Jonathan Stribling-Uss, Esq. Concomms.org Info@concomms.org
Constitutional Communications PGP: 4106 D0F4 A182 DDC2 B372 4966 7B63 16FB DEBB 1E32
7/20/17

Why Professionals Must Encrypt: Attorneys, Journalists and Professionals Must Learn Secure Communications

WORKING DRAFT

"Anyone who has an obligation to protect the privacy interests of their clients is facing a new and challenging world, and we need new professional training and new professional standards to make sure that we have mechanisms to ensure that the average member of our society can have a reasonable measure of faith in the skills of all the members of these professions." – Edward Snowden[1]

1. The dark glass rubik's cube at the center of the Internet

Just twenty miles southwest of Baltimore, off the "NSA employees only" exit of Maryland's route 295 South, there is a "dark glass rubik's cube" of office buildings in which sits what, until 2013, was the world's most unknown agency.[2] Until last year, The National Security Agency (NSA), was jokingly referred to as "No Such Agency." But a year's worth of shocking news stories have earned the world's largest secret agency - which has a classified budget of more then 20 billion dollars and over 30,000 employees - a new acronym, "Not Secret Anymore."[3]

This article aims to show that professionals of all types must change their behavior and expectations when using electronics in light of the secrets that have been revealed about the NSA. The NSA's current practices of mass electronic surveillance destroy the professional integrity, independence and self-regulating structures of professional associations in the United States and around the world. This includes but is not limited to organizations like the American Bar Association (ABA) and the Society of Professional Journalists. Professionals who have a duty to protect the information of their clients and sources must take immediate steps, including regular use of encryption for client communication. Only this will maintain the independence of our professions, and ensure we do not lose client trust to NSA overreach.

As the UN's Special Rapporteur, the highest official for counter-terrorism and human rights, concluded in his recent report on the Snowden revelations, "The hard truth is that the use of mass surveillance technology effectively does away

1 "Edward Snowden urges professionals to encrypt client communications" by Alan Rusbridger et al. www.theguardian.com/world/2014/jul/17/edward-snowden-professionals-encrypt-client-communications-nsa-spy

2 "Body of Secrets: Anatomy of the Ultra-Secret National Security Agency" By James Bamford, 2001

3 "What the NSA costs taxpayers" by Jeanne Sahadi http://money.cnn.com/2013/06/07/news/economy/nsa-surveillance-cost/index.html

with the right to privacy of communications on the Internet altogether."[4] Even if we leave the NSA's Surveillance aside, we have reached a critical tipping point on the issue of secure communications, internet privacy and information control. After countless major data breaches at big banks and retail chains, like Chase, Target and Home Depot, it is clear that personal data is not adequately protected.[5]

Even for people unconcerned with the NSA Snowden has repeatedly stated, "unencrypted communications on the internet are no longer safe" and that "all professionals must encrypt" their communication by default.[6] The overreach of the NSA, the increasing accessibility of encryption technology, and the popular awareness of the insecurity of current information systems, make it clear that the time has come for professionals, from attorneys to reporters, to develop competency in secure communications and encryption.

2. Collect it all

The Snowden documents reveal that the NSA works with the intelligence agencies of the United Kingdom, Canada, New Zealand, and Australia. These five nations - self-titled as the "five Eyes" - have a shared agreement through which they act as a secret coalition of intelligence agencies to conduct global mass electronic surveillance.[7] In 2011, they held an annual conference at which they agreed upon a "new collection posture." A key element of that posture is to "collect it all." "Collect it all" means that the security services of the five governments with the most advanced electronic capabilities have decided that it is their role to collect and hold all electronic information globally.[8]

This "collect it all" posture is not a wild dream or an empty threat. In secret, the Five Eyes have constructed the largest data holding facility ever created in Bluffsdale, Utah. In 2013 the facility official opened with the capacity to hold a "yottabyte" of data.[9] A yottabyte is one thousand times the amount of data that will be stored on the entire Internet in 2015. They are filling this facility with information by tapping the undersea cables that transmit the information of the Internet. They are taking pictures of all internet activity while it passes though the fiber optic lines. The NSA then holds all of this information for at least five years.[10]

---

4 "UN Report on Human Rights and Terrorism", Sept. 23. 2014. https://firstlook.org/theintercept/document/2014/10/15/un-report-human-rights-terrorism/

5 "Encryption Makes Us All Safer" by Nuala O'Connor https://cdt.org/blog/encryption-makes-us-all-safer/

