

FREEDOM = OF THE PRESS = FOUNDATION

Home About Organizations Blog WikiLeaks Encryption
SecureDrop



SecureDrop is an open-source whistleblower submission system that media organizations can install to securely accept documents from anonymous sources. It was originally coded by the late Aaron Swartz and is now managed by Freedom of the Press Foundation. For more information, you can go [here](#).

Organization	Landing Page	Tor Hidden Service Address
BalkanLeaks	https://www.balkanleaks.eu	vchcskzthbw6l4ba.onion
ExposeFacts	https://exposefacts.org	znig4bc5rlwyj4mz.onion
Gawker Media	https://gawkermediagroup.com/securedrop	gawker5oxtsc6fa7.onion
The Globe and Mail	https://sec.theglobeandmail.com/securedrop	n572ltk4nld3bsz.onion
Greenpeace New Zealand	https://www.safesource.org.nz	vtjkwwcq5osuo6uq.onion

[Privacy Policy](#) Follow on Twitter: [@FreedomofPress](#)

Like our Facebook page [Google+](#)

The Guardian	https://securedrop.theguardian.com	33y6fjyhs3phzfjj.onion
The Intercept	https://firstlook.org/theintercept/securedrop	y6xjgkgwj47us5ca.onion
NEOSleaks	https://neos.eu/leaks/	udrciwei14qe63p.onion
The New Yorker	https://projects.newyorker.com/strongbox	strngbxhwyuu37a3.onion
NRKbeta	https://nrkbeta.no/tips	swdi5ymnwmrqhycl.onio
Project On Gov't Oversight (POGO)	https://securedrop.pogo.org	dqeamlf3jld2kz.onion
ProPublica	https://securedrop.propublica.org	pubdrop4dw6rk3aq.onior
Radio24syv	https://securedrop.radio24syv.dk	hpjw636qnt5avq62.onior
BayLeaks	https://bayleaks.com	wd5x5eexdqjrqfa.onion
Barton Gellman	https://tcfmailvault.info	v6gdwmm7ed4oifvd.onio
The Washington Post	https://www.washingtonpost.com/wp-stat/securedrop/securedrop.html	vbmwh445kf3fs2v4.onior
Wired's Kevin Poulsen	https://freedom.press/about/tech/kevin-poulsen	poulsensqiv6ocq4.onion

Last updated Thu Jul 9 11:58:30 AM PST 2015

This list is available as a [tab-delimited text file](#) with a [signature](#) from [SecureDrop's public key](#).

How to verify the integrity of this
information using GPG

Maintained by [Kevin](#).

TRENDING ?????????? ?? ????? ??? ?? ??????? 16 ?????. ??.

BalkanLeaks

HOME DECENTRALIZED INFRASTRUCTURE FOR WIKILEAKS ANONYMITY

BIG LEAKS  TIMELINE 

Wanna leak? Open this link in TOR browser <http://vchcskzthbw6l4ba.onion>

Don't forget to keep your [Tor Browser Bundl?](#) updated!

[\[bulgarian cyr\]](#) [\[serbian cyr\]](#) [\[serbian lat\]](#) [\[macedonian cyr\]](#)

Dear friends,

Following the example of the whistleblowers site Wikileaks we opened this site to promote transparency and fight the nexus of organized crime and political corruption in the Balkan states.

We are deeply convinced that we're not alone in this battle. There are plenty of people out there that want to change the Balkans for good and are ready to take on the challenge. We're offering them a hand.

If you have any confidential documents related to political, criminal or financial topics and you want to share them with the press in a [secure, anonymous way](#), you can use our secured and encrypted upload server. We will review the

Search

Search

RECE



documents and publish them after checking the information.

To submit just follow those simple steps:

1. Download and install the **Tor Browser Bundle** for your system.
2. Launch the Tor browser and connect to our BalkanDrop, tor enabled server: <http://vchcskzthbw6l4ba.onion>
3. Wait! Tor is secure, but slow 😞 If it really takes too long to join the page reload the tor browser.
4. Upload the files and disconnect.

Tor is working in such a way that nobody, including the administrators of the site can't guess who is the real submitter.

Tor offers a pretty high level of security and anonymity, but if you wish to do even better follow the recommendation:

- do not use your home or work internet connection for submitting;
- use a public, password free WiFi point;
- if possible, use a VPN connection to a server outside your home country.

Please, respect the following requirements for your uploads:

- Upload only documents which are either:
 - not available in the public space or
 - are in the public space but reveal data not known from previous journalistic investigations.
- Please, join a short description of your uploads;
- Name and number the documents in a comprehensive way;
- Do not upload opinions and allegations without document proofs.

Please, prefer the PDF format.

Thank you for your contribution.

The Balkan Leaks team

—BEGIN PGP PUBLIC KEY BLOCK—

Version: GnuPG v1.4.12 (GNU/Linux)

mQINBFHhFbcBEADZPI6mPRTyYKe4An6/iRH34qPjkHkvBxbmi1Yf2sxxhAJAITAJ0

SZJX5l1Vs42yevXpldyFLsydhZE9kwgEMbYy48nyiE/Kmht4VSnGXYSvxxPVAI6+
5cANIRkXRLwa2ETJIFbd2MNE724fHc1HI2VUTRUsym7z75/3RexNv/nVtj8FmTJL
bOH0bmbbVF1tsqNITx3N4ZR++9cLqqvCOzMiOoTeN6eCcRnhsu+sm1u6/G5pZLq4
m4TwyoP4Gc2e/QECfJ2oQMqW9clyk71HIJUkrwK4EIEZoAAH5unOndhRRO3pTU4q
buHPaLLIbDBov4s9/02Qfyqs68xrX+yBR99buz4FBTPhC7L01a6MMIqDRmLSa4OO
TTWSY0++YfopPx5c1oxOCnV4UtB9tfbKhbbBRv5GjToIS5dWC2uEnJ7doNofiGMn
rdHfANEY1oWMtZzAD1vmFBTDDa+CkFz+S/b9R+zk1OHetLU5KZgAK7yZnb1a0ves
V1/AconzslmPrtJmfog4bVXXrcIzj0jofsaSUiBQcWcJ346wfwU6Wb5Qi8Vlai4
SxO26E0O9HG+kmb97rXA2dzp1/da6sylKWlBv3WtOjt8F3/GVQB2kJwlwoBtEH6+
4NKMfKwwzIbCunN7mTuMsPI5FaoXqKU3VDnpvC+Dc7fz1xPVcRP5crdB6wARAQAB
tDtCYWxrYW5MZWFrcyAoU2VjdXJlIGNvbW11bmljYXRpb24pIDxjb250YWN0QGJh
bGthbmxlYWtzLmV1PokCOAQTAAQIAIgcUUCUeEVtwlBawYLCQgHAwIGFQgCCQoLBBYC
AwECHgECF4AACgkQO45/5ynkOIVqZxAakz5piTHRYG/O+o+Qw55OgUqfSk5hluKY
XUmZCivtySG3mFfvlwjEtCMnbZQ+SbLqwS/QP6d1odp1oOEVeCIROODczF+wcRoF
ipRmtlKL8pj7rl1s/Vgkh34tFOINvuy86G9tNPZoNGB2xHosQ+KDsxEIN23TLhuL
Dv5xjXpvppozQ3udY5OaZDtk83pt0Lt10VpShTaL8vE5cKpx3YbrqcxSN6rRSV1A
KM7v5wr+M80P3pr8QGnqaY/7bjiKIWIHh6GNDdYNERQ8ebL/t8t00ZtnLvwnZuU
E3slWx4WL0pAK7tCIUZ9gmoNvQJ8Jdt5TpbP42wWbFRd0QLZgNTdMM9I+oRlJPmz
ZS50C1ClicoaSy59r9Au1tpJ4f6ZPByZDucXaOsFq6u3yw4TyjCM1uUQykGwm4kg

41kcXmv2tMuvioFWuN0ZxejgqoILKucfTOWvCNmo5PX4oPMT0GuniyCJjJDP1KzE
lsD6bKUeBAU7QRv3kthHj74Insu2GJZkAK3cWjTDSY3nRTcdg8DbybGzDQBN0z9V
CUhxjzb7+wK8/pU2ff/VZbdf0MYeEjRzVf5ib3vmrcc3zDTZaDx8nWllf7eHGE3w
lO4C8zG4Wks/fogk+4gb+7npAZGrkesNwsqPo8mL9mipZxcM2N1bcm1apdtGk/Q4
ouyqpZmZ3Qy5Ag0EUeEVtwEQAMZDRJWfG7Iff7yWwwlhmdn9tctvpoXPoR0bsrZk
80cXnE63vg8wk7AeP2G4NAoJVtVL6xi8D188mCMEEu+kIWJq7H7O0etusq9cCoQp
NvuMLaDA8GuVHt5fBb14KmC/NxE9zIbpafy6bbGoNRpHihgXnhQ19y6Ao4GeaQMn
T3DVOSwAgsvC9khvuXQAR7ARsx5Jz4A2OnKpLSG90D3Mvyhod9cSaUISrq8FHACK
1vTINN6pSOAYM+x2HwPnyUAWSZi/vID9MUaYtuPUepvFseRqPoL5Ebewl3hX+Asc
wB1TYVEcY6dK35nOKR36mvYIJzhMC7LuMB5WVFIixULRyLyX5EvYi/ubRi1bIVXy
FYoiWmxkocwc7+w+bujB/xtUxCbGBGs0hpuRPILxW4FqL+3LN4NoMIOwNs1A3rk6
M7OWXqRbb7EjiuQ0ehl9Ejp/SmuHTYhbM7LpmxxzaOj+nk99CYjw8MxEUJYNVn
lk+WkrXLGUnNhP+QEgQL+wGMNrqGm46eRRBcJfghamXWysWLSL0Ghkk7Hh2jMN2r
bpntfbkva+0tvUWXpDLgl/iuadesVcPgz8oUtt5nVVukoOgCwN/bSRIKuEKzHMf7
5pVnmfKZOKnAgXjLv6+IO5yHVSoNzr5Z+I3jpAK4TLUnWPaLuqvwKXegqI4Yo5n7
Lh03ABEBAAGJA8EGAECAAKFAIHhFbcGwwACgkQO45/5ynkOIXxaw/7BeX4/1rn
JhNUzkljENYCa8PJUNHL0wsrVcbmshiSJgmm2d0Aj5qazjgGrnlabF+gB3L4pLF7
6aqJHnDrXQ/5Aj7vnPS6uV/1NLLzJPpTn68KaDJKXzARdabPh/qyvuArDskf5dNX
JJDcbIHRw/279vmG8BrdGYynUAfleKxD4K1qEgL4mRrvt2rXdLyNOk59bIXnJKNG
8F58gqidGtyff0d2Q7X433h9NQzJBBIW9BoYO4rnvpZxGvf8qYNvu7g6dYwiUC6U
ryupmnkM9GAoPxAyz/Z6o8JfRDVOgw/jaQ9+t+mDrYNd0aKJEKMNZvpVoJ8ekVtT
YBJZL6bNy+JU880XF5RdwktilFNvkGa+YRf2GxdX6brKBjWDBwGvrcMt4yoEPLaU
ICQ54ieZXvqNEvKW8VmtZXKSzytfV+thKyh/f70dixNm+PsWNbk4Ny9b2IQWU/j2
jTy2z9TqUc8RzkafF0egp7C2HH04SpkZshl8mZ09W8clFXRCa4QewyQicVaGWv5/
eQT97+1/QNWwFczetEOH0FZVmjD/7+1xJxmHAw0PQc7XaW0OiezYrzJX404ZYcth
+87RRjOy2cozYRSRf1YlufQIEKZiHkNmDBS/tW06aQWFeuOjF3PLTqB+M7pOpIEU
Kyk3UoqC8CInW0zBZ5G0ZldCK5ys4kbJ4Qs=
=ByQY
—END PGP PUBLIC KEY BLOCK—

????????????,?

????????? ?????? ?? ?????? ?? ?????????? ?? ?????????? ??? ??? Wikileaks, ???
????????? ? ????, ?? ?? ?????? ? ?????????????? ? ?? ?? ?? ?????? ????? ? ??????????????
????????????? ? ?????????????? ?????????? ?? ??????????.

?? ?? ? ?????????? ?????????, ?? ?? ?? ? ??? ? ?????? ??????. ? ? ? ???? ???? , ????? ? ? ?????
?? ?????? ? ?????????????????????????? ? ?? ?????? ????? ?????????? ?????????? . ? ????????? ? ??
???? ?? .

?? ?? ??? ????????? ? ?? ? ?????, ?????????????? ??? ????????????? ? ?????? ???? , ????????? ?
????????????, ?????????????????? ??? ? ????????? ? ?? ?????? ? ????????? ?? ? ?????????? ?
????????? ?? ?????????, ?????????? ???? , ?????????????? ??? ??? ?????????? ? ????????????? ??????
?? ? ? ???? ????? ? ?????? ?????? ? ? ? ? ? ????????????? ? ?????? ?????????? ?? ??????????????????
??.

?? ?? ????????????? ? ?????????? ????????????? ????? ????????? ?????????:

- 1. ????????? ? ????????????????? **Tor Browser Bundle** ?? ??? ??? ????????????????? ????????? ?.
- 2. ??? ????? Tor ?????????? ? ?? ?????? ??? ? ????? ?????: <http://vchcskzthbw6l4ba.onion>
- 3. ?????????! ??? ? ?????????, ?? ????? ???? ????????????????? ?????? ? ????????? ? ???? ???? ?
????? ????? ? ????? ????? ???? tor ??????????.
- 4. ????????? ? ?????????? ? ?????? ????? ? ? ?????? ?????.

??? ??????? ? ? ?????, ????? ? ? ????????????? ? ? ?????, ????? ? ? ? ? ????????????????????? ? ? ?????
?? ?????????? ?????????????? ??? ?????????? ?? ??????????

Tor ????????????? ????????????? ?????? ????? ? ? ?????????? ? ????????? ?????, ?? ??? ? ????????? ? ? ?

??-????? ?? ???? ?????????? ???? ?????????? :

- ?? ????????????? ???? ?? ???? ?? ???? ?????????? ?? ?????????? ??????, ?? ?? ?????? ?? ? ??????;
- ????????????? ???? ????????? WiFi ?????? ?? ? ?????????? ??? ??????;
- ?? ???? ?? ???? ?????????????? VPN ?????? ?? ? ?????? ?????? ?? ???? ??????.

