

Politricksnology
December 2006

**Censorship, Transparency, and
the Cyberdissidence Toolkit**

Jamie Wilkinson
Eyebeam R&D

Part 1:

Analytical Framework

Constitutional Basis for the Practice of Dissidence

Governments are instituted among Men, deriving their just powers from the consent of the governed... whenever any Form of Government becomes destructive of these ends, it is the Right of the People to alter or to abolish it....

- US Declaration of Independence, 1776

The United States Constitution was built on an understanding of the importance of free speech and the protection of dissenting opinion. The Founding Fathers believed open discourse and the threat of revolt to be a source of strength and not weakness and thus created a system of checks and balances between government and citizen. The first two amendments of the Bill of Rights put to writing the idea that a government should respect and fear its citizens, and not vice versa. The first amendment laid a guarantee of protection from the Government for fundamental human rights: free speech, assembly, free exercise of religion, freedom of the press, and so on. In the second amendment lay the mechanism by which the people would protect themselves: the right to bear arms and to establish and maintain armed militia. James Madison was one of its loudest supporters:

Besides the advantage of being armed, [militia] forms a barrier against the enterprises of ambition, more insurmountable than any which a simple government of any form can

admit of. The governments of Europe are afraid to trust the people with arms. If they did, the people would surely shake off the yoke of tyranny, as America did.¹

Many Federalists and other Founding Fathers in fact advocated keeping the headcount of the standing army to a minimum, preferring that ultimate military authority rest with the militia.

Noah Webster:

Tyranny is the exercise of some power over a man, which is not warranted by law, or necessary for the public safety. A people can never be deprived of their liberties, while they retain in their own hands, a power sufficient to any other power in the state.²

The breadth of this trust in the common citizen and *distrust* of the government is a precursor to a long history of libertarianism in America. This rugged individualist cowboy ethos has driven the expansion westward, manifested itself in the success of our free market economy, developed a fairly progressive and socially responsible national culture, and given birth to the whole concept of the American Dream. This ethos has not been without its faults – nature itself refuses to allow any kind of perfect efficiency, and human nature surely fares worse – but the classic American respect for the rights of the individual and an understanding of the necessity for accountability in government are two positive traits which are worthy of defense and propagation.

¹ *Annals of Congress* 438, June 8, 1789

² Webster, Noah. “An Examination of the Leading Principles of the Federal Constitution”. 10 Oct 1787

Militia Revisited: The Need for Transparency

In the 18th century it was not unreasonable to expect the average male to be as adept as the professional soldier with the tools and tactics of his day – muzzle-loaded rifles, line formations, and horse-drawn carriage. In the age of modern warfare one can hardly expect a citizens' militia to be fully versed in the operation of fighter jets, aircraft carriers, and laser-guided missiles. Nonetheless the principles belying the 2nd amendment warrant vigilance; in the absence of the ability to maintain a militia more potent than the standing army it is necessary to find other means to maintain accountability in government. The Mazdoor Kisan Shakti Sangathan, a grassroots 'right to information' group in India, was founded on the idea that "government information should be able to be leveraged by ordinary citizens to enhance their participation in governance and decision making and thereby improve their own lives."³ Transparency of information, action, and decision-making lies at the heart of establishing increased accountability.

The open-source and open-content movements – collectively referred to as the free culture movement by author and Creative Commons founder Lawrence Lessing⁴ – have built a successful model on total transparency and provides the inspiration for further research into the adoption of more transparent practices in other areas, particularly the government and any industry dealing with public goods. Advocates of free culture assert that an organization that is confident enough in its practice to invite open review is one that has nothing to hide and nothing

³ *freedominfo.org*, "Case Study: The Right to Know is the Right to Live." Available online at <http://www.freedominfo.org/features/20040630.htm>

⁴ *Lessig, Lawrence*. Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity. *Penguin Press*, 2004.

to fear from its principals. The establishment of trust between government and citizen the most important step in building accountability, and the perception of honesty a necessary precursor to trust. Unabashed transparency is a declaration of honesty and pride in action and intention; inviting transparency is the most important step in building trust, and thus building a more responsive and responsible government.