6 "Edward Snowden urges professionals to encrypt client communications" by Alan Rusbridger et al. www.theguardian.com/world/2014/jul/17/edward-snowden-professionals-encrypt-client-communications-nsa-sp

7 "No Place to Hide: Edward Snowden, the NSA and the Surveillance State." Glenn Greenwald http://glenngreenwald.net/#BookDocuments

8 "No Place to Hide: Edward Snowden, the NSA and the Surveillance State." Glenn Greenwald http://glenngreenwald.net/#BookDocuments , See also, http://leaksource.info/2014/07/31/glenn-greenwalds-no-place-to-hide-nsa-documents-excerpts/

9 "The NSA is building the Country's Biggest Spy Center (Watch What You Say)" By James Bamford, Wired, 2012

10 "No Place to Hide: Edward Snowden, the NSA and the Surveillance State." Glenn Greenwald

This holding time allows the NSA to sift through the data for useful patterns and insights.

The NSA's formal mandate is to collect foreign information. They are not supposed to collect the data or communications of U.S. citizens who are on U.S. soil. But internet traffic does not respect national boundaries. The Internet is structured so information is transferred in the most efficient and cheapest way. This means that, instead of traveling the most geographically direct route, messages from one person in the US to another person in the US may travel outside of the country to reach their destination. The NSA exploits the supranational structure of the Internet to allow it to collect data from and communication between US citizens who are communicating within the territorial United States.[11] The NSA also has information sharing agreements with the Five Eyes governments. These other governments collect information on U.S. citizens, which they then share with the NSA or the other partners. So even if the NSA does not directly collect the communications of U.S. citizens, they can access that data through the United Kingdom or other members of the Five Eyes.

This dragnet collection is the basis of the term "mass electronic surveillance." The UN defines "mass surveillance" as a situation in which "states with high levels of Internet penetration can…gain access to the telephone and e-mail content of an effectively unlimited number of users and maintain an overview of Internet activity associated with particular websites." The UN report states that in a system of "mass surveillance, all of this is possible without any prior suspicion related to a specific individual or organization."

3. The year 2014 less 30: the destruction of client and source trust means end of professional integrity

The United States Privacy and Civil Liberties Oversight Board concluded that, "Permitting the government to routinely collect the calling records of the entire nation fundamentally shifts the balance of power between the state and its citizens."[12] The UN Rapporteur mirrored that conclusion, finding that without drastic change we allow "a risk that systematic interference with the security of digital communications will continue to proliferate without any serious consideration being given to the implications of the wholesale abandonment of the right to online privacy."[13]

---

http://glenngreenwald.net/#BookDocuments

11 "Loopholes for Circumventing the Constitution: Warrantless Bulk Surveillance on Americans by Collecting Network Traffic Abroad", Harvard University, Berkman Center for Internet & Society, June 27, 2014, Sharon Goldberg et al.

12 The Privacy and Civil Liberties Oversight Board's Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report.pdf

13 "UN Report on Human Rights and Terrorism", Sept. 23. 2014. https://firstlook.org/theintercept/document/2014/10/15/un-report-human-rights-terrorism/

All professionals are impacted, but attorneys have clear ethical responsibility to protect client data. Rule 1.6 of the Model Rules of Professional Responsibility states that, “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.”[14] Each state bar has its own interpretation of how to define reasonable effort, and - even before the Snowden revelations -some state bars encouraged attorneys to use encryption to protect their clients.

If professionals do not begin to publicly offer encrypted methods for communication, they will cut themselves off from clients and sources who need to protect their information. Edward Snowden’s story provides a good example of this challenge. Snowden tried to establish contact with Glenn Greenwald, the reporter and attorney who later helped to break Snowden’s story. Greenwald was unable to get Snowden’s messages for more then six months, because he was not competent in the use of encryption.
If lawyers do not use encryption, many clients who are threatened by the government will not trust attorneys enough to approach them. Clients who want to engage in trade negotiations will not approach a firm, unless they are sure they can trust the attorneys to protect their data by keeping sensitive information off of electronic medium.[15] Journalists will only be able to report stories that valorize the government, because sources won’t trust them with information that could anger the government agencies. These losses will be invisible, because we will never hear from the people who did not trust our communications technologies enough to establish contact.

4. “What’s the threat?”