? ???, ?????????? ?????????? ?????????? ?? ?????????? ?????? ?????:

- ?????????? ?????????????? ?????? ?????, ??????:
 - ?? ?? ?????????? ?????????? ???
 - ?????????? ??????, ?????? ?? ?? ?????????? ?? ??????? ?? ? ?????????????????? ??????????
- ? ???, ?????????????? ?????? ?????? ? ?????? ?????????? ? ????????? ? ???;
- ? ?????????? ?????????????? ? ? ??? ?????????? ?????? ??????;
- ? ? ?????????? ? ?????? ? ??????????, ?????? ?? ?? ?????????????? ? ?????? ?????;

? ???, ????????????????? PDF ? ??? ???.

???????????? ?? ?? ?????????????????????.

?????? ?? Balkan Leaks

????? ????????? ?,

???????? ???? ?? ???? ???? ?????????? ? ???? ?? ???? ????? Wikileaks, ?????????? ?? ? ?????? ???? ? ?????????? ? ?????????????????????? ? ?????? ????????? ?????????????????????? ????? ?????? ? ????????? ?????????? ? ??? ? ?? ? ?????????.

???????? ???? ? ?????????? ?? ? ?????????? ?????? ???? ? ? ??????? ? ???? ? ??? ???? ? ??? ???? ???? ??

- **???? ??????????, ??? ?????????? ?????????? ??? ?????????? ?? ?????????????? ??? ?????????????? ?;**

- **???? ??? ?????????? ????? ?????? ?????? ??? ?????????? ???;**
- **?? ?????? ? ??? ?????? ??? ?????? ????? ?? ?????? ? ?? ??????;**
- **??? ??? ?????????? ??? ? ?? ? ? ?????? ? ??? ?????? ?????????? ??? ?????? ?????????????? ?????**

? ????? ? ??? ?? ?????? ????? ?????????? ??? ?????????????? ? PDF ? ??? ???.

?????? ??? ? ??? ?? ?? ??????? ?.

Balkan Leaks ???

Dragi prijatelji,

Prateci primer sajta za otkrivanje tajnih informacija Wikileaks, otvorili smo ovaj sajt u cilju pod transparentnosti i borbe protiv organizovanog kriminala i politicke korupcije u zemljama Balka

Duboko smo uvereni da u ovoj bici nismo sami. Postoji mnogo ljudi koji žele trajno da promer spremni su da odgovore na izazov. Mi im nudimo pomoc.

Ako imate ikakve poverljive dokumente u vezi sa politickim, kriminalnim ili finansijskim temar ih podelite sa medijima na bezbedan, anoniman nacin, možete koristiti naš obezbeden i šifrov otpremanje. Mi cemo ih pregledati i objaviti kada proverimo informacije koje dokumenti sadrže

Da biste objavili dokumente, sledite ove jednostavne korake:

1. Preuzmite i instalirajte **Tor Browser Bundle** za vaš operativni sistem.
2. Pokrenite pregledac Tor i povežite se sa našim serverom omogucenim za tor na sledecoj <http://vchcskzthbw6l4ba.onion>

3. Sacekajte! Tor je bezbedan, ali spor Ako otvaranje stranice potraje predugo, isključite pokrenite pregledac.
4. Otpremite datoteke i prekinite vezu.

Tor funkcioniše na takav način da niko, uključujući i administratore sajta, ne može da sazna p osobe koja je otpremila dokumente.

Tor nudi veoma visok nivo bezbednosti i anonimnosti, ali ako želite dodatno da se zaštitite, sle preporuke:

- za otpremanje nemojte koristiti kućnu ili poslovnu Internet vezu;
- koristite javnu WiFi pristupnu tačku bez lozinke;
- ukoliko je moguće, koristite VPN vezu sa serverom izvan vaše matične zemlje.

Molimo vas da prilikom otpremanja poštujuete sledece zahteve:

- Otpremajte samo dokumente koji:
 - nisu javno dostupni ili
 - jesu javno dostupni, ali otkrivaju podatke koji nisu poznati iz prethodnih žurnalisticki
- pružite kratak opis dokumenata koje otpremate;
- imenujte i numerišite dokumente na razumljiv način;
- nemojte iznositi mišljenja i tvrdnje koje nisu potkrepljene dokumentovanim dokazima.

Molimo vas da dokumente otpremate prvenstveno u PDF formatu.

Zahvaljujemo vam se na saradnji.

Balkan Leaks tim

[home](#) [about](#) [blogs](#) [editorial board](#) [advisory board](#) [donate](#)

ExposeFacts: For Whistleblowing, Journalism & Democracy

BLOG

RIGHT TO KNOW

By Marcy Wheeler

ExposeFacts Investigative Journalist



In Political Press, Hillary Clinton Gets Subjected to the Thomas Drake and Jeffrey Sterling Standard

The political press is attacking Hillary Clinton using the same standards of retroactive classification DOJ used against whistleblowers Thomas Drake and Jeffrey Sterling.

ANALYSIS

Below the surface: what's happening and why it matters.

Assessing the Candidates: Obama's Whistleblower War Leaves Dangerous Legacy for Future Presidents

Here's the thing about President Obama's war on whistleblowers: In bringing espionage charges in nine cases involving disclosures or alleged misuse of classified information, the current administration has set a floor, rather than a ceiling, on the number and types of whistleblower espionage cases a future President can bring. And here's another thing: With leaders [\[Read More...\]](#)

SPECIAL COVERAGE

Reporting on the Jeffrey Sterling trial and the CIA's Operation Merlin

The trial of Jeffrey Sterling is over, but the in-depth coverage from ExposeFacts is illuminating some of its hidden realities and long-term implications.



CIA Mission: Destroy the Whistleblower and Perfume the Stench of 'Operation Merlin'

The leak trial of CIA officer Jeffrey Sterling never got near a smoking gun, but the entire circumstantial case was a smokescreen. Prosecutors were hell-bent on torching the defendant to vindicate Operation Merlin, nine years after a book by James Risen reported that it “may have been one of the most reckless operations in the [\[Read More...\]](#)



Watch Pentagon Papers whistleblower Daniel Ellsberg explain the importance of ExposeFacts

For Whistleblowing, Journalism & Democracy

Launched by the Institute for Public Accuracy in June 2014, ExposeFacts.org represents a new approach for encouraging whistleblowers to disclose information that citizens need to make truly informed decisions in a democracy. From the outset, our message is clear: “Whistleblowers Welcome at ExposeFacts.org.”

ExposeFacts aims to shed light on concealed activities that are relevant to human rights, corporate malfeasance, the environment, civil liberties and war. At a time when key provisions of the First, Fourth and Fifth Amendments are under assault, we are standing up for a free press, privacy, transparency and due process as we seek to reveal official information—whether governmental or corporate—that the public has a right to know.

SUBMISSION & ANALYSIS PROCESS



While no software can provide an ironclad guarantee of confidentiality, ExposeFacts—assisted by the [Freedom of the Press Foundation](#) and its “[SecureDrop](#)” whistleblower submission



system—is utilizing the latest technology on behalf of anonymity for anyone submitting materials via the ExposeFacts.org website.

As journalists we are committed to the goal of protecting the identity of every source who wishes to remain anonymous.

The seasoned editorial board of ExposeFacts will be assessing all the submitted material and, when deemed appropriate, will arrange for journalistic release of information.

In exercising its judgment, the editorial board is able to call on the expertise of the [ExposeFacts advisory board](#), which includes more than 40 journalists, whistleblowers, former U.S. government officials and others with wide-ranging expertise.

We are proud that Pentagon Papers whistleblower Daniel Ellsberg was the first person to become a member of the ExposeFacts advisory board.

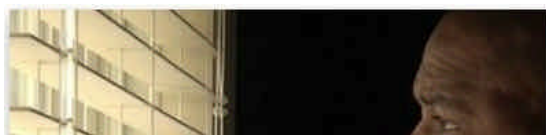
The [SecureDrop](#) implementation for ExposeFacts overseen by the Freedom of the Press Foundation **is only accessible using the [Tor](#) browser**. As the Freedom of the Press Foundation notes, no one can guarantee 100 percent security, but this provides a “significantly more secure environment for sources to get information than exists through normal digital channels, but there are always risks.” ExposeFacts follows all guidelines as recommended by Freedom of the Press Foundation, and whistleblowers should too; the SecureDrop onion URL should only be accessed with the Tor browser — and, for added security, be running the [Tails](#) operating system. Whistleblowers should not log-in to SecureDrop from a home or office Internet connection, but rather from public wifi, preferably one you do not frequent. Whistleblowers should keep to a minimum interacting with whistleblowing-related websites unless they are using such secure software.

Copy and paste this URL into the Tor Browser to access SecureDrop:

<http://znig4bc5rlwyj4mz.onion>

A black and white poster for ExposeFacts.org. On the left is a portrait of Daniel Ellsberg. To the right, green text reads: "DON'T DO WHAT I DID. DON'T WAIT UNTIL A NEW WAR HAS STARTED. DON'T WAIT UNTIL THOUSANDS MORE HAVE DIED. BEFORE YOU TELL THE TRUTH WITH DOCUMENTS THAT REVEAL LIES OR CRIMES OR INTERNAL PROJECTIONS OF COSTS AND DANGERS. YOU MIGHT SAVE A WAR'S WORTH OF LIVES." Below this is the name "DANIEL ELLSBERG". At the bottom right is the ExposeFacts.org logo and the text "ExposeFacts.org whistleblowers welcome". A small caption below the portrait reads: "Daniel Ellsberg revealed the top secret Pentagon Papers in 1971. He is now a member of the ExposeFacts advisory board." The logo for "RootsAction" is visible in the bottom left corner of the poster.

VIDEO



Welcome to the Gawker Media SecureDrop

We want you to leak us things. Sometimes an email will suffice, or a call to our tips line, or even an anonymous comment on a post. But sometimes sources want to contact us without leaving a digital trail.

SecureDrop is designed to help you do just that. It is a way for you to send us things—messages, tips, files, documents—while maximizing your anonymity and frustrating any attempts (including by us) to identify you as the source.

For details on how SecureDrop protects your anonymity, please see our privacy terms below. And for other secure ways to reach us, including encrypted email, encrypted chats, and snail mail, please go [here](#).

To use SecureDrop:

1. Download and install the [Tor Browser Bundle](#). This will permit you to visit the SecureDrop connection page, which operates as a Tor "hidden service" and is not accessible via standard internet browsers. We recommend that you not download, install, or use Tor from your office or any network that might be monitored that you are known to use. Instead, go to a coffee shop or some other public, open network.
2. Open the Tor browser and paste this URL into the address bar:
gawker5oxtsc6fa7.onion
3. Follow the instructions you find there to send us messages, receive our replies, and upload files.

How SecureDrop Works

Created by [Aaron Swartz](#) and developed by the [Freedom of the Press Foundation](#), SecureDrop employs rigorous security protocols and makes use of the Tor network to establish a communications channel that is hardened against interception or subsequent leak investigations. Your messages will be encrypted and read on a machine that is not connected to the internet. Gawker Media's SecureDrop will not record or retain your IP address or any information about your browser or your visit, nor will it place

any persistent cookies or third-party trackers on your machine. And the use of the Tor's anonymizing software makes it extremely difficult for anyone to prove or even suspect that you used SecureDrop.

Please read our privacy terms carefully. It explains what type of information SecureDrop does and does not collect, and why.

Gawker Media SecureDrop Privacy Terms

- We don't ask or require you to provide any personally identifying information when you submit materials through SecureDrop.
- The system does not record your IP address, information about your browser, computer, or operating system. Furthermore, the SecureDrop pages do not embed third-party content or deliver persistent cookies to your browser.
- The server will only store the date and time of the newest message sent from each source. Once you send a new message, the time and date of your previous message is automatically deleted.
- Reporters decrypt and read each message on a machine that has never been connected to the internet, and will delete messages from the server on a regular basis. The date and time of any message will be securely deleted from the server when the message is deleted.
- Please keep in mind that the actual messages you send and receive through SecureDrop may include personally identifying information. For this reason, once you read a reporter's message, we recommend you delete it. It will then be securely deleted from the file system.

Also please note that when you submit certain types of files through SecureDrop, you may inadvertently be sending us metadata associated with that file.

For example, if you submit a photo through SecureDrop in JPEG format, the file may include information about the date, time, and the GPS location of where it was taken, and the type of device used to take the photo. Similarly, if you submit a Word file (.doc or .docx), it may include the identity of the document's author, the author's operating system, GPS data about the author's location, and the date and time when the document was created.

Our policy is to scrub metadata from the files we receive through SecureDrop before publication. If you don't want to send us metadata, please use the [Metadata Anonymization Toolkit](#) to scrub the file before you submit it.

Collection of Information About Reporters' Use of SecureDrop

Gawker Media collects information about our own reporters' use of SecureDrop for security monitoring and to make sure the system works properly.

This information includes details about the device, browser, and operating system Gawker Media staffers use when accessing the system, and the date and time of each session.

We retain these access logs for 7 days, and then delete them.

Data Security

Gawker Media works diligently to protect the identities of our sources and keep the information they give us confidential.

SecureDrop servers are under the physical control of Gawker Media and are isolated from our network infrastructure.

However, no one can guarantee 100 percent security of any system against all adversaries. Like all software, SecureDrop may contain bugs. Ultimately, you use the SecureDrop service at your own risk.

Changes to This Policy

We may revise these privacy terms from time to time. The most current version of the policy will govern our collection and use of personal information and will always be published on this page. If we make changes that we believe are material, we will prominently display a notice on our site before we make those changes.

Contact

Gawker Media welcomes questions, concerns, and feedback about this policy. If you have suggestions for us, feel free to let us know at tips@gawker.com. If you work for a media organization and are interested in installing SecureDrop, please contact the [Freedom of the Press Foundation](#).

SecureDrop at The Globe and Mail

What is it?

The Globe and Mail's SecureDrop service provides a way to share information with our journalists with more security and anonymity than traditional means. The software comes from the **Freedom of the Press Foundation**, who have worked with **other news organizations** to provide a safer way for sources to talk to reporters.



Before getting started

To reduce the probability that a third party, such as your employer or a government agency, can tell that you're using SecureDrop, you should connect to it from a network that you don't normally use, such as a public wifi network at a cafe that you've never visited before.

You should also use a computer that you control, because a laptop issued to you by your employer may contain monitoring software that captures keystrokes or tracks the sites that you visit.

I'm at a coffee shop with my computer, now what?

1. Once you are connected to a network that you don't normally use, download and install [the Tor Browser](#) – this provides an anonymous way to use to access the service

2. Once you have installed the Tor Browser, open the browser and enter this address in the address bar:

3. Once you are on the website, you will be provided to upload files and leave messages

You will be asked to enter a code phrase as part of the process. If you want to use the service later, you will need to use this code phrase. Ideally, you should not write it down. In any event, keep it safe. You should not contact our journalists in connection with your SecureDrop uploads through any other method, such via social media or email.

