013/dec/18/nsa-bulk-collection-phone-date-obama-review-panel

20 December 2013: Alan Rusbridger's editorial following the US Review Panel's report: "*What a relief. It is, after all, possible to discuss the operations of modern intelligence agencies without*

having to prove one's patriotism, be turned over by the police, summoned by politicians or visited by state-employed technicians with instructions to smash up one's computers." At least in the US. http://gu.com/p/3yc4a

20 December 2013: Sir Simon Jenkins questions yet again attitudes to cybersecurity. He points out the disparity between the threat: "*It is near impossible to understand what "national security" means to Britain any more. The country is existentially safe, and so is Europe as a whole: safe from invasion or conquest, and vulnerable only to its own financial incompetence*", and the resources spent on defence http://gu.com/p/3yc48

21 December 2013: The US fiction writer Dave Eggers recalls the McCarthy era and relents the self-censorship in supposedly-private communications, and acquiescence in it, practiced by colleagues, in order to avoid supplying "evidence" to possible adversaries who are agents of a state. I am glad that Eggers is bringing such matters again to our attention. There are good reasons for privacy, as many Europeans are aware, having suffered from the consequences from the 1930's through the 1980's http://gu.com/p/3yatv

21 December 2013: It's not just a question of whether current UK surveillance activities violate Article 8 of the EHCR; it can be argued that other provisions of the EHCR are violated by English law as well. An article by Geoffrey Robertson QC on an unrelated matter (a criminal trial in the UK, involving one of his friends as a witness) points out that, in denying witnesses in trials the chance to defend themselves against an accusation of "bad character", "*English law is in blatant breach of the European convention on human rights by providing no effective way for witnesses to protect their reputations*" http://gu.com/p/3ycmy

21 December 2013: There is also a "state doctrine" in English law, which says roughly that claims may not be pursued in court if they are likely to harm relations between states, even if those claims are apparently well-justified. In the case of Abdel Hakim Belhaj, a Libyan dissent who it is claimed was "rendered" in a joint US-UK operation to Colonel Quaddafi's Libya where he was allegedly tortured, Mr. Justice Simon ruled, with deep reservations according to this report by Richard Norton-Taylor, that Belhaj may not pursue his claim in English court http://gu.com/p/3yctg I wonder whether this "state doctrine" will be used to inhibit cases in English courts which allegedly involve joint NSA-GCHQ operations?

21 December 2013: Nick Hopkins and Patrick Wintour report on the latest revelations, in the Guardian, New York Times and der Spiegel, that GCHQ operations targeted European Commission Vice-President Joaquín Almunia, the Commissioner reponsible for competition policy. The European Commission said this is "*not the type of behaviour that we expect from strategic partners, let alone from our own member states".* Groups such as Médécins du Monde and the head of the Ideas Center, which lobbies on behalf of African cotton producers and exporters against -consumer-state subsidies for local cotton production, as well as Israeli government officials, were also the target of surveillance. No one has suggested that any of these have anything to do with terrorist activity http://gu.com/p/3yd2e

21 December 2013: James Glanz and Andrew W. Lehren report on the same matter in the New York Times http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html

21 December 2013: The Guardian points out in an editorial that much of the surveillance activity seems to have a "boys and their toys" nature, having been conducted on people and organisations who in no way can be considered threatening at all, let alone "terrorist" http://gu.com/p/3ydxh

22 December 2013: An editorial in the Observer catalogues the continuing differences between US and UK reaction to the revelations on electronic surveillance http://gu.com/p/3yd54

21 December 2013: Reuters reports that the computer-security company RSA received a payment of $10m from the NSA on contract, to install the NSA's recommended random-number-generation algorithm as its default RNG in its security software Bsafe. This is now widely suspected to include a "backdoor", allowing NSA to decrypt material so encrypted http://www.theguardian.com/world/2013/dec/20/nsa-internet-security-rsa-secret-10m-encryption See the initial announcement above from RSA on 21 September about the "weak" default RNG.

22 December 2013: Associated Press reports on the declassification by US Director of National Security James Clapper of documents concerning the origin of the bulk electronic-data collection programs during the administration of George H.W. Bush. This is to comply with a Federal Court order to make public its previous legal arguments for keeping the program secret http://www.theguardian.com/world/2013/dec/21/national-intelligence-bush-era-nsa-documents

23 December 2013: AP reports that "senior Israeli officials" have called on the US to stop electronic eavesdropping on the Israeli government. The Intelligence Minister, Yuval Steinitz, has said the NSA activities are "not legitimate" and has called for a bilateral agreement, the second country (as I recall) to do so after Germany http://gu.com/p/3yd9y

24 December 2013: Amongst those "senior Israeli officials" saying the spying is "unacceptable" is the Prime Minister, Binyamin Netanyahu, who will also pursue negotiations for the release of Jonathan Pollard, serving a jail sentence in the US for spying for Israel http://www.theguardian.com/world/2013/dec/24/israel-demand-release-spy-jonathan-pollard-peace-talks

25 December 2013: The UK's BBC broadcasts a message from the english Queen every Christmas Day in the afternoon, on its Channel 1 (BBC1). BBC Channel 4 has broadcast an "alternative Christmas message" for a couple of decades, and in 2013 it is by Edward Snowden, in a film by Laura Poitras warning about the dangers of a loss of privacy http://www.theguardian.com/world/2013/dec/24/edward-snowden-channel-4-christmas-day-message

27 December 2013: Haroon Siddique reports that UN High Commissioner for Human Rights chief Navi Pillay has been asked to produce a written report on protection of the right to privacy. The UN passed a resolution unanimously on December 18 that "*affirms that the same rights that people have offline must also be protected online, including the right to privacy*". The resolution was introduced by Brazil and Germany http://gu.com/p/3yeh5

