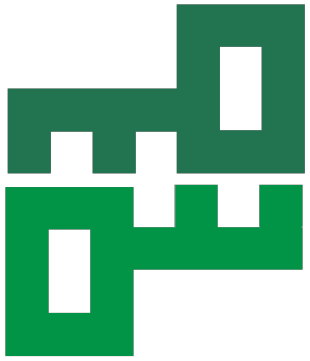
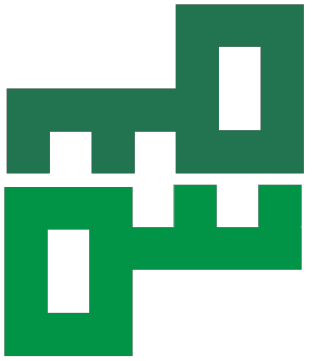
Journalists and mass surveillance

Anton, Cryptoparty Graz
https://cryptoparty.at/graz



2015-04-18
Barcamp Graz, FH Joanneum



PGP: Anton <an.to_n-73 at riseup.net>
0x49d1abf2a2a97d7d, 4096R, 2013-12-08
0B4C DF2C CB22 5DF4 25EA F212 49D1 ABF2 A2A9 7D7D

- Actual situation: Automatized, worldwide mass surveillance.

- Partly applied: Full take. Machinable interception and analysis of all electronic communication in a whole country.

- Confirmed: NSA, 6 countries status 10/2013 *[Gel14]*. Iraq, Afghanistan, Bahamas, USA. *[CNN13a] [CNN13b]*

- Strong indicators, but *outstanding confirmation:* **Austria**, altogether ca. 13 countries. *[Hor14] [Kes15]*

Misuse of mass surveillance. Examples and potentials

Italy. 1997 - 2006. Criminal cell in Telecom and police. Collection of kompromat, blackmailing of politicians and managers. *[Dat06]*

Argentina. Intelligence service SIDE out of control. Wiretapping of opposition, journalists and own president. *[Sue06] [LaN15]*

Syria. Use of internet as weapon, targeted exploits against computers of “adversaries”. *[Tan15] [Zak14]*

China. Use of communication and cloud data by Guoanbu to accuse opposition members. *[Köc15]*

Ethiopia. Targeted hacking of exiled journalists. *[Mar14]*

Colombia. Military intelligence service CIME wire-tapped NGOs, journalists, politicians. *[For14a] [For14b]*

Bulgaria. State National Security Agency (DANS) wiretapped protesters, politicians and journalists. *[Nov08] [Fit09] [Nov15]*

Macedonia. Illegal wiretapping of several thousand politicians, journalists, ministers and citizens. *[Bor15]*

USA. Wiretapping of journalists who work with sources in security services (email, phone, key cards). *[Ris06] [Ros09] [Mac20] [Isi11] [Stel13]*

UK. GCHQ intercepted “by accident” journalists e-mails. Rating of journalists as threat. *[Bal15]*

Australia. Access to communication metadata by many govt. agencies w/o warrant. Threat for sources in administration. *[Far14]*

Germany. Targeted wiretapping of single journalists by interior intelligence service and German Telekom *[Kri06] [Spi08] [Ble10] [Spi13] [Buc14] [Bun14]*

France. Bugging of editorial office *[Ang10]*. Use of telephone metadata to find source in administration *[LeM10]*.

Poland. Wiretapping of journalists phones to find the sources in the government *[Pol10]*

European Comission. Use of collected office emails to journalists for intimidation of employee. *[Sta09]*

Uber. Tracking of journalists. Senior Vice President E. Michael’s plan for critical press: "look into 'your personal lives, your families,' and give the media a taste of its own medicine". Plan not realized until now. *[Bhu14] [Smi14]*

=> The security services work for and act in the interest of the people in government, administration and security services (i. e. their own interest ...)!

=> These interests are partly not the interests of the governed and sentineled society!

=> In case of errors/scandals in government and administration the surveillance is directed against the own population to foresee the reaction.
<u>And especially against journalists to find the leaks</u>.

"*Security is the security of the state from its own population*" (Noam Chomsky)

Scenario for journalists

- Source in public administration

- Information important for society, but classified (*National Security* ™ or *Staatswohl* ™ etc.)

- How to communicate? Only one single set of metadata is too much.

→ Retrospective analysis after publication.

Who could access the information? Who of them communicated with the media? → Match!

- Personal meeting: Storage of location data of cellular phones. → Analysis same as above.

- Meeting w/o phones: Video surveillance and facial recognition (application and reliability yet unknown).