SecureDrop provides an anonymous connection to The Globe and Mail, and securely encrypts any files you upload to the service. However, it cannot protect the original files on your own computer, or prevent your computer from being compromised by malware. For added security we recommend using [Tails](#), an operating system that loads from a USB stick and wipes any trace of its use when you shut down your computer. You should also consider encrypting sensitive files on your computer.

How does SecureDrop work?

SecureDrop uses the Tor network to anonymize your interactions with us. It provides a Tor hidden service, hosted on computers isolated from our main internal network and under our physical control. Files and messages uploaded to this service are encrypted using PGP, and can only be decrypted by our journalists on a dedicated air-gapped decryption station also under The Globe and Mail's control.

Files and messages may be uploaded for the attention of any of our

journalists, but only a small number of senior investigative reporters have access to the SecureDrop station. After uploads have been decrypted, they are sent securely to the intended journalist, who will treat the information as sensitive data.

When I have as a source if I use SecureDrop

The SecureDrop system does not log any of your interactions with the SecureDrop system, including your visit to this page. It installs no tracking cookies or tracking software of any kind on your computer as part of the process. Your identity is not exposed to us during the upload process, and we do not know your unique code phrase. This means that even if a code phrase is compromised, we cannot comply with demands to provide documents that were uploaded by a source with that code phrase. SecureDrop itself is an open-source project that is subject to regular security audits, reducing the risk of bugs that could compromise your information.

Information provided through SecureDrop is handled appropriately by our journalists. Journalists working with uploaded files are required to use only computers with encrypted hard drives and follow security best practices. Anonymous sources are a critical element of journalism, and The Globe and Mail has always protected its sources to the best of its abilities. In most circumstances, there will be no need to require any information from you. However, there may be times when a Globe and Mail journalist might seek your permission to meet before certain information is published. The use of anonymous sources is governed by our [Editorial Code of Conduct](#).

No form of communication, electronic or otherwise, can be made 100%

secure. Correct use of the SecureDrop service, along with appropriate security practices on your own computer, will provide you with a great deal of security beyond traditional methods. As with all other methods, there are steps we can take to protect you as a source, but u



The Globe and Mail Inc. All Rights Reserved.

444 Front St. W., Toronto, ON Canada M5V 2S9

Phillip Crawley, Publisher



SAFESOURCE

A SECURE, SAFE WAY TO SHARE THE TRUTH



THE SAFESOURCE PROJECT

**READ
MORE**



**WHY SAFESOURCE IS
NECESSARY**

READ

MORE



SAFESOURCE SECURITY

READ
MORE



FREQUENTLY ASKED QUESTIONS

READ
MORE

TO USE SAFESOURCE, JUST FOLLOW THESE TWO STEPS:

1. Download and install Tor Browser from: torproject.org
This should only take a few minutes.
2. Open your Tor Browser, type the SafeSource SecureDrop URL below in the address bar and hit enter (return):

<http://vtjkwqcq5osuo6uq.onion>

3. You will then find further instructions on how to submit files and messages to Greenpeace. You will be assigned a randomly generated and unique code name.

If a staff member at Greenpeace (referred to within as a journalist) wants to contact you about the information you have submitted, he or she will leave a message for you in the SafeSource SecureDrop.

These messages are the only way we will be able to reach you, and this message can only be accessed using your code name.

NOTE: The SafeSource SecureDrop servers are pro-actively maintained and security patches are strictly applied. This means that the servers be temporarily unavailable for up to 60mins any day of the week from 9-930am. Please avoid using the service during this period.

DISCLAIMER

You should be aware that depending on your situation and

national law, there could be legal consequences if you
share information with us.

© GREENPEACE 2014 || PRIVATE BAG 92507, WELLESLEY STREET,
AUCKLAND, NEW ZEALAND || PHONE 09-630-6317

theguardian



A way of sharing stories with us Securely & Confidentially

A way of sharing stories with us securely and confidentially outside of traditional email.

You can of course use postal services but for sensitive information this is not advisable.

SecureDrop supports anonymity, something that is virtually unachievable with email.

The platform is designed to work hand in hand with the Tor network to maximise confidentiality

Whilst the platform itself uses Tor hidden services to support anonymity it is advisable careful where you access it from. Small networks where Tor usage may be monitored restricted, or public places where your screen may be viewed by CCTV should be avoided when using the platform. We recommend that you don't jump straight from the landing page to the SecureDrop site when uploading, especially on business networks may be monitored. Best practise would be to make a note of the Tor url and upload your content from a different machine at a later time for example an hour later

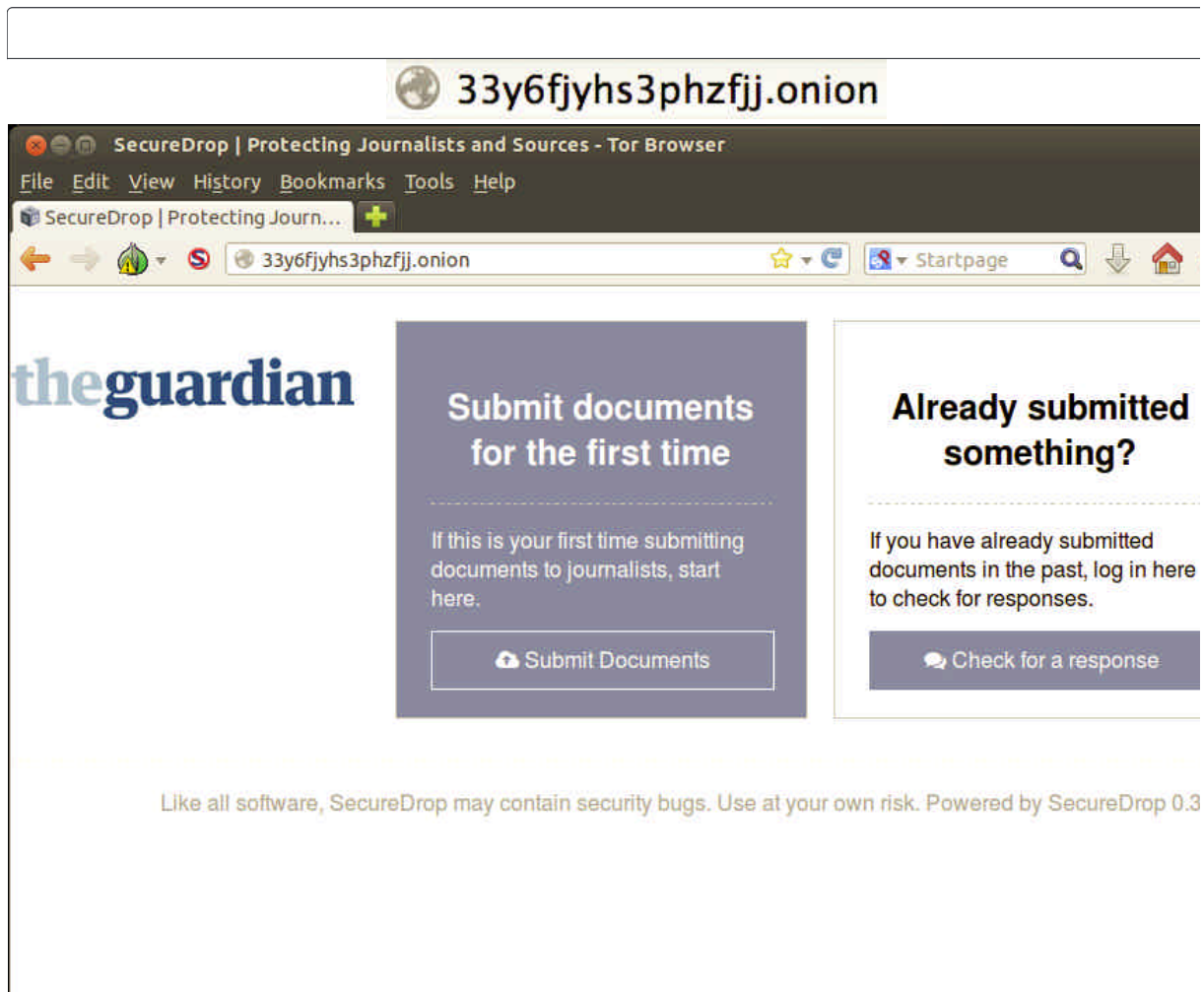
MAINTENANCE

SecureDrop will be unavailable 26th June to 31st July during a Newsroom move.

How to use it

GET TOR BROWSER BUNDLE or GET TAILS LIVE DVD

Once the Tor browser is launched and the Tor connection is complete you can access the platform at the following onion URL



About the SecureDrop platform

The SecureDrop software is an open source project sponsored by the

Freedom of the Press Foundation.

The software has been through thorough independent security reviews to ensure that it meets stringent confidentiality and anti-leakage requirements.

The platform has been built and commissioned with the latest fixes for the Heartbleed SSL vulnerability

Terms of Use

1. Provided that you use the Tor Browser or TAILS secure browser to access the Guardian SecureDrop platform confidentiality is assured via the Tor hidden service, however it cannot be guaranteed by this alone
2. If you are using the Tor browser you should ensure that there is no keylogging malware on your PC,MAC or tablet. The TAILS live DVD may be preferable
3. Any content uploaded to the platform will be treated in the utmost confidentiality by us to protect your anonymity unless you indicate you wish to waive it.
4. Uploading of content to the platform is no guarantee that an article will be published referencing that data. Guardian Editorial policy will be the ultimate arbiter of what is used.
5. When accessing this landing page we will not set cookies, fingerprint your browser/machine or display third party content
6. When accessing the Guardian SecureDrop platform we will not log your IP address, we will not set cookies, fingerprint your browser/machine or display third party content
7. Do not abuse the platform by uploading pornographic or obscene imagery
8. Use of The Guardian SecureDrop platform is at the user's own risk

Copyright © Guardian News and Media 2015

**The
Intercept_**

How to Contact The Intercept Anonymously



If this is your first time using The Intercept's SecureDrop server, read this page carefully first. For more detailed operational security advice, read the [How to Leak to The Intercept](#) blog post.

The Intercept is serious about protecting our sources. With our SecureDrop server, you can share messages and files with our

journalists in a way that should help you remain secure and anonymous, even from us. Messages and files that you send to us will be encrypted.

How to Use The Intercept's SecureDrop Server

Everything you do on the Internet leaves trails. Before following these instructions, go to a public wifi network, such as at a coffee shop that you don't normally frequent, and follow them from there. Or connect to a VPN.

- Download and install the Tor Browser Bundle from <https://www.torproject.org/>.
- Open the Tor Browser and copy and paste this into the address bar: **<https://y6xjgkgwj47us5ca.onion/>**
- Follow the instructions to send us information. You will be given a codename that you can use to log back in and check for responses in the future.

Don't access our SecureDrop server from your home or office. If you wish to ensure maximum privacy, use the [Tails](#) operating system instead of the Tor Browser.



[SecureDrop](#) is an open source whistleblower submission systems, originally programmed by the late Aaron Swartz, that is maintained by the [Freedom of the Press Foundation](#).

Privacy Information

=

Our SecureDrop servers are under the physical control of *The Intercept's* staff. When you interact with our SecureDrop servers, we don't log any information about your IP address, web browser, or operating system, nor do we deliver persistent cookies to your browser. When you use Tor to connect to our SecureDrop server, your connection is encrypted. Using the Tor network helps mask your activity from anyone that is monitoring your Internet connection, and it helps mask your identity from anyone monitoring our Internet connection.

When you send messages or upload files to this server, these messages and files are stored encrypted. Journalists at *The Intercept* store the encryption keys on air-gapped computers that never connect to the Internet. Even if our SecureDrop server got hacked or the physical hardware got confiscated, the messages and files you have submitted previously should still be shielded from the attacker.

However, no system is 100% secure, so we cannot absolutely guarantee your security. SecureDrop is regularly audited by independent security experts, but like all software, it could have security bugs that could be exploited by attackers.

If the computer you are using to submit documents is already compromised, any activities, including communications through SecureDrop, could be compromised as well.

Ultimately, you use the service at your own risk.



NEOS LEAKS

vertraulich leaken

[Warum NEOSleaks](#)

[Wie verwende ich NEOSleaks](#)

[Tor herunterladen](#)

[FAQ](#)

Warum NEOSleaks?

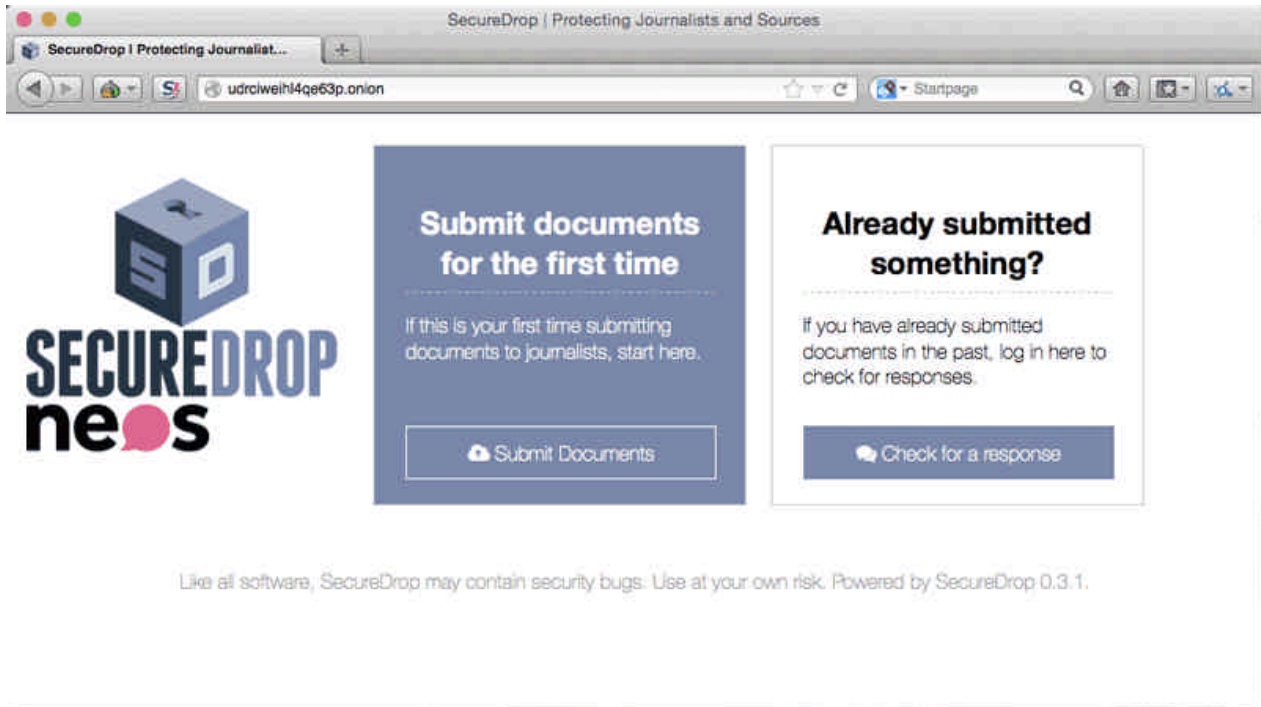
Hinweisgeber_innen, die über Informationen zu großen Missständen und Korruptionenfällen verfügen, gelingt es derzeit in Österreich kaum, anonym zu bleiben. Bestehende Plattformen sorgen nicht dafür, Quellen ausreichend zu verschleiern. NEOS setzt daher dabei auf die gleichen Sicherheitsstandards wie der Guardian oder die Washington Post. Diese Vorreiter in Sachen Whistleblowing-Datenschutz haben nach den Enthüllungen durch Edward Snowden die technische Hürden für Angriffsversuche von Außen so hoch angesetzt, dass es nicht mehr möglich ist, Absender rückzuverfolgen oder übermittelte Daten abzugreifen. Diese Maßnahmen sind durch die Enthüllungen von Edward Snowden nötig geworden.