In the open-source model a software developer freely publishes the code to his or her programs, encouraging other developers to tinker with it and contribute back their changes. The online collaborative encyclopedia Wikipedia is written in a similar fashion, inviting all visitors to become contributors just by clicking “edit this page,” adding or modifying the work, and then saving the new page for the all future visitors to benefit from. Generally these kinds of projects are published with unrestrictive ‘copyleft’ licenses, which allow anyone to freely use, modify, and even redistribute the work, so long as the resulting work is covered under the same license. This has led to numerous ‘forks’ of projects, where developers with different opinions about the technical or philosophical direction of the project take the existing source code and turn it into a new project. The ‘right to fork’ is not dissimilar from the intentions of the Founding Fathers in establishing the 2nd Amendment and the belief in a dominant citizens militia capable of threatening the government into acting responsibly. It is a moving statement: “be good or we will overthrow you.”

The revolution in modern telecommunications has enabled free culture projects to enjoy great success, both in terms of popular adoption and technical superiority. Much of the Internet is

powered by open-source software.⁵ A recent study conducted by Nature found that the average Encyclopedia Britannica article to contain 3 factual errors per page, and the equivalent Wikipedia encyclopedia entry contains 4 articles per pages, but contains 2.5 times more information.⁶ The success of this open model, a kind of completely universal peer review, has led to the formulation of “Linus’ Law⁷: given enough eyes, all problems are simple. Beyond simple ease, security problems can be more easily spotted and more quickly corrected. Arguably the same benefits could be applied to government practices, the drafting of legislation, and the accountability of politicians and bureaucrats.

As transparency and participation increases organizations become increasingly dispersed and decentralized. A great deal of academic study has been conducted on the management practices and organizational effectiveness of ‘virtual’ business models, in which core business functions have been outsourced. Positive attributes of virtual organizations include immense flexibility and the ability to adapt to the needs of its customers (Dawson, 1998) which free culture and free software groups exemplify, since many of their “customers” actually create the product. They also enjoy spatial and temporal independence (Boudreau, 1998), which traditionally means the company can be easily relocated; these groups take it a step farther by using the Internet to give their customers universal, on-demand access. Disadvantages of virtual organizations include dysfunctional communication (Koch, 2000) and trust and monitoring issues. With a larger and more dispersed number of contributors to the final project, it is difficult to facilitate cooperation, which can manifest itself as quality control issues and intra-group tensions. Since the

⁵ Chris DiBona, Sam Ockman, Mark Stone. *Open Sources: Voices from the Open Source Revolution*, O'Reilly Books, 1999

⁶ “Internet encyclopedias go head to head,” *Nature* 438, 15 December 2005

⁷ Named after the creator of the open-source operating system Linux

government would probably not logistically be able to achieve a great deal of ‘virtualness’ these are really only addendums to any recommendations.

More applicable to government is free culture groups’ ‘radically transparent’ political process, by which all decision-making is carried out publicly, including decisions about the decision making process itself. Any action is considered to lack legitimacy until a clear, radically transparent decision has been made concerning them. The process makes actions significantly more accountable than even the best principal-agent communication practices, since it requires decision making to be transparent right from the beginning of the decision making process.

Traditional accountability, by contrast, is a process of verifying the quality of decisions or actions after they have been taken. This difference implies that while accountability generally implements some sort of punishment mechanism against individuals or institutions judged to have taken poor quality decisions or actions – after those decisions have been taken or actions carried out – radical transparency encourages corrections and improvements to decisions to be made long before poor quality decisions have the chance to be enacted. Hence, radical transparency potentially helps avoid the need for punishment mechanisms. In the corporate environment involving employees in decision-making process has been shown to greatly increase the acceptance and follow-through of those decisions.

An analysis of current transparency practices in the US government reveals some exercise of radical transparency, but even more shortcomings. All meetings of the US Congress are videotaped and publicly disseminated on C-SPAN and via the Internet, but sub-committee meetings, where much of the actual legislative gatekeeping takes place, are still held in private. Meetings between politicians and lobbyists and political supporters are held completely in

private, as are meetings of political parties. Moreover, given the logical and linguistic complexity of typical national laws, public participation is difficult despite the radical transparency at the formal congressional level. In other words, increased radical transparency is necessary, *but not sufficient*, for public participation in political decisions. The very nature of legislation excludes the common person from understanding and influencing political decisions. Accountability is impossible when your political agent's actions are indecipherable.

