

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

USENIX Security 2017

Susan E. McGregor

Columbia Journalism School
Elizabeth Anne Watkins
Columbia University



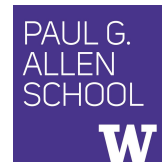
Kelly Caine

Clemson University
Mahdi Nasrullah Al-Ameen
Clemson University



Franziska Roesner

University of Washington



This work is supported in part by the National Science Foundation under Awards CNS-1513575, CNS-1513875, and CNS-1513663.

Failure is common in computer security

**Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0**

DNC Hacks: How Spear Phishing Emails Were Used

**Six million Verizon accounts
exposed after cloud server
security flaw**

And users are often implicated

The Human Element: The Weakest Link in Information Security

Amazon's massive AWS outage was caused by human error

The Biggest Threat To Data Security? Humans, Of Course

How do we transform this narrative?

Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security

The weakest link revisited [information security]

WATCH - The Weakest Link

WATCH Series - Kelly Caine - Sept 15, 2016 - Noon - Room 110

September 15, 2016 12:00 PM to

September 15, 2016 1:00 PM

NSF Room 110

Case Study

THE PANAMA PAPERS

Politicians, Criminals and the Rogue Industry That Hides Their Cash

- ~400 journalists
- >120 news organizations
- >2.5TB of leaked documents
- Led by the International Consortium of Investigative Journalists (ICIJ).

Our Team | Our Work

Journalism,
computer
security and
human factors
experts

- In-depth interviews with all ICIJ team members on the project (5)
- Analysis of 118 survey responses from participating journalists

The Panama Papers' Security: What We Know

Over the year-long investigation, this diverse and globally-distributed group **maintained key security goals:**

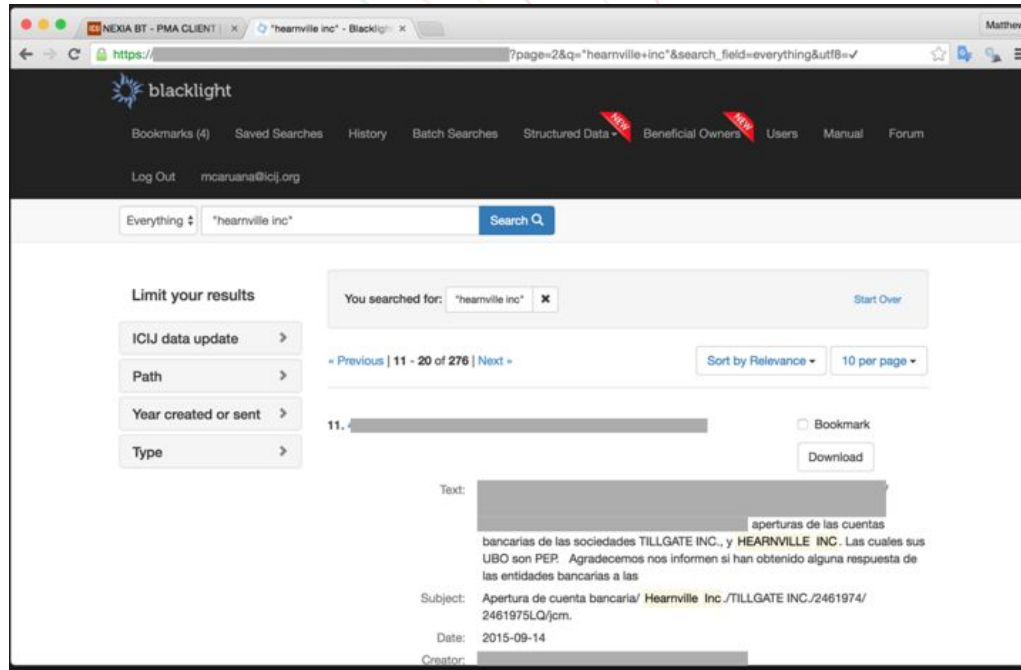
- Protecting the source of the data
- Maintaining control of the documents and preventing their early disclosure
- Maintaining access to the documents for collaborators and protecting them from attackers
- Keeping the project secret

The Panama Papers' Security: What We *Don't* Know

To the best of ICIJ's knowledge, they met their own security goals. We note, however, that:

- We cannot know definitively that there were *zero* security compromises
- These systems/approaches aren't perfect
- Seeking expert advice (as ICIJ did) and following best practices is always essential; threats and capacities will change