Schon der Anti-Korruptionsreport 2014 der Europäischen Kommission hebt hervor, wie wichtig der Schutz von Whistleblowern ist und welchen wichtigen Beitrag sie im Kampf gegen Korruption leisten. Daher fordert Transparency International bereits seit Jahren den Ausbau dafür geeigneter Plattformen und kritisiert im überblicks-Report 2013 das fehlende Bewusstsein vor allem seitens der Politik und fehlende Initiativen.

Wie verwende ich NEOSleaks?

Für gewöhnlich werden im Internet Spuren hinterlassen. Daher wird empfohlen trotz der von uns gesetzten Maßnahmen einen öffentlichen Internet-Hotspot aufzurufen, das keinen Rückschluss auf Sie zulässt

1. Tor-Browser herunterladen und installieren: <https://www.torproject.org>
2. Tor-Browser starten und Adresse von NEOSleaks aufrufen: <http://udrciweiH4qe63p.onion/>
3. Den Anweisungen folgen. Um Nachrichten empfangen oder senden zu können muss der Codename notiert werden



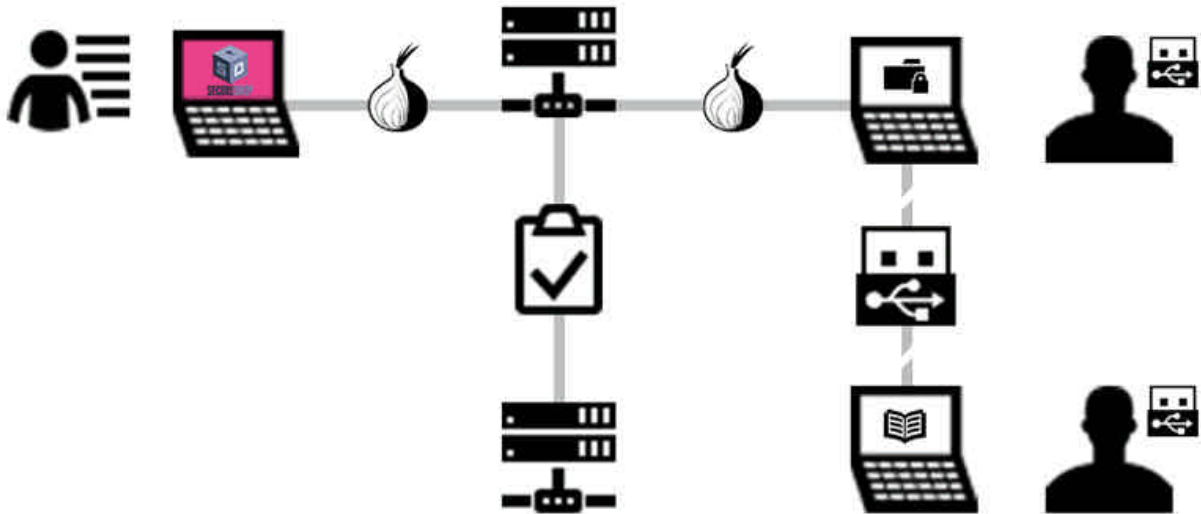
Frequently Asked Questions

Was passiert mit hochgeladenen Daten?

Hochgeladene Daten werden verschlüsselt gespeichert und werden vom Daten-Team sensibel behandelt. Daten, welche über NEOSleaks einlangen, werden nach hohen kryptographischen Standards behandelt und liegen erst dann in lesbarer Form und entschlüsselt vor, wenn das Risiko durch mögliches Ausspähen quasi nicht mehr gegeben ist.

Whistleblower ruft leaks.neos.eu auf

NEOSleaks-Team lädt Datei von Server
Entschlüsselt Datei nach der Air-Gap



Welche Daten werden von NEOSleaks gespeichert?

Der NEOSleaks-Server wird beim Hochladen von Dateien über das Tor-Netzwerk aufgerufen. Weder wir noch die Plattform verfügen daher über Verbindungsdaten. Darüber hinaus sind wir bemüht, sämtliche Metadaten in Dokumenten sofort zu entfernen.

Der Tor Client wählt eine zufällige Route über drei Tor-Knoten, um an das Ziel zu gelangen.



Bei herkömmlichen Verbindungen ist der ISP die Schnittstelle zum Ziel



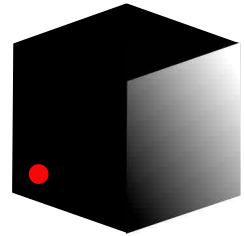
Welche Dokumente können geleakt werden?



NEOSleaks versteht sich als Plattform die auf große Missstände und Korruption abzielt.

Keinesfalls fallen persönliche Denunzierungen in unseren Kompetenzbereich.

THE NEW YORKER STRONGBOX



Strongbox is a method for you to share tips, information, and files whose importance or sensitivity demands a greater degree of anonymity and security than is afforded by conventional e-mail.

To help protect your anonymity, Strongbox is only accessible using the Tor network (<https://torproject.org>). When using Strongbox, [*The New Yorker*](#) will not record your I.P. address or information about your browser, computer, or operating system, and will not embed third-party content or deliver persistent cookies to your browser.

You can read our full privacy promise [here](#).

The New Yorker Strongbox is powered by [SecureDrop](#).

TO GET TO STRONGBOX AND BEGIN USING IT TO CONTACT WRITERS AND EDITORS AT *THE NEW YORKER*, FOLLOW THE THREE STEPS BELOW.

1. Download and install software to access the Tor network:

<https://www.torproject.org>. This should only take a few minutes.

2. Once you load the Tor browser, copy and paste the URL **<http://strngbxhwyuu37a3.onion>** into the Tor address bar. When the page loads, you will find further instructions on how to submit files and messages to *The New Yorker*.
3. You will be assigned a randomly generated and unique code name. If a writer or editor at *The New Yorker* wants to contact you about the information you have submitted, he or she will leave a message for you in Strongbox. These messages are the only way we will be able to reach you, and this message can only be accessed using your code name.

For security reasons, we advise you, especially if you are uploading documents, not to use your home or work network, and instead to use a public Wi-Fi network in an area where your screen is not visible to security cameras. Alternately, you can boot your computer from a USB key loaded with the Tails secure operating system, which is available at **<https://tails.boum.org>** and includes the Tor web browser.

Please note: general fiction, poetry, art, and PR submissions sent via Strongbox will not be assessed.

For more about *The New Yorker's* Strongbox project, read the introductory posts written by [Amy Davidson](#), [Kevin Poulsen](#), and [Joshua Rothman](#).

Our privacy promise

[The New Yorker's](#) Strongbox is designed to let you communicate with

our writers and editors with greater anonymity and security than afforded by conventional e-mail.

When you visit or use our public Strongbox server at <http://strngbxhwyuu37a3.onion>, [The New Yorker](#) and our parent company, Condé Nast, will not record your I.P. address or information about your browser, computer, or operating system, nor will we embed third-party content or deliver cookies to your browser.

Strongbox servers are under the physical control of [The New Yorker](#) and Condé Nast.

Strongbox is designed to be accessed only through a “hidden service” on the Tor anonymity network, which is set up to conceal both your online and physical location from us and to offer full end-to-end encryption for your communications with us. This provides a higher level of security and anonymity in your communication with us than afforded by standard e-mail or unencrypted Web forms. Strongbox does not provide perfect security. Among other risks, if you share your unique code name, or if your computer is compromised, any activities, including communications through Strongbox, should be considered compromised as well.

The system is provided on an “as is” basis, with no warranties or representations, and any use of it is at the user's own risk.

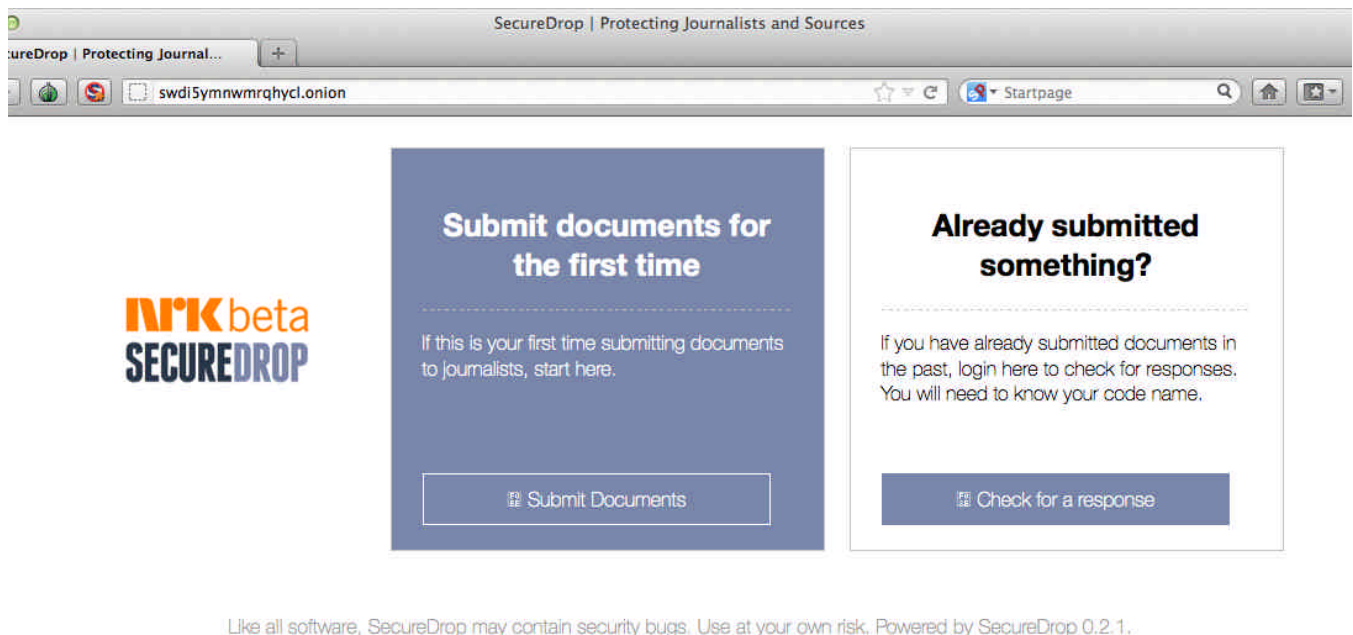
Slik tar du sikkert og anonymt kontakt med NRKbeta.

For oss er det viktig å være i stand til å kommunisere sikkert med kilder, uten frykt for avlytting av utenforstående. Dette gjelder spesielt informasjon som er så sensitiv at den deles anonymt med oss.

På grunn av dette har vi implementert systemet SecureDrop (<https://www.schneier.com/blog/archives/2013/10/securedrop.html>).

SecureDrop er et system som lar deg kommunisere sikkert over en kryptert kanal med NRKbeta, uten frykt for at utenforstående skal kunne avlytte kanalen. Du forblir dermed helt anonym, til og med for oss – om dette er ønskelig.

Systemet SecureDrop benytter seg av Tor-nettverket (<https://nrkbeta.no/2013/10/03/velkommen-til-tors-verden>) for å kryptere og anonymisere kommunikasjonen. Cookies og andre identifiserende faktorer er også fjernet.



SecureDrop | Protecting Journalists and Sources

swdi5ymnwrmrqhycl.onion

Startpage

NRKbeta
SECUREDROP

Submit documents for the first time

If this is your first time submitting documents to journalists, start here.

Submit Documents

Already submitted something?

If you have already submitted documents in the past, login here to check for responses. You will need to know your code name.

Check for a response

Like all software, SecureDrop may contain security bugs. Use at your own risk. Powered by SecureDrop 0.2.1.

Hvem er denne løsningen for?

SecureDrop-plattformen er opprettet for å gjøre det mulig å ta kontakt med NRK i saker som omhandler kritikkverdige forhold i samfunnet, og hvor du som varsler står ovenfor store represalier hvis din identitet avsløres.

Meldingene som sendes via SecureDrop-plattformen, er tilgjengelig for en håndfull journalister i NRK, som har lang erfaring med datasikkerhet og gravende journalistikk.

For normale nyhetstips, er tjenesten [NRK Nyhetstips](#) å foretrekke. Også her går all kommunikasjon over HTTPS, og ditt tips vil bli bearbeidet og sendt til riktig redaksjon.

Hvordan bruker jeg SecureDrop?

Før du leser instruksjonene nedenfor, anbefaler vi deg å ikke sende oss informasjon fra ditt eget hjemmenettverk. For å oppnå maksimal anonymitet, anbefaler vi at du sender oss informasjonen fra et offentlig sted, som for eksempel en kafé med gratis WiFi.

- Last ned Tor Browser til ditt operativsystem. Tor Browser finner du her: <https://www.torproject.org/projects/torbrowser.html.en>
- Start Tor Browser, og gå til denne adressen for å sende oss informasjon: <http://swdi5ymnwrmrghycl.onion/>
- På siden ovenfor får du informasjon om hvordan du sender tips til NRKbetas journalister.

Hvilke steg tas for å sikre kildevernet?