Last December a federal judge concluded that the US government could not “cite a single case in which analysis of the NSA’s bulk metadata collection actually stopped an imminent terrorist attack.”[16]
President Obama’s own Review Group on Intelligence and Communications Technologies concluded that mass surveillance “was not essential to preventing attacks” and that information to detect terrorist plots could “readily have been obtained in a timely manner using conventional [court] orders.”[17]

---

14 The Model Rules of Professional Conduct: www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html

15 Letter from ABA to NSA www.americanbar.org/content/dam/aba/uncategorized/GAO/2014feb20_privilegedinformation_l.authcheckdam.pdf

16 The Report of the President’s Review Group on Intelligence and Communications Technologies (PRGICT) www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

17 Officials’ defenses of NSA phone program may be unraveling www.washingtonpost.com/world/national-security/officials-defenses-of-nsa-phone-program-may-be-unraveling/2013/12/19/6927d8a2-68d3-11e3-ae56-22de072140a2_story.html

If invasive mass electronic surveillance technologies are not particularly effective against terrorism, then why have the intelligence agencies decided to put so much energy and time into building mass surveillance? “The Role of National Interest, Money and Egos” - a presentation which was developed for a handful of NSA officials concerning NSA planning for the Internet as a whole and which was leaked by Edward Snowden - can help us to assess the NSA’s real intentions. It states, “What country doesn’t want to make the world a better place…for itself?” Next it addresses US domination over the Internet stating, “What’s the threat? Lets be blunt. The western world (especially the US) gained influence and made a lot of money via the drafting of earlier standards.”[18]

The reasons for the “collect it all” posture are primarily global control, not security. One of the key NSA strategic planning documents leaked by Snowden is the 2009 “Quadrennial Intelligence Community Review Final Report.” The Quadrennial report is the 25 year strategic planning for the NSA and the US intelligence community. The report lays out the top six strategic priorities for the coming decades. One of the six key priorities, that top NSA officials identify as their strategic “hedge” is “technology acquisition by all means.” They go on to specify that the NSA should ensure US technical domination of emerging technologies “by all means.” The planning document uses an “illustrative example” of how this process works with a hypothetical about infiltrating an Indian and Russian technological agreement on a possible new form of superconductors. In the hypothetical they state that the NSA would make “separate clandestine approaches to India and Russia to break up the partnership. [The NSA] conducts cyber operations against research facilities in the two countries, as well as the intellectual “supply chain” supporting these facilities. Finally, it assesses whether and how its findings would be useful to U.S. industry.” It is clear that they have already begun to implement aspects of this strategy. The Snowden documents show that the NSA is spying on financial targets such as the Brazilian oil giant Petrobras; economic summits; international credit card and banking systems; the EU antitrust commissioner investigating Google, Microsoft, and Intel; and the International Monetary Fund and World Bank in order to commit economic and technical espionage.[19] This is an expansion of an NSA strategy for control of intellectual property that goes back to at least 1994. In one instance, this has played out publicly in a series of patient lawsuits between US and German wind turbine manufactures resulting in increased control of intellectual property for US based corporations.[20]

---

18 “No Place to Hide: Edward Snowden, the NSA and the Surveillance State.” Glenn Greenwald http://glenngreenwald.net/#BookDocuments

19 “Letter about NSA spying on economic summits” by Glenn Greenwald, http://epoca.globo.com/tempo/noticia/2013/08/carta-em-que-o-atual-bembaixadorb-americano-no-brasil-bagradece-o-apoio-da-nsab.html ; “Follow the Money': NSA Spies on International Payments” by Der Spiegel www.spiegel.de/international/europe/nsa-spying-european-parliamentarians-call-for-swift-suspension-a-922920.html ;“NSA spied on EU antitrust official who sparred with US tech giants” http://www.cnet.com/news/nsa-spied-on-eu-antitrust-official-who-sparred-with-us-tech-giants/ ; “Obama halted NSA spying on IMF and World Bank headquarters” By Mark Hosenball www.reuters.com/article/2013/10/31/us-usa-security-imf-idUSBRE99U1EQ20131031 ; “NSA accused of spying on Brazilian oil company Petrobras” by Jonathan Watts, www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras

20 European Parliament: Temporary Committee on the ECHELON Interception System. “Report on the existence of a global system for the interception of private and commercial communications”, 7/11/2001. www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=EN

This is the guiding strategy of the current NSA posture.[21] It has remarkable similarities to other historical variants like imperialism or colonialism, but they have been updated to what Prabir Purkayastha has called the "digital colonialism" of the current era.[22]

5. Icreach, Metadata and "Parallel construction"

Attorney's relationships with clients are being collected and logged by the NSA in many ways. One of the most significant methods of collection is the federal multi-agency collaboration surrounding the "Icreach" database.[23]

Icreach is a database of "five eyes" metadata intercepts used by a dozen federal agencies for domestic criminal prosecutions. The NSA legally justifies the domestic use of the Icreach database by using Executive Order 12333, a broad interpretation of a 1982 Reagan era executive signing statement,[24] although Executive Order 12333 was adopted by President Reagan as a signing statement and was never subject to any judicial or legislative input or oversight.[25] The DEA runs this multi-agency collaboration under the unit title "Special Operations Division"(SOD). The SOD is a $125 million unit with hundreds of employees from a dozen federal agencies including the FBI, CIA, NSA, IRS and DHS.

