Understanding and Designing for End Users' Security Expectations

Case Studies with Journalists and Lawyers



Franziska Roesner

franzi@cs.washington.edu

Computer Science & Engineering

University of Washington



with: Kelly Caine (Clemson), Ada Lerner (UW),
Susan McGregor (Columbia), Eric Zeng (UW)

Understanding and Designing for End Users' Security Expectations

Case Studies with Journalists and Lawyers



Franziska Roesner

franzi@cs.washington.edu

Computer Science & Engineering

University of Washington

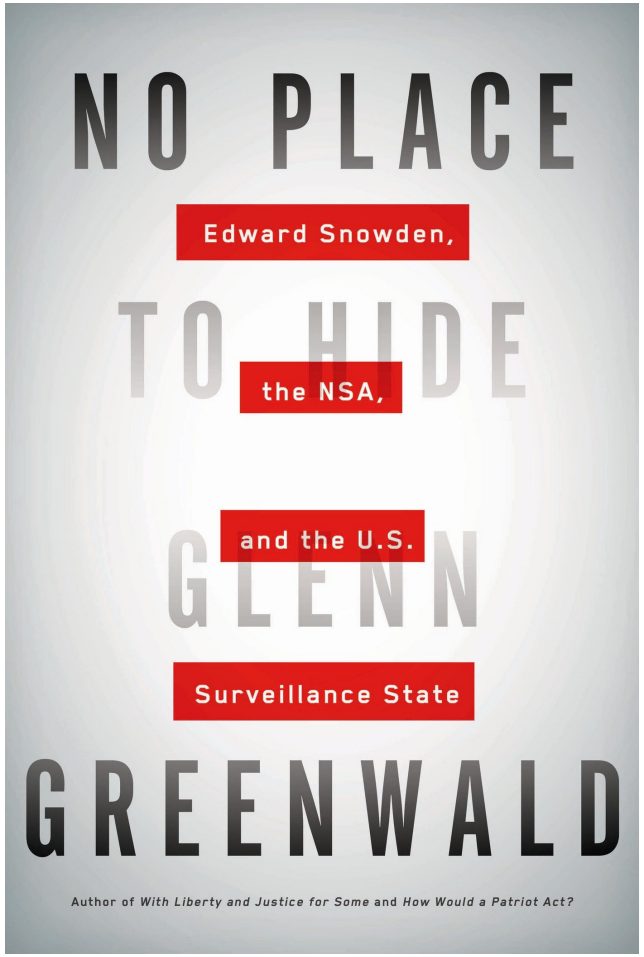


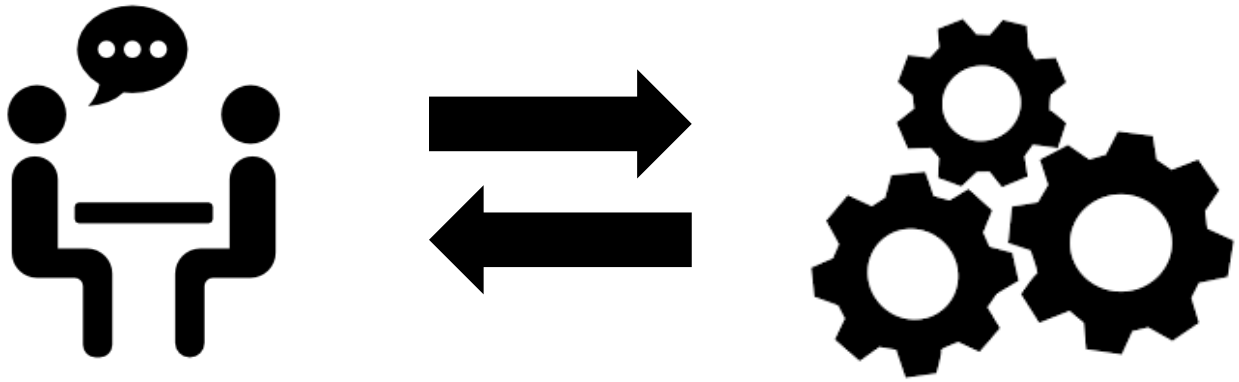
with: Kelly Caine (Clemson), Ada Lerner (UW),
Susan McGregor (Columbia), Eric Zeng (UW)

Using encryption software was something I had long intended to do...