Ved å bruke NRKbetas SecureDrop-portal er du sikret at:

- Kommunikasjonen mellom din nettleser og våre servere er kryptert
- Identiteten din er skjult av Tor, gjennom minst tre krypterte hopp på nettverket
- Informasjonen du sender oss er kryptert med flere teknologier på serveren, og våre journalister bearbeider informasjonen på helt sikre datamaskiner som aldri har vært tilkoblet internett.

Vår SecureDrop-portal ligger på eksterne servere som er separat fra NRKbetas øvrige serverarkitektur.

Det er også mulig å kryptere innholdet med NRKbetas PGP-nøkkel (<https://nrkbeta.no/nrkbeta.pub>).

SecureDrop at the Project On Government Oversight



SECUREDROP

The Project On Government Oversight's SecureDrop server is a way for you to share information and files directly with POGO **more securely than with conventional email, other electronic means, or a phone call.**

Those methods might be appropriate for communications that are not sensitive or confidential, but to protect you and the information you are providing, please realize that certain steps must be followed, which are outlined below.

SecureDrop is an open-source whistleblower submission system developed by the Freedom of the Press Foundation, and the below information is based on their guidelines for using SecureDrop.

To help protect your anonymity, our SecureDrop server is only accessible using the Tor Browser, a modified version of Firefox that allows you to navigate the web with increased anonymity. When you use SecureDrop, nei-

ther POGO nor any third parties will record your IP address or information about your browser, computer or operating system. You will be able to communicate directly back and forth with POGO without revealing your identity. SecureDrop does not provide perfect security. Your anonymity can be compromised if, among other things, you share your unique codename or if your computer is compromised.

In order to use SecureDrop:

- Go to a place with a public internet connection, one that you don't normally frequent. Leave behind your cell phone and any other devices with a wireless internet connection, and do not purchase anything using a credit card. **Do not use a government or work computer to contact POGO.**
- Download and install the Tor browser bundle from <https://www.torproject.org/>
- Open the Tor browser, and copy this url into the browser address bar: **<http://dqeasamlf3jld2kz.onion>**
- From this url, you will be able to send secure, encrypted messages and files to POGO. Please provide a brief, but detailed description of the wrongdoing, the government agency involved, and if you can provide any documents to support your statement.
- You will be provided with a codename that you will use to log in to check for replies from us. **You must periodically come back to SecureDrop to check if POGO has left you a message. This is the only way we can communicate with you. Whether you make it possible for POGO to communicate with you on a follow-up basis is your choice, but please be aware that if you do not it may be difficult or impossible for us to investigate and corroborate your information.**

How SecureDrop works:

Sources who wish to communicate directly with POGO through SecureDrop will be given a codename and any documents or messages they send will be encrypted by SecureDrop. This codename should be remembered so it can be used in the future to access SecureDrop, and it allows sources to develop a relationship with POGO. Each source is known to POGO by a different codename so as to preserve the source's anonymity, even from POGO. Any documents that POGO receives will be encrypted and stored on an air-gapped computer that never connects to the internet. The SecureDrop servers are physically stored at POGO in a secure location and are separate from the servers that run the rest of POGO's website.

SecureDrop does not promise 100% security

SecureDrop is significantly more secure than email or other electronic ways of contacting POGO, but no system is 100 percent secure. There are always risks to whistleblowing and exposing corruption.

Exposed whistleblowers are almost always reprimanded, fired, and/or harassed, even if they have not "gone public" and even if their allegations are proven to be true. It takes a lot of courage and forethought to take on a powerful government agency or a private contractor or grantee. The mental, emotional, and financial hardships that a whistleblower may encounter should be fully understood before any steps are taken to disseminate information – publicly or not.

POGO's SecureDrop system is provided on an "as is" basis, with no warranties or representations, and any use of it is at the user's own risk.

What POGO does not do

- We do not deal with local and state issues unless federal money is in-

volved.

- We do not provide legal advice or representation. Moreover, we will not recommend a specific legal counsel.
- We do not look at individual cases of fraud or waste unless they are directly representative of systemic or widespread problems in the federal government and/or its contractors.
- We do not expose cases that cannot be verified or independently corroborated by government records or other sources.

POGO evaluates every lead we receive. However, because we are a small organization, we can only pursue the few tips that meet our internal guidelines and allow us to maximize our impact by performing the greatest public service. Thank you for understanding our intentions and limitations.

[Learn more about SecureDrop.](#)

[Learn more about the Tor Browser.](#)

SecureDrop Server

Update, April 17, 2015: Please note that our postal mail address below has changed. You may view the source code of this page for PGP verification.

ProPublica's SecureDrop server is a way for you to share information and files with ProPublica more securely than with conventional email or other electronic means.

To help protect your anonymity, our SecureDrop server is only accessible using the Tor system. We will not record your IP address or information about your browser, computer or operating system.

How to Use ProPublica's SecureDrop Server

Although you need to download special software to connect to ProPublica's SecureDrop server, the software is quite easy to use. It functions a lot like using a web browser, though in a more secure way.

- Visit [TorProject.org](http://torproject.org) and follow the directions to download Tor.
- Run the Tor application, which will launch the Tor Browser.
- In the Tor Browser, copy and paste the following into its address bar: **`http://pubdrop4dw6rk3aq.onion/`**
- You can follow the instructions on that website to send us files and messages.
- When you use the site, you will get a *code name*, which is your login for SecureDrop. You can come back and log in with this *code*

name to submit more information; you can also log in from time to time to see if we have sent a response to you.

If you seek maximum confidentiality, do not submit material using the network at your home or work. If you can, use public WiFi, such as at a coffeeshop. You can also boot your computer from a USB key containing the [TAILS secure operating system](#), which includes the Tor Browser.

Tor is designed to hide your IP address and seeks to make it very difficult for anybody to determine who is sending the files. However, be on your guard and know who might be watching you. We want you to be safe and to understand the risks you face before you send us anything, especially if your documents involve the national security of a technologically sophisticated country.

Postal Mail

Postal mail is also a very good way to reach ProPublica securely. U.S. postal mail without a return address is one of the most secure ways to communicate -- a warrant is needed to open it. Be sure to mail your package from an unfamiliar sidewalk box instead of going to a post office.

Our mailing address is:

ProPublica
155 Avenue of the Americas
13th Floor
New York, NY 10013-1507

Terms

ProPublica's SecureDrop server is designed to provide our sources with greater anonymity and security than with conventional e-mail.

When you visit or use our server at <http://pubdrop4dw6rk3aq.onion/> following the instructions provided above, we will not record your IP address or information about your browser, computer or operating system, nor will we embed third-party content or deliver persistent cookies to your browser.

Our SecureDrop servers are under our physical control in a physically and logically segregated area within the ProPublica newsroom.

SecureDrop is designed to be accessed only through a "hidden service" on the Tor system, which is set up to conceal both your online and physical location from us and to offer encryption for your communications with us. This provides a higher level of security and anonymity in your communication with us than does standard e-mail or similar methods.

Though it is our intention to keep you and your information safe, SecureDrop does not provide perfect security -- nor does any technology. Among other risks, if your computer is compromised, any activities, including communications through SecureDrop, could be compromised as well.

The system is provided on an "as is" basis, with no warranties or representations, and any use of it is at the user's own risk.

About SecureDrop



The SecureDrop software we use is a project of the [Freedom](#)

SECUREDROP [of the Press Foundation.](#)

PGP users may check this page for veracity with the following command. View page source for more information. « `curl`

`https://securedrop.propublica.org | gpg »`

Signing Key: [4034 E60A A782 7C5D F21A 89AA A993 E715
6E0E 9923 \(mike.tigas@propublica.org\)](#)

SECUREDROP BLOG

SecureDrop

Kære Whistleblower.

Velkommen til Radio24syvs SecureDrop.

Det er et sted vi har oprettet, så du trygt og uden risiko kan fortælle radioen om interessante historier, magtmisbrug, korruption, ulovligheder og sjusk i samfundet.

Med SecureDrop kan du være helt sikker på at ingen, absolut ingen – hverken os på radioen eller andre – kan finde ud af hvem du er. Du er 100 % anonym.

SecureDrop modtager og krypterer dine meddelelser, dokumenter og filer fra nettet, som derefter gemmes hos os. På Radio24syv er der kun en journalist der har adgang til SecureDrop – Anders Kjærulff fra [Aflyttet](#).

Før du kan bruge SecureDrop skal du først have installeret Tor og Tor-browseren. Det er browseren, du bruger til at få adgang. Du henter det hele her: <https://www.torproject.org/>

Og husk at opdatere browseren, når den beder om det.

Når du har installeret og startet Tor og din Tor-browser, så kan du besøge vores

SecureDrop på adressen: ***hpjw636qnt5avq62.onion*** (kopier adressen til din Tor-browser).

Status: **SecureDrop er oppe.**

Vores system skaber så et unikt kodenavn til dig, som betyder, at du kan etablere kontakt til os uden på nogen måde at afsløre din egen identitet.

Gem kodenavnet et sikkert sted, du skal nemlig bruge det til at logge ind, hvis du senere vil i kontakt med os.

Det smarte og sikre ved SecureDrop er, at vi på Radio24syv ikke aner hvem du er. Og ikke kan finde ud af det. Skulle nogen prøve at tvinge os til at røbe en kilde, kan det simpelthen ikke lade sig gøre.

Vi kan skrive en besked til dig og du kan skrive til os, og hvis det er rigtig vigtigt kan vi aftale et møde – men det er alt sammen op til dig. Og kun dig.

SecureDrop bruger tre servere for at sikre sig mod aflytning: En server tilsluttet nettet, en server der gemmer alt materialet og endelig en server, der tjekker sikkerheden for dem begge. Du kan læse mere om hvordan systemet fungerer

her: <https://pressfreedomfoundation.org/securedrop>

Husk: Brug ikke en arbejdscomputer og fortæl ikke andre om dit kodenavn.

Vi håber at høre fra dig

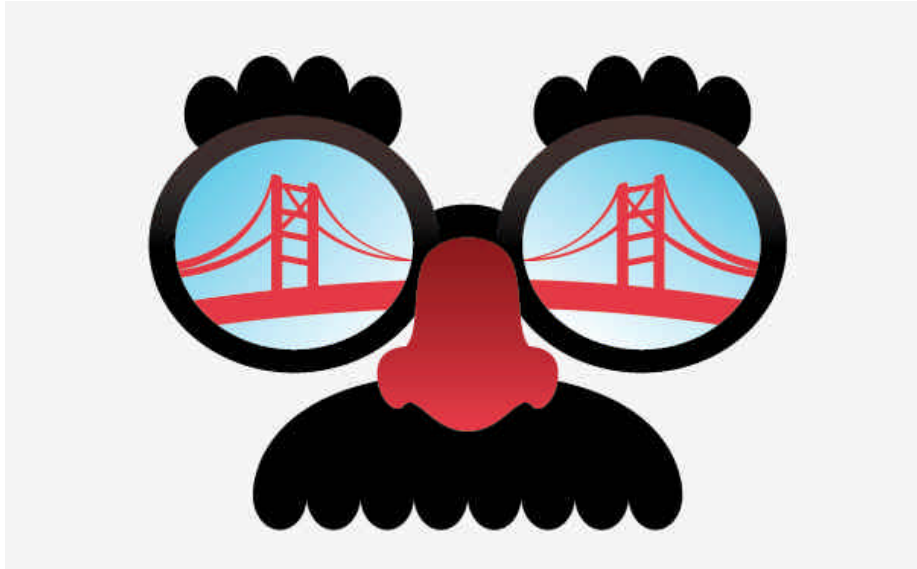
Radio24syv

Nye indlæg

Velkommen til et NYT SecureDrop!

Vi læser – og opgraderer!

SECUREDROP STATUS – Kinesere i maskinen?



Welcome to BayLeaks

Is there something you'd like to share?

BayLeaks was created to facilitate high-impact investigative journalism throughout the San Francisco Bay Area. BayLeaks uses SecureDrop, an encrypted, anonymized communications system, to enable users to securely share information that's newsworthy and relevant to the public interest. We work with a variety of media partners to publish stories based on information shared through our system.

We believe increased transparency and public accountability can discourage bad behavior by powerful individuals and organizations.

Our SecureDrop system's onion address is **wd5x5eexdqcjrqfa.onion**. We encourage use of SecureDrop, but you may also contact us via encrypted email at bayleaks@riseup.net. Scroll down for our [PGP key](#).

If you'd like to get started sharing information now, go directly to our [BayLeaks How-To Guide](#).

About SecureDrop

BayLeaks uses SecureDrop, a secure communications system developed by the [Freedom of the Press Foundation](#), a nonprofit organization dedicated to helping support and defend public-interest journalism. SecureDrop uses end-to-end encryption and the Tor anonymity network to provide strong security to its users. For a more detailed explanation of how SecureDrop works, please

[visit the Freedom of the Press Foundation website.](#)

About protecting our sources

Used properly, BayLeaks' SecureDrop system provides strong technical protections for people sharing information, preventing anyone — including us — from seeing names, IP addresses and other identifying information. It should be noted that BayLeaks can only provide a layer of technical digital security.

Important information before you begin

You should only open Tor Browser at a public location, such as a library or a café. This offers greater security than connecting to the Internet from a residence or place of employment, where it would be easier for a third party to detect you as a Tor user. After sharing information, you may continue to communicate securely with the BayLeaks team through SecureDrop using the codename you were assigned on your first visit.

BayLeaks How-To Guide

Follow these instructions carefully to share information.

1. Download the Tor Browser Bundle

The Tor Browser Bundle is an easy way to access the Tor network, which our SecureDrop system uses to protect users' anonymity. Here's how to get it!

- Go to a coffee shop or library that offers public Wi-Fi. Make sure you are not connecting from your home or work Internet connection.
- Open your web browser and visit <https://www.torproject.org>
- Look under "Our Projects," locate "Tor Browser," and click on it.
- Click the button that says "Download Tor Browser Bundle."
- Look under "Tor Browser Bundle Downloads" to find the right version for your computer's operating system. Choose from Microsoft Windows, Mac OSX, or Linux.
- Follow the prompts to install the Tor Browser.

2. Share documents and information with BayLeaks

Open your Tor Browser. Again, make sure you are on public Wi-Fi for added security!

Type or copy our onion URL into the address bar and press Enter:
wd5x5eexdqjrqfa.onion

Follow the instructions on our SecureDrop site to share documents and information. If you have a specific media partner in mind, please name them in a message to the BayLeaks team. If you want to check back later for responses or send follow-up messages, memorize your codename or write it down and store it in a safe place.

3. Check for responses

Open the Tor Browser and return to the SecureDrop site at **wd5x5eexdqcrqfa.onion**. Use your codename to log in and check for replies from the BayLeaks team or share more information. When you're finished communicating with the BayLeaks team, throw away your codename. Then delete Tor Browser from your computer.