The Icreach database intercepts "metadata," a kind of data that shows the relationships between people. Metadata is the "who" and "when" about communication on the phone and online. It is the "outside of the envelope" for normal phone calls. It tells the time someone placed a call, to whom the call was made and how long the call was. Similar data exists for all types of communication: instant messages, emails, text, and the geo-location of computers and cell phones. For cell phones, metadata can include all the physical locations of the cell phone over time. Metadata is the "digital fingerprint," and it provides information to map social networks through the connections established through electronic communication. This metadata is turned into contact chains and linked in the Icreach database to allow for easy warrantless "google type"

21 The U.S. Government's Secret Plans to Spy for American Corporations https://firstlook.org/theintercept/2014/09/05/us-governments-plans-use-economic-espionage-benefit-american-corporations/

22 "U.S. Control of the Internet: Problems Facing the Movement to International Governance" Prabir Purkayastha and Rishab Bailey, Monthly Review, 2014, Volume 66, Issue 03 (July-August)

23 "The Surveillance Engine: How the NSA Built Its Own Secret Google" by Ryan Gallagher, https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

24 "Use of Executive Order 12333", www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html

25 "The Surveillance Engine: How the NSA Built Its Own Secret Google" by Ryan Gallagher, https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

searches of the communication and location tracking of US citizens and others. While the actual application of Icreach data in criminal cases is still mostly kept secret, hypothetically this mapping can be used to cast suspicion on anyone who has had electronic communication with someone who the government suspects of criminal activity. While we don't know their extent, we do know that prosecutions have been initiated based on Icreach relationship-mapping.

Icreach based prosecutions use a procedure called "parallel construction" to hide the NSA intercept information from court filings. In practice, this often means that law enforcement agents, including local police, systemically lie to prosecutors about the existence of the Icreach database and its use as the original source for a tip that begins an investigation. For example, a current federal prosecutor in Florida confirmed to Reuters that, "in a drug case he was handling, a DEA agent told him the investigation of a U.S. citizen began with a tip from an informant. When the prosecutor pressed for more information, a DEA supervisor intervened and revealed that the tip had actually come through the SOD and from an NSA intercept".[26]
The warrentless use of such a database and the fact that the individual agents use "parallel construction" to hide the use of the data base from the judiciary destroys the sixth amendment right for a defendant to see the evidence against them in an open court. The current vice chairman of the criminal justice section of the American Bar Association, James Felman, calls this domestic use of NSA intercepts "outrageous" and "indefensible." Nancy Gertner, a Harvard Law School professor and former federal judge, said that, "It is one thing to create special rules for national security, ordinary crime is entirely different. It sounds like they are phonying up investigations."[27] It is unclear how many thousands of cases may be based on this type of illegal evidence, but, as of October 2014, the use of "parallel construction" is being investigated by the Justice Department.

7. What is NSA Targeting and how targeting happens

"Targeting" is a term the NSA uses to describe more extensive infiltration of particular electronic and computer systems. This is an internally defined process with little judicial oversight or outside review mechanisms. It is difficult to tell what criterion the NSA is using to determine who it will target more intensively. Individual agents are given a huge degree of leeway and discretion, and there are few consequences for targeting the wrong person accidentally. As Snowden has stated, "At my desk, I could be wiretapping anyone in America, from a federal

26 "U.S. directs agents to cover up program used to investigate Americans", by John Shiffman and Kristina Cooke, www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805

27 "U.S. directs agents to cover up program used to investigate Americans", by John Shiffman and Kristina Cooke, www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805

judge to the President of the United States."[28] This statement is verified by the fact that, even as early as 2009, the New York Times reported that an NSA agent had targeted and read President Clinton's personal email.[29] Snowden documents show that, according to the NSA's own policy from their Office of General Counsel, discovering that an American has accidentally been selected for intensive surveillance is "nothing to worry about." It must only be logged in an internal quarterly report.[30]

From the NSA's internal records, it has become clear that the NSA has developed strategic priorities for targeting certain groups. These groups are Muslims leaders of all types,[31] "radicalizers" generally,[32] Palestinian leaders, the "human network" associated with Wikileaks, anyone searching for privacy tools on the internet, computer network system operators, drug dealers, terrorists, presidents, the UN, people who make cryptography, and others[33].