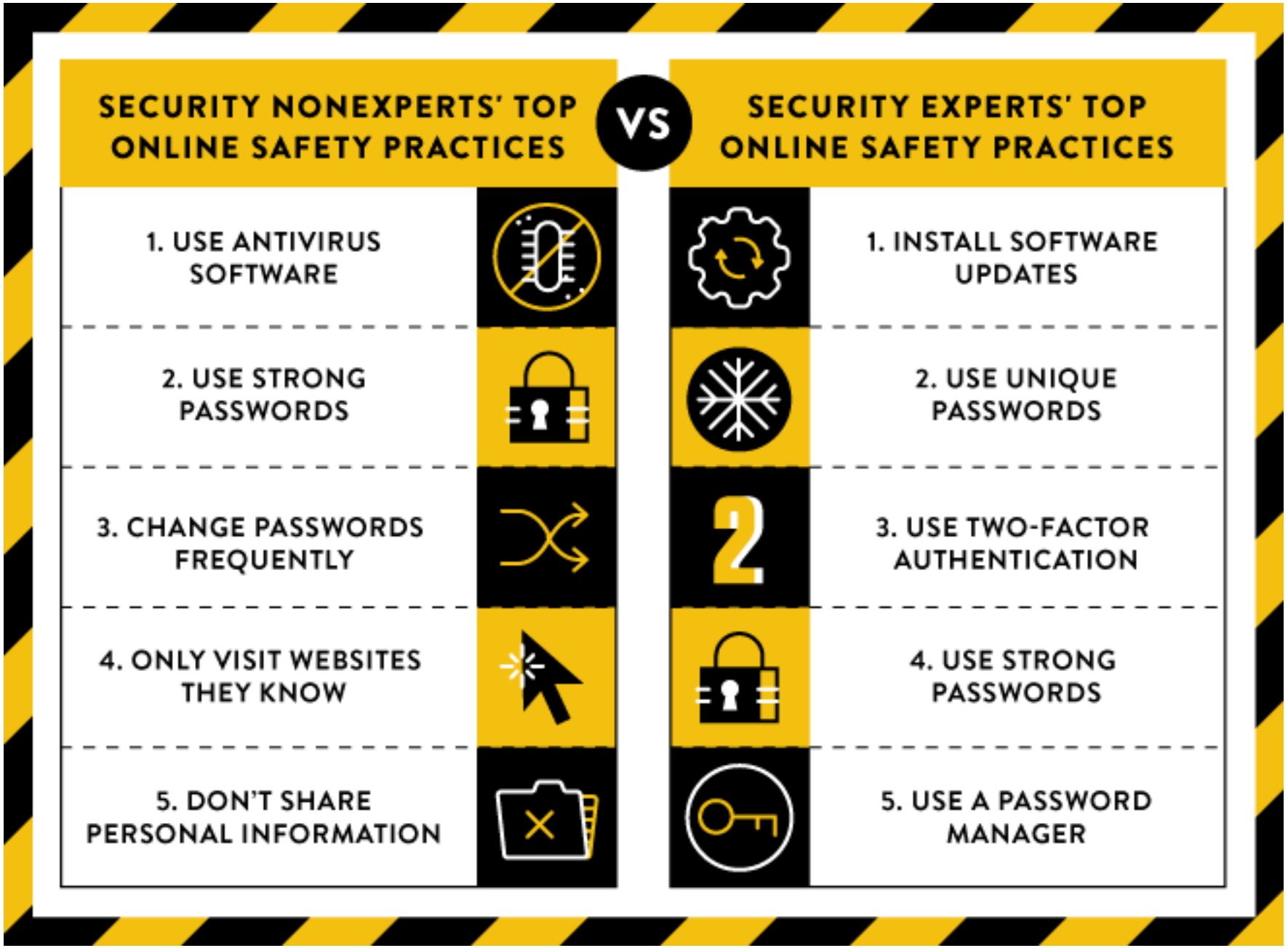
But [PGP] is complicated, especially for someone who had very little skill in programming and computers, like me...

It never became pressing enough for me to stop other things and focus on it.