Sending encrypted email

We strongly encourage you to use our SecureDrop system, but if you'd prefer to email us instead, you can send an encrypted email to the BayLeaks team at bayleaks@riseup.net. Scroll down for our PGP key.

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v1.4.11 (GNU/Linux)

```
mQINBFRf1E4BEAClFZPVMuIDSc30LLzGK3le6eKnfFfVJeBEg9JOUoGI2X4nXII
2h9natWDYlP2DFbKkOfolOpfm3elJTQYYFo1DDQ3f0/tBdpWZHxf9HMgPdmu5ZI
mRFp9Ajb4M5n4hsqicc+Od20+ZBacpqhOdLkdOjt6I0wXW5JgTQ2AvWPhQcvPOI
0KwvhgpAFQC0n6W1m9dgUPGzIWhISJpWGahwjHB+cnnwAt8CmVrXeNMYNoE9C(
hkFi/rcKGklKj4eLRFr10HNojexsyqcDoTpR2R6Xr5ptF4JivontD+9DdyGNdiq
pFigQ0IBvAo3sDKgMIs/NapDHyZmD3aqDTKFidWdSUIj6g2JR1lRuch2+hRk+V
FK1nTLaidUBmp2bPSQXilkhjys6W1TtaOoxG9mtvrnhPRCwo6VUyEk2Rdl7xtvy
4XN4vWDCVrsQ7eWvrXVuDvZpeEsZPHn5hw1LGhmu9l0xxvSRNrvV++qRaLZzEXI
KzU7pbH1jINwSej0JRMbELOa9tysMbRtFp/joHH4BQVlEdvzv2f1gio9lLLElvc
EQNw9FPVcRfY51ttllw2ZgQPrB7F0CRE35MfVuZfBMHlERYtuBELUYQRkjhd1Kr
WGvX5HkMgyQNaap21AYZw0kfN0tShUlI1PEhoSrkrT8wC+GSOPi4JG1wPQARAQ?
tB5CYXlMZWFrcyA8YmF5bGVha3NACmlzZXVwLm5ldD6JAjgEEwECACIFAlRf1E
GwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJEEGosjIcGRtmEr0P/jEgU+v
EX48jDRAh1V+/euvMsv101pDjHy1SXwKFYVOEizxYSSd1/DQSk9FuvwJv0VAow?
s7HzInPEb9hP+bnH2zlysUFHfzeyG0ZiEHwD0X7RpRMtSPCaQ5kMCDcAQALc0u
kNHwRxF3DyfUtPDkNG7+ehmqy+3I3vKgoBULVfd/f0m6vw1IAeqgtmKoL/ekqZ(
3pM8S4WYP6RqyennF/GZVbghzL3zTX71MWF9hhyeRPIF9ziJ/i0920XxpF5h0Ll
hG3nLbUn2pcyj2ktlNrfL/niISWQuEKRF0imOW/yVagNMIwOQPEUvu9jWhw5QHl
70J9BzOlvsY7bJU6L9f5iKxcVl0hAohkUHBGKcA+gIjp8Qf3WF7HPE3Q1CAk9j(
RBwRv3EwkVqo+9jJfDybPEe3uNdJI84zpiL3rdnHIdQj/9yFNwZ1wkg2QyJC0dl
b6gDyMk064pNn5nRMKzoTzziDEX0QfYkrsbb8FX0UTzhYt+wpZxcBE5lE6SDDec
RXrrBLbw+cS8zwv+GI67wjfZA9+jhhSUGej2bRG+xOZgXwqXlnX1tHoXWWaTVc
3SAJPR+iF5fIyzJYiZhE8Ch/agWNCmeuv36bmoL38LYQ3zgZFicI7oJAaL86avt
```

```
QiHE5P4XBhl0nwTmW8eJl5P/OgqvWy4IrLIsuQINBFRf1E4BEADPvFWsfrCuoJc
Jc/f8qAqm0KVsfTvjs1TYESram2aD2JZwhjewugO8/r3hGYTgOCkTChk2hSHw2I
l6qOP8o71TVvzSDJlH+vkfeIZSPtK8LLrgiJZOwsikaovRj8KrdER18V5fwnwa
lmsrXx/QhKTGVc3CbvpmVcTZKT6R7UntTIHlUzPlmE6hGQSVEJrkjqSP7ey86v!
MgCpKqFDhnyusBuBsRlDjNgqHJGgl2atV/Gg8PJu3N1YJ7jpdOWx0NB19XxLxBu
VcOYi8VcQxxHN88Q7YRLIBvXteIB9iFfXCil/Mw5AxSwHxNdfhZH+PUCh9CIQl(
uq42i9ukTnPSH/yeiLcuE7LrieBCEX60txib353Er6cYPBKytQieQhZUpobVb3y
hrxviFP1G2v2KiupAe7tDpgvq+HyuWicxFMcmLzps7U263EJ8ICQaSGKUJDwsbr
cwkgA+OIOFVpFwh3X48C4WZ/DjuX/GEUqPJntGYwjZDute04oTKuLoBNmLLfyDf
C+w2gyzcfS/krQwXi8VSEd3upzhGne/61LAXV6k33T6qT9E2cq5x4rRD5mbes2y
tnS6j56lnZ15GXkg5xABOn6iIXau7EgSTlUKSiuhGQwVt8CDAoeShJgw6u6wpyc
pt2FmDRkwoE4ZMMYvwnOSPnkIAovQARAQABiQIfBBgBAGAJBQJUX9ROAhsMAAA
EEGosjIcGRtmXjUP/ikMi6jf4Wk5H1/gjPTHcJSZTnooVW5GWBNGhU+sOTOTFR(
uhHbP8fsCjfg4/Euw2PYEEzUtuhglVAFukwMlSKUGpL/Fb0mV7AOpRKeyP9Dvq(
pnFzrVpafJWgGcfxy6Q0y0tweZG7YHT/lzFg0b0723d1Yh4U+lZV/+c1DCFxm+q
UvRGxqmb6iDFagqObt1ROZPjywoVNs484PVpZdxYxTW1Sh2+k7Q816OQfz1h3m.
7OIFBj6WR+1YjT3fn9NPbc5GSyQW8juol2sP9DmmOgGGtrc0nSttjks/KNg8qf
uNvXiEXluDp95dbCiG2z05KPa88t8vuASOIyiqZdc9wicyHaHp9aTlwV0pFVc7h
ZyvLGPRuZF5TzZMXMWzrDDhfnWeI/ENic16VfdmyEkZBhSR0AKplzFwq+TVpO+s
tX3lB/XDR6NqA3yZErOYDIzcDZeyiTzGszPndFHJNybDC09mfV8ULmLqhM6oXdl
7T1VMzsuCxsuYaqKGIzChMziMkvpjlr+YlnquPGlpuB1mZs9wZivPUarqPhSJ3(
Ex1Ec49HEVliyjXZuBFMSbOhdAT+dbV07Ai+SBgcyKqNHwEc/J+VaM/qpawziic
X3wWSwXY4LB5hvh0eDzZLKAJC7Wxk5+ue8LmWLDdOIJZTzPH/wNRnKffUZI8
=CIZc
```

-----END PGP PUBLIC KEY BLOCK-----

BayLeaks Privacy Policy

When BayLeaks users visit our SecureDrop site following the instructions in our How-To Guide, we will not record their IP address or information about their browser, computer, or operating system, nor will we embed third-party content or deliver persistent cookies to their computers. Our servers are under the physical control of BayLeaks team members in a protected location.

Though it is our intention to keep you and your information safe, BayLeaks does not guarantee 100% perfect security — nor does any technology. Among other risks, if your computer is compromised, any activities, including communications through SecureDrop, could be compromised as well. The system is provided on an “as is” basis, with no warranties or representations, and any use of it is at the user's own risk.



TCFMAILVAULT

MailVault is the safest way to make contact with journalists and fellows at The Century Foundation. Without revealing your identity, even to us, you may send confidential messages or files. All communications are routed to senior fellow [Barton Gellman](#). No one else will have the keys to read them. At your direction, he will share what you send with a colleague.

MailVault keeps you anonymous by disguising your location and the IP address of your computer. Encryption scrambles the content of your message so that no one can read it in transit.

[WHO WE ARE](#) | [LEARN MORE](#) | [PRIVACY POLICY](#)

Read more about MailVault below, then take three simple steps.

- Download the [Tor Browser Bundle](#), a web browser that aims to protect the anonymity of users.

- Launch Tor Browser and copy-paste this link into the Tor browser's address bar (not your usual browser's): <http://v6gdwmm7ed4oifvd.onion>.
- Follow further instructions on screen about how to submit.

For security reasons, it is recommended that you do not use MailVault from your work or home, and instead use it from a public wifi network, such as at a coffee shop.

WHO WE ARE

A full list of Century Foundation fellows and staff is [here](#). At present, only Barton Gellman will be able to see what you send through **MailVault**.

BARTON GELLMAN

is a Pulitzer Prize winning reporter and author, now writing about surveillance, privacy and the [NSA](#) with documents he received from Edward Snowden.

LEARN MORE

When you enter **MailVault**, you will receive a unique code name and password. Step by step instructions will guide you after that.

MailVault is based on [SecureDrop](#), a communications system for whistleblowers and others who need to exchange information privately. It uses well-respected, open source tools for anonymity (Tor) and encryption (GPG, also known as OpenPGP). Outside experts have [audited and improved](#) the technology, but no system offers perfect security. For example, if someone installs spyware or a hardware

key-logger on your computer, your communications with us may be compromised.

If the stakes of anonymity are very high, you may increase your protection against surveillance by browsing to Mail Vault:

(1) from a bootable thumb drive running [TAILS](#), a portable operating system built for maximum privacy...

(2) on a public computer or a computer you use for nothing else...

(3) and connected to a wired or wireless network away from your home and workplace.

PRIVACY POLICY

When you visit the **MailVault** onion URL, the Century Foundation cannot see your computer's I.P. address. We will not record information about your browser, computer, or operating system, nor will we embed third-party content or deliver cookies to your browser. On this page, tcfmailvault.info, we do not embed any third party content or log I.P. addresses either.

If you send us messages or files, we will make no attempt to identify you without your consent.

Our **MailVault** servers are kept under lock and key in the physical control of the Century Foundation, segregated from our other computers and networks. We host the system on a Tor "hidden service," which conceals your location and online identity as well as ours. We encrypt all communications from your computer to ours.

All that said, the system is provided on an "as is" basis. We can make no warranty about its security, or yours, and in the end you must assess the risks for yourself.

ABOUT THE CENTURY FOUNDATION |

What is SecureDrop?

The Washington Post's SecureDrop is a discreet way for readers to share messages and materials with our journalists. It offers greater security and anonymity than conventional e-mail and Web forms.



How do I use it?

SecureDrop relies on Tor, an application designed to encrypt your communications and obscure your computer's IP address.

In order to use SecureDrop:

- Go to a place with a public Internet connection, one that you don't normally frequent.
- Download and install the Tor browser bundle from <https://www.torproject.org/>.
- Open the Tor browser and copy this url into the browser address bar:
<http://vbmwh445kf3fs2v4.onion>.
- From this url, you will be able to send messages and files to a secure dropbox that we will check periodically.
- You will be provided with a codename that you will use it to log in to check for replies from The Post.

Keep the codename you are provided safe and secure. We will not know your codename, and you should never share it with anyone. If you forget your codename, we will have no other way to contact you.

What steps are taken to protect my privacy and anonymity?

Nearly all digital communications can leave a trail. The Washington Post's SecureDrop is designed to minimize these digital trails using best practices, such as:

- limiting collection of information logged about your browser, computer or operating system;
- using Tor to encrypt and anonymize your communications with us;
- storing submissions in encrypted form on our systems;
- physically isolating SecureDrop from the rest of our network.

However, no system is 100 percent secure, and even with these measures, there might be a risk of someone discovering who you are or what you are sending. In addition to using SecureDrop, we recommend that you:

- use a secure computer to communicate with us - one that does not maintain enterprise software or malware that might be used to record your activities;
- use an operating system that helps preserve your privacy and anonymity, such as [Tails](#);
- delete trails of communication that you store on your computer, such as copies of messages or your secure codename assigned when using the service;
- run any files you sent to us through a metadata-scrubbing tool to minimize the risk of unintentionally sending us information embedded in the documents, such as an author's name.

Other fine print

The Washington Post works diligently to protect the identities of our sources and keep the information they give us confidential. We do not make any warranties as to SecureDrop; use of the system is on an

"as is" basis, at your own risk.

[New Posts](#)[Popular](#)[Lists](#)[Video](#)[How to use SafeSource](#)[Download Tor](#)[Privacy Policy](#)

At Forbes, we want individuals with newsworthy information to come forward and communicate with our journalists free from outside surveillance, especially when what they're communicating is so sensitive that it must be sent anonymously. We've created SafeSource to offer that extra protection. You can use our app or tips to our online dropbox without having your identity known--even to us.

By routing your messages through the Tor anonymity network and avoiding any cookies or other tracking visitors, SafeSource is designed to protect both the content of your communications and your identity more strongly than traditional email.

SafeSource is based on the open-source, [security-audited](#) architecture known as SecureDrop, created by James Dolan and the late Aaron Swartz and funded in part by the Freedom of the Press Foundation.

How To Use SafeSource

- Simply visit [Torproject.org](http://torproject.org) and follow the directions to download Tor.
- Then run Tor, which launches the Tor Browser, and copy the following into its address bar:
<http://bczjr6ciiblco5ti.onion/>
- From there you'll be provided with more instructions and a passphrase for your personal SafeSource account so that you can begin communicating anonymously with our reporters.
- We'll work to investigate any tips or documents you provide so that your information has the maximum impact on Forbes.com and in the pages of Forbes Magazine.



[New Posts](#)

[Popular](#)

[Lists](#)

[Video](#)

Our Privacy Policy

SafeSource is a product owned and physically controlled by Forbes Media LLC ("Forbes"), ([www](#)) Through SafeSource, we have produced a mechanism that enables you to contact our writers an anonymously, providing for greater security than using conventional e-mail. Forbes values your p not store or record information about your operating system, browser, computer and/or your IP ac you use or visit the SafeSource server ("the Server") located at <http://bczjr6ciiblco5ti.onion/>. W embed or deliver cookies to your browser.

The SafeSource server is located in a separate and secure data center. SafeSource is an indepe and Forbes' infrastructure and network share no commonalities with it.

SafeSource is intended to be accessed only through a network called the Tor anonymity network as a service, is set up to conceal both your online and physical location from Forbes and offers ft encryption for your communications with us.

