

Vulnerable Populations

Lecture 21

Prof. Daniel Votipka
Spring 2021

(some slides courtesy of Adam Aviv)

Administrivia

- Homework 4 is due on Thursday (4/22)
 - Q1 is individual and Q2 should be done as project teams
- Meet your professor 1:1 by end of the month for **5 points on your final grade**

What we did last time!

- Network Defenders
 - Issues they face
 - Threat modeling
- Hackers
 - Processes and mental models
 - How to build better tools and education

What are we doing today?

- Vulnerable populations
 - Journalists
 - Undocumented Immigrants
 - Victims of intimate partner abuse
- Other groups?
- What makes these (and other) user groups different?

What are we doing today?

- Vulnerable populations
 - Journalists
 - Undocumented Immigrants
 - Victims of intimate partner abuse

Journalists

Crypto Wars

On April 16, 1993, the New York Times broke the story of the Clipper Chip, an encryption technology developed by the National Security Agency that allows government to eavesdrop on the communications of criminals, suspects, and unfortunately, law-abiding citizens alike.

On February 9, 1994, the U.S. Department of Commerce and Vice President of the United States summarily announced that the Clipper Chip is the U.S. Government standard, and that the Government will do everything in its power to encourage its use in the private sector and the international community.

They'll excuse us if we don't wish them luck.

SINK CLIPPER!

Because some things
are better left unread.



- Cryptography treated like weapons
 - Subject to export control
- Fear that with strong cryptography the government couldn't ~~spy on~~ protect its citizens



Encrypted Email and Encrypted Phone Calls



AT&T TSD-3600-E

Telephone Encryptor

The TSD-3600-E was an advanced telephone security device, developed by [AT&T](#) (USA) in 1992. It was based on the controversial [Clipper Chip](#), forcing users to escrow their cryptographic keys. The TSD-3600 was a small white box that was connected between the handset and the phone.

The image on the right shows a TSD-3600-E unit. It only has two buttons and an LCD at the front, two sockets on the right (for connecting the phone) and a power connector at the rear.



Also at the rear is a socket for a module, that adapts the TSD-3600 to the characteristics of the telephone's handset. A number of suitable modules was usually delivered with each phone and additional modules — for other handsets — could be ordered from the manufacturer. The TSD-3600-E box is inserted [between the phone and its handset](#), by means of a short cable.

The TSD-3600-E was introduced in 1993 and the first large order was placed by the United States Government themselves. Eventually, the US Government appeared to be the only major customer for the device. It later turned out that many boxes remained unopened for over 10 years, catching nothing but dust. The cost of a single TSD-3600-E unit in 1993 was \$1000 [3].



Key Escrow



Second Crypto Wars

On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures

BY PARKER HIGGINS | APRIL 16, 2015

The FBI has complained about the impending doom of communications "going dark" for decades now. You can read FBI testimony from the 1990s that is [virtually indistinguishable from the same misguided statements today](#). As the overwhelming majority of security experts will tell you, inserting backdoors in the security software we rely on makes us all less safe. As we articulated over 20 years ago, "key escrow" is really "key surrender," and isn't part of a coherent security strategy. And that's [just one of the epic failures](#) that come from government efforts to regulate cryptography.

<https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures>

What's all this about Europe wanting crypto backdoors?

Natasha Lomas @riptari / 7:44 AM EST • November 9, 2020



The EU in Crypto War



November, 2020!!!

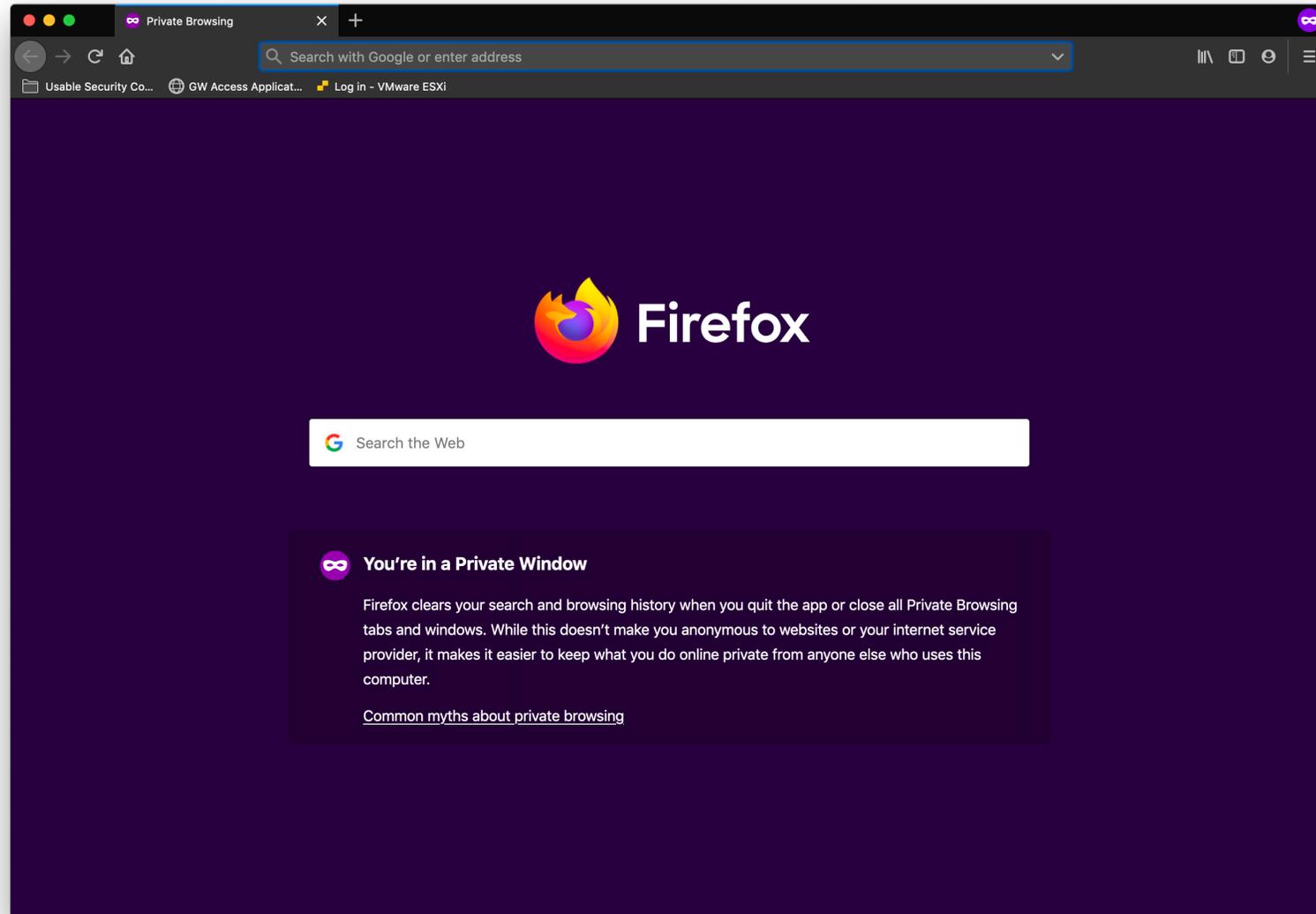


Matthias Monroy

Once again, the EU member states demand the weakening of encryption, associations and activists protest vehemently

How do users try to achieve privacy online?