27 December 2013: Adam Liptak and Michael S. Schmidt report in the NYT at http://nyti.ms/1efBxw4 on Judge William H. Pauley III's decision in the Federal District Court of Southern New York in the case brought by the American Civil Liberties Union against the Director of National Intelligence and others concerning surveillance. Dan Roberts reported the same at http://www.theguardian.com/world/2013/dec/27/judge-rules-nsa-phone-data-collection-legal Judge Pauley ruled, in contrast to Judge Leon, that the collection of metadata on phone calls was broadly acceptable. Commentators suggest that the US Supreme Court is now almost bound to step in to produce a definitive judgement. The ruling is on-line at https://www.aclu.org/files/assets/order_granting_governments_motion_to_dismiss_and_denying_aclu_motion_for_preliminary_injunction.pdf

29 December 2013: A longish article by John Naughton in the Observer considers the "democratic

dilemma" involved in balancing secrecy with democratic accountability. http://gu.com/p/3yf2j He suggests that the UK "*semblance of accountability*" is looking "*threadbare*". He notes, for example, that "*[UK Foreign Secretary William] Hague, [Chair of the ISC, the oversight committee] Sir Malcolm Rifkind et al maintain that collecting metadata is innocuous because it does not involve reading the content of communications..... This complacency reveals an alarming ignorance of digital technology."* He notes German politician Malte Spitz's investigations into the holding of his metadata by phone companies http://www.zeit.de/datenschutz/malte-spitz-data-retention and "*from it reconstructed an alarmingly accurate, detailed picture of his activities, communications and movements over a period of six months.*" He also refers to an example of sophisticated inference from metadata of people's personal relationships. Researchers from Facebook, Inc. and Cornell University show what one can infer of people's romantic relationships from analysing so-called network graphs http://arxiv.org/pdf/1310.6753v1.pdf One issue Naughton raises is that we may be concerned about government analysing our lives minutely through our electronic traces, but for some big Internet companies similar surveillance is a business model.

29 December 2013: Princeton Computer Science and Public Affairs Professor Ed Felton makes it quite clear through a series of examples in his expert-witness testimony before the Pauley court considering ACLU vs. Clapper et al. In the US District Court for Southern New York what can be inferred from metadata, and how. His testimony is very easily readable http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf

29 December 2013: The Observer points out in an editorial that the kind of surveillance many are concerned with when conducted by NSA and GCHQ is in fact part of the business model of many large Internet companies http://gu.com/p/3yfbk

29 December 2013: German weekly Der Spiegel publishes an article detailing some of the work by the NSA's Tailored Access Operations unit, including intercepting hardware being delivered to surveillance targets to install HW and SW backdoors before delivery http://www.spiegel.de/international/world/the-nsa-uses-powerful-toolbox-in-effort-to-spy-on-global-networks-a-940969.html

31 December 2013: Bruce Schneier considers in his blog the NSA TAO operations as revealed by Der Spiegel https://www.schneier.com/blog/archives/2013/12/more_about_the.html

31 December 2013: The organisation Democratic Audit has published a redacted copy of a lecture by former UK Director of Public Prosecutions Lord MacDonald arguing that oversight of the intelligence services is inadequate and needs to be improved significantly. The lecture contains proposals for reform: that the current Intelligence and Security Committee (ISC) a "group of parliamentarians" appointed by the Prime Minister and usually headed by someone with previous responsibility for security services, become a full parliamentary select committee. This recommendation was already made by the Joint Committee on Human Rights, and substantiated by the Foreign Affairs Select Committee in 2004 but, says Lord MacDonald, never followed through. He goes on to recommend membership by election of both houses of parliament,; that it have specific powers to obtain evidence; that it have an independent secretariat and independent legal advice; that its Chair be a member of the parliamentary opposition (that is, from a party not in government); and finally that available expertise by increased "*to ensure that human rights are at the heart of policy and strategies in this area* ." http://www.democraticaudit.com/?p=2020 I am not sure how the final suggestion can be implemented; indeed, it is not quite clear in this précis whence it is derived. It is shown in the full lecture, well worth reading at http://www.democraticaudit.com/wp-content/uploads/2013/12/FAMann-lecture2.pdf (Thanks to Martyn Thomas for the pointer.)

Lord MacDonald considers the case of Binyim Mohamed, who was detained in Pakistan by US operatives, and tortured (MacDonald describes how). This has been established in US Federal court. Mohamed was sent to Guantanamo Bay, and after some years back to Britain. He sued the UK government for complicity in UK court. The UK government tried to prevent details of his mistreatment being used in court (and therefore becoming public) on grounds of "national security". This argument did not prevail in the Court of Appeal. Since then, the UK government has succeeded in introducing "Closed Material Procedures", under which a judge can hear evidence said to "endanger national security" in hearings, which are even closed to the plaintiff. Lord MacDonald has worries about the precedent: how one side is able to claim the privilege of CMP, and how the other is unable to know, let alone to test, the evidence presented. In this, CMP seems to violate some basic principles on which some thought British law is based. I noted above (date: 21 December) that in the recent case of Abdel Hakim Belhaj, who was "renditioned" (*rendered*?) with the cooperation of British services, to Libya, where he was allegedly tortured, the UK judge did not give him permission to proceed with a claim in UK court. Lord MacDonald suggests that the Mohamed case shows that improved oversight of the actions of UK security services is needed. Were the Belhaj claims allowed and tested in court, they might well have substantiated this point.