Forbes does not make any representations or warranties as to SafeSource, and your use of Safe "as is" basis, at your own risk. We do not represent that SafeSource provides perfect security. Yo is unique. Please do not share it with others. Forbes is under no liability for any problems or actio you sharing your passphrase with others. We maintain no liability in the event your computer is c and you should consider any communications through SafeSource in such an event to be compi Forbes also does not make any guarantee as to SafeSource's uptime.

Channels

- Business
- Investing
- Technology
- Entrepreneurs
- Op/Ed
- Leadership
- Lifestyle
- Lists

Company Info

- Forbes Careers
- Advertising Information
- Forbes Press Room
- Forbes Newsfeeds
- Investment Newsletters
- Reprints & Permissions
- Terms and Conditions
- Privacy Statement

Affiliate Sites

- Forbes China
- Forbes India
- Forbes Israel
- Forbes Mexico
- Forbes Middle East
- Forbes Poland
- Forbes Romania
- Forbes Russia
- Forbes Ukraine
- RealClear Politics
- RealClear Markets

Forbes Conferences

- Forbes Asia's Power Business Women
- Forbes Women's Summit
- Forbes 400 Philanthropy Summit
- Global CEO Conference
- Forbes Healthcare Summit
- Forbes CMO

Publications



- Free Trial Iss
- Subscriber S
- Buy Back Iss
- Data Partn
- Market Data
- Morningstar
- Thomson Re
- AdChoices



Help

New Posts

Popular

Lists

Video

- Under A Billion
- Techonomy
- Forbes Innovators
- Forbes and NAPFA
Advisor
- iConference
- Forbes
Reinventing
America Summit

2013 Forbes.com LLC™ All Rights Reserved

Threat Model

This is a work in progress

(inspired by [Pond's threat model](#) by Adam Langley)

The threat model is defined in terms of what each possible adversary can achieve. The list is intended to be exhaustive, i.e. if an entity can do something that is not listed here then that should count as a break of SecureDrop.

Assumptions about the SecureDrop user (either a source or a journalist):

- The user acts reasonably and in good faith. (Ex: if the user were to give their private key material to the attacker that would be unreasonable.)
- The user obtains an authentic copy of the Tor Browser Bundle.

Assumptions about the source user:

- They would like to not be known as a SecureDrop user, even against a forensic attacker.
 - This is a very hard requirement to meet.

Assumptions about the user's computer:

- The computer is not compromised by malware.
 - Is this a good assumption? We should be recommending for the source to use tails which would help mitigate malware on the source's

host [#needsticket](#)

Assumptions about the journalist organization, which hosts the SecureDrop instance and receives documents from sources:

- The journalist organization acts in the interest of allowing whistleblowers to submit documents, regardless of the contents of these documents.
- The journalist organization is interested in preserving the anonymity of sources.
- Every person within the journalist organization with physical access to the SecureDrop servers can be trusted to uphold the previous assumptions unless the entire journalist organization is itself compromised (see next point).
- It is possible for the journalist organization to be forced to collude with a government agency to prevent document submissions and deanonymize sources without the knowledge of any third party.
- The journalist organization has an authentic copy of the SecureDrop software and has correctly set it up.

Assumptions about the world:

- The security assumptions of our public cryptosystem (currently RSA, 4096-bit keys) are valid.
- The security assumptions of our hashing/key derivation function (scrypt with randomly-generated salts) are valid.
- The security/anonymity assumptions of Tor are valid, particularly those of the Tor Hidden Service protocol. (This is a somewhat contentious assumption when the application is a web application.)

What a SecureDrop server can and can't achieve:

- The SD server sees the plaintext codename (login identifier and passphrase) of every source.
- The SD server sees all HTTP requests made by each source and journalist.
- The SD server sees the plaintext documents submitted by a source.
- The SD server sees the plaintext replies from journalists to sources.
- The SD server stores a salted hash (using scrypt) of the source's codename.
- The SD server DOES NOT see the true IP address of the source, because it is a Tor Hidden Service.
- The SD server DOES NOT store plaintext documents or replies on disk, nor does it store the codenames at all on disk.

What a physical seizure of the source's property can and can't achieve:

- We assume that some sources will write down or save their codename in order to remember it for future logins. In this case, physical seizure of the source's property may result in the attacker obtaining the source's codename.
- An attacker with the source's codename can login to SecureDrop, submit documents, and reply to journalists as that source. The attacker can see any undeleted messages from the journalist to the source. The attacker CANNOT see past messages from the journalist to the source, because these ~~are automatically~~ should be deleted immediately after viewing once.
 - This is not true - the replies are not automatically deleted (although the UX encourages sources to delete them, it is not required). We should either clarify that, or open an issue to automatically delete replies, either after first view or a set timeframe.
 - Yes. Marking this as [#needsticket](#)

What a compromise of the source's computer can and can't achieve:

- A compromise of the source's computer can obtain all messages between the source and the SecureDrop server from the point of compromise, onwards.
- It cannot obtain a history of submissions prior to the point of compromise, or the plaintext content of any replies that were sent (and subsequently deleted by the source) prior to the point of compromise.

What a compromise of the journalist's personal computer can achieve:

- An attacker who compromises the journalist's personal computer gets the journalist's login credentials to the SecureDrop journalist interface. This means they can see the hashes of source codenames, encrypted submitted documents, and replies to sources. The attacker can also forge replies to sources.
- The attacker can see any documents on the journalist's computer that were stored in decrypted form. (Journalists are supposed to encrypt documents with their personal GPG key before taking them off the Secure Viewing Station, but we assume they leave documents decrypted while working on them.)

What a physical seizure of a SecureDrop server can achieve:

- ~~If the SD server is powered on,~~ physical seizure can obtain the submitted documents encrypted with the GPG key of the journalist organization, the hashes of the source codenames, the replies from journalists to sources that have not yet been read by sources (which are encrypted with a different GPG key per source), and the GPG private key of each source

encrypted with the codename of the source as the passphrase.

- ^also the script GPG and ID pepper values.
- What about persistent storage of incidental data on the server, like logs? Even with FDE it can be a good idea to minimize logging.
 - The servers do NOT have FDE enabled.
- good point, not sure what logs we store (if any?)
- pretty sure we don't log at all right now (need to verify with dolanjs). in the future we may keep a short rolling logging window to collect data for proposed DoS mitigation techniques.
 - For the Source Interface, tor is set to safe logging and apache error log writes to /dev/null and an access log is not configured. For the Document Interface, tor is set to safe logging but there is an error and access log. Admin access (ssh, and actions performed by the admin) are also logged.
- ~~If the server is powered off, physical seizure achieves nothing assuming that full-disk encryption works as expected.~~
 - The servers do NOT have FDE. They are set to auto install security updates and reboot if required. Because of the app/monitor server are set to auto reboot for sec updates, the servers would require manual intervention to reboot.

What a compromise of a SecureDrop server can achieve:

- If a SD server is compromised, the attacker can read and modify all plaintext document submissions and plaintext communications between journalists and sources from the point of compromise onwards.
- The attacker can also see when journalists, sources, and SD admins (via ssh) are accessing the server.
- The attacker can forge messages as any source/journalist.

What a physical seizure of the Secure Viewing Station (SVS) can achieve:

- If the SVS is seized while on, the attacker can get the passphrase-encrypted GPG private key of the journalist organization.
- If the SVS is seized while a Tails non-persistent volume is mounted, the attacker has access to the plaintext of some set of the organization's submitted documents. Journalists are encouraged to decrypt documents only as needed in separate Tails sessions (wiping the Tails non-persistent volume in between).
- If the SVS is powered off, physical seizure achieves nothing assuming that Tail's implementation of full-disk encryption works as expected.

What a compromise of the Secure Viewing Station can achieve:

- If the SVS is compromised by malware, the attacker can modify/delete documents before the journalist sees them and install/execute arbitrary programs, such as keyloggers.
- If the SVS is compromised by malware that is able to copy files to the USB stick that the journalist uses to transfer documents from the SVS to a non-airgapped computer, the attacker can achieve remote access to any files from the SVS, including plaintext documents and logs.

Question: Since the SVS is not "truly" air-gapped — there is still sneakernet, and it must run complex software that is hard to secure — is Tails paying for itself in terms of a benefit/complexity trade-off? We do (have to?) assume that the user's computer is not infected with malware (a quite strong assumption), so maybe a virtual machine running any OS on the user's laptop is just as good? I am trying to think of a way to figure out how to balance the usability/rigamarole/special behaviors costs vs. the security benefits.

- I am always in favor of simplifying this procedure when we can without

compromising security goals.

- Quibble: is it correct to say that it's not "truly" air-gapped? AIUI, air-gapped just means no network access. A computer without any way to communicate (sneakernet) would not be of much use. But it is important to codify the potential risk of a malicious submission compromising reused USB sticks, or possibly using some kind of BadBIOS-esque exfiltration vector.

What a local network (where securedrop has been deployed) attacker can achieve:

- Prevent a source or journalist from using SecureDrop by blocking Tor.
- On the source's network: see the sizes of plaintext uploaded documents.
- On the journalist's network: see the sizes of encrypted downloaded documents.
- Observe which users are using Tor at any time and may be able to deduce that they are using SecureDrop via traffic analysis (by looking at request sizes, for instance).

What a global, passive adversary (one who can observe all Internet traffic) can achieve:

- Possible ability to detect SD traffic via traffic analysis/profiling. (Ex: we have less than 10 HTML pages total on the source interface, and most of them are static. Sources using SecureDrop will tend to make a certain sequence of GETs/POSTs, and the response lengths are usually predictable/distinguishable.)
- Possible ability to link sources to SD servers, or journalists to SD servers
- Possible ability to link sources to journalists, if they are replying back and forth to each other with low-ish latency

- Possible ability to correlate whistleblower traffic when learning how to submit to SD accessing the media website from a list of given suspects provided by the organization who's material has been leaked

What a global, active adversary (one who can observe and arbitrarily modify/block Internet traffic) can achieve (in addition to the abilities of a global, passive adversary):

Threat Model

- Ability to prevent sources/journalists from using SecureDrop by blocking Tor.
 - Perhaps fteproxy.org can help here?

What an adversary that can generate forged CA certificates (in addition to the abilities of a global, active adversary) can achieve:

(I might just call that a "strong, global, active adversary")

- MITM compromise of the "landing pages" used by each journalist organization to communicate instructions for using SecureDrop, as well as the Tor Hidden Service URL.
 - Could trick users into visiting a fraudulent Tor Hidden Service designed to collect submissions, and potentially de-anonymize sources by analyzing submission document metadata or convincing them to share identifying information.
 - Could trick users into using a compromised version of the Tor Browser Bundle, since a download link is usually included on this page.
 - Can't we make it harder to forge/poison TBB and other software? Package signing that is automatically verified, an observatory/public log for software package hashes that is easy/automatic to check, et c?
 - That is a project entirely separate from SD, of course.

What a random person on the Internet can achieve:

(Maybe it is better to call this a global active attacker; maybe it is better to distinguish "powerful" vs. "weaker" than "global" and "random". Not sure.)

- A random person can attempt to DoS the SD server.
- A random person can attempt to trick other people into submitting to fake SD servers.
- A random person can attempt to get sensitive information from SD users' browser sessions (CSRF tokens, codenames from cookies).
- A random person can attempt to trick other people into downloading fake versions of the Tor Browser Bundle.
- A random person can attempt to compromise the SD server by attacking the exposed attack surface (kernel network stack, Tor, HTTP server, web app, Python, SSH server, TLS implementation, any other services, etc.).
- A random person can submit forged documents.
- A random person can submit malicious documents (e.g. malware to compromise the SVS).

What a local network (where "landing pages" of the media has been deployed or where the whistleblower use to connect to the internet, such as work proxy or home connection, to read landing pages) attacker can achieve:

- Log access from whistleblowers learning how to submit to SD, with possible ability to correlate whistleblower's IP/identity from a list of given suspects provided by the organization who's material has been leaked

The following threats/risks/threat actors are explicitly out of scope (proposed — feel free to bring things back in scope):

- SMM/firmware/BIOS malware on users' machines, SD servers or SVS
- TEMPEST/emissions security defense.
- Arguably (?) many/most forms of DoS can be considered out of scope. Not because they are not problems, but because DoS is generally very easy.
 - Sadly, yes. We have some ideas (and open issues) to raise the bar for potential DoS, but it is impossible to prevent it (especially difficult to prevent for a THS). So - preventing trivial DoS should be in scope, IMHO.
 - Yes; I'd include CPU or RAM DoS due to small/singular inputs as being in scope.
- Do we really want to bring in the web app traffic profiling/analysis thing in scope?
 - A web app this simple (by web app standards) might make it actually possible.
 - As mentioned on the crypto-ops list, I think web app traffic profiling is in scope.
- Government warrants on the journalist org. to hand over the organization's private keys.
 - Since such a compromise would be forward looking (modulo e.g. the logs issue), this would seem to motivate the use of GPG on the clients (not on the servers) (which I know you are working on)
 - Yep, we're thinking about building client-side GPG into securedrop for 1.0. This has been proposed multiple times but not designed.
 - I have a lot of ideas regarding this. Starting to dump them into the 1.0 roadmap.
- Remote tamper evidence by TPM-backed remote attestation (or some other means?!)
 - Physical security recommendations for the journalist org: in scope or out? I (CP) certainly have no clue on that front.

- As far as physical security, we rely a lot on the legal protections provided a news organization in the US [but below we assume black bag jobs happen]. We recommend for the news organization to not host the servers with a 3rd party, have the servers in their office or their lawyers. The servers should be in a locked room with video monitoring of access.
- How do/can we know if the journalist org does/could do a better job of physically securing the server than a 3rd party? There is a technical skill issue (is a journalist org technically willing capable of protecting the server, better than a specialist?), and a legal issue (I don't know anything about the latter of course — physical property rights might still hold, unlike privacy rights, when you defer management of the property to a 3rd party?).
- From the talks we have had with EFF lawyers, that decision was based on the likelihood that the 3rd party would be served a gag order while being forced to provide physical access. Hosting the servers in the news orgs/lawyers office is more about mitigating 3rd party gag orders. Don't actually think a news org office would be more secure in the case of black ops B&E.
 - Makes sense. It is safest to assume black bag jobs are routinely performed on journalist orgs, but also it'd help to have some way of getting a handle on just how often.
 - Think we have to assume that black bag jobs occur against news orgs in the US and possibly more so for any news org that hosts outside of the US. Do not know how to confirm or get any type of estimate on the frequency.
 - Relevant document: [Answering the client vs. server side crypto debate](#)

Open Questions

- What is the bare minimum software dependency set? Hardware?
- Under what scenarios can an entirely well-meaning user (journalist or admin) *accidentally* compromise the security goals?
- |



DuckDuckGo

Community Platform

- [Develop](#)
- [Translate](#)
- [Help](#)
- [Forums](#)
- [Blog](#)

[Sign up](#) [Login](#)

[Home](#) > [DuckDuckGo Blog posts](#) > 2015 Open Source Donations

19 Mar

2015 Open Source Donations

4 months and 9 days ago posted by  [yegg](#) Staff

We just made our Free and Open Source Software (FOSS) donations for 2015, totaling \$125,000 across five projects. Thank you for all the [community nominations](#) .