Private Browsing



VPNs

Your IP: 128.164.102.225 · ISP: The George Washington University · Your Status: **Unprotected**



[Features](#) [Pricing](#) [Servers](#) [VPN Apps](#) [Blog](#) [Help](#) [My Account](#)

Recommended by  & 

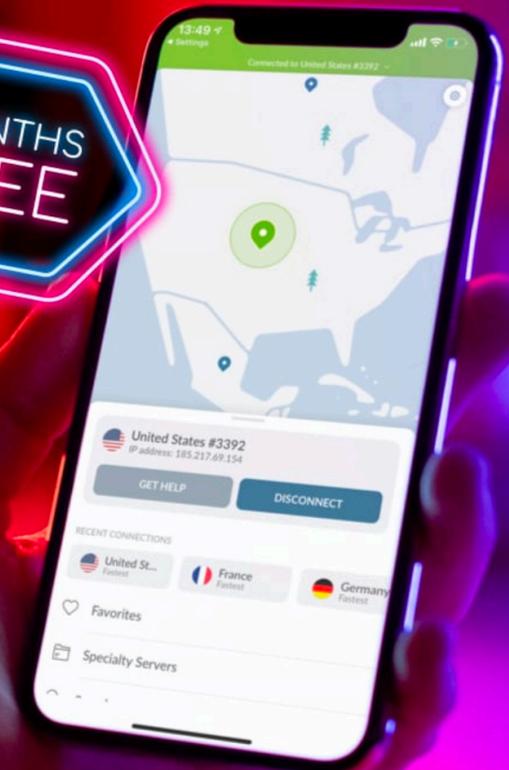
Get cyber deal + 3 months free. Now only \$3.49/mo.

Grab the 3-year NordVPN deal and enjoy ultimate online security.

00 : 09 : 38 : 55
days hours minutes seconds

Get It With 70% Off

 30-day money-back guarantee



Trar

https://www.torproject.org/videos/Tor_Animation_en.mp4

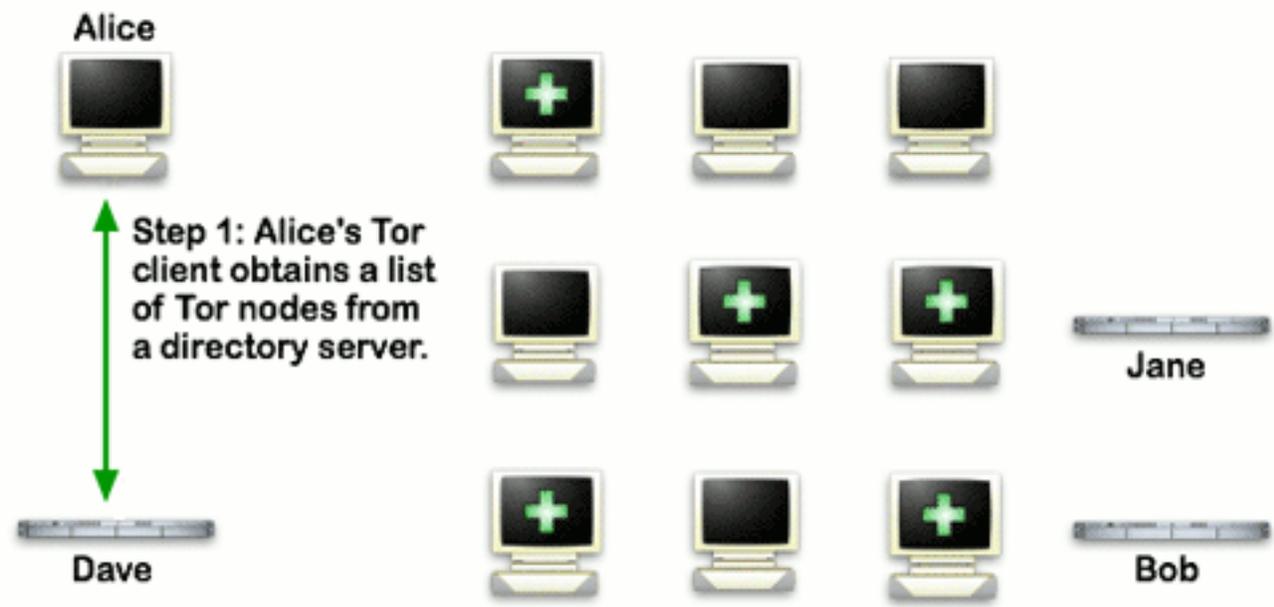
How Tor Works: 1

+

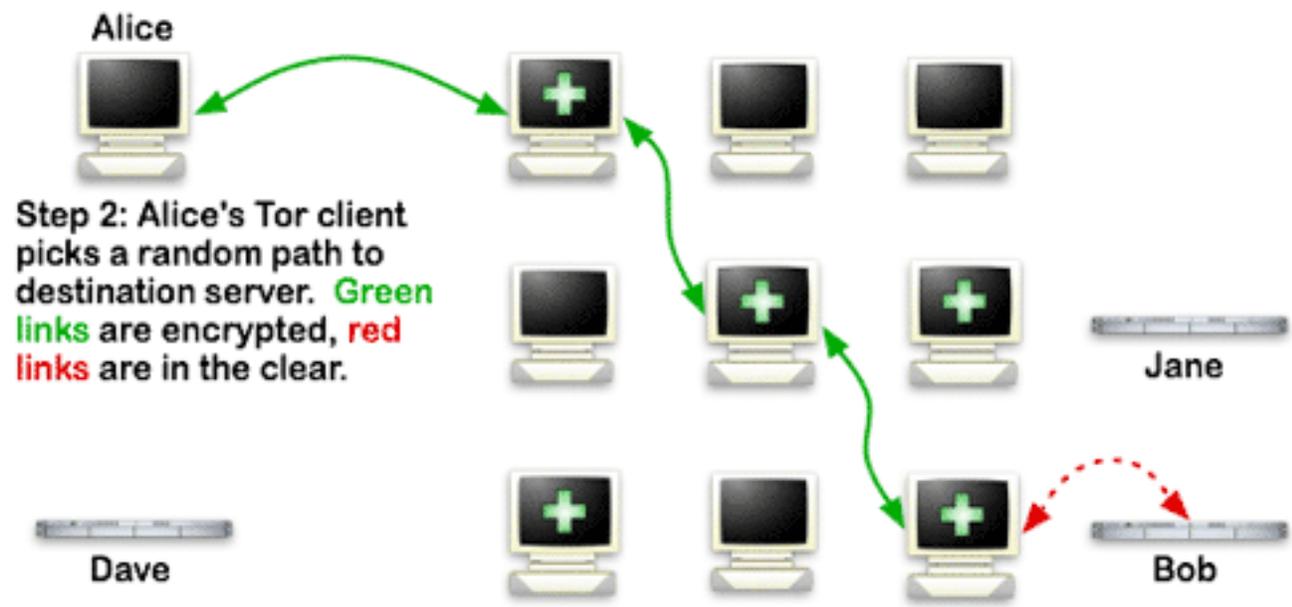
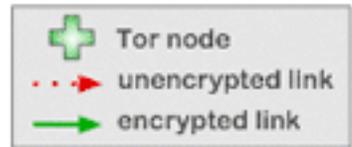
Tor node

... → unencrypted link

→ encrypted link

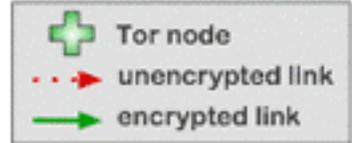


How Tor Works: 2



Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.