31 December 2013: Lord Macdonald refers to a recent article by Sir Stephen Sedley, a judge of the Court of Appeal from 1999 to 2011, in the London Review of Books 35(17), 12 September 2013 http://www.lrb.co.uk/v35/n17/stephen-sedley/beware-kite-flyers In the guise of a review of a book on the constitution of Great Britain, Sir Stephen considers what is acceptable and what not concerning government surveillance. For example,

> *One result has been a statutory surveillance regime shrouded in secrecy, part of a growing constitutional model which has led some of us to wonder whether the tripartite separation of powers – legislature, judiciary, executive – conventionally derived from Locke, Montesquieu and Madison still holds good. The security apparatus is today able in many democracies to exert a measure of power over the other limbs of the state that approaches autonomy: procuring legislation which prioritises its own interests over individual rights, dominating executive decision-making, locking its antagonists out of judicial processes and operating almost free of public scrutiny. The arbitrary use of sweeping powers of detention, search and interrogation created by the (pre-9/11) Terrorism Act, which recently made headlines with the detention of David Miranda at Heathrow, illustrates a long-term shift both in what is constitutionally permissible and in what is constitutionally acceptable. The former may be a matter for Parliament, but the latter is still a matter for the rest of us.*

We may conclude that serious debate has started.

31 December 2013: Dominic Rushe reports that Apple denies any knowledge of the DROPOUTJEEP tool supposedly used by the NSA to access iPhones http://www.theguardian.com/technology/2013/dec/31/apple-nsa-backdoor-iphone-program

1 January 2014: EFF member Trevor Timm argues that claims have been made by senior US politicians, including the President, that the NSA has not abused its capabilities; and that recent disclosures of FICA secret-court judgements obtained by the EFF under the US Freedom of Information Act show that such claimes are categorically not true: the FICA court has complained on more than one occasion that NSA activities exceeded statutory powers http://www.theguardian.com/commentisfree/2013/dec/31/nsa-powers-have-been-abused

2 January 2014: An editorial in the Guardian makes the case for a pardon for Edward Snowden http://gu.com/p/3yhx2

2 January 2014: An editorial in the New York Times also makes the case for a pardon for Edward Snowden http://nyti.ms/Kls11i

3 January 2014: I came across a video of a Workshop, the "Crypto Festival", held at Goldsmith's, University of London, in December. The first two speakers are Annie Machon, a former MI5 employee in the 1990's who went public with her concerns about inappropriate behavior after being ignored by management, and Ross Anderson of Cambridge University. Each talk is about twenty minutes long. There are two further talks, but I haven't watched them yet (as of 2014-01-14).

Ms. Machon tells about some of the things she endured as a "whistleblower". To understand some of her references, though, you need to know about recent revelations in Britain about undercover policemen infiltrating protest groups. There are two main issues which have led to debate. The policemen (they were mostly men) assumed the identities of children who would have been of the same age as them, but who died young. This has outraged the parents of the deceased children, and others also. Also, many or most of them were male, sometimes with families, and many entered sexual relationships with women in the groups, and fathered children with them in some cases, disappearing regularly on some weekend (to spend time with their "real" families) and eventually for good, leaving the women with no partner and children which they would then have to raise without a father. I'll say straight out here: I find this morally abhorrent. These are public servants and this is what they did in what some apparently consider the line of duty. On the matter of gender, there is no mention of any undercover policewomen fathering children with protesters. Small wonder.

Ross Anderson gives a take on the revelations about surveillance, and the possible consequences, which I have not seen in written material so far. As usual from him, well worth perusing.

3 January: I also came across a series of talks "Snowden and the Future" from Eben Moglen, Professor of Law at Columbia University and Founding Director of the Software Freedom Law Center. He gave four talks from October through December 2013 about the Snowden revelations of NSA behavior and how this behavior relates to constitutional and other legal principles in the US. I appreciate the language in which he discusses the issues – he raises them up to scrutiny along with historical legal principles, and there is much here to learn – but find his rhetorical style a little distracting, in that it isn't clear to me how to make his points tell against someone who disagrees with them. It's law, of course, in which he is expert and I am not, but still one can wish for reusable arguments. One observation which is worth noting – he points out that privacy, which used to be a transactional notion, is now an ecological one, thanks to e-mail technology
http://www.snowdenandthefuture.info/

3 January: Yet another Brit accused of "hacking into" US government computers possibly faces extradition http://www.bbc.co.uk/news/uk-england-suffolk-24807822

4 January: A declaration by a few hundred academics deploring the mass surveillance revealed by the Snowden documents. Signatures are being collected. http://academicsagainstsurveillance.net/

8 January: Patrick Wintour reports that the Liberal Democratic Party in Britain, one of the two parties in the coalition government, is to formulate as policy that "*Judicial oversight of state surveillance and a regular release of the number of data requests made by the security services should be among the issues examined by a government "commission of experts" into all the recent allegations raised by the whistleblower Edward Snowden..... They will also call for the commission to review the effectiveness of all legislation surrounding the security services, including the system of parliamentary accountability.*" http://gu.com/p/3yybk

10 January: Nick Hopkins and Ian Traynor report that the European Parliament's civil liberties committee has written a report, available to some in draft, that says the mass surveillance programs of the NSA and GCHQ appear to be illegal, and condemn them in the "*strongest possible terms*" http://gu.com/p/3ym2j

10 January 2014: Bernd Sieker has put together a playlist of the videos uploaded to YouTube of talks on surveillance at the 30th Chaos Computer Congress in December 2013 in Hamburg, known as 30C3. This congress, held every year, is one of the most important practical computer security conferences. I have never attended, because, first, the thought of spending many days around geeks in geek heaven is no longer my idea of fun, and, second, I have come to look forward to the time between Christmas and New Year as a peaceful time of reflection, on both work and play and stuf besides. But I miss some important info. For example, the talk "The Year in Crypto" has at 29:55 a reference to the weaknesses in DUAL_EC_DRBG. I understand at time of writing that not all relevant talks are yet uploaded; more are to come http://www.youtube.com/playlist?list=PLqb-QtlNmRUobxxtGcFcfO3T37t1W4vDI&feature=em-share_playlist_user