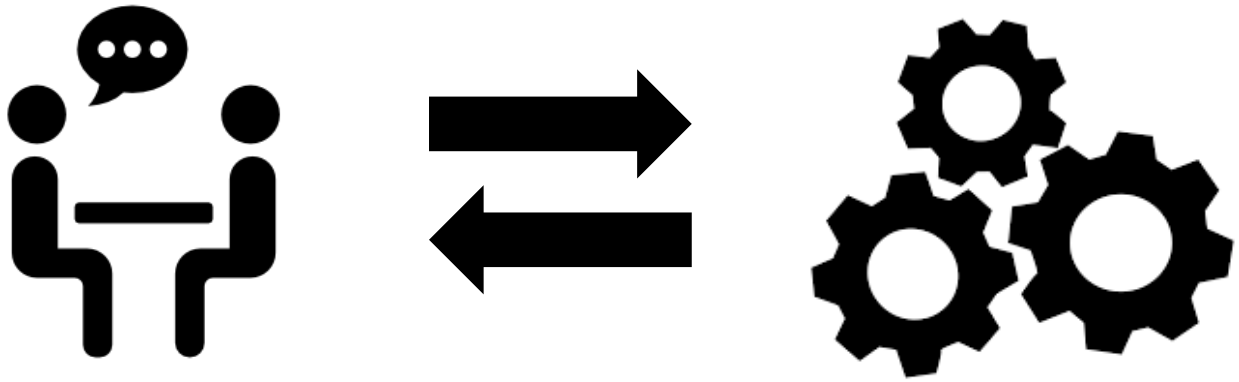




To build effective and usable security/privacy tools, we must work to understand our users.



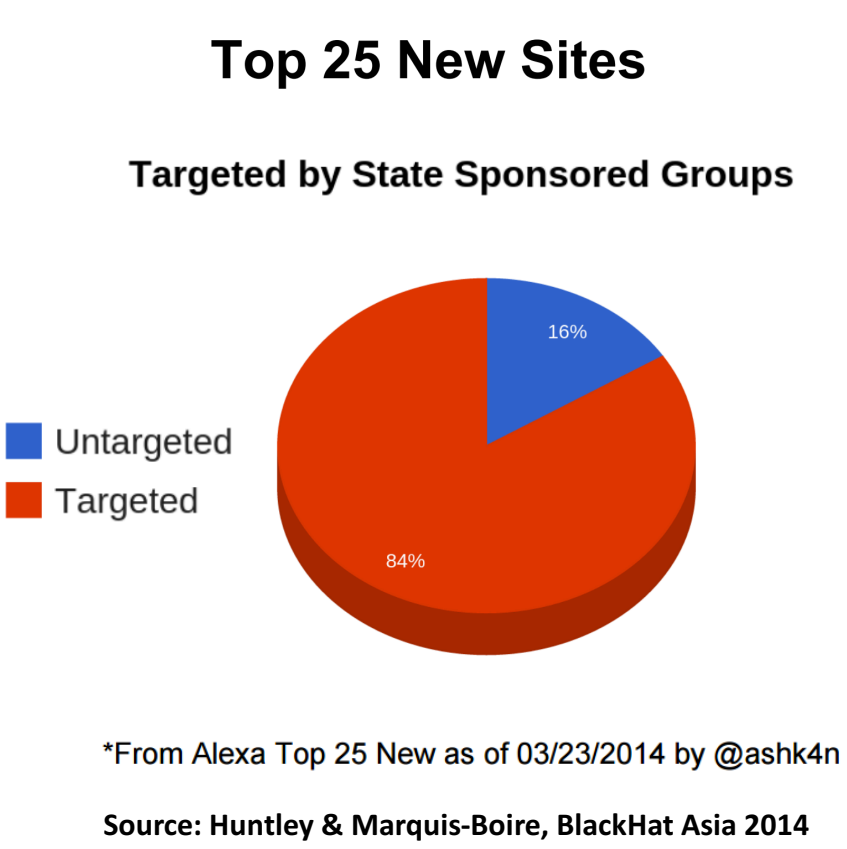
Source: https://security.googleblog.com/2015/07/new-research-comparing-how-security.html, **based on Ion et al., *SOUPS '15***



To build effective and usable security/privacy tools, we must work to understand our users.

This talk: case studies with journalists and lawyers.

Journalists can benefit from security tools…



Google warns journalists and professors: Your account is under attack

A flurry of social media reports suggests a major hacking campaign has been uncovered.