How Tor Works: 3



Alice



Step 3: If at a later time, the user visits another site, Alice's tor client selects a second random path. Again, green links are encrypted, red links are in the clear.



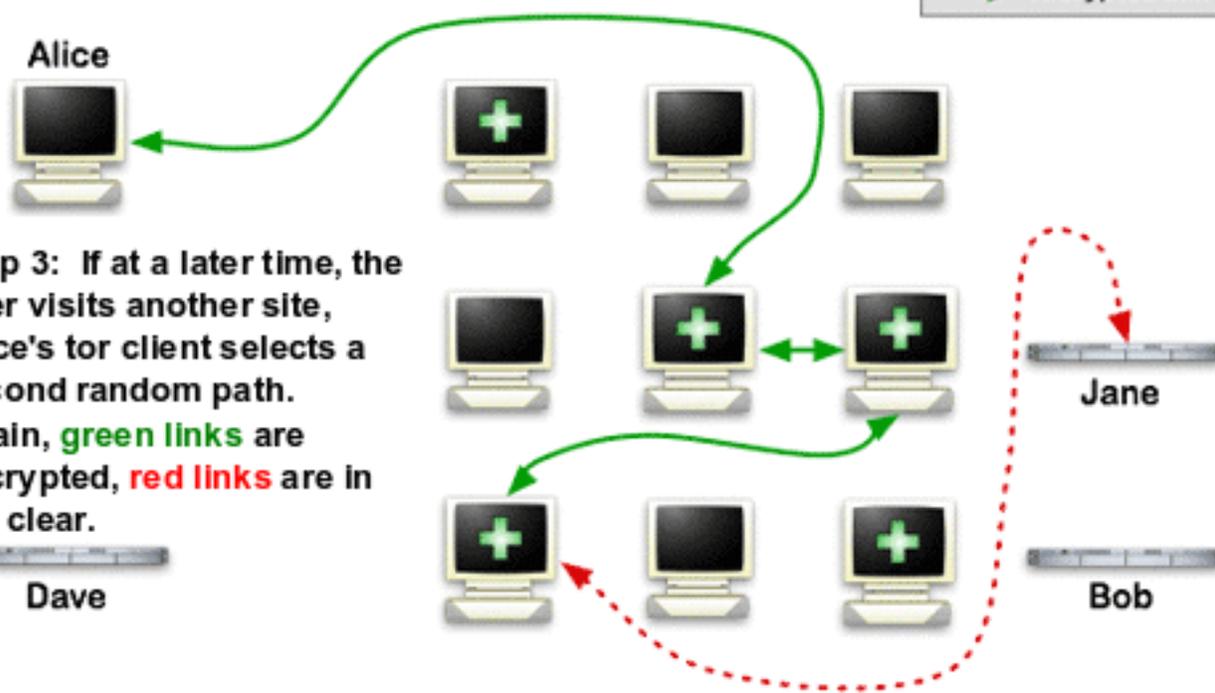
Dave



Jane



Bob



Tor's Protection

- Low latency anonymity system
- Protection against a global adversary
 - Can view entire network
 - Can't correlate input to output

Why Johnny Can't Blow the Whistle

- Tor's Browser Bundle (TBB)

- Asked participants to install and use TBB
 - Identify “stop points”

- Studies
 - Lab study
 - Implementation changes

USEC 2014

Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems

Greg Norcie
Indiana University
gnorcie@indiana.edu

Jim Blythe
Information Sciences Institute
blythe@isi.edu

Kelly Caine
Clemson University
caine@clemson.edu

L. Jean Camp
Indiana University
ljcamp@indiana.edu

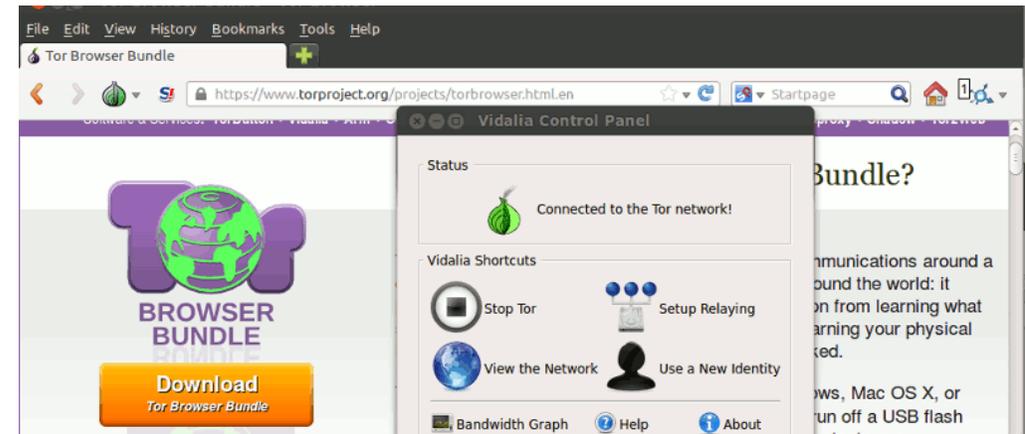
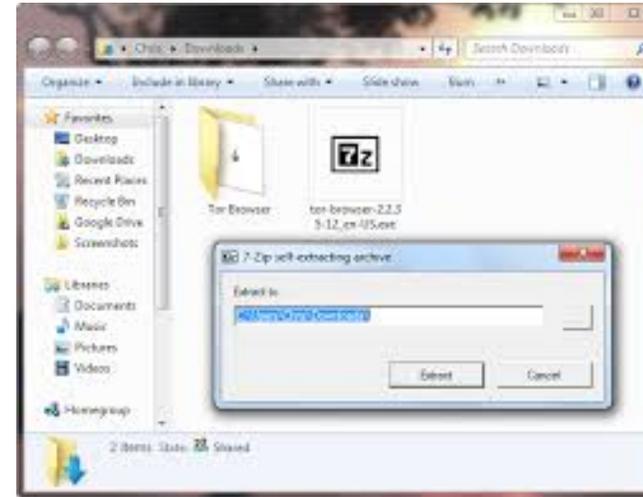
Abstract—Tor is one of the most widely used anonymity networks in the world. The anonymity provided to any individual Tor user is a function of the total number of Tor users. Adoption of anonymity tools, including Tor, can be hindered by a lack of usability. Therefore, enhancing Tor's usability and making it easier for more people to use Tor successfully increases security for all Tor users. To enhance Tor usability we begin by identifying stop-points which may act as barriers to using the Tor Browser Bundle (TBB). We suggest changes based on our analysis of these stop-points. To follow through, in our second study we test whether the changes we recommended to the Tor Project are effective in increasing usability, and find a significant decrease in stop-points across the board. Based on these studies, we both suggest new design heuristics appropriate for improving the usability of anonymity systems and identify design heuristics which are particularly salient in the design of anonymity systems.