14 January 2014: Philip Oltermann reports on a story originating with the Süddeutsche Zeitung. There is to be no bilateral agreement between Germany and the US about mutual restrictions on spying. "*As well as refusing to inform German authorities of when the NSA had been bugging the chancellor's mobile phone, the US is not commenting on plans for current or future surveillance activities in relation to German political leaders. A request for access to what is assumed to be a surveillance centre in the top floor of the US embassy next to Berlin's Brandenburg Gate has also been rejected. The German government has told the Obama administration it would consider such a "nest of spies" a breach of the Vienna Convention on Diplomatic Relations.*" http://www.theguardian.com/world/2014/jan/14/us-not-entering-no-spy-agreement-germany-media

15 January 2014: David E. Sanger and Thom Shanker report at length in the New York Times on the NSA's program of what one might call "hardware trojans", designed to obtain information from computers that may not be connected to the Internet http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html

15 January 2014: January's Crypto-Gram from Bruce Schneier has an article from The Atlantic Monthly about how the NSA's activities are affecting Internet security, and about the security risks to embedded systems. Schneier has also started cataloguing "an exploit a day" on his blog, and is summarising them in Cryptogram https://www.schneier.com/crypto-gram-1401.html

16 January 2014: Juliet Garside reports that Vodaphone is to ask the governments of all 25 countries in which it operates, including Britain, for permission to disclose the number of requests it receives for wiretapping, and for customer (meta)data http://gu.com/p/3yqth

16 January 2014: James Ball reports that the NSA collects up to 200 million text messages a day from phone transmissions, in a program called DISHFIRE http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

17 January 2014: Spencer Ackerman reports on the speech by President Barack Obama announcing future procedures for and controls on NSA surveillance of phone and Internet data http://www.theguardian.com/world/2014/jan/17/obama-end-nsa-bulk-storage-telephone-metadata

17 January 2014: Nick Hopkins contrasts the statement by Barack Obama about future NSA surveillance with the comparative silence of the British government http://gu.com/p/3mxge

17 January 2014: Heather Brooke, Professor of Journalism at City University, contrasts the US and British regulatory environments in surveillance http://gu.com/p/3mx68

17 January 2014: The Guardian's editors opine that Britain should follow the US example in overhauling its surveillance activities, and making the limitations public http://gu.com/p/3mxhx

19 January 2014: Alexandra Topping reports on British MP Dominic Raab's proposal that Britain should review and reform its surveillance organisations and operations http://gu.com/p/3m26j

21 January 2014: Charles Arthur interviews Eric Schmidt, Google's executive chairman. "*He said he had no knowledge of the US National Security Agency's tapping of the company's data, despite having a sufficiently high security clearance to have been told. He said that he and other members of the search company were outraged by the tapping carried out by the NSA and the UK's GCHQ ..... and that they had "complained at great length" to the US government over the intrusion. Google had since begun encrypting internal traffic to prevent further spying, he said.*" http://www.theguardian.com/technology/2014/jan/21/google-eric-schmidt-nsa-tapping-knowledge

22 January: Ewen MacAskill reports on the announcement at the World Economic Forum in Davos of a commission jointly set up by Chatham House (the common name of the Royal Institute of International Affairs in London) and CIGI, chaired by Swedish foreign minister Carl Bildt, to investigate the future of the Internet after the Snowden revelations. The sponsor organisations spoke of a threat to net freedom and said "*This threat to a free, open and universal internet comes from two principal sources. First, a number of authoritarian states are waging a campaign to exert greater state control over critical internet resources. Second, revelations about the nature and extent of online surveillance have led to a loss of trust.*" This suggests that the inquiry will address state-censorship issues as well as surveillance activities. http://gu.com/p/3m4hb

24 January 2014: Nick Hopkins reports in the Guardian on Britain's road cameras. There are now 8,000 cameras installed, given access to 26 million images a day. The systems use numberplate recognition technology, a system called ANPR, with images shorted in the National ANPR Data Center, NADC, but they also take full images of the vehicle, showing the driver's face. NADC is reported to contain 17 billion images. The police say they the cameras are indispensable for "help[ing] to cut crime and save lives". The article interviews Julian Blazeby, the lead on ANPR for the Assocation of Chief Police Officers, and Nick Pickles of Big Brother Watch, who is concerned about the privacy issues. Blazeby suggests more can be done to make the use of the system more clear to the public. Pickles is worried that such an intrusive technology is in place with "zero public debate". Of course the concept "counter-terror" is introduced somewhere in the catalogue of things said, which is why I am citing this article here. I remember a report of some analytical tools being introduced which allow automatic calculation of average speed over a stretch of road, even when the vehicle does not remain on the same stretch of road. But that's not counter-terror, it's road safety. http://gu.com/p/3m638

24 January 2014: Paul Lewis, Spencer Ackerman and Dan Roberts report that U.S. Attorney General Eric Holder hinted in an MSNBC inteview at the prospect of a plea bargain with Edward Snowden. http://www.theguardian.com/world/2014/jan/23/edward-snowden-nsa-plea-bargain-russia The Guardian article references an article on the NBC WWW site by Pete Williams and Michael O'Brien of NBC at http://nbcpolitics.nbcnews.com/_news/2014/01/23/22417513-holder-clemency-for-snowden-too-far-but-open-to-resolution

24 January 2014: Nick Hopkins reports that the European Court of Human Rights has "fast tracked" a case about GCHQ surveillance brought by Big Brother Watch, the Open Rights Group, and