DAN GOODIN - 11/23/2016, 5:15 PM

Washington Post Joins List of News Media Hacked by the Chinese

By NICOLE PERLROTH FEB. 1, 2013

C.I.A. Officer Is Found Guilty in Leak Tied to Times Reporter

By MATT APUZZO JAN. 26, 2015

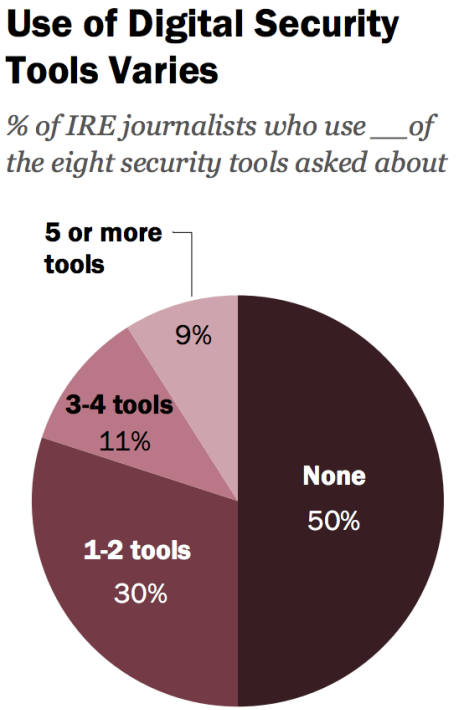
GCHQ captured emails of journalists from top international media

19 January 2015

… but don't often use these tools in practice.



Why not?!



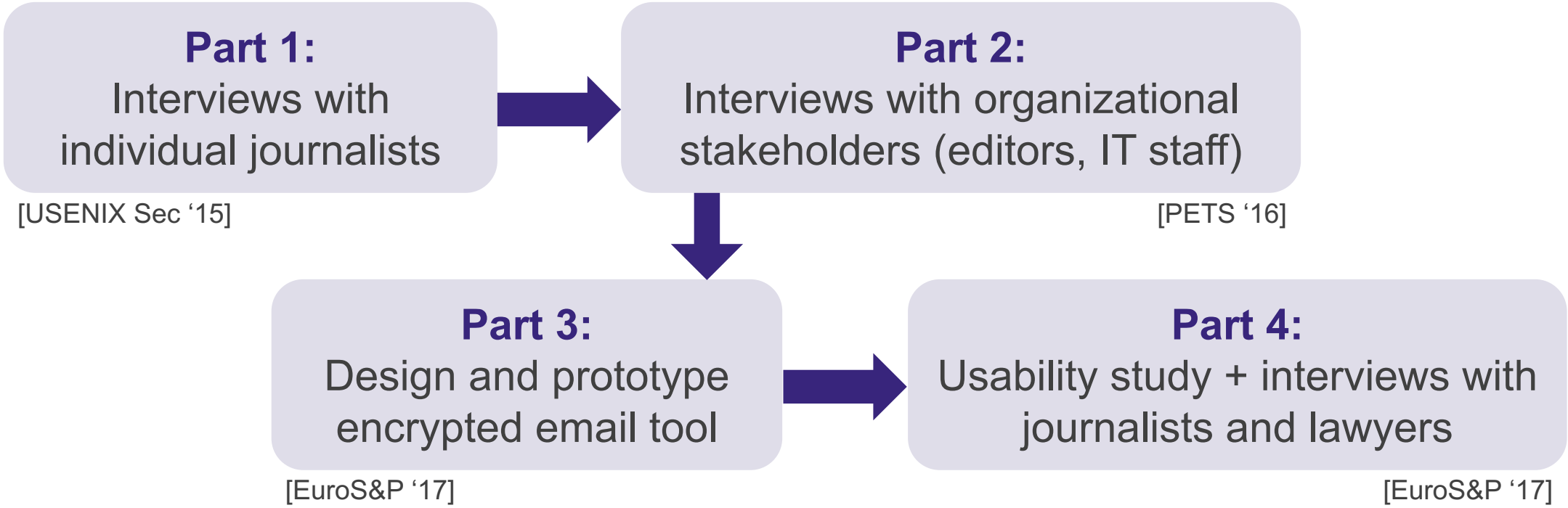
Goals: (1) **Study** the practices, constraints, and needs of journalists & lawyers, to guide (2) the **design** of new technical security/privacy **tools**.

Susan E. McGregor, Polina Charters, Tobin Holliday, and Franziska Roesner. "Investigating the Computer Security Practices and Needs of Journalists." 24th USENIX Security Symposium, August 2015.