- Same is valid for source in “Big Data company”.

- Attention: Data of sources from less critical businesses could be researched, bought or stolen

Inform yourself in-depth about communication security and metadata.
Do not change your communication habits immediately.

Use separate computers and public WiFi
→ **Everything not connected with your identity!**

Secure your computers. *[Car14] [Smy15]*

Learn how to leak. *[Lee15]*

Ang10, Angeli C., 2010-11-14, *Sarko supervise l'espionnage des journalistes*
http://blog-de-canard.blog4ever.com/sarko-supervise-l-espionnage-des-journalistes
Bal15, Ball J., 2015-01-19, *GCHQ captured emails of journalists from top international media*
http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le
Bhu14, Bhuiyan J., 2014-11-19, *“God View”: Uber Investigates Its Top New York Executive For Privacy Violations*
http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy
Ble10, Blechschmidt P., 2010-05-17, *Susanne Koelbl im Interview "Ich konnte es nicht glauben"*
http://www.sueddeutsche.de/politik/susanne-koelbl-im-interview-ich-konnte-es-nicht-glauben-1.220175
Bor15, Borchard R., 2015-02-11, *Regierung soll Bürger illegal abgehört haben*
http://www.deutschlandfunk.de/mazedonien-regierung-soll-buerger-illegal-abgehoert-haben.795.de.html?dram:
Buc14, Buchen S., 2014-05-14, *Journalistengespräch vom LKA abgehört*
https://www.ndr.de/fernsehen/sendungen/zapp/Abhoerprotokoll-LKA-neugierig-auf-Recherche,delhaes104.htm
Bun14, Dt. Bundesregierung, 2014-05-09, *Mögliche Bespitzelung von Journalisten und Journalistinnen durch den Verfassungsschutz (…)*, Drucksache 18/1386
http://dip21.bundestag.de/dip21/btd/18/013/1801386.pdf
Car14, Carlo S., 2014-11, *Information Security for jounalists*, The Centre for Investigative Journalism, London
http://www.tcij.org/resources/handbooks/infosec
CNN13a, CNN, 2013-05-01, Erin Burnett Outfront
Tim Clemente, former FBI employee: *"No, welcome to America. All of that stuff is being captured as we speak whether we know it or like it or not."*
http://transcripts.cnn.com/TRANSCRIPTS/1305/01/ebo.01.html
CNN13b, CNN, 2013-05-02, CNN Newsroom
Tim Clemente, former FBI employee: *" I'm talking about all digital communications are -- there's a way to look at digital communications in the past. I can't go into detail of how that's done or what's done. But I can tell you that no digital communication is secure."*
http://transcripts.cnn.com/TRANSCRIPTS/1305/02/cnr.03.html
Dat06, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, 2006-10, *Abhör- und Überwachungsskandal in Italien*
https://www.datenschutzzentrum.de/allgemein/061018_italien.htm

Far14, Farrell P., 2014-04-25, *Journalists' sources are no longer safe in Australia*
http://www.theguardian.com/commentisfree/2014/apr/25/journalists-sources-are-no-longer-safe
Fit09, Fitsanakis J., 2009-01-14, *Bulgarian intelligence service found to have wiretapped "all national media"*
http://intelnews.org/2009/01/14/02-38
For14a, Forero M., 2014-10-28, *La polémica lista de Inteligencia Militar*
http://www.semana.com/nacion/articulo/la-lista-de-periodistas-funcionarios-que-tenia-la-central-de-inteligencia-
For14b, Forero M., 2014-10-28, *Los de la lista*
http://www.semana.com/nacion/articulo/inteligencia-militar-lista-de-periodistas-funcionarios-del-gobierno/40729
Gel14, Gellman B., 2014-03-18, *NSA surveillance program reaches 'into the past' to retrieve, replay phone calls*
http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retri
Hor14, Horcicka F., 2014-04-07, *NSA zielt auf Österreich*
http://www.format.at/news/oesterreich/nsa-oesterreich-374054
Isi11, Isikoff M., 2011-02-25, *DOJ gets reporter's phone, credit card records in leak probe*
http://www.nbcnews.com/id/41787944
Kes15, Kessler M., 2015-02-24, *Gesamte Telekommunikation in Österreich wird gespeichert*
http://futurezone.at/netzpolitik/gesamte-telekommunikation-in-oesterreich-wird-gespeichert/116.081.559
Köc15, Köckritz A., 2015-01-14, *They Have Miao*
DIE ZEIT, iss. 2/2015, Hamburg, ZEIT Verlagsgruppe 2015
http://www.zeit.de/feature/freedom-of-press-china-zhang-miao-imprisonment
Kri06, Krischer M., 2006-05-15, *Systematisch infiltriert*
http://www.focus.de/politik/deutschland/skandal-systematisch-infiltriert_aid_213467.html
LaN15, La Nacion, 2015-01-15, *El juez de la causa AMIA dijo que no autorizó las escuchas que realizó Nisman*
http://www.lanacion.com.ar/1760269-el-juez-de-la-causa-amia-dijo-que-no-autorizo-las-escuchas-que-realizo-n
Lee15, Lee M., 2015-01-28, *How to Leak to The Intercept*
https://firstlook.org/theintercept/2015/01/28/how-to-leak-to-the-intercept