English PEN (the writer's union). The Court has given the British government a deadline in May for submission of arguments as to whether the surveillance programs violate the right to privacy under Article 8 of the Convention http://www.theguardian.com/uk-news/2014/jan/24/justify-gchq-mass-surveillance-european-court-human-rights

26 January 2014: Rowena Mason reports in the Observer that the UK Ministry of Defence was considering reviewing the D-notice system, whereby British newspapers are advised of items whose revelation is considered (by the D-notice committee) to be detrimental to British national security. The D-notice system has been considered by some as a form of government censorship and criticised by those who compare with the situation in the US. But it is voluntary. The fear is that the government could make such a system compulsory. That is, the MoD could censor the British press with the force of law. http://gu.com/p/3m7fc

26 January 2014: A philosopher at the University of Oregon, Colin Koopman, opines in the New York Times's Opinionator blog that we are in an age of "*Infopolitics*", and that "*we lack the intellectual framework to grasp the new kinds of political injustices characteristic of today's information society.*" http://nyti.ms/1i1Kyfd

27 January 2014: James Glanz, Jeff Larsen and Andrew W. Lehren report in the New York Times of the NSA program to infiltrate smartphone apps to retrieve information. The article includes a link to an NSA slide presentation of the program http://nyti.ms/1jXjRc6

27 January 2014: Matt Apuzzo and Nicole Perlroth report in the New York Times that rules for the disclosure of when the government has demanded information are being relaxed. Microsoft, Google, Yahoo and Facebook have thus dropped their lawsuits before the FISA court. Previously, companies could reveal FISA-approved mandates for information only in increments of 1,000. Now, they can reveal exact numbers, but may not distinguish between FISA orders and national security letters, or may reveal separately but only in increments of 1,000 (doesn't this sound like the rules for a board game?) http://nyti.ms/LgWK06

27 January 2014: David Drummond, Google's chief legal officer, tells Adam Blenforth of the BBC that new rules on surveillance announced by President Obama on 17 January do not go far enough http://www.bbc.co.uk/news/technology-25910694

27 January 2014: German journalist Joseph Seipel interviews Edward Snowden in Moscow for the German state broadcaster ARD https://www.youtube.com/watch?v=4x38jkFlPeg I understand this video (in english) is available in Germany only.

28 January 2014: Barristers Jemima Stratford QC and Tim Johnston of Brick Court Chambers have issued an opinion in response to a request from Tom Watson MP, Chair of the All-Party Parliamentary Group on Drones of the UK Parliament. http://www.brickcourt.co.uk/news/detail/opinion-by-jemima-stratford-qc-and-tim-johnston-makes-front-page-of-the-guardian Watson had described a scenario whereby electronic communications between two UK residents was intercepted and used to target others which were then subject to a drone attack. The scenario has five steps, each of which involve actions which the lawyers say straight out are illegal; or are legal according to RIPA (the 2000 Act of Parliament allowing certain anti-terrorism measures) but contravene Article 8 of the ECHR (which is also British law); or are likely illegal. This seem to be a fairly hefty indictment of a variety of possible current practices. The 33-page opinion is at http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf The scenarios are described in paragraph 2. A summary of the lawyers' findings is contained in paragraph 7.

28 January 2014: Nick Hopkins reports on the Brick Court lawyers' findings: "*GCHQ's mass surveillance spying programmes are probably illegal and have been signed off by ministers in breach of human rights and surveillance laws, according to a hard-hitting legal opinion that has been provided to MPs.*" http://gu.com/p/3m9cd

29 January 2014: Mark Mazzetti and Devid E. Sanger of the New York Times report that US director of national intelligence James Clapper testified to Congress that Snowden's revelations had damaged US national security and caused terrorists to change their behavior http://nyti.ms/1k81d1d

29 January 2014: Alison Smale reports in the New York Times on German Chancellor Merkel's speech to the German parliament (Bundestag) in which she said that the US government had endangered its international standing by violating the freedom of the individual, a value for which it previously had been internationally admired http://nyti.ms/MfmZEw The Guardian's Philip Oltermann also reported Chancellor Merkel saying about surveillance that "*A programme in which the end justifies all means, in which everything that is technically possible is then acted out, violates trust and spreads mistrust.....In the end, it produces not more but less security.*" http://gu.com/p/3mavh

29 January 2014: Robert Mackey of the New York Times's Lede blog republishes the Snowden interview with Seipel http://nyti.ms/1k8F3vS

30 January 2014: Charlie Savage reports in the New York Times on a Federal Court case in Colorado in which lawyers for a defendant charged with terrorism-related offences have filed a brief to bar prosecutors from introduced evidence derived from warrantless surveillance by the NSA, on the basis that the NSA program violates the Fourth Amendment to the US Constitution. In a separate case before the Federal District Court for the Nother District of Illinois, the judge ordered the government to show the defendant's lawyer classified material relating to the national security surveillance of the defendant (the NYT article contains a link to the court document). Apparently no defence lawyer has been allowed to see such material since the passage of FISA in 1978. The NYT speculates that either or both of these cases could end up before the US Supreme Court, which must decide on matters of interpretation of the Constitution. http://nyti.ms/1ka4QUB

31 January 2014: In the Belhaj case, counsel for the UK government, GCHQ, MI5 and MI6 has given the court assurance that he (his team) will not read any mails between Belhaj, his wife and their legal team that might have been intercepted. http://gu.com/p/3mbca

31 January 2014: UK Prime Minister Cameron has told a UK parliamentary select committee that, after the next election, a cross-party consensus should be formed on revision of legislation for surveillance by police and by intelligence services. The provision "after the next election" is analysed in the article http://gu.com/p/3mbb7

