Journalists and Security Tools

Some Introductory Tips on Protecting Your Communications, Research, and Data

Dave Maass, Investigative Researcher
Electronic Frontier Foundation
@maassive

About EFF

Free speech, privacy, transparency, fair use, and innovation

Founded in 1990, we defend your civil liberties in the digital world through litigation, activism, and development of technological tools.

We're based in San Francisco, but work on the local, national, and international stages.

About me

Investigative Researcher =
Muckraker/noisemaker on EFF's Activism Team

Former reporter for alt weeklies in every state along the Mexico border

Staff writer at Santa Fe Reporter 2007-2009

Some Examples of Why You Should Care About Security

National Security

Under sweeping subpoenas, Justice Department obtained AP phone records in leak investigation

POLITICS

DOJ seized phone records for Fox News numbers, reporter's parents

Federal police admit seeking access to reporter's metadata without warrant

AFP asked for 'subscriber checks' relating to Guardian Australia journalist Paul Farrell in attempt to identify his sources

State high court censures Taos DA, prosecutor-turned-judge over subpoena violations

Surveillance Self-Defense

ssd.eff.org

“Playlist” for journalists just starting out with security tools:
https://ssd.eff.org/en/playlist/journalism-student

Caveat

There's no such thing as perfect security; threats are constantly evolving.

Targeted surveillance by advanced adversaries harder to combat than mass surveillance or surveillance by less-advanced adversaries.

Tools are presented as options, not endorsements (except when we made them)

Cooper says:

"Teaching security tools without first teaching **threat modeling** is like handing someone a bunch of pills and saying take some of these if you're sick."

Threat modeling basics

Digital security isn't about which tools you use; rather, it's about understanding the threats you face and how you can counter those threats.

To become more secure, you must determine what you need to protect and whom you need to protect it from.

Five Questions

1. What do you want to protect?
2. Who do you want to protect it from?
3. How likely is it that you will need to protect it?
4. How bad are the consequences if you fail?
5. How much trouble are you willing to go through in order to try to prevent those?

What do you want to protect?

Write down a list of data that you keep, where it's kept, who has access to it, and what stops others from accessing it

Who do you want to protect it from?

Make a list of who might want to get ahold of your data or communications. It might be an individual, a government agency, or a corporation.

Write down what your adversary might want to do with your private data.

Threat vs. Risk

While a threat is a bad thing that can happen, risk is the likelihood that the threat will occur.

For instance, there is a threat that your building might collapse, but the risk of this happening is far greater in San Francisco

Practice

Should I lock my door?
What kind of lock or locks should I invest in?
Do I need a more advanced security system?
What are the assets in this scenario?
What is the threat?
What is the actual risk of someone breaking in? Is it likely?

Vitamins?

But, Cooper, aren't there some baseline, preventative health things I should do?

Like the security equivalent of vitamins, exercise, self-examinations, tooth-brushing?

Basic Digital Hygiene

Social media privacy settings
Advertising Opt-outs
Strong Passwords
Password Managers (e.g. KeePass)

HTTPS Everywhere
https://www.eff.org/HTTPS-EVERYWHERE

Two Tools for Assessing Your Browsing Privacy

https://panopticlick.eff.org/

https://privacybadger.org

Panopticlick

Panopticlick will analyze how well your browser and add-ons protect you against online tracking techniques.

panopticlick.eff.org

Test	Result
Is your browser blocking tracking ads?	✗ no
Is your browser blocking invisible trackers?	✗ no
Does your browser unblock 3rd parties that promise to honor Do Not Track?	✗ no
Does your browser protect from fingerprinting?	✗ your browser has a unique fingerprint