Susan E. McGregor, Franziska Roesner, and Kelly Caine. "Individual versus Organizational Computer Security and Privacy Concerns in Journalism." 16th Privacy Enhancing Technologies Symposium (PETS), July 2016.

Ada (Adam) Lerner, Eric Zeng, and Franziska Roesner. "Confidante: Usable Encrypted Email - A Case Study With Lawyers and Journalists." 2nd IEEE European Symposium on Security and Privacy (EuroS&P), April 2017.

Our Process: Collaboration between experts in the journalism, usability, and computer security communities.



Part 1: Interviews with Journalists

Goal: Study individual journalists to understand their *general practices and constraints*, and their *computer security needs, concerns, and threat models.*



x15

Choice of communication technology is often **driven by the source** – and many sources are not tech-savvy.

[The source] probably understand[s] the threat model they're under better than I would. **People's first impression is that they would go by what the source feels comfortable doing. As opposed to stepping in and being paternalistic about it.**



Long-term sources are common, with trust built over time; **truly anonymous sources are rare.**

If I don't know who they are and can't check their background, **I'm not going to use the information they give.**



Part 2: Interviews with Journalistic Orgs



Goal: Identify *differences in computer security related priorities, practices, concerns* between journalists and institutional stakeholders (editors and IT staff).


x7


x7

Journalists and organizational stakeholders share some concerns and perspectives but **differ on others.**

Shared: source protection, reputational risk to organization

Mostly Editors/IT: phishing, passwords, 3rd party apps, finite resources

Journalists and organizational stakeholders share some concerns and perspectives but **differ on others.**

Shared: source protection, reputational risk to organization

Mostly Editors/IT: phishing, passwords, **3rd party apps**, finite resources

> Sometimes I'm just walking through the organization and I'll see someone with an Evernote open—and it's like, **just making sure that you're not putting your source phone numbers in there!** If you want to keep your recipes in there that's fine, but be careful.



Journalists and organizational stakeholders share some concerns and perspectives but **differ on others.**

Shared: source protection, reputational risk to organization

Mostly Editors/IT: phishing, passwords, 3rd party apps, **finite resources**

It's a case of: **Who owns this? Who's going to pay for it?** … Is this a strategic imperative? **Who controls it?**



The lack of universal use of [security technology] is problematic for journalists as well as others.

I had one experience with a prominent lawyer and he said, “Yeah, I’ve heard about this PGP stuff, I’d like to use it,” but he was working for a big firm and his IT department basically said, “No, we just don’t support that.”



Lawyers slow to adopt email encryption and other forms of secure communications, ABA survey finds

POSTED OCT 05, 2015 04:10 PM CDT

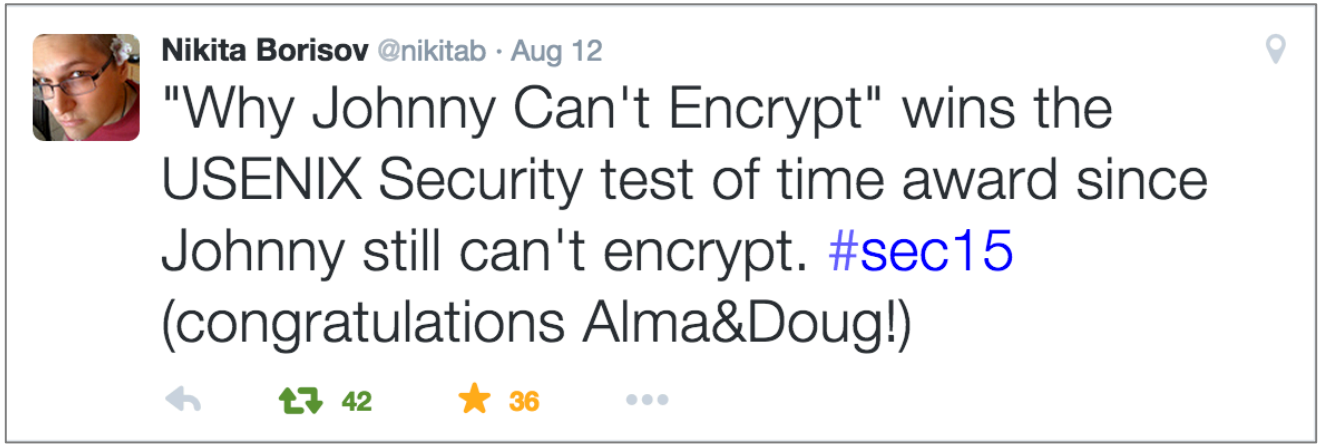
BY VICTOR LI

Part 3: Tool Design and Prototype



Usable Encrypted Email?