1 February 2014: Spencer Ackerman reports that President Obama has said that National Security Director Clapper should have been "more careful" when giving evidence before the US Senate in March 2013 that the NSA does "not wittingly" collect data on non-suspect Americans. Bruce Schneier has pointed out that the US intelligence community has a special meaning for the word "collect". http://www.theguardian.com/world/2014/jan/31/obama-admits-intelligence-chief-fault-senate-testimony

2 February 2014: Peter Preston, former editor of the Guardian and now columnist for The Observer, opines on the purpose of D-notices, the voluntary press self-censorship recommendation system in the UK. It certainly has its good uses, but there has been suggestion that it be made mandatory. Preston argues against. http://gu.com/p/3mbmn

3 February 2014: Melissa Eddy reports in the NYT that the Chaos Computer Club in Germany has filed a criminal complaint against Chancellor Merkel and certain government members, accusing them of helping the US and the UK spy on German citizens http://nyti.ms/1bnGhRt

4 February 2014: Spencer Ackerman reports that the US House of Representatives Judiciary Committee, specifically James Sensenbrenner, urged (rather, warned) the Executive, specifically deputy attorney general James Cole, to get behind the new bill aimed at ending the routine surveillance of telephone calls and metadata http://www.theguardian.com/world/2014/feb/04/house-committee-us-government-nsa-reform-obama

5 February 2014: Charlie Savage reports in the NYT that, in the NYR summary, US "House Republicans offered sharply divergent views about secret government surveillance programs and the leaks that made them public, underscoring the unsettled nature of a political debate that has scrambled the usual partisan lines." http://nyti.ms/1jdFt6u

7 February 2014: Randeep Ramesh in the Guardian reports on David Davis MP 's claim that "backdoors" are built in to the new UK healthcare database to allow police and government access to people's medical data, rather than the current regime which requires a court order http://gu.com/p/3mgzy

8 February 2014: Charlie Savage reports in the NYT on a Washington Post story that the NSA is raking up data on "less than a third" of American's phone calls, down from a much higher proportion ("nearly all") in 2006 http://nyti.ms/NgibQb

8 February 2014: David E. Sanger and Eric Schmitt report in the NYT that US intelligence officials say that Snowden used a common-or-garden web crawler to obtain his material http://nyti.ms/LZNhKW

11 February 2014: Nicholas Watt reports in the Guardian on the Hugo Young lecture delivered by the leader of the UK opposition, Labor's Ed Miliband. Amongst other matters, Miliband proposed that the intelligence agencies perform necessary work but that oversight of intelligence needs reform; and that ministerial "sign-off" is an important safeguard. That makes all three major-party leaders in the UK who have said that intelligence oversight needs reform http://gu.com/p/3mja2

12 February 2014: Ewen MacAskill and Richard Norton-Taylor report on evidence given to the UK parliamentary Home Affairs Select Committee by Sir Anthony May, interception of communications commissioner, responsible for oversight of GCHQ, and Sir David Omand, former GCHQ head and now an academic. May said that the number of intercept requests per year from all sources was "large, possibly too large" at 570,000. He is preparing a report on Ripa (2000). Omand said Snowden was "not a whistleblower" and that other avenues had been open rather than leaking material to journalists http://gu.com/p/3mk9y

12 February 2014: Ian Traynor reports from Brussels that the European Commission has criticised US-centric governance of the Internet, through ICANN in California, in particular in wake of the recent revelations about surveillance, and has said a "transition to a more global model" is necessary http://gu.com/p/3my4q

15 February 2014: Bruce Schneier's Crypto-Gram includes a story derived from Glenn Greenwald's new on-line journal The Intercept on the use of drones to identify the location of "persons of interest" from their Internet use, from Greenwald and Jeremy Scahill. Also more NSA exploits from the blog; various links to the US Privacy and Civil Liberties Oversight Board judgement that NSA

mass surveillance of Americans is probably illegal, as well as comment on that from the EFF and EPIC https://www.schneier.com/crypto-gram-1402.html

19 February: Alan Travis, Matthew Taylor and Patrick Wintour report on the decision of the court concerning the detention of David Miranda for nine hours at London Heathrow airport as he was in transition from Berlin to Rio de Janeiro. "*The judges accepted that Miranda's detention and the seizure of computer material was "an indirect interference with press freedom" but said this was justified by legitimate and "very pressing" interests of national security.*
The three judges, Lord Justice Laws, Mr Justice Ouseley and Mr Justice Openshaw, concluded that Miranda's detention at Heathrow under schedule 7 to the Terrorism 2000 Act was lawful, proportionate and did not breach European human rights protections of freedom of expression." As we shall see from commentary from senior jurists, the grounds for this decision seem to be hard to understand. For example, I and colleagues discussed the reasoning in this finding: "*Greenwald told the judges that the security services were well aware that the seized material was in connection with journalism and not terrorism. He said there was no evidence to indicate that any disclosure had actually threatened or endangered life or any specific operation.....Miranda said the material was so heavily encrypted that he was unable to open it.*
The judges dismissed Greenwald's claims, saying there was "no perceptible foundation" for the suggestion that they were not putting national security or lives at risk by possessing the material."