Censorship in the US: History

Censorship represents one of the most dangerous breakdowns of trust between a government and its citizens, and a lack of transparency in the process of deciding what can be censored is a potentially explosive source of antagonism. The First Amendment's guarantees on the freedom of the press led to the US government's adoption of a largely hands-off policy when it comes to media censorship, and in recent years we've seen increased efforts to promote transparency via legislation like the Freedom of Information Act. Unfortunately the increased US military presence abroad and the particular personality of the Bush administration have given rise to flagrant exercises in wartime powers and increased infringements of citizens' rights.

Providing some basis for comparison is a list of exceptions to this hands-off censorship policy throughout the last two centuries:

- The Sedition Act of 1798, which made it a crime to publish “false, scandalous, and malicious writing” against the government or its officials.

- The Office of Censorship, an emergency wartime agency, heavily censored reporting during World War II. On December 19, 1941 Roosevelt signed Executive Order 8985, which established the office and conferred on its director the power to censor international communications in “his absolute discretion.”⁸
- Under the Invention Secrecy Act of 1951 and the Atomic Energy Act of 1956, patents may be withheld and kept secret on grounds of national security.
- The Hollywood “Production Code”, a set of ethical guidelines for the film industry, was adopted in 1930 after the United States Supreme Court ruled in the 1915 Mutual Film Corporation v. Industrial Commission of Ohio case that the First Amendment did not protect motion pictures. Shortly after cities began to pass ordinances banning the public exhibition of “immoral” films. The film studios feared that state or federal regulations were not far off and the MPPDA (later MPAA) began self-regulating.
- Current FCC regulation of “indecent” free-to-air programming, which levies fines on programming its commissioners find in violation. There is no clear-cut, public definition of indecency.
- International Traffic in Arms regulations classifies software capable of strong cryptography as a “munition” and prohibits its export,⁹ acting as meta-censorship by restricting a citizens’ ability to effectively protect his privacy.

Reporters Without Borders’ publishes an index of press freedom in more than 170 countries every September¹⁰ (it should be noted that they also openly publish the questionnaires and

⁸ *Fiset, Louis. Return to Sender: U.S. Censorship of Enemy Alien Mail in World War II, Prologue Magazine Spring 2001, Vol. 33, No. 1. Retrieved from U.S. Government National Archives.*

⁹ *Code of Federal Regulations, Arms Export Control Act, Title 22 (Foreign Relations), Chapter I (Department of State), Subchapter M*

methodology used to produce their rankings). The United States has fallen to a middling 53rd of 168, a far cry from its initial place as 17th in 2002, the first year the index was published. From RSF's report:

Relations between the media and the Bush administration sharply deteriorated after the president used the pretext of "national security" to regard as suspicious any journalist who questioned his "war on terrorism." The zeal of federal courts which, unlike those in 33 US states, refuse to recognize the media's right not to reveal its sources, even threatens journalists whose investigations have no connection at all with terrorism.

They proceed to list several specific incidents in which Freedom of the Press was grossly violated this year, including:

- Freelance journalist and blogger Josh Wolf was imprisoned when he refused to hand over his video archives
- Sudanese cameraman Sami al-Haj, who works for the pan-Arab broadcaster Al-Jazeera, has been held without trial since June 2002 at the US military base at Guantanamo
- Associated Press photographer Bilal Hussein has been held by US authorities in Iraq since April this year.

These infractions highlight trends within the government that further prove the case for increased transparency. The act of monitoring someone's private communications is at the very least an

¹⁰ *Reporters Sans Frontieres, "Annual Worldwide Press Freedom Index – 2006." Available online at http://www.rsf.org/rubrique.php3?id_rubrique=639*

invasion of privacy, and a precursor to censorship and information gatekeeping; at worst they reflect the emergence of a police state. Working from our understanding of the importance of dialogue and dissent in the betterment of society the need for defense of civil liberties (in the form of modern updates to the tools of militia) becomes clear.