NSA documents show that people that the NSA views as "radicalizers" have been targeted for "reputational" attacks for their behavior on the internet, like watching porn, online promiscuity, or even simply "not checking facts in their articles." Internal memos from NSA executives make it clear that the NSA views these targeted people, some of whom are US citizens, as "radicalizers" specifically because of their political speech; for visibly and influentially making arguments like "the US brought the 9/11 attacks on itself".[34]

There are many attorneys that have been or currently are subject to intensive NSA surveillance. We know that Muslim-American attorneys have been subject to intensive Foreign Intelligence Surveillance Act (FISA) court surveillance, and we also know that attorneys who have worked for Wikileaks and attorneys employed in global firms working on trade negotiations have also been targeted.[35] When the Washington Post analyzed the final information used in twenty two thousand leaked NSA surveillance reports, 89% of the information was from those who are associates of the targeted individuals, while only 11% was from the individuals

---

28 "Edward Snowden Interview" Glenn Greenwald, http://mic.com/articles/47355/edward-snowden-interview-transcript-full-text-read-the-guardian-s-entire-interview-with-the-man-who-leaked-prism

29 "NSA Secret Database Ensnared President Clinton's Private E-mail" by Kim Zetter www.wired.com/2009/06/pinwale

30 "No Place to Hide: Edward Snowden, the NSA and the Surveillance State." pg. 189, Greenwald, Glenn, http://glenngreenwald.net/#BookDocuments, See also "NSA broke privacy rules thousands of times per year, audit finds", By Barton Gellman, www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html

31 "Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On", by Glenn Greenwald, https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/

32 "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'" www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html

33 "No Place to Hide: Edward Snowden, the NSA and the Surveillance State" by Glenn Greenwald, http://glenngreenwald.net/#BookDocuments

34 "Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit 'Radicalizers'" www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html

35 "Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On," https://firstlook.org/theintercept/article/2014/07/09/under-surveillance/, See also, "No Place to Hide: Edward Snowden, the NSA and the Surveillance State." by Glenn Greenwald, http://glenngreenwald.net/#BookDocuments

who are designated NSA targets.[36] These facts make it virtually certain that privileged conversations are caught in the surveillance web. Because of this mass collection structure, legally privileged information will likely be compromised in the normal course of non-secure attorney client communication. The NSA has no filtering procedure for privileged attorney-client information.

8. Targeting the technology professionals rely on

The NSA put “back doors” (a term for a flaw in the software construction that allows surveillance programs to access supposedly secured information) in some proprietary encryption.[37] The NSA did this by paying $10 million to an encryption manufacturer, named RSA to weaken the math that secured its encryption. They also created a section of the National Standardization Board for Encryption within the US National Institute of Standards and Technology (NIST) that would take encryption programs and insert a backdoor (random number generator) into the product, which would allow the NSA to guess the outcome of otherwise random code construction.[38] In Germany and China, the NSA also directly inserted human agents into the encryption industry to undermine encryption technologies that these nations are developing.[39]

Over 80 software and hardware companies have close “partnership” relationships with the NSA, but their level of cooperation is not fully known.[40] Microsoft partners with the NSA by giving them knowledge of software bugs before releasing them to the public or the anti-virus companies.[41] This means that, at regular intervals, the NSA is able to get access to all computers running Microsoft for a period of time before the holes in the code are patched. This sort of access has allowed the NSA to put Computer Network Extracting (CNE) keyloggers on between 50,000-100,000 computers. A computer infected with a keylogger or screen logger allows the NSA to read a record of every key typed or every screen viewed, often in real time.