The Guardian summarises the judgement as follows:
"The high court ruled that David Miranda's nine-hour detention and the seizure of his computer equipment was lawful under schedule 7 of the Terrorism Act 2000 because:

- *Although it was "an indirect interference with press freedom", there was not only compelling but "very pressing" evidence of a risk to national security.*

- *It was justified because a Cabinet Office official testified that the release of 58,000 highly classified GCHQ files Miranda was carrying would be very likely to cause great damage to security and possible loss of life.*

- *The judges refused to recognise that the seized files were "journalistic material" and insisted they included stolen raw data that did not warrant any freedom of expression safeguards.*

- *The judges dismissed claims that schedule 7 was used by the police only because it avoided any need to get prior authorisation from a judge to seize material from individuals involved in journalism."*

http://gu.com/p/3mqx4

19 February 2014: Spencer Ackerman reports that US director of national intelligence Clapper told an interviewer that there would not have been such a furore had the NSA been more open to the public about the data it collects and why http://www.theguardian.com/world/2014/feb/18/us-intelligence-chief-nsa-open-bulk-phone-collection

19 February 2014: Mark Scott reports in the NYT that President Hollande and Chancellor Merkel have been discussing ways to keep telecommunications data entirely within EU borders, to avoid eavesdropping from outside http://nyti.ms/1cmtf7d

20 February 2014: Lady Kennedy, a QC and member of the UK House of Lords, who does "*a lot of terrorist work in the courts*" says (with studied understatement) that the Miranda judgement is

"*disappointing, to say the least*" and says further "*We've been here before. Schedule 7 suffers the same glaring flaws as the old section 44 counter-terrorism power that also allowed stop and search without suspicion. Such laws leave themselves wide open to discriminatory misuse: section 44 never once led to a terrorism conviction but was used to stop people like journalist Pennie Quinton.....schedule 7 may be lawful, but it is really rotten law.*" http://gu.com/p/3mqd4

20 February 2014: US Senator Rand Paul of Kentucky comments on US national director of intelligence Clapper's suggestion that, had the NSA told people that and why it is collecting the data on them, things would have been OK. First, Paul is not OK that Clapper "*lied under oath*". Second, he thinks Clapper is being "*disingenuous .... Part of the reason our government does some things behind Americans' backs is not for security, but because certain activities, if known, would outrage the public. Spying on every American certainly falls into this category. I also believe it is blatantly unconstitutional*" http://www.theguardian.com/commentisfree/2014/feb/20/nsa-violating-american-rights-rand-paul

21 February 2014: Jeremy Waldron, Chichele Professor of Social and Political Theory at the University of Oxford, writes of "*a shameful failure of the rule of law embodied in [the] decision in the case of David Miranda*" in a letter to the Guardian http://gu.com/p/3nvkz

22 February 2014: Decca Aikenhead's Saturday interview in the Guardian is with playwright David Hare. Hare says of the security services *"Well, they're running the country, aren't they? I mean, the reason I'm writing about the security services is that there is no democratic control of them whatsoever. And now it seems the judiciary is joining in."* Aikenhead observes *"The judgment certainly appears to support the central thesis of Hare's latest trilogy of BBC films, about an MI5 agent disillusioned by his employer's rampant abuse of power."* http://gu.com/p/3nxak

23 February 2014: Former Guardian editor Peter Preston observes that Lord Justice Laws, who just handed down the Miranda decision, was the government's prosecutor in the Spycatcher case, about the Thatcher government's attempt to stop publication of an autobiographical book written by a former intelligence operative. http://gu.com/p/3nxa7

24 February 2014: Alex Hern reports in the Guardian that T-Systems and GSMK are to offer at the CeBIT fair an app for Android devices that encrypts mobile-phone-network voice and text communications http://gu.com/p/3n2q6

28 February 2014: Spencer Ackerman and James Ball report that GCHQ is collecting Yahoo webcam images in bulk in a program called Optic Nerve. Apparently 1.8m users were "targeted" in a six-month period. The collection also involves pictures of an intimate nature and there is reported to be an GCHQ internal warning about viewing them http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

28 February 2014: Bruce Schneier discusses "collection" of material by "algorithms" or by humans. First, data only counts as "collected" according to the US intelligence services definition if a human has surveyed it. Second, even if the assembled data just sits in a database without having been humanly surveyed, there is still a risk of exposure http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier

3 March 2014: Yvette Cooper, the UK's shadow home secretary (member of the parliamentary opposition "shadow cabinet" responsible for home affairs) has enunciated the Labor Party's position on surveillance reform, following party leader Ed Miliband's Hugo Young memorial lecture. Cooper says that "*The oversight and legal frameworks are now out of date. In particular that means we*

need major reforms to oversight and a thorough review of the legal framework to keep up with changing technology." Report by Patrick Wintour. http://gu.com/p/3n7m2

4 March 2014: UK Deputy Prime Minister Nick Clegg, leader of the Social Democratic Party, has made an important policy statement on surveillance and oversight today in the Guardian. He has commissioned a review by the Royal United Services Institute, which will report in a similar time frame to the review by the ISC. He proposes three measures. First, transparency of a sort: a report on government requests made for data from telecom and Internet companies, along with a WWW portal detailing the work of the security services. Second, reform of the ISC to make it more nearly a parliamentary select committee – increase in membership to 11; chair a member of the opposition; public hearings wherever possible; budget set five years in advance. Also, grant right of appeal against rulings of the Investigatory Powers Tribunal, and make reasoning and judgements public. Third, create an inspector general for intelligence, bringing together two roles presently held by commissioners: the interception of communications commissioner and the intelligence services commissioner. He mentions he does not yet have the agreement of coalition partners, the Conservative Party, for these measures. All three major UK political parties have now acknowledged the need for reform http://gu.com/p/3n8fy

Documentation of Stable Interest

Some relevant documents remain of interest throughout the political process round about the revelations of the extent of electronic surveillance by the US and UK, and are listed below.