Censorship in the US: Surveillance Tactics

The current administration often argues that surveillance is necessary for the protection of national security, which has been a particularly convincing argument to the public at large in a post-9/11 America. Freedom of speech laws stop when the speaker is revealing national security secrets; police can request warrants for wiretaps of your home as well as petition for your bank records, educational transcripts, criminal record, and more. But the 4th Amendment prevents unwarranted search and seizure, and so all of the above cases necessitate cause: action, or at least suspicion. Blanket surveillance is completely without basis, and the Supreme Court has developed a solid foundation around the right to privacy. Legal experts believe the widespread warrantless surveillance currently being conducted is a violation of the Foreign Intelligence Surveillance Act of 1978, which allows warrantless searches of foreign powers (and terrorist organizations, as amended the PATRIOT Act of 2001) but specifically forbids its application to US citizens, including corporations. The Bush administration has responded by claiming that FISA is an unconstitutional infringement of executive power and concedes that they will not adhere to its regulations.

On December 16th, 2005 *New York Times* ran a story claiming that following the September 11th attacks, “President Bush secretly authorized the National Security Agency to eavesdrop on

Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying”¹¹

Under a presidential order signed in 2002, the intelligence agency monitored the international telephone calls and international e-mail messages of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible “dirty numbers” linked to Al Qaeda, the officials said.

The USA Today headline on May 11th, 2006 read, “NSA has massive database of Americans’ phone calls.”¹² Anonymous whistleblowers came forward about a call-record data collection project the National Security Agency has been operating since approximately 7 months before the September 11th terrorist attacks. It is claimed the NSA database contains over details of over 1.9 trillion phone calls made to and from the US. While the entries do not contain audio or transcripts of the content, all the other information – source, destination, and length of call – provides a ripe source for traffic analysis and data mining.

The NSA Call Database has prompted fierce objections from those who view it as a warrantless or illegal search and a violation of the ‘pen register’¹³ provisions of the Foreign Intelligence Surveillance Act and the Fourth Amendment of the United States Constitution. The Electronic Frontier Foundation levied a suit against AT&T earlier in the year alleging it had given the NSA

¹¹ James Risen, Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts", *The New York Times*, December 16, 2005.

¹² “NSA has massive database of Americans’ phone calls”, *USA Today*, May 11th, 2006. Available online at http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm

¹³ *Pen register: A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is dedicated. (Title 18, United States Code)*

access to its call-detail records, a charge that was reiterated by the USA Today article. Major telecom companies including Verizon, BellSouth, and Qwest have claimed they have not cooperated with the NSA's requests, but US Code permits companies to lie about their activities when the President believes that telling the truth would compromise national security.¹⁴

The EFF has also recently brought suit against the government over the Stored Communications Act of 1986, which allows the government to search and seize emails stored with an Internet Service Provider (ISP) or webmail provider like Hotmail or Gmail. The Supreme Court's decisions over the right to privacy extend to areas where people can "reasonably expect" privacy, and your personal inboxes certainly applies, regardless of where it is stored. The EFF has put forward the argument the email should be protected by the Fourth Amendment as much as phone calls, postal mail, or private papers you keep in your home.¹⁵

The Freedom of Information Act of 1966 (updated in 1996 to cover more recent technological changes) allows citizens the right to petition government agencies for records, a noble but underutilized and disrespected practice to improve accountability. The Electronic Frontier Foundation's FLAG project¹⁶ is using FOIA requests and litigation to expose the government's expanding use of technology that invades privacy. As more and more information is released about government infringement of citizens' civil rights the need for across-the-board transparency becomes increasingly clear. The FLAG project aims to expose negative practices and mobilize public opinion about the actions of their political agents. Taking advantage of

¹⁴ *US Codes of Law, Title 15, Chapter 2B, § 78m (b)(3)(A)*

¹⁵ "EFF Fights to Shield Email from Secret Government Searches", *EFF press release, November 27, 2006.* Available online at http://www.eff.org/news/archives/2006_11.php

¹⁶ *EFF FLAG (FOIA Litigation for Accountable Government) Project, <http://www.eff.org/flag/>*

FOIA is a good step towards improving client-agent communication, and thus accountability, but government agencies routinely disregard the time restriction and sometimes the entire request for the procurement of documents. Improved enforcement (and thus better support from the top) is needed.