Motivation: Journalists frequently use email with sources. Unfortunately, *usable encrypted email is a longstanding problem.*



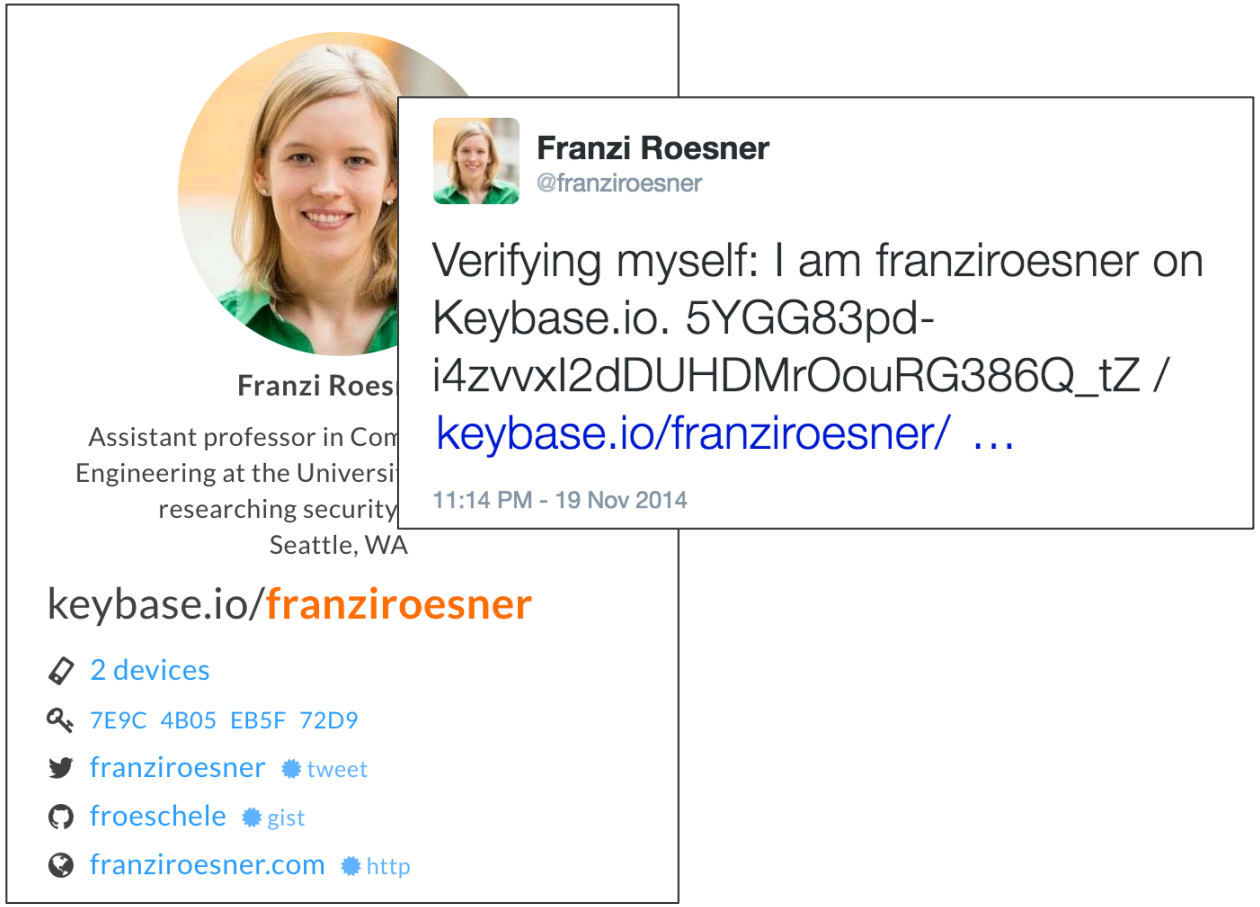
Towards (More) Usable Encrypted Email

What's different now?