The European Convention on Human Rights is readable in a variety of languages at http://www.echr.coe.int/Pages/home.aspx?p=basictexts&c=#n1359128122487_pointer (thanks to Ra Sicking for the reference)

The Guardian's page on Data and Computer Security is a constantly updated source containing the articles referring to the technology stemming from the Snowden revelations http://www.theguardian.com/technology/data-computer-security

Bruce Schneier's Crypto-Gram newsletter appears on the 15th of each month and is not only a major source of information (as far as I am aware, he is the only computer scientist of standing to have had direct access to the Snowden material through Glenn Greenwald) but also a fruitful source of wider references to on-line material than here. Schneier is currently a Visiting Fellow at Harvard Law's Berkman Center for Internet and Society https://www.schneier.com/crypto-gram.html Schneier blogs at https://www.schneier.com/

The Economist http://www.economist.com/ is a worthwhile source of commentary on many political-scientific issues including this one, but has a low article limit without registration, and sits behind a paywall. I subscribe, indeed have done for over thirty years, but it is not clear to me how to select for those who don't. A shame.

I have found the Cambridge security blog http://www.lightbluetouchpaper.org/ to be consistently entertaining and informative, as well as disturbing. For non-British readers, "light blue touch paper" is for more than half a century the instruction on fireworks to set them off. The "Light Blues" is also the nickname of a boat-race team who sometimes win. As well as other sports teams there.

The judgement of the German constitutional court ("Bunderverfassunggericht") concerning retention of metadata ("Vorratsdatenspeicherung", VDS). In German, of course https://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html?Suchbegriff=Vorratsdatenspeicherung Because VDS was very restricted, the Max Planck Institute

was tasked by the government to report if there are any "holes" in intelligence which have appeared because of the restrictions. The report, also in German, is from 2011 http://www.mpg.de/5000721/vorratsdatenspeicherung.pdf The German constitutional court has also judged the legality of the state using mechanisms implanted in individual computers to collect information on their users, so-called "State Trojans", "Staatstrojaner" https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html There is a lot of material on all this, mostly in German. The German situation is very different from that in France, which has just passed a law saying collection and retention of electronic metadata by the state is allowed essentially without restriction (as I understand it).

The U.S. President's Review Group on Intelligence and Communications Technology released a 300pp report with 46 recommendations on 16th December 2013. (See the entries for 18-19 December above.) Readable on-line at http://www.theguardian.com/world/interactive/2013/dec/18/nsa-review-panel-report-document

There has been some debate about content and so-called metadata, that is, the electronic tags that accompany e-mails and WWW browsing: who sent to whom, who viewed what, when, and where. Some politicians concerned with surveillance oversight have suggested that metadata is benign and not that intrusive. This is not so. This is indeed known not to be so by most computer scientists who know about these things. To enable an informed debate, I think it a good idea if this was more widely understood – by the public and politicians alike! John Naughton gives two useful on-line references to examples in his article of 29 December 2013. German politician Malte Spitz asserted his legal right to his metadata held by telephone companies, from which metadata he was able to reconstruct a picture of where he was, what he did, and with whom he communicated, for the previous months. An english-language version is at http://www.zeit.de/datenschutz/malte-spitz-data-retention Researchers from Facebook and Cornell University show what one can infer of people's romantic relationships from analysing so-called network graphs at http://arxiv.org/pdf/1310.6753v1.pdf There is also the statement of Professor Ed Felten in the case ACLU vs. Klapper, Alexander, Hagel, Holder, Mueller decided on 27 December 2013 by Judge William H. Pauley III in the Federal District Court for Southern New York http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf

In his expert-witness testimony before the Pauley court considering ACLU vs. Clapper et al. In the US District Court for Southern New York, Princeton Professor Ed Felton makes it quite clear through a series of examples what can be inferred from metadata, and how. http://ia601803.us.archive.org/22/items/gov.uscourts.nysd.413072/gov.uscourts.nysd.413072.27.0.pdf

Former UK Director of Public Prosecutions Lord MacDonald argues that oversight of the UK intelligence services is inadequate and needs to be improved significantly. The lecture contains proposals for oversight reform. A redacted version is at http://www.democraticaudit.com/?p=2020 The full lecture is well worth reading at http://www.democraticaudit.com/wp-content/uploads/2013/12/FAMann-lecture2.pdf More comment may be found above under the entry for 31 December 2013.

Sir Stephen Sedley, a judge formerly on the Court of Appeal of England and Wales, published a book review on 12 September 2013 concerning the British constitution, considering inter alia what surveillance activities might and might not be constitutionally acceptable. One of the unfortunately still rare cases of intellectually significant contribution to debate over surveillance http://www.lrb.co.uk/v35/n17/stephen-sedley/beware-kite-flyers Some more comment may be found above under the entry for 31 December 2013.

Bernd Sieker put together a playlist of the videos uploaded to YouTube of talks relevant to surveillance at the 30th Chaos Computer Congress in December 2013 in Hamburg, known as 30C3. This congress, held every year, is one of the most important practical computer security conferences. I think the talk "The Year in Crypto" is particularly noteworthy. It has at 29:55 a reference to the weaknesses in DUAL_EC_DRBG. http://www.youtube.com/playlist?list=PLqb-QtlNmRUobxxtGcFcfO3T37t1W4vDI&feature=em-share_playlist_user

Barristers Jemima Stratford QC and Tim Johnston of Brick Court Chambers issued a legal opinion on 29 January 2014 in response to a request from Tom Watson MP, Chair of the All-Party Parliamentary Group on Drones of the UK Parliament. Watson had described a scenario whereby electronic communications between two UK residents was intercepted and used to target others which were then subject to a drone attack. The scenario has five steps, each of which involve actions which the lawyers say straight out are illegal; or are legal according to RIPA (the 2000 Act of Parliament allowing certain anti-terrorism measures) but contravene Article 8 of the ECHR (which is also British law); or are likely illegal. The scenarios are described in paragraph 2 and a summary of the findings in paragraph 7 of the 33-page opinion at http://www.brickcourt.co.uk/news-attachments/APPG_Final_(2).pdf