Censorship in the US: Technical Capacities

Surveillance of personal communications is conducted through a variety of means, and a great deal of leeway is given the government in demanding cooperation from telecom and Internet service providers. The legality of these practices as exercised on US citizens is dubious but the methods by which they are conducted are fairly well understood.

Following the NSA Call Database scandal Mark Klein, an employee at AT&T, came forward and produced internal company documents detailing the technical process of setting up monitoring facilities for voice communication.¹⁷ Beyond his testimony Klein produced three internal company documents: a Dec. 10, 2002, manual titled “Study Group 3, LGX/Splitter Wiring, San Francisco,” a Jan. 13, 2003, document titled “SIMS, Splitter Cut-In and Test Procedure” and a second “Cut-In and Test Procedure” dated Jan. 24, 2003. Klein testified to the presence of “secret rooms” that were constructed inside AT&T’s central offices in several cities, to which only technicians with NSA clearance were given access. The manuals detail how to

¹⁷ “Whistle-Blower’s Evidence, Uncut”. *Wired Magazine*, May 22, 2006. Available online at <http://www.wired.com/news/technology/0,70944-0.html>

splice monitoring equipment into the company's data routing infrastructure; furthermore, "Cabinet Naming" lists revealed the presence of a 'Narus STA 6400.'

The (Narus) STA Platform consists of standalone traffic analyzers that collect network and customer usage information in real time directly from the message.... These analyzers sit on the message pipe into the ISP (internet service provider) cloud rather than tap into each router or ISP device.¹⁸

A Narus press release (1 Dec., 1999) also boasts that its Semantic Traffic Analysis technology "captures comprehensive customer usage data ... and transforms it into actionable information.... (It) is the only technology that provides complete visibility for all Internet applications.

The US government has also been involved in the development of 'policeware' applications for conducting digital wiretapping, a kind of 'man-in-the-middle' attack that is used to monitor email messages and other internet traffic. The FBI claims the software has "a unique ability to distinguish between communications which may be lawfully intercepted and those which may not."¹⁹ Security experts dispute the claim and have asked for more detailed information, which the FBI has been less-than-forthcoming about. Carnivore was renamed to the less ominous "DCS-1000" It has been reported that as of the middle of January 2005 that the FBI has essentially abandoned the use of Carnivore in 2001 in favor of commercially available software,

¹⁸ *Telecommunications Magazine*, April 2000

¹⁹ Forno, Richard. "Who's Afraid of Carnivore? Not me!" Available online at <http://cryptome.org/carnivore-rf.htm>

but due to the FBI's continued non-cooperation with FOIA requests it is impossible to verify their claims.

Most recently the San Jose Mercury broke a story²⁰ about the Bush administration demanding that major search engines, including Google, Yahoo, AOL, and MSN, turn over aggregate search information to “help revive a child protection law” by finding out how much pornography shows up in online searches and how often people may seek it. The request was given worrying strength when a Federal court judge ruled that Google, the only search engine who refused to turn over the data, was compelled to comply. While the data requested does not include any personal identifying markers like IP addresses or cookies it is foreseeable future requests would.

Conclusions

The threat of censorship and civil rights violations increasingly illustrates the need for a more accountable and responsible government. The open-source/free culture model provides an upper boundary to which transparency efforts can aspire. When decision-making is made in a radically transparent environment it is easier for all to accept and quicker to be implemented. Few efforts are made to expose and make comprehensible the workings of government; independent projects like FundRace²¹ help map out the source of campaign contributions, which is data the government makes public but almost completely inaccessible. The same lack of accessibility is found in the basic language of legislation and government conduct. Most current efforts at

20

²¹ *FundRace*, available online at <http://fundrace.org>

transparency and respect for the private citizen are a sham, and voters must collectively act in demanding more genuine and respectful government.

In the effort to help defend criticism of the government, improve accountability, and establish a 21st-century beachhead for the 2nd amendment and a genuine ‘threat of fork’ we have worked at Eyebeam to develop telecommunications techniques that help bloggers and activists hide their communications and identities from would-be persecutors: the Eyebeam Dissidence Toolkit.