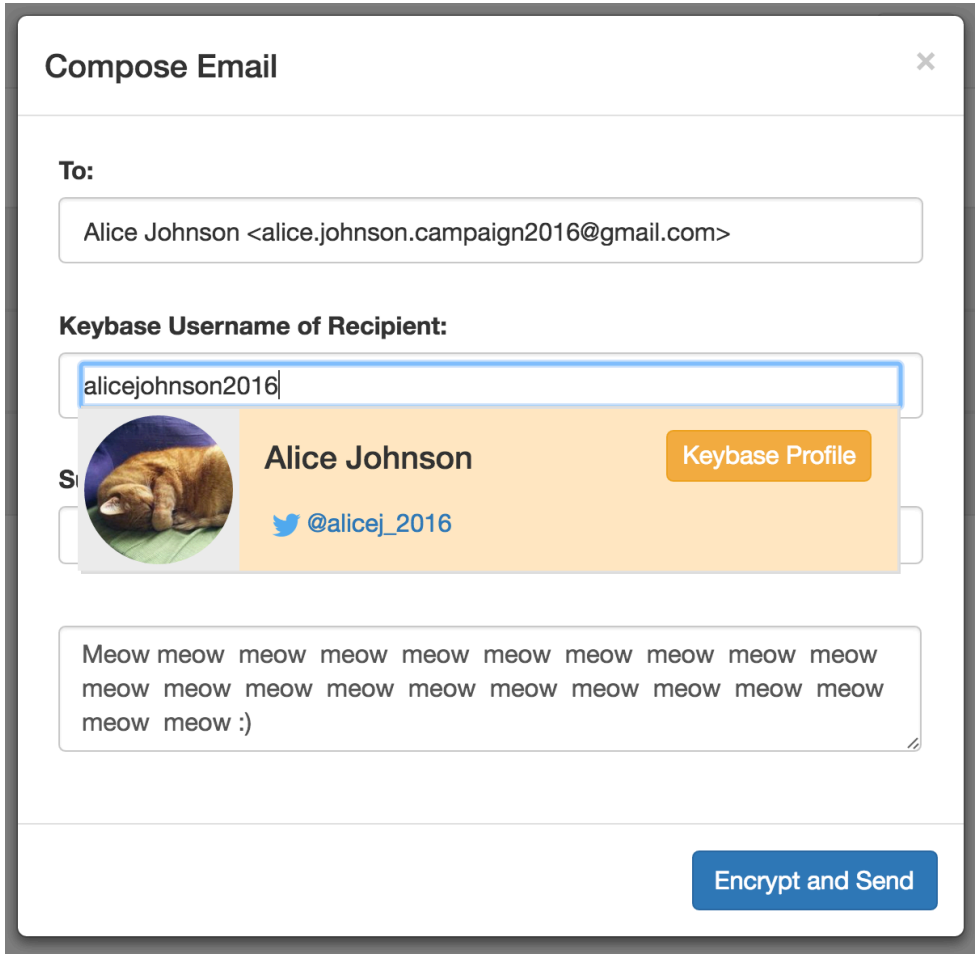
Informally authenticating your contacts' social media accounts is common.

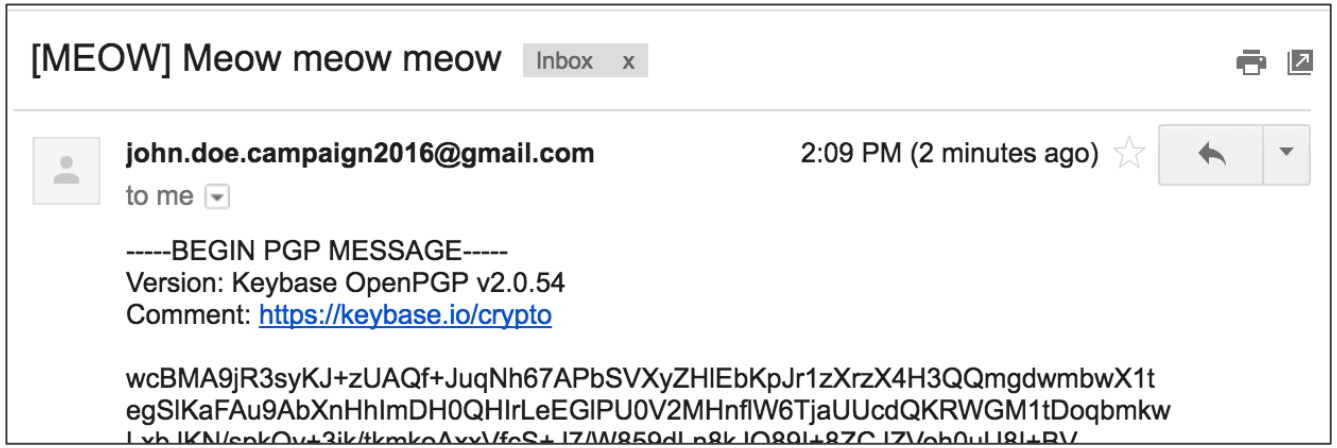
Keybase leverages this: a public key directory with verifiable links to social media profiles.