Tor uses onion routing [24] to prevent third parties from observing or transparently interjecting themselves into a user's web activity. The term “onion routing” refers to Tor's layered encryption, analogous to the layers in an onion, which prevents third parties (including Tor nodes) from observing the content of packets in transit. Tor also prevents the linkage of the source and destination of any packet in the Tor network. Of course, there are attacks that threaten privacy even when using Tor, including subversion via control of malicious nodes and timing attacks. However, the largest challenge facing Tor arguably is not timing attacks, but rather the relatively small number of Tor users. In terms of providing anonymity, more users is better.

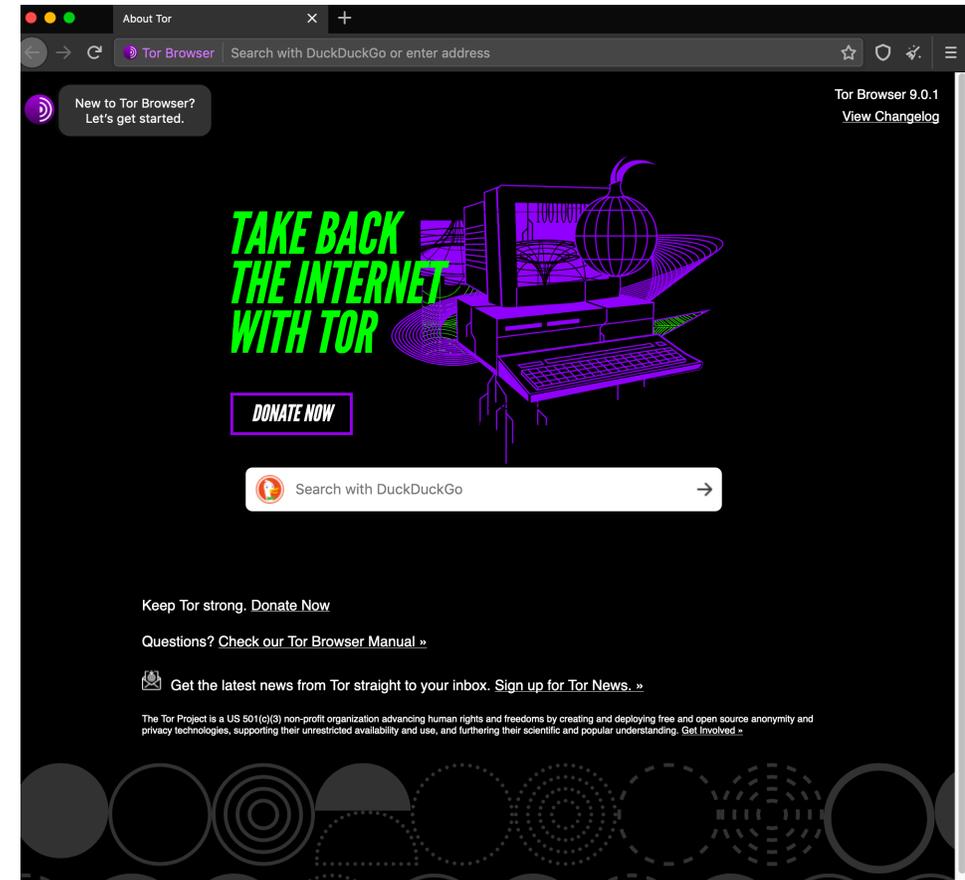
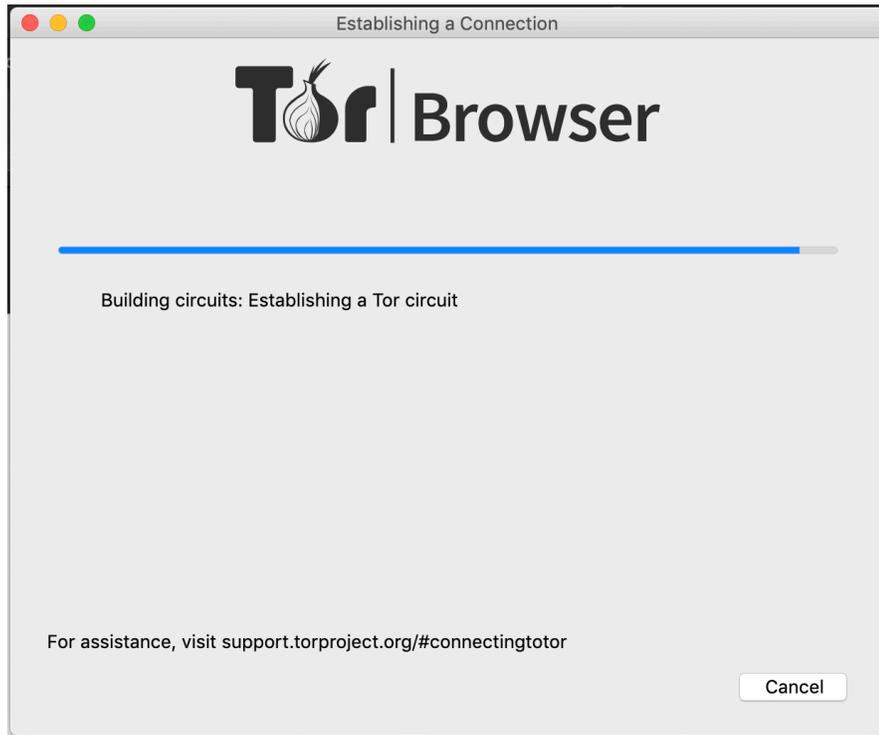
As Dingleline and Mathewson [16] point out, there is a strong network effect present in anonymity networks like Tor.

Identified Issues

- Launch times
 - Slow to launch and setup
- Browsing delays
 - Browsing was delayed
- Download Criteria
 - Unclear of which package to download
- Windows Discriminability
 - Which window as TBB which was normal browser
- Archive Confusion
 - Couldn't unzip the archive and follow installation instructions
- Icon Salience
 - The icon didn't convey privacy
- Security Measure Confusion
 - Internal security measures, like redirecting to duckduckgo from google, confused users



Tor Browser Today



Who uses Tor, anyway?

SOLOVE POST-AUTHOR PAGES (SUPER FINAL).DOC

2/7/2008 3:16:38 PM

Mass data collection can
have a chilling effect

**“I’ve Got Nothing to Hide” and Other
Misunderstandings of Privacy**

The harms consist of those created by
bureaucracies—indifference, errors,
abuses, frustration, and lack of
transparency and accountability

[View all blog posts »](#)

Who Uses Tor?



Family & Friends

People like you and your family use Tor to protect themselves, their children, and their dignity while using the

Internet.



Businesses

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal

accountability.



Activists

Activists use Tor to anonymously report abuses from danger zones.

Whistleblowers use Tor to safely report

on corruption.



Media

Journalists and the media use Tor to protect their research and sources online.



Military & Law Enforcement

Militaries and law enforcement use Tor to protect their communications, investigations, and intelligence

gathering online.

Media



Journalists and their audience use Tor

- **Reporters without Borders** tracks Internet prisoners of conscience and jailed or harmed journalists all over the world. They advise journalists, sources, bloggers, and dissidents to use Tor to ensure their privacy and safety.
- Tor is part of **SecureDrop**, an open-source whistleblower submission system that media organizations can use to securely accept documents from and communicate with anonymous sources. **Many news organizations** use SecureDrop, including the Associated Press, The Washington Post, The New York Times, The CBC, ProPublica, Dagbladet, and more.
- Tor preserves the ability of people behind national firewalls or under the surveillance of repressive regimes to obtain a global perspective on controversial topics including democracy, economics and religion.
- **Citizen journalists in China** use Tor to write about local events to encourage social change and political reform.
- **Citizens and journalists in Internet black holes** use Tor to research state propaganda and opposing viewpoints, to file stories with non-State controlled media, and to avoid risking the personal consequences of intellectual curiosity.