Part 2:

The Eyebeam Dissidence Toolkit

You shall know the truth and the truth shall make you free.

- (*John 8:32*)

Overview

Transparency and free, copyleft publication of both work and process is the principle behind the establishment of the Eyebeam R&D OpenLab, which serves as incubator for “experimental technologies and media that directly enrich the public domain.”²² A driving force behind our practices is the belief that there can be no genuine security, and thus there should be no secrets. To this end we support all efforts to defend freedom of speech and the freedom of the press, and work to promote transparency and information sharing.

In response to the growing threat posed by unregulated and unmonitored surveillance of private citizens by world governments Eyebeam R&D has committed resources to the development of free and open-source tools that enable the average citizen to exercise their “right to bear arms” in defense of their freedoms in the 21st century. We have traded our muskets for telecommunications and our gunpowder for encryption. Specific emphasis has been placed on

²² From the Eyebeam R&D OpenLab website, <http://research.eyebeam.org/>

protecting the ability of individuals and groups to maintain secure communications in an attempt to defend their freedom of assembly and thus more effectively protect themselves.

Much of our work has been inspired by Reporters Without Borders' *Handbook for Bloggers and Cyber-Dissidents*, published in 2005. The 88-page document proffers advice and experiences from bloggers in nations who face persecution for expressing dissenting opinions, and describes several technical means by which one can anonymously blog, send email, and browse the Internet. Unfortunately many of their recommendations are based on commercial software or services, since these are the simplest and most available tools. Besides the obvious barrier of cost, widely available tools are easier targets to stop. It is trivial to put barriers in place to block users from running or even obtaining well understood and easily identified software.

We hope to remedy these shortcomings through the development and publication of software and hardware that enable the circumvention of restrictive firewalls and content-control software, and the strong encryption needed to protect transferred data from unwanted eavesdropping.

Additionally we will establish our own server infrastructure to serve as home to a group of adopted dissidents/beta-testers and provide communications infrastructure (blogging software, mailing lists, chat channels, etc.)

Tools

Connections on the Internet are regulated by firewalls, security devices that are configured to allow or deny data according to a specified security policy. Their basic task is to control traffic between networks with different levels of trust, preventing potentially dangerous data from passing either way. Corporations and universities use firewalls to both defend against external intrusion and prevent unwanted internal use of the Internet, by using content-control software to censor websites or access to personal email. Governments that practice Internet censorship of their citizens also use firewalls. For example, the ‘Great Firewall of China’ denies Internet users access to pages containing information about the Tiananmen Square protests and other information deemed a threat to national security. This kind of Orwellian control of information is an effort to rewrite history and deny access to the truth.

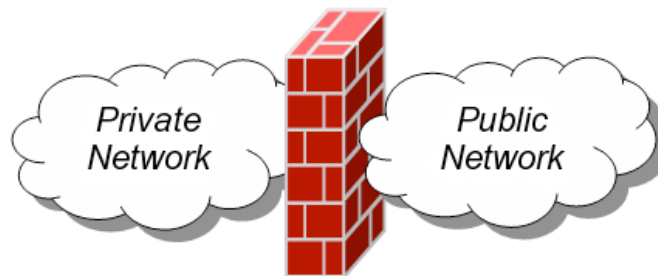


Exhibit: a metaphorical firewall.

The Dissidence Toolkit composes a number of applications all targeted towards securing data transmission, masking the user’s identity, and circumventing restrictive firewalls. Since firewall circumvention inherently relies on the presence of at least one server that the client can trust the

tools have been designed with fluid server interchange in mind, allowing fallbacks as specific servers are discovered and blocked.