https://keybase.io



Our Tool: Confidante





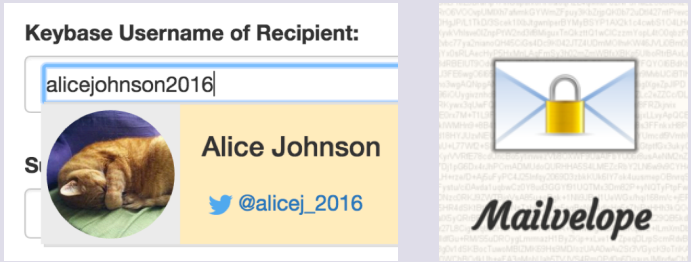


Part 4: Usability Study

Goals: (1) *Evaluate design decisions* we made in Confidante, and (2) more generally, learn more about the *encrypted email use cases and security needs* for journalists and lawyers.


x7


x8



Compare with Mailvelope.

Using Keybase for automated key management is promising: **easy to use, many errors avoided.**

The easiest PGP experience I ever had … I could see, in a way that you never could with PGP before, [sending] a one-page instructional thing on how to set this up, and **trust that [sources] could actually do it themselves.**



It's no different to use than just using Gmail directly.



If something like this caught on, **I could see putting my Keybase on my business card**, or putting it in the signature line of my email.



Security concerns and usability challenges remain...

For example:

- Lack of trust (“too easy”)
- Drawing suspicion
- No metadata protection
- Private key management

Because this is so easy… **it really feels like there must be something wrong**... [PGP is] a rite of passage.



[Sources]... would say “Is this actually going make it more likely for this to **raise a red flag with my employer**?”



Journalists and lawyers have **different operational constraints** and **different threat models.**

Examples: Sources vs. clients, Technical vs. legal protections

Attorney-client privilege is… sacrosanct.

If I have a document that's a privileged document, **if somebody breaks into my office and looks at it, that doesn't defeat the privilege.** But if I leave it out where somebody walking by can see it, that could. So you'd have to take **reasonable precautions**.





Part 1:
Interviews with individual journalists

Part 2:
Interviews with organizational stakeholders (editors, IT staff)

Part 3:
Design and prototype encrypted email tool

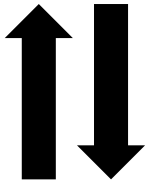
Part 4:
Usability study + interviews with journalists and lawyers

Conclusion

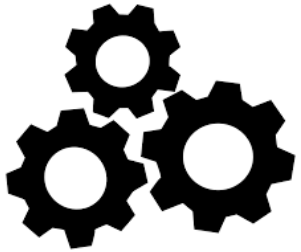
Study and test with target user groups: Our tools must be informed by their security needs and operational constraints.



One size doesn't fit all: Different groups may need *entirely different tools.*



Going forward: Study these and other user groups and build/evaluate tools in those contexts.



Acknowledgements



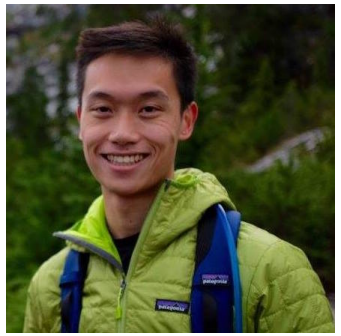
Kelly Caine
(Clemson)



Susan McGregor
(Columbia)



Ada Lerner
(UW)



Eric Zeng
(UW)

Additional collaborators:
Polina Charters (UW)
Tobin Holliday (UW)
Byron Lowens (Clemson)
Mahdi Nasrullah Al-Ameen (Clemson)
Mitali Palekar (UW)
Elizabeth Watkins (Columbia)



This work is supported in part by NSF Awards CNS-1463968 and CNS-1513575.



Thanks!

franzi@cs.washington.edu

@franziroesner

https://www.franziroesner.com