SECUREDROP

Have a document to share?

You are not anonymous while using this browser!

Here's what you need to do to download Tor Browser to be anonymous online:

1. Go to <https://www.torproject.org>.
2. Download and install Tor Browser.
3. Launch Tor Browser and return to this site. You are now anonymous online.

Get SecureDrop at your organization >

Journalists

High Profile Leakers and Whistle Blowers





Remember that Glenn couldn't encrypt

Edward Snowden



Glenn Grenwald



But Laura Poitras could!

Edward Snowden



Laura Poitras



Reality Winner



Leaked information about 2016 Russian Election Interference



TOP-SECRET NSA REPORT DETAILS RUSSIAN HACKING EFFORT DAYS BEFORE 2016 ELECTION

A top-secret National Security Agency report details a months-long Russian hacking effort against the U.S. election infrastructure.



Matthew Cole, Richard Esposito, Sam Biddle, Ryan Grim

June 5 2017, 3:44 p.m.

← June 5, 2017

[LEIA EM PORTUGUÊS →](#)

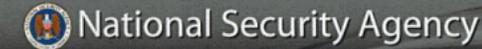
RUSSIAN MILITARY INTELLIGENCE executed a cyberattack on at least one U.S. voting software supplier and sent spear-phishing emails to more than 100 local election officials just days before last November's presidential election, according to a highly classified intelligence report obtained by The Intercept.

The top-secret National Security Agency document, which was provided anonymously to The Intercept and independently authenticated, analyzes intelligence very recently acquired by the agency about a months-long Russian intelligence cyber effort against elements of the U.S. election and voting infrastructure. The report, dated May 5, 2017, is the most detailed

Published the ORIGINAL documents in PDF

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA

DIRNSA



Russia/Cybersecurity: Main Intelligence Directorate Cyber Actors, Target U.S. Companies and Local U.S. Government Officials Using Voter Registration-Themed Emails, Spoof Election-Related Products and Services, Research Absentee Ballot Email Addresses; August to November 2016 (TS//SI//OC/REL TO USA, FVEY/FISA)

(U//FOUO) INTELLIGENCE PURPOSES ONLY: (U//FOUO) The information in this report is provided for intelligence purposes only but may be used to develop potential investigative leads. No information contained in this report, nor any information derived therefrom, may be used in any proceeding (whether criminal or civil), to include any trial, hearing, or other proceeding before any court, department, agency, regulatory body, or other authority of the United States without the advance approval of the Attorney General and/or the agency or department which originated the information contained in this report. These restrictions apply to any information extracted from this document and used in derivative publications or briefings.

(U//FOUO) CYBERSECURITY INFORMATION: (U//FOUO) The unclassified data in this report is protected from public disclosure by Federal Law. This report includes sensitive technical information related to computer network operations that could be used against U.S. Government information systems. Any scanning, probing, or electronic surveying of IP addresses, domains, email addresses, or user names identified in this report is strictly prohibited. Information identified as UNCLASSIFIED//FOR OFFICIAL USE ONLY may be shared for cybersecurity purposes at the UNCLASSIFIED level once it is disassociated from NSA/CSS. Consult the originator prior to release of this information to any foreign government outside of the original recipients.

SUMMARY (U)

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [redacted] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance [redacted]

Declassify On: 20420505

After Reality Winner's Arrest, Media Asks: Did 'Intercept' Expose a Source?



Sharing an original document when asking questions of government officials, as The Intercept appears to have done, can expose metadata and high-tech watermarks that may reveal a leaker's identity. And [an affidavit](#) asserts that The Intercept revealed to a second contractor that the document was mailed from Augusta, Ga., where Ms. Winner resides.



Reality Leigh Winner. Instagram, via Reuters

possession of what it believed to be a classified document authored by the U.S. Government Agency. The News Outlet provided the U.S. Government Agency with a copy of this document. Subsequent analysis by the U.S. Government Agency confirmed that the document in the News Outlet's possession is intelligence reporting dated on or about May 5, 2017 (the "intelligence reporting"). This intelligence reporting is classified at the Top Secret level, indicating that its unauthorized disclosure could reasonably result in exceptionally grave damage to the national security, and is marked as such. The U.S. Government Agency has since confirmed that the reporting contains information that was classified at that level at the time that the reporting was published on or about May 5, 2017, and that such information currently remains classified at that level.

14. The U.S. Government Agency examined the document shared by the News Outlet and determined the pages of the intelligence reporting appeared to be folded and/or creased, suggesting they had been printed and hand-carried out of a secured space.

15. The U.S. Government Agency conducted an internal audit to determine who accessed the intelligence reporting since its publication. The U.S. Government Agency determined that six individuals printed this reporting. These six individuals included WINNER. A further audit of the six individuals' desk computers revealed that WINNER had e-mail contact with the News Outlet. The audit did not reveal that any of the other individuals had e-mail contact with the News Outlet.

16. The U.S. Government Agency determined that WINNER had e-mail communication with the News Outlet on or about March 30, 2017, and March 31, 2017. The first

What went wrong? Why is this so hard?

What technologies and skills do journalists need to protect sources?

- What are the general practices of journalists in communicating with their sources?
- What are the security concerns and threat models of journalists with respect to source communication?
- What, if any, defensive strategies (technical or otherwise) do journalists employ to protect themselves or their sources? How and why do some possible defensive strategies succeed and others fail?
- What are the needs of journalists in their communications with sources that are currently hampered or unfulfilled by computer security technologies?

USENIX Security 2015

Investigating the Computer Security Practices and Needs of Journalists

Susan E. McGregor
*Tow Center for Digital Journalism
Columbia Journalism School*

Polina Charters, Tobin Holliday
*Master of HCI + Design, DUB Group
University of Washington*

Franziska Roesner
*Computer Science & Engineering
University of Washington*

Abstract

Though journalists are often cited as potential users of computer security technologies, their practices and mental models have not been deeply studied by the academic computer security community. Such an understanding, however, is critical to developing technical solutions that can address the real needs of journalists and integrate into their existing practices. We seek to provide that insight in this paper, by investigating the general and computer security practices of 15 journalists in the U.S. and France via in-depth, semi-structured interviews. Among our findings is evidence that existing security tools fail not only due to usability issues but when they actively interfere with other aspects of the journalistic process; that communication methods are typically driven by sources rather than journalists; and that journalists' organizations

and sources cross the line from legal consequences to the potential for physical harm [42, 57, 58].

Responses to these escalating threats have included guides to best computer security practices for journalists (e.g., [17, 43, 47, 62]), which recommend the use of tools like PGP [67], Tor [22], and OTR [14]. More generally, the computer security community has developed many secure or anonymous communication tools (e.g., [4, 10, 14, 21–23, 63, 67]). These tools have seen relatively little adoption within the journalism community, however, even among the investigative journalists that should arguably be their earliest adopters [48].