Requirements for tools used and/or developed:

- Free & open-source
- Cross-platform (Microsoft Windows, Apple Mac OS X, free UNIX-based operating systems)
- Portable
- Wide range of applicability to, e.g. able to interface with or over existing software without modification

The formal goals of the project are:

- Remove identifying information from your data using Tor Onion Routing
- Transparent, encrypted connections using SSH tunneling to hide information sent and received
- Establishment of redundant trusted proxy servers throughout the global to act as information relays and hosts for communications infrastructure (mailing lists, chat rooms, blogs, instant message relays, etc.)
- Distribution of server locations using Distributed Hash Tables (DHT), providing redundant failover

Tor Onion Routing

The Tor Onion Routing Network is a low-latency network for packet anonymization, providing resistance to traffic analysis, eavesdropping, and other attacks both by outsiders (e.g. Internet routers) and insiders (Onion Routing servers themselves). It was originally developed by the US Navy in 1999 but has been released to the open-source community at large. An explanation of the common dangers of traffic analysis:

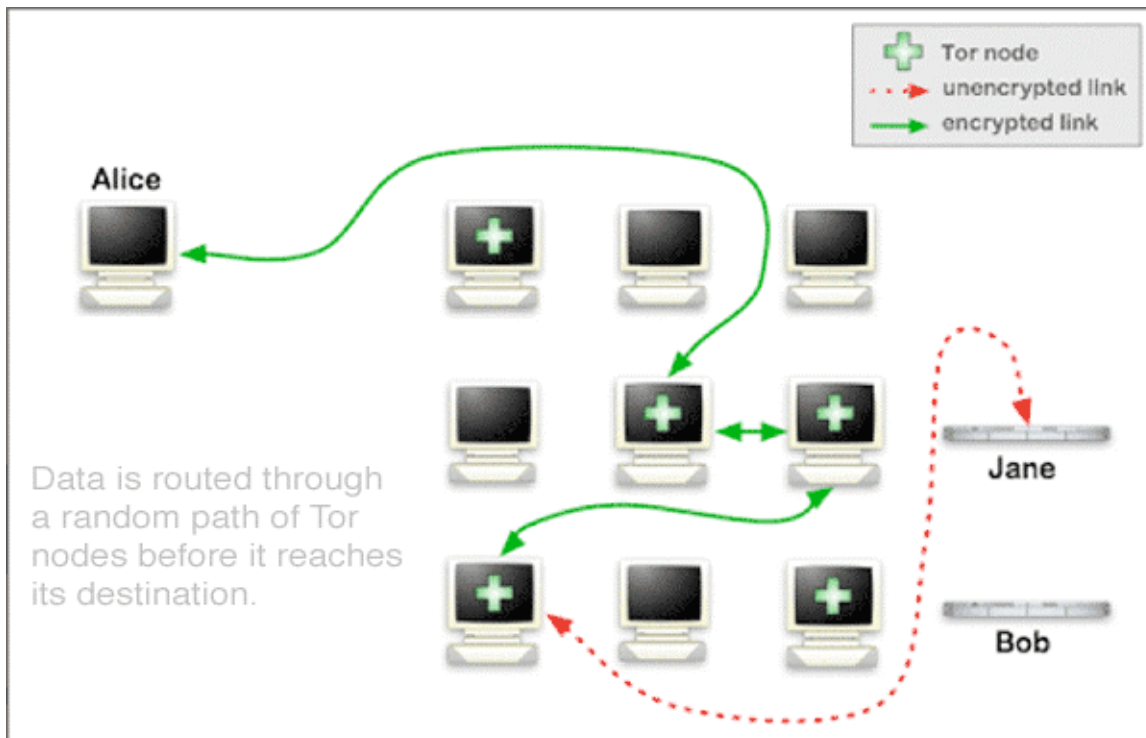
Knowing the source and destination of your Internet traffic allows others to track your behavior and interests. This can impact your checkbook if, for example, an e-commerce site uses price discrimination based on your country or institution of origin. It can even threaten your job and physical safety by revealing who and where you are. For example, if you're traveling abroad and you connect to your employer's computers to check or send mail, you can inadvertently reveal your national origin and professional affiliation to anyone observing the network, even if the connection is encrypted.²³

Internet data packets have two parts: a data payload and a header used for routing. The data payload is whatever is being sent, whether that's an email message, a web page, or an audio file. Even if you encrypt the data payload of your communications, traffic analysis still reveals a great deal about what you're doing and, possibly, what you're saying. That's because it focuses on the header, which discloses source, destination, size, timing, and so on. An attacker with far-reaching access to information networks like the government can compile a huge amount of data on the communication patterns of organizations and individuals, even if it is not able to specifically read the content.