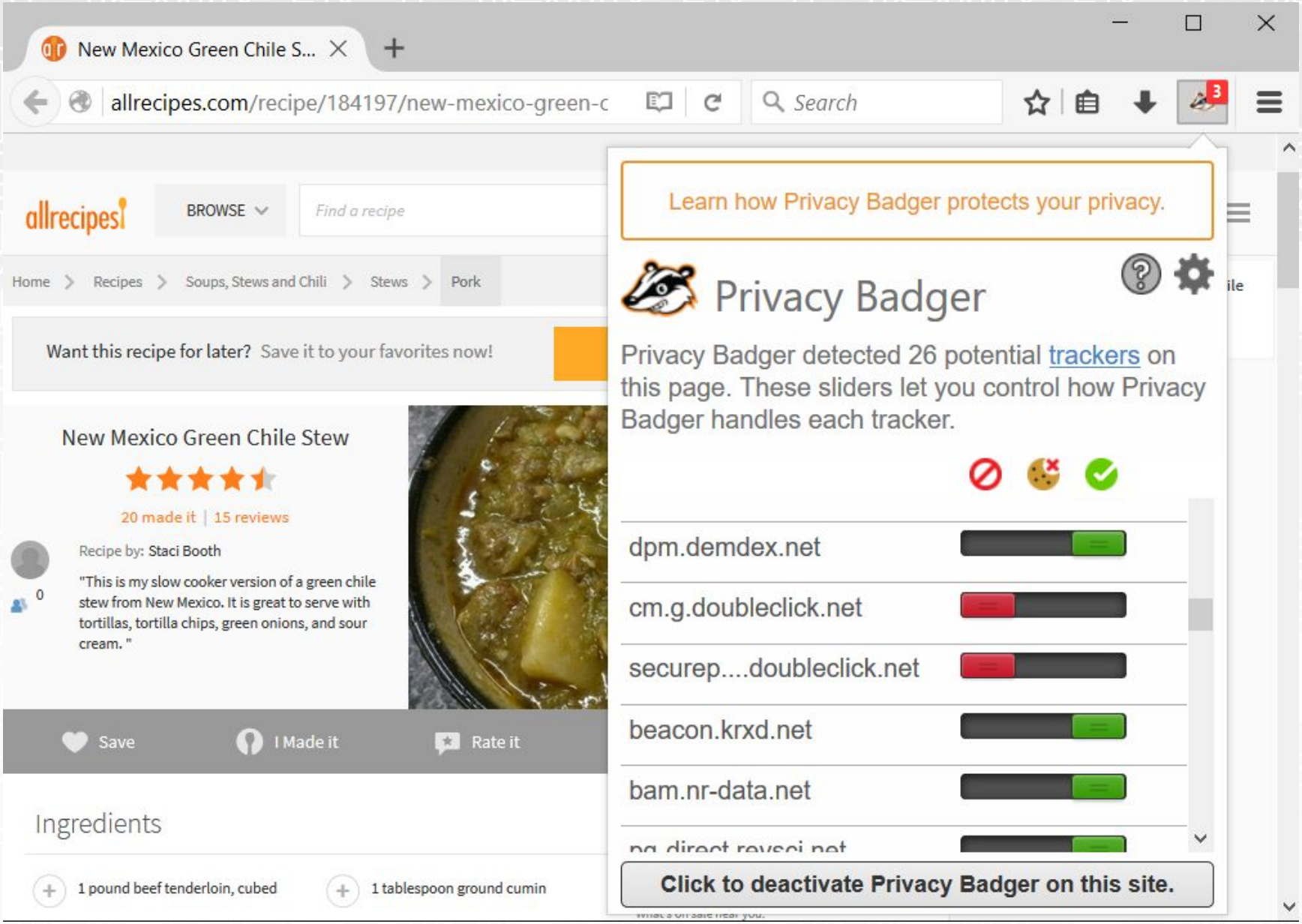
Note: because tracking techniques are complex, subtle, and constantly evolving, Panopticlick does not measure all forms of tracking and protection.

Your browser fingerprint **appears to be unique** among the 138,176 tested so far.

Currently, we estimate that your browser has a fingerprint that conveys **at least 17.08 bits of identifying information.**

Privacy Badger
privacybadger.org

Privacy Badger 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.


New Mexico Green Chile S...
allrecipes.com/recipe/184197/new-mexico-green-c
Search
allrecipes
BROWSE
Find a recipe
Home > Recipes > Soups, Stews and Chili > Stews > Pork
Want this recipe for later? Save it to your favorites now!
New Mexico Green Chile Stew
20 made it | 15 reviews
Recipe by: Staci Booth
"This is my slow cooker version of a green chile stew from New Mexico. It is great to serve with tortillas, tortilla chips, green onions, and sour cream. "
Save
I Made it
Rate it
Ingredients
1 pound beef tenderloin, cubed
1 tablespoon ground cumin
Learn how Privacy Badger protects your privacy.
Privacy Badger
Privacy Badger detected 26 potential trackers on this page. These sliders let you control how Privacy Badger handles each tracker.
dpm.demdex.net
cm.g.doubleclick.net
securep....doubleclick.net
beacon.krxd.net
bam.nr-data.net
Click to deactivate Privacy Badger on this site.