Our primary focus this year was to support FOSS projects that are bringing privacy tools to those who need them. We chose four projects we think are of paramount importance to achieving that goal:



\$25,000 to [The Freedom of the Press Foundation](#) to support [SecureDrop](#) , which "is an open-source whistleblower submission system managed by Freedom of the Press Foundation that media organizations use to securely accept documents from anonymous sources. It was originally coded by the late [Aaron Swartz](#) ." SecureDrop installations are now provided [by over 15 media organizations](#) , and we hope with our donation that we can help them increase this number significantly.

[Contribute code](#) | [Donate money](#)



\$25,000 to the [Electronic Frontier Foundation](#) to support [PrivacyBadger](#) , which "is a browser add-on that stops advertisers and other third-party trackers from secretly tracking where you go and what pages you look at on the web. If an advertiser seems to be tracking you across multiple websites without your permission, Privacy Badger automatically blocks that advertiser from loading any more content in your browser. To the advertiser, it's like you suddenly disappeared." Only [one developer](#) works on PrivacyBadger right now, and we hope with our donation he and others can get through [more issues](#) .

[Contribute code](#) | [Donate money](#)



\$25,000 to [GPGTools](#) to support [GPG Suite](#) , which is a tool for OS X that has "everything you need to get started with secure communication and encrypting files in one simple package. Use GPG Suite to encrypt, decrypt, sign and verify files or messages." We hope with our donation the part-time GPGTools team can spend a lot more time on the project this year.

[Contribute code](#) | [Donate money](#)



\$25,000 to [Riseup](#) to support [Tails](#) , which is "a live operating system, that you can start on almost any computer from a DVD, USB stick, or SD card. It aims at preserving your privacy and anonymity." It is recommended to use with SecureDrop for sources and journalists. We hope with our donation that more of the [Tails Roadmap](#) can be accomplished this year.

[Contribute](#) | [Donate money](#)

In addition to privacy tools, we would like to do our part to increase diversity in the open source community. To that end we also gave to a fifth project:



\$25,000 to [Girl Develop It \(GDI\)](#) to support their upcoming Open Source Mentorship program "with the goal of getting more women involved in the Open Source community through civic hacking projects. [GDI chapters](#) and [Code for America \(CfA\) brigades](#) will team up in five cities, pairing ~10 students in each who are learning to code through GDI along with seasoned developers working on civic hacking projects from within the local CfA brigades. The program will run for three months and will consist of skills-building workshops and weekly hacking on social good projects."

[Contribute](#) | [Donate money](#)

That's \$125,000 to FOSS projects this year, which is our most ever by far. We are very proud to be in the position to be able to give this support.

[6 Tweet](#)

You must be logged in to comment. Please [Log in](#) or [Register](#).



Why not donate to medical organizations instead?

posted by [Jop](#) • 1 month and 22 days ago • [Link](#)

Tails just released their monthly report thanking you guys and gals, and I wanted to do the same. Thank you for donating to five great programs! Thank you Duckduckgo from the bottom of my heart. Keep being awesome.

posted by <hidden> • 3 months and 19 days ago • [Link](#)

Wow. If I wasn't sold on DuckDuckGo before (which I was) I sure as heck am now.

posted by <hidden> • 3 months and 21 days ago • [Link](#)



Yeah thanks! Please also address <https://duck.co/forum/thread/11534/making-duckduckgo-s-javascript-free> ASAP - no donations remove your responsibility to not provide users with non-free software to run on their computers...

posted by [Gryllida](#) • 3 months and 22 days ago • [Link](#)



Gabriel, I want to thank you for caring about these kind of projects and donating to them!

posted by [preemeijer](#) 🍌 • 4 months and 2 days ago • [Link](#)



You're very welcome!

posted by [yegg](#) Staff • 4 months and 2 days ago • [Link](#)
[Show More Links](#)

Topics

- [Activity](#)
- [Android](#)
- [Community Platform](#)
- [DuckDuckGo](#)
- [DuckDuckHack](#)
- [Guest Post](#)
- [Meetups](#)

- [Newsletter](#)
- [Partners](#)
- [Privacy](#)
- [Sports](#)

Contribute to DDG

- [Github](#)
- [Community Platform](#)
- [Feedback](#)
- [Spread DDG](#)

Some things you should know...



Feeds

[Twitter reddit /r/duckduckgo title='DuckDuckGo Blog RSS feed'> RSS](#)

Monthly Newsletter

DuckDuckGo:

- [Spread DuckDuckGo](#)
- [Get DuckDuckGo Gear](#)

- [Follow DuckDuckGo](#)

DuckDuckHack:

- [Develop Instant Answers](#)
- [Instant Answers](#)
- [Follow DuckDuckHack on Twitter](#)

Duck.co:

- [Develop this site](#)
- [Chat via XMPP](#)
- [Follow Duck.co on Twitter](#)

[Home Feedback](#)

Powered by [Perl](#). Source at [GitHub](#). © [DuckDuckGo, Inc.](#)

Login

<input type="text"/>
<input type="password"/>
<input type="button" value="Cancel"/> <input type="button" value="Login"/>

[Forgot your password?](#)

Don't have an account? [Sign up](#)

[Main](#)[About](#)[Donate](#)[Banking Blockade](#)[Submissions](#)[Press](#)[Mirrors](#)[Chat](#)[Support us](#)[Archives
2006-2010](#)**Editorials**

2011-09-22

Julian Assange:
Statement on the
Unauthorised,
Secret Publishing of
the Julian Assange
"autobiography" by
Canongate

2011-09-19

WikiLeaks
Launches the First of
Four Fundraising
Auctions

2011-08-24

US espionage
investigation against
WikiLeaks:

PATRIOT Act order
unsealed

2011-06-15

In Conversation
with Julian Assange
Part II

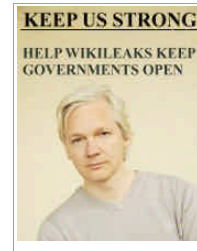
2011-05-24

"WikiSecrets"
Julian Assange Full
Interview Footage

SUBMISSIONS

**NOTE: At the moment
WikiLeaks is not accepting
new submissions due to
re-engineering
improvements the site to
make it both more secure
and more user-friendly. Since we are not
currently accepting submissions during the**

**re-engineering, we have also temporarily closed our online chat support for how
to make a submission. We anticipate reopening the electronic drop box and live
chat support in the near future.**

**1. Material we accept**

Wikileaks will accept restricted or censored material of political, ethical, diplomatic or historical significance. We do not accept rumor, opinion, other kinds of first hand accounts or material that is publicly available elsewhere. This is because our journalists write news stories based on the material, and then provide a link to the supporting documentation to prove our stories are true. It's not news if it has been publicly available elsewhere first, and we are a news organisation. However, from time to time, the editors may re-publish material that has been made public previously elsewhere if the information is in the public interest but did not have proper news analysis when first released.

If you are sending us something, we encourage you to include a brief description of why the documents is important and what the most significant parts are within the document. It will help our journalists to write up and released the story much faster.

2 Our anonymous electronic drop box

Wikileaks has an anonymous electronic drop box if you wish to provide original material to our journalists. Wikileaks accepts a range of material, but we do not solicit it. If you are going to send in material it should be done as securely as possible. That is why we have created our novel method of submission based on a suite of security technologies designed to provide anonymity. We have put a great deal of technical and design work into the drop box because we take the journalist-source relationship very seriously.

2.1 Its easy to submit

Our drop box is easy to use and provides military-grade encryption protection.

Submitting documents to our journalists is protected by law in better democracies. For other countries, the electronic drop box is there to offer help and protection. It is particularly designed to keep your identity hidden from everyone, including WikiLeaks. We never keep logs of who uses the drop box or where they are coming from.

There are several ways to send in material, but the most secure and anonymous is at the following link.

(currently closed for re-engineering security and useability improvements)

To add another layer of protection,you might also want to use the secure TOR network

2011-05-23

In Conversation
with Julian Assange
Part I

(<http://suw74isz7qqzpmgu.onion/>) Tor is a secure anonymous distributed network that provides maximum security.

2.2 Help with any questions about submitting

You can also chat to us online and we will answer any questions or solve any problems you might have with submitting (<https://chat.wikileaks.org>) (Currently temporarily closed with the electronic drop box for re-engineering.) Our chat is designed to be secure and anonymous. Visitors are protected by many layers of security. They can not see each other. There is a mechanism in place to stop logging and the server forbids potentially dangerous commands that could reveal other user's identity. Communication is secured with SSL encryption.

2.3 Protection for you

Wikileaks does not record any source-identifying information and there are a number of mechanisms in place to protect even the most sensitive submitted documents from being sourced. We do not keep any logs. We can not comply with requests for information on sources because we simply do not have the information to begin with. Similarly we can not see your real identity in any anonymised chat sessions with us. Our only knowledge of you as a source is if you provide a coded name to us. A lot of careful thought by world experts in security technologies has gone into the design of these systems to provide the maximum protection to you. Wikileaks has never revealed a source.

2.4 How it works

When WikiLeaks receives a document, our accredited journalists assess the submission. If it meets the criteria, our journalists then write or produce a news piece based on the document. This typically includes a description of the document, an analysis of why it is important, and an explanation of what it signifies to broader society. The news piece might also highlight the parts of the document that are most newsworthy. Our news stories are deliberately analytical regarding the wider significance of the document. We then link from the news piece to the original submission.

Submissions establish a journalist-source relationship. Online submissions are routed via countries which have strong shield laws to provide additional protection to sources and journalists.

Some documents submitted contain highly sensitive information. WikiLeaks has developed a harm minimisation procedure to clean documents which might endanger innocent lives. In other instances, WikiLeaks may delay publishing some news stories and their supporting documents until the publication will not cause danger to such people. However in all cases, WikiLeaks will only redact the details that are absolutely necessary to this end. Everything else will be published to support the news story exactly as it appeared in the original document.

WikiLeaks has a overriding objective to publish and bring information into the public arena to encourage an informed society. It will stay doggedly true to this goal.

3. Directions for how to submit material

If you want to send us a message of your own, as opposed to a document, please see Contact.

3.1 Submissions via secure upload

Fast, easy and automatically encrypted with the best banking-grade encryption. We

keep no records as to where you uploaded from, your time zone, browser or even as to when your submission was made (if you choose a non-zero publishing delay, we set the file time record to be the release date + a random time within that day).

If you are anonymously submitting a Microsoft word file (".doc") that you have edited at some stage, please try to send a PDF document (".pdf") instead, as Word documents may include your name or the name of your computer, see Word file redaction for further information. If you have no means to produce a PDF file your document will be converted by WikiLeaks staff.

The process your document will undergo is outlined for understanding submissions.

NOTE: At the moment WikiLeaks is not accepting new submissions due to re-engineering improvements the site to make it both more secure and more user-friendly. Since we are not currently accepting submissions during the re-engineering, we have also temporarily closed our online chat support for how to make a submission. We anticipate reopening the electronic drop box and live chat support in the near future.

You can also use secure TOR network (secure, anonymous, distributed network for maximum security)

3.2 Submissions via our discreet postal network

Submissions to our postal network offer a strong form of anonymity and are good for bulk truth-telling.

Steps:

- First place your leak onto a floppy disk, CD, DVD or a USB Flash Drive. If you are using a floppy disks, please create two as they are often unreliable. If you only have paper documents, we will scan them if they are of significant political or media interest (if you are unsure whether this may be the case, please contact us first). This will delay the process however.
- Post your information to one of our trusted truth facilitators listed below. You may post to whatever country in the list that you feel most suitable given the nature of the material and your postal service. If your country's mail system is unreliable, you may wish to send multiple copies, use DHL, FedEx or another postal courier service.

WikiLeaks truth facilitators will then upload your submission using their fast internet connection. If you use a floppy disk, be sure to send two for increased reliability.

You can use whatever return address you like, but make doubly sure you have written the destination correctly as postal workers will not be able to return the envelope to you.

After receiving your postal submission our facilitators upload the data to WikiLeaks and then destroy the mailed package.

3.3 High risk postal submissions

If your leak is extremely high risk, you may wish to post away from your local post office at a location that has no witnesses or video monitoring.

Many CD and DVD writers will include the serial number of the DVD or CD writer onto the CD/DVDs they write. If the post is intercepted this information can in theory be used to track down the manufacturer and with their co-operation, the distributor, the sales agent and so on. Consider whether there are financial records connecting you to the CD/DVD writer sale if your adversary is capable of intercepting your letter to us and has the will to do this type of expensive investigation. Pay cash if you can for the CD/DVD writer.

Similarly, CD and DVD media themselves include a non-unique manufacturing "batch number" for each group of around 10,000 CD/DVDs made. Pay cash when buying the CD or DVD. Try to choose a store without video cameras at the register.

Although we are aware of no instances where the above has been successfully used to trace an individual, anti-piracy operations have used the information to trace piracy outfits who sell tens or hundreds of thousands of counterfeit CDs or DVDs.

If you post it to us, a good option is to encrypt the USB file/CD file and then contact us at a later date via live online chat with the encryptin passphrase. That way if the post is intercepted, the data can not be copied.

If you suspect you are under physical surveillance, discreetly give the letter to a trusted friend or relative to post. On some rare occasions, targets of substantial political surveillance have been followed to the post office and have had their posted mail seized covertly. In this rare case if you are not intending to encrypt the data and if the police or intelligence services in your country are equipped to perform DNA and/or fingerprint analysis you may wish to take the appropriate handling precautions.

3.4 Postal addresses of our trusted truth facilitators

You may post to any country in our network.

Pick one that best suits your circumstances. If the country you are residing in has a postal system that is unreliable or frequently censored, you may wish to send your material to multiple addresses concurrently. For unlisted postal addresses, please contact us.

In Australia:

To: "WL" or any name likely to evade postal censorship in your country.

BOX 4080

Australia Post Office - University of Melbourne Branch

Victoria 3052

Australia

 Send to Friend  Print