Mac10, MacBride N., 2010-12-22, *Indictment, United States of America v. Jeffrey Alexander Sterling, Unauthorized disclosure of national defense information*, case no. 1:10CR485 (LMB), United States District Court for the Eastern District of Virginia, Alexandria 2010, p. 13 - 17
http://www.fas.org/sgp/jud/sterling/indict.pdf
Mar14, Marczak B., 2014-02-12, *Hacking Team and the Targeting of Ethiopian Journalists*
https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists
Nov08, Novinite, 2008-10-02, *Bulgaria Security Agency Director Ordered Spying on Media in August*
http://www.novinite.com/newsletter/print.php?id=97493
Nov15, Novinite, 2015-02-05, *Bulgaria's 2014 Anti-Govt Protests Accompanied by Large-Scale Wiretapping – MP*
http://www.novinite.com/newsletter/print.php?id=166361
Pol10, polskieradio.pl, 2010-10-08, *Journalists' phones monitored in politically inspired investigation?*
http://www2.polskieradio.pl/eo/dokument.aspx?iid=141157
Ris06, Risen J., 2006-10-24, *State of war*
Free Press, New York 2006 ISBN 9780743270670
http://books.simonandschuster.com/State-of-War/James-Risen/9780743270670
http://www.theguardian.com/environment/2006/jan/05/energy.g2
Ros09, Rosen J., 2009-06-11, *North Korea Intends to Match U.N. Resolution With New Nuclear Test*
http://www.foxnews.com/politics/2009/06/11/north-korea-intends-match-resolution-new-nuclear-test
Smi14, Smith B., 2014-11-18, *Uber Executive Suggests Digging Up Dirt On Journalists*
http://www.buzzfeed.com/bensmith/uber-executive-suggests-digging-up-dirt-on-journalists
Smy15, Smyth F., 2015-02, *CPJ Journalist Security Guide*, chapter 3, Committee to Protect Journalists, New York
https://cpj.org/reports/2012/04/journalist-security-guide.php
Spi08, DER SPIEGEL, 2008-05-26, *Telecommunications Scandal: Did Deutsche Telekom Spy on Journalists and Board Members?*
http://www.spiegel.de/international/business/telecommunications-scandal-did-deutsche-telekom-spy-on-journal
Spi13, DER SPIEGEL, 2013-09-30, *Journalisten unter Beobachtung*
DER SPIEGEL, iss. 40/2013, p. 17, SPIEGEL Gruppe, Hamburg 2013, ISSN 0038-7452
Sta09, Stabenow M., 2009-02-11, *Der EU sind Reporter verdächtig*
http://www.faz.net/aktuell/feuilleton/medien/medien-der-eu-sind-reporter-verdaechtig-1769826.html

Stel13, Stelter B., 2013-05-20, *Justice Dept. Investigated Fox Reporter Over Leak*
http://www.nytimes.com/2013/05/21/us/politics/white-house-defends-tracking-fox-reporter.html
Sue06, Sued G., 2006-05-23, *Espian e-mails de políticos y periodistas*
http://www.lanacion.com.ar/808286-espian-e-mails-de-politicos-y-periodistas
Tan15, Tanriverdi H., 2015-01-04, *Das Internet wird als Kriegswaffe Eingesetzt*
http://www.sueddeutsche.de/digital/buergerkrieg-in-syrien-das-internet-wird-als-kriegswaffe-eingesetzt-1.22898
Zak14, Zakorzjevsky V., 2014-04-28, *New Flash Player 0-day (CVE-2014-0515) Used in Watering-hole Attacks*
http://securelist.com/blog/incidents/59399/new-flash-player-0-day-cve-2014-0515-used-in-watering-hole-attacks