To design and build tools that will successfully protect journalist-source communications, it is critical that the technical computer security community understand the

Contact with sources

Please think about a specific story that you have published in approximately the last year for which you spoke with a source. (There is no need to tell us the specific story or source, unless you believe this information is not sensitive and would like to share it.)

- Whether they had a relationship with the source prior to this story;
- How they first contacted the source about the story;
- Primary form(s) of communication with the source;
- Whether they would feel comfortable asking this source to use a specific communication method; and
- How representative this example is of their communication with sources in general.

How they work as a journalist

- Their note-taking and storage process, and whether they take any steps to protect or share their notes;
- Problems that might arise if their digital notes or communications were revealed;
- Any non-technological strategies they use to protect themselves or their sources;
- Whether someone has ever recommended they use security-related technology in their work;
- How they define “sensitive” information or sources in their work;
- Any specific security-related problems to which they wish they had a solution;
- What kinds of devices they use, and who owns and/or administers them;
- Whether they have anyone, inside or outside of their organization, to whom they can go for help with computer security or other technologies; and
- Their self-described comfort level with technology and security-related technology.

Recruitment

<i>Number</i>	<i>Identifier</i>	Participant		Interview			Technical Expertise	
		<i>Gender</i>	<i>Organization (Type)</i>	<i>Location</i>	<i>Language</i>	<i>Length</i>	<i>General</i>	<i>Security</i>
1	P0	Male	Large, established	France	English	32 min	High	High
2	P1	Female	Large, new	USA	English	31 min	High	Medium
3	P2	Female	Large, established	France	English	39 min	Medium	Low
4	P3	Female	Large, established	France	English	39 min	High	Medium
5	P4	Female	Large, established	France	English	42 min	Medium	Low
6	P5	Male	Large, established	France	French	24 min	Medium	Low
7	P6	Male	Large, established	France	French	23 min	Medium	Medium
8	P7	Female	Large, established	France	English	27 min	High	Low
9	P8	Male	Large, established	France	English	20 min	High	Medium
10	P9	Male	Large, new	USA	English	41 min	High	Medium
11	P10	Female	Large, new	USA	English	31 min	Medium	Medium
12	P11	Female	Large, new	USA	English	19 min	Medium	Low
13	P12	Female	Small, new	USA	English	17 min	Medium	Low
14	P13	Female	Small, new	USA	English	34 min	High	Low
15	P14	Female	Small, established	USA	English	25 min	Medium	Medium

What would you expect?

Key Findings

- Concern levels
 - More expected: govt. surveillance, disciplinary action against sources
 - Less expected: financial impact on organizations
- Usability and adoption
 - Conflict between privacy needs and journalistic needs
 - Authenticating anonymous sources
 - Better general knowledge management, e.g., don't just use google doc or evernote
- Driven by the source
 - Communication level set by the source, not the journalists
 - What the source is comfortable with is what the journalist will use
- Digital divide
 - Source populations do not have access to or knowledge about technology
 - Habits of sources are a bigger hindrance than that of journalists

Choice of communication technology

- Conflict between removing barriers for communication and keeping the source safe

[The source] probably understand[s] the threat model they're under better than I would. So, it brings up an interesting question: do you go with what they're comfortable with? Or do you say, alright, actually let me assess what's going on and get back to you with what would be appropriate. [...] People's first impression is that they would go by what the source feels comfortable doing. As opposed to stepping in and being paternalistic about it.

Tool or technology	Number of participants (of 15)	Inter-coder agreement (κ)
Phone	15	1.00
Email (unencrypted)	15	1.00
Google Docs/Drive	8	1.00
Microsoft Word	8	1.00
SMS	8	1.00
Social media	7	0.83
Dropbox	4	1.00
Skype	4	1.00
Evernote	3	1.00
Text editor	2	1.00
Chat (unencrypted)	1	1.00
Scrivener	1	1.00

Table 2: **Non-security-specific tools.** This table reports the number of participants who mentioned using various non-security-specific tools or technologies in their work.

Security Concerns

Category	Concern	Number of participants (of 15)	Inter-coder agreement (κ)
<i>Threats to sources</i>	Discovery by government	6	0.88
	Disciplinary action (e.g., lost job)	6	0.88
	Reputation/personal consequences	6	0.88
	Generally vulnerable populations (e.g., abuse victims)	4	0.65
	Discovery by others wishing to reveal identity	3	0.80
	Physical danger	3	0.86
	Prison	2	1.00
<i>Threats to journalist or organization</i>	Reputation consequences (incl. loss of source's trust)	9	0.89
	Being "scooped" (i.e., journalistic competition)	6	1.00
	False or misleading information from a source	4	0.36
	Physical threats (incl. theft)	2	0.50
	Financial consequences	1	1.00
<i>Threats to others</i>	Political / foreign relations consequences	1	0.50
	Other	1	1.00

Table 3: **Security concerns.** We report how many participants mentioned various threats to themselves, to their sources, to their organizations, or to others. These are not necessarily threats that participants have directly encountered or acted on themselves — that is, they discussed threats both in a hypothetical sense (concerns they have) and a concrete sense (real issues they have encountered).

Defensive Strategies

Category	Defense	Number of participants (of 15)	Inter-coder agreement (κ)
<i>Technical defenses</i>	Encrypting digital notes	6	1.00
	Keeping files local (not in the cloud)	5	0.89
	Encrypted communication with colleagues	3	0.81
	Circumventing organization's admin rights on computer	2	0.50
	Encrypted communication with sources	2	0.50
	Anonymous communication (e.g., over Tor)	2	1.00
	Air-gapping a computer (keeping it off the internet)	1	1.00
	Using additional, secret devices or temporary burner phones	1	1.00
	Visually obscuring information in photos/videos (e.g., blurring)	1	0.50
<i>Ad hoc non-technical strategies</i>	Using code names in communications or notes	8	1.00
	Claiming bad handwriting as a defense for written notes	3	1.00
	Contacting sources through intermediaries	2	0.81
	Citing multiple sources to create plausible deniability	1	1.00
	Using some method to authenticate source	1	1.00
<i>Explicitly avoiding technology</i>	Communicating in person	7	0.72
	Self-censoring (avoiding saying things in notes/email)	6	0.86
	Communicating only vague information electronically	5	0.83
	Physically mailing digital data (e.g., on USB stick)	2	1.00
<i>Physical defenses</i>	Home alarm system	1	1.00
	Physical safe (e.g., to store notes)	1	1.00
	Shredding paper documents	1	1.00

Table 4: **Defensive techniques.** We report the number of participants who mentioned using various defensive techniques to protect themselves, their notes, and/or their sources.

What security tools are used

Security tool or technology	Number of participants (of 15)				Inter-coder agreement (κ)
	<i>Use regularly</i>	<i>Tried but don't use</i>	<i>Haven't tried</i>	<i>Not mentioned</i>	
Dispatch	0	0	1	14	1.00
Encrypted chat (e.g., OTR, CryptoCat)	5	0	1	9	0.90
Encrypted email (e.g., GPG, Mailvelope)	4	4	1	6	0.92
Encrypted messaging (e.g., Wickr, Telegram)	0	1	0	14	1.00
Encrypted phone (e.g., SilentCircle)	0	2	0	13	1.00
Other encryption (e.g., hard drive, cloud)	5	1	0	9	1.00
Password manager	1	0	1	13	1.00
SecureDrop	0	0	1	14	1.00
Tor	2	1	0	12	0.89
VPN	2	1	0	12	1.00

Table 5: **Security tools.** This table lists security technologies discussed by participants. We report on the number who regularly use, have tried but don't regularly use, and haven't tried each tool. We consider use to be "regular" even if it depends on the sensitivity of the source or story, i.e., if the journalist regularly employs that tool when appropriate, even if not in every communication.