²³ From the Tor website, <http://tor.eff.org/>

Tor solves the problem by passing your data over multiple places on the Internet, so no single link from you to your destination exists. The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you—and then periodically erasing your footprints. Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several servers that cover your tracks so no observer at any single point can tell where the data came from or where it's going. The Tor network is a peer-to-peer network in which all people using the software are also acting as relays for the other users, in addition to many universities and groups that have volunteered their bandwidth to support the network. It is impossible for a Tor node to tell if the packets it is relaying actually originated with the sender, removing any kind of legal liability.

Exhibit: Tor Onion Routing



Tor Onion Routing has a number of shortcomings. It protects only the transport of data and not the data itself. It is also relatively easy to identify machines running the Tor software, and while specific data could not be traced to the user, simply running the software can attract unwanted attention

Tor Onion Routing software is licensed under a variant of the 3-clause BSD license and is available online at <http://tor.eff.org/>

The CULT OF THE DEAD COW “hactivist” group recently released Torpark,²⁴ which is a version of the Portable Firefox web browser with Tor Onion Routing built-in. It also runs a local SOCKS proxy that allows other applications to use the onion routing obfuscation. Torpark is currently only available for Microsoft Windows, but it is still being evaluated for inclusion in the Dissidence Toolkit.

jtunnel

jtunnel is a collection of client- and server-side scripts and applications that facilitate the establishment of encrypted connections using SSH, a system that uses well-understood and time-tested asymmetric public key cryptography to hide the contents of data being sent back and forth. SSH suffers from the fact that it is so widely used – firewall administrators typically block the

²⁴ “*Hactivismo Releases Torpark,*”

ports used by standard SSH connections, and it is easy to identify SSH packets themselves if passed through non-standard ports. j tunnel uses two hybrid connection techniques to overcome these limitations:

SSH-over-HTTPS allows SSH connections to masquerade as and/or proxy through secure HTTP connections. To firewalls and eavesdroppers the connections and data transferred appear to be ordinary connections to secure websites, such as eCommerce websites, or NYUHome. One limitation is that HTTPS connections do not typically last nearly as long as SSH connections, and so it is recommended that j tunnel users do not use a single server for an extended period of time.

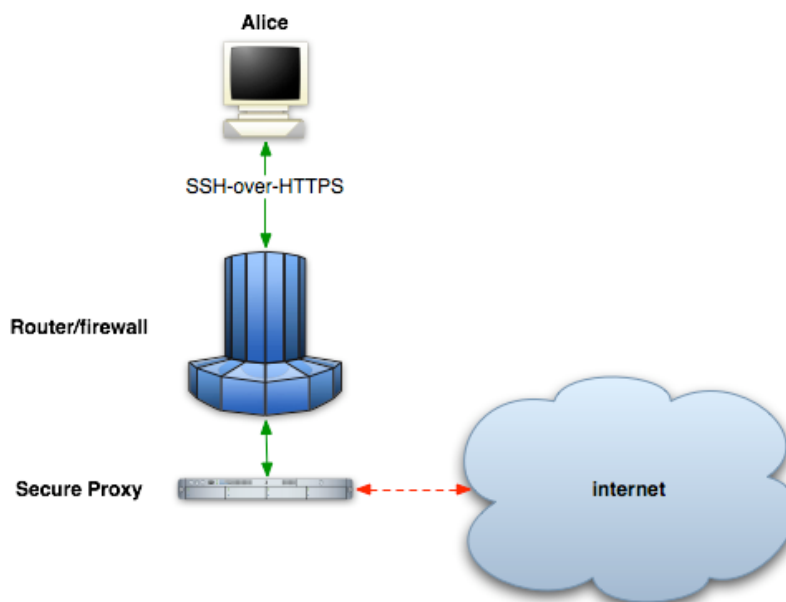


Exhibit: SSH tunneling

IP-over-DNS allows standard Internet traffic to be relayed through the protocols typically reserved for the translation of “example.com” to the unique IP address

To the author's knowledge no existing firewall or packet sniffing software is outfitted to monitor the fake DNS traffic. IP-over-DNS also allows its user to establish full send/receive connectivity from crippled or limited Internet connections, such as those found in airports or in public kiosks.

jtunnel is released under the GNU Public License and is available online at

<http://tramchase.com/jtunnel>