Basic Encryption

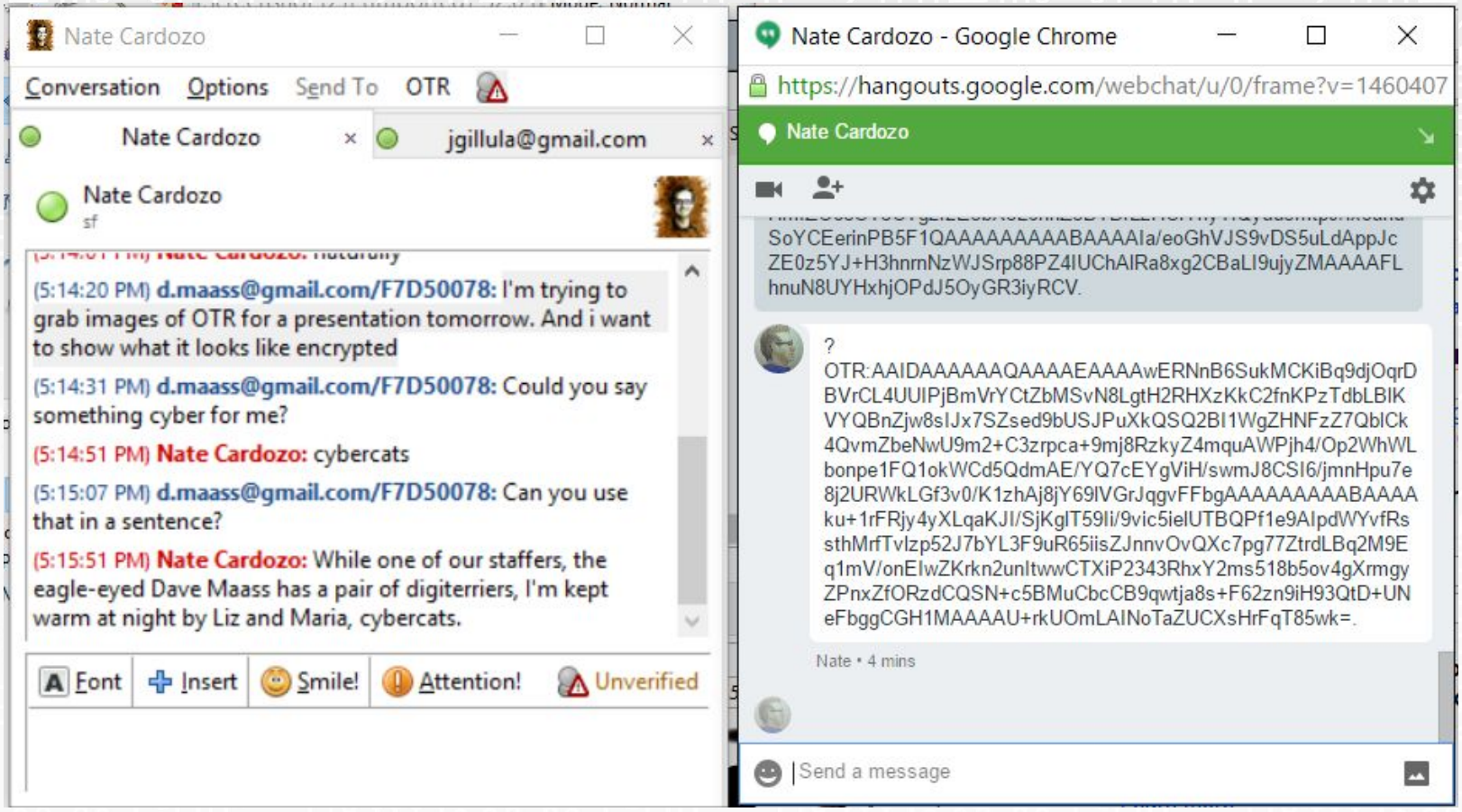
Encrypted Chat
Adium and Pidgin (with OTR), Whatsapp, TextSecure

Phone:
Signal, Silent Circle

PGP (Pretty Good Privacy) Encrypted Email
https://gpgtools.org

See: EFF's Secure Messaging Scorecard
https://www.eff.org/secure-messaging-scorecard

What does encryption look like?



Pidgin with OTR

Not Just Sources

Think about communication between members of the newsroom, such as reporters and editors

More Advanced

SecureDrop – Whisteblower sharing system
https://securedrop.org/

OnionShare 0.9
https://onionshare.org/

Anonymized Browsing

Anonymous Searches (e.g. DuckDuckGo)
Tor Browser

Herd Immunity

Even if you don't think you need encryption, it can help everyone who does need it if you increase the noise.

In the Physical World

Your phones can leak your whereabouts
Tip: Leave your phone at home or turn it off when meeting sources

Automated License Plate Readers document your driving patterns.
Tip: Take alternative transportation When meeting sources

More resources

Surveillance Self Defense for Journalists Traveling Abroad
https://ssd.eff.org/en/playlist/journalist-move

Freedom of the Press Foundation
Encryption works
https://freedom.press/encryption-works

Julia Angwin's Privacy Tools (ProPublica)
http://juliaangwin.com/privacy-tools/

Questions?

Dave Maass
dm@eff.org
415-436-9333 x151

Twitter: @maassive