9. Why open source is a solution

---

36 “In NSA-intercepted data, those not targeted far outnumber the foreigners who are” by Barton Gellman, www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html

37 “Revealed: how US and UK spy agencies defeat internet privacy and security” by Glenn Greenwald et al. http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security

38 “Exclusive: Secret contract tied NSA and security industry pioneer” by Joseph Menn http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220

39 “Core Secrets: NSA Saboteurs in China and Germany” by Peter Maass and Laura Poitras, https://firstlook.org/theintercept/2014/10/10/core-secrets/

40 “No Place to Hide: Edward Snowden, the NSA and the Surveillance State.” By Glenn Greenwald http://glenngreenwald.net/#BookDocuments, See Also http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

41 “U.S. Agencies Said to Swap Data With Thousands of Firms” By Michael Riley www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html

Open source software allows for software engineers and users to fully control all aspects of a computer system. Proprietary standards, like Microsoft and Apple Operating Systems, all provide legal and technical prohibitions on users and engineers that keep them from viewing the actual functioning of the codes that make the computer programs run.[42] Open source software, like Linux or Debian, allows for software engineers and users to fully control all aspects of a computer system. This doesn't mean that open source programs are flawless or bug free. The idea is that the public and code developers should know about their bugs at the same time the NSA does. This allows engineers and users to quickly know if their computer may have been compromised.[43] Open source standards allow for a more scientific process of transparent and verifiable software improvements that are not dependent on a closed group that could be directly cooperating with the NSA. Many countries, including the governments of Uruguay, Ecuador, and Brasil, are now running most of their information technology on open source platforms.[44]

10. Why encryption is a solution

Encryption is - simply - writing in code.[45] Current encryption programs apply very rigorous math, logic and technology to the basic process that all people engage in when creating dialects or languages. In a strange twist of technological progress, the current application of this science allows for anyone with a home computer to create encryption advanced enough that it, when properly implemented, cannot be broken by all the computer power in the world.[46] As Snowden has stated "Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on."[47] This means that an everyday computer user with medium competency can currently download a free open source encryption program from the Internet that, when properly implemented and verified, allows them to encode information in a way that is impossible for even the NSA to break[48].

11. The great encrypting starts with you

42 "Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance" by Micah Lee https://pressfreedomfoundation.org/encryption-works

43 "Help Support the Little-Known Privacy Tool That Has Been Critical to Journalists Reporting on the NSA" by Trevor Timm https://freedom.press/blog/2014/04/help-support-little-known-privacy-tool-has-been-critical-journalists-reporting-nsa

44 "Software Libre en América Latina" www.telesurtv.net/news/Software-Libre-en-America-Latina-20140919-0071.html

45 "Handbook of Applied Cryptography" http://cacr.uwaterloo.ca/hac/

46 "Attacking Tor: how the NSA targets users' online anonymity" by Bruce Schneier www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity

47 "Revealed: how US and UK spy agencies defeat internet privacy and security" By Glenn Greenwald et al. http://www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220 See also "Prying Eyes: Inside the NSA's War on Internet Security" http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html

48 Tactical Tech Collective, https://tacticaltech.org/survival-digital-age , See also, Surveillance Self-Defense https://ssd.eff.org/

Professionals and everyday people are already transitioning to encryption en masse. A global survey of nearly five thousand businesses found encryption use has increased six percent in the past year to the point where 35% of organizations now have an encryption strategy applied consistently across the entire enterprise.[49] In the United States, encrypted traffic has jumped from 2.29 percent of all peak hour traffic before Snowden to 3.8 percent after Snowden, and in Latin America it has gone from 1.8 percent to 10.37 percent.[50] More then ten major global newspapers - including *The New York Times*, *The New Yorker*, *The Washington Post*, *The Guardian* and *The Intercept* - have embraced encrypted "dropboxes" for first contact with new sources.[51] Hundreds of journalists are using encrypted emails for source protection.

However, without a massive increase in the level of encryption in society and politics, we consign ourselves to professional associations that will be unable to retain integrity and public trust[52]. This can be avoided if we each seek to encrypt our information and push our professional organizations to do the same. Once the use of encryption increases to around fifteen percent of all Internet traffic in the United States it will significantly impede governments' use of mass electronic surveillance technology against the Internet as a whole. At that point, we would be able to secure communication generally and thus restore privacy, ensuring professional integrity and First, Fourth and Sixth Amendment rights in the information age.[53]

49 "Encryption use continues to grow", www.net-security.org/secworld.php?id=16340 see also http://www.reuters.com/article/2014/02/11/fl-thales-idUSnBw115819a+100+BSW20140211

50 "Encrypted Web Traffic More Than Doubles After NSA Revelations" www.wired.com/2014/05/sandvine-report/

51 SecureDrop, https://freedom.press/securedrop

52 "Communities @ Risk: Targeted Digital Threats Against Civil Society" Citizen Lab, Munk School of Global Affairs, University of Toronto www.targetedthreats.net

53 "NSA Surveillance: The implications for civil liberties" By Shayana Kadidal, Esq