Reasons for not using security tools

Usability, reliability, and education

In addition to the well-known usability challenges with many security tools, participant P10 described the difficulty of knowing which tools to trust:

A lot of services out there say they're secure, but having to know which ones are actually audited and approved by security professionals — it takes a lot of work to find that out.

Institutional Support

Though some participants described supportive organizations, 9 of 15 mentioned that they did *not* have anyone to go to for help with computer security issues who was both within their organization and whose role explicitly involved providing technical support of this nature.

Digital Divide

As our participants described, this challenge applies particularly to vulnerable populations, such as low-income communities, abuse victims, homeless people, etc. To take just one example, P12 discussed the digital divide as follows:

Most of the [sensitive sources] I've worked with [are] also people who probably aren't very tech-savvy. Like, entry-level people in prisons, or something like that. So if they were really concerned about communication, I don't quite know what a secure, non-intimidatingly-techy way would be. [...] Some of them don't even necessarily have email addresses.

Functions impeded by security technology

- Anonymous communication may make it difficult for journalists to authenticate sources, or to authenticate themselves to sources
- Using security tools may impede communications with colleagues who don't use or understand them.
- Constraints on communications with sources may reduce the quality of information journalists can get

In order to develop computer security technologies that will be widely adopted by journalists, the computer security community must understand such failures of existing tools. We emphasize that these failures are not merely the result of computer security tools being hard to use (a common culprit [65]) but often arise when a tool did not sufficiently account for functions important in a journalist's process, such as the ability to authenticate sources.

First Contact Problem

The first contact is never or very rarely anonymous or protected. If someone wants to give me some information and we don't already know each other, how would he do it? He could send me an email, yeah, okay—but then how could I be sure it's him? Unless he contacts me with his real identity first. It's very difficult to have the first contact secure.

Recommendations for Security Community

- First contact and authentication
 - Post special sentence on twitter
 - Use tools similar to keybase
- Metadata protection
 - Legally and largely unprotected
- Focus on Sources
 - Who and what is being protected is slightly different than traditional threat models
- Knowledge Management
 - Do not have a clear systemization of good practices
- Understanding the journalistic process
 - Differs from a typical user
- Broader applicability
 - Useful beyond journalists, like lawyers and dissidents

What's going on today with news sites?

Got a confidential news tip?

Do you have the next big story? Want to share it with The New York Times? We offer several ways to get in touch with and provide materials to our journalists. No communication system is completely secure, but these tools can help protect your anonymity. We've outlined each below, but please review any app's terms and instructions as well. Please do not send feedback, story ideas, pitches or press releases through these channels. For more general correspondence visit our [contact](#) page.

WhatsApp

Signal

The free and open source messaging app Signal lets you send encrypted messages, photos and videos. Signal does not collect or store any metadata surrounding your messages to self-destruct on your phone (once it's deleted).

Add us: +1 646-951-1234

[Instructions](#)

Email

You may see that your email is an encrypted document. This makes it easier to send an email you're

concerned about. We do not collect recipient, subject or information about when the email was sent. This metadata will be available to your email provider.

Fingerprint: 44B6 6121 3CE6 66D6 5403 B4CC 44A3 475A E1AA A9EB
Email: tips@nytimes.com

SecureDrop

This encrypted submission system set up by The Times uses the Tor anonymity software to protect your identity, location and the information you send us. We do not ask for or require any identifiable information, nor do we track or log information surrounding our communication.

We strongly recommend that tips be sent using a public Wi-Fi network, and that the computer you use is free of malware. If the computer is compromised, communications using SecureDrop may be compromised as well. The steps below outline best practices for use of SecureDrop, as well as the steps that we take to protect your privacy.

[Details](#)

Confidential Tips

Maximize your data security

The Washington Post offers several ways to securely send information and documents to Post journalists. No system is 100% secure, but these tools attempt to create a more secure environment than that provided by normal communication channels. Please review the fine print before using any of these tools so you can choose the best option for your communication needs.

[See more](#)

Signal

This is a free, end-to-end encrypted messaging app, which allows you to communicate directly with The Post. You can send text messages, images and video. It also allows you to talk securely with a reporter by calling them via the Signal app. No metadata is retained by Signal. It can be downloaded from the app store. Signal can be configured to delete messages automatically at a designated time interval.

The Post's Signal phone number: **202-222-5862**

Download Signal from iTunes

WhatsApp

This is a free messaging app with end-to-end encryption that also allows the transfer of documents, photos and videos. WhatsApp can be used to make secure phone calls. It is owned by Facebook. Some data is retained by WhatsApp.

The Post's WhatsApp phone number: **202-222-5862**

Download WhatsApp

Encrypted Email

If you use PGP encryption, here is our fingerprint and link to our public key. If you use our public key with a mail encryption plugin, for example Mailvelope or Enigmail, this encrypts the contents of your message but not the subject line or the name of the sender.

Fingerprint: **88D9 812E D074 7AEA EA1E C219 DC81 6CC4 FE3D 535C**

Email: **lockbox@washpost.com**

The Post's public key

Maybe this is a usability success story?

- Panama Papers
 - 2TB of leaked documents about private bank accounts in Panama
- Large journalistic collaboration
 - Using privacy preserving tools
 - Keep project secret until publication
- Survey study of 118 participating journalists
- Semi structured interviews with the designers and implementers of the technical systems

USENIX Security 2017

When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers

Susan E. McGregor
Columbia Journalism School

Elizabeth Anne Watkins
Columbia University

Mahdi Nasrullah Al-Ameen
Clemson University

Kelly Caine
Clemson University

Franziska Roesner
University of Washington

Abstract

Success stories in usable security are rare. In this paper, however, we examine one notable security success: the year-long collaborative investigation of more than two terabytes of leaked documents during the “Panama Papers” project. During this effort, a large, diverse group of globally-distributed journalists met and maintained critical security goals—including protecting the source of the leaked documents and preserving the secrecy of the project until the desired launch date—all while hundreds of journalists collaborated remotely on a near-daily basis.

Through survey data from 118 participating journalists, as well as in-depth, semi-structured interviews with

Mexico, Pakistan, and others [42].

Facilitated by the International Consortium of Investigative Journalists (ICIJ), the Panama Papers project [31] represents a uniquely positive security case study, wherein systems designed, implemented, and managed by a handful of ICIJ staffers helped meet and maintain the organization’s security goals for the project. While it is impossible to state definitively that this (or any) system could *not* have been compromised, ICIJ’s efforts appear to have been successful in maintaining their primary security goals, including: (1) protecting the identity of the source of the Panama Papers’ documents (2) maintaining control of the documents within

Built/Refined Special Tools for Journalists

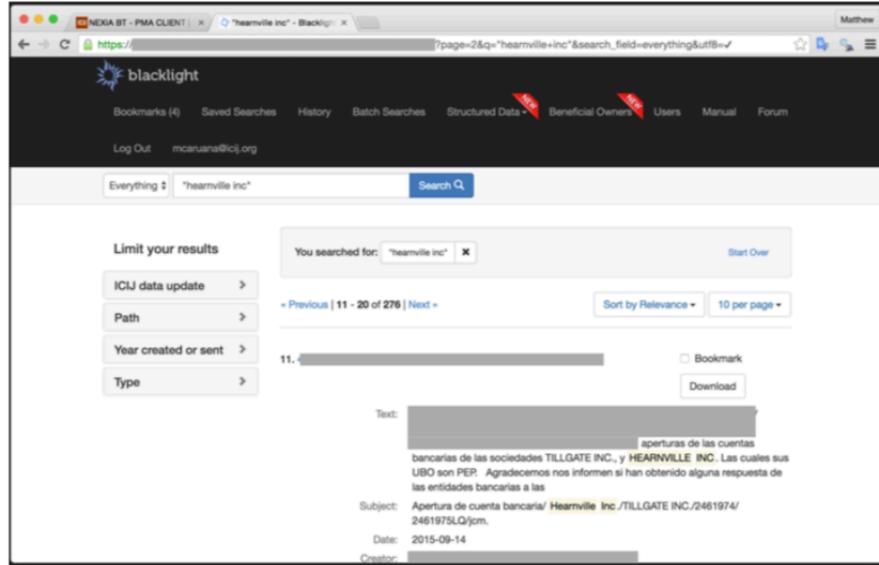


Figure 1: **Blacklight**. Screenshot of the document search platform. *Courtesy: ICIJ.*

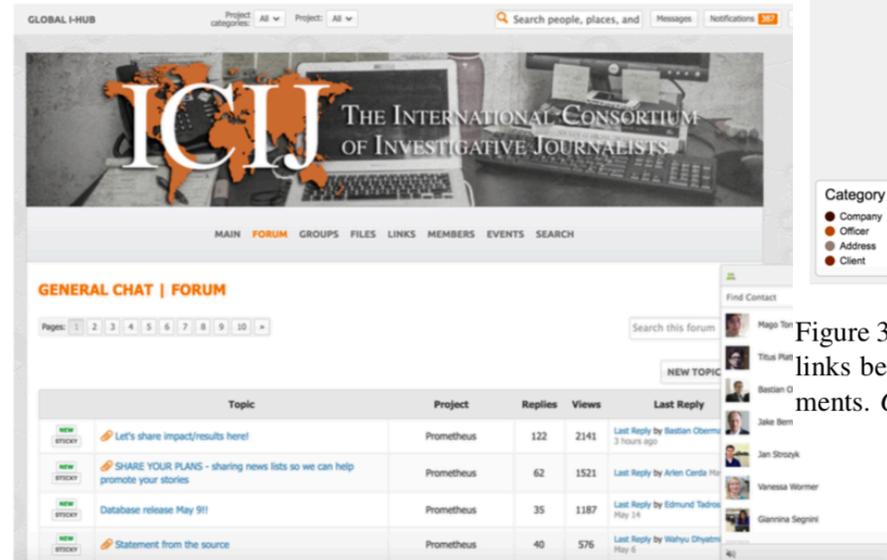


Figure 2: **I-Hub**. Screenshot of the collaboration and communication platform. *Courtesy: ICIJ.*

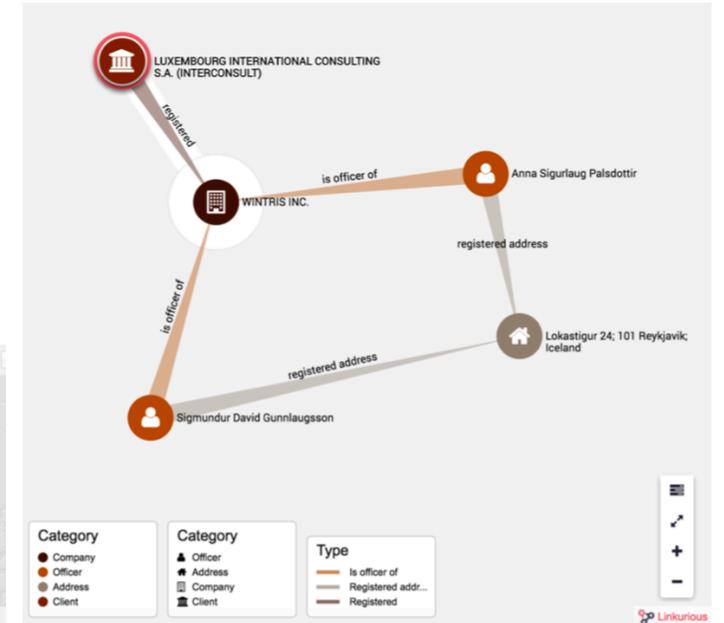


Figure 3: **Linkurious**. Screenshot of the system that visualizes links between entities mentioned in the Panama Papers documents. *Courtesy: ICIJ.*

Prior Security Experience/Practices

Are these surprising?

Security Practice	Unaware	Never	Few	Occasionally	Frequently
Passphrase	9%	21%	13%	15%	52%
Two-factor	16%	29%	14%	13%	42%
PGP	14%	34%	10%	17%	25%

High or low?

Table 1: **Familiarity with and Usage of Security Practices Prior to Project (N=118)**. Scale items were “Never heard of it before” (Unaware); “Knew about it, hadn’t used” (Never); “Had used a few times” (Few); “Used occasionally” (Occasionally) and; “Used frequently” (Frequently).

Feedback about security

The Google Authenticator [sic] tool... when I changed my phone (twice during the investigation) I had to communicate with the support team to reboot the passwords. (J118)

At certain times security turned into a barrier into getting more done... Every time a cellphone died or went missing (frequently) I needed to reconfigure authentication. (J68)

This is sensitive data that has been leaked to ICIJ for a reason, and that those sources are trusting us with being... guardians of that information and protectors. So it's not for us to give away to anybody, not even a trusted colleague. (E2)

Making Security Required

It was not a choice... If somebody did not get themselves a PGP, he did not get access to the forum and to the I-Hub. (E1)

We had a rule in our team that whatever is about the Panama Papers—and if it's only about, I don't know, "Let's meet at nine, okay?" then we encrypt it because we encrypt everything that has to do with the Panama Papers. So that was our rule... the automatic step was to encrypt. (E1)

Good or a bad thing?

What made this successful?

- Useful and necessary system functionality
 - Journalists had to use security and also had to use the systems to do their jobs
- Normalizing and sustained emphasis on Security
 - Security practice was the norm, everyone used it, so not using it would be ineffective
- Multiple forms of secure communication
 - Not just pgp, but also secure messengers like Signal
- Mutual respect and reciprocity through relationships built on trust
 - Journalists respected work of developers in building in security
 - Developers respect the work of journalists

Discussion

- How do we compare the Panama papers article to the prior article?
- What other factors do you think made this such a success?
 - Why might this have worked better than other settings?
- Can these successes be replicated in other settings?
 - What about at a university setting?

What we did today!

- Vulnerable populations
 - Journalists
 - Undocumented Immigrants
 - Victims of intimate partner abuse

What's next?

- Vulnerable populations
 - Journalists
 - Undocumented Immigrants
 - Victims of intimate partner abuse