Background: ICIJ's Collaboration Systems



Blacklight document search platform

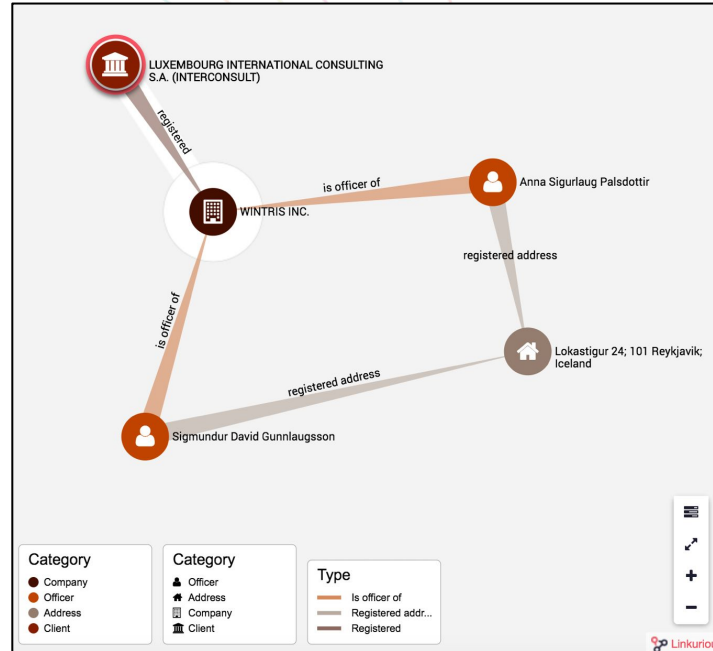
Background: ICIJ's Collaboration Systems

The screenshot displays the Global I-Hub forum interface. At the top, there is a navigation bar with 'Project categories' and 'Project' dropdowns, a search bar, and user information for Matthew Caruana Galizia. The main header features the ICIJ logo and the text 'THE INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS'. Below the header is a navigation menu with 'MAIN', 'FORUM', 'GROUPS', 'FILES', 'LINKS', 'MEMBERS', 'EVENTS', and 'SEARCH'. The main content area is titled 'GENERAL CHAT | FORUM' and includes a pagination control showing pages 1 through 10. A table of forum posts is displayed with columns for Topic, Project, Replies, Views, and Last Reply. A chat window is open on the right side of the screen, showing a list of contacts and a search bar.

	Topic	Project	Replies	Views	Last Reply
NEW STICKY	Let's share impact/results here!	Prometheus	122	2141	Last Reply by Bastian Oberme 3 hours ago
NEW STICKY	SHARE YOUR PLANS - sharing news lists so we can help promote your stories	Prometheus	62	1521	Last Reply by Arlen Cerda Ma
NEW STICKY	Database release May 9!!	Prometheus	35	1187	Last Reply by Edmund Tadros May 14
NEW STICKY	Statement from the source	Prometheus	40	576	Last Reply by Wahyu Dhyatni May 6

Global I-Hub forum

Background: ICIJ's Collaboration Systems



Linkurious network visualization

Findings: Threat Model

- Not entire governments, but implicated politicians
- Companies whose activities were revealed
- Other newsrooms
- Criminals

Findings: System Design

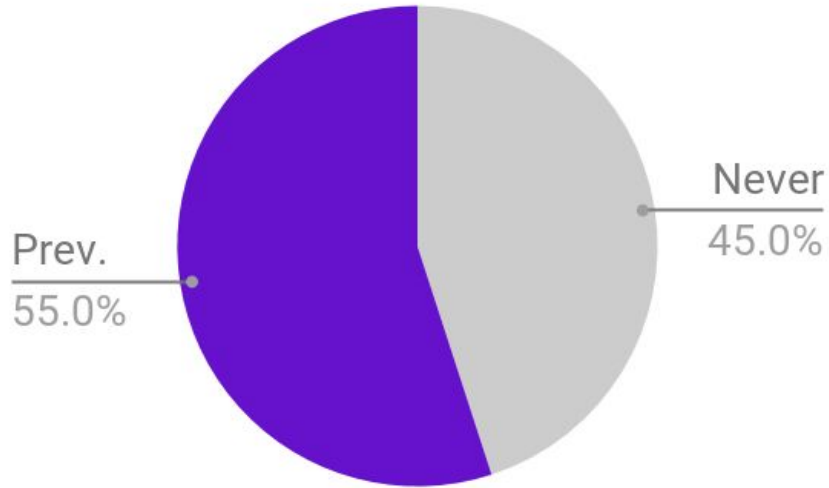
- Data and document systems were centralized in order to support the scale and control requirements of the project
- All systems relied on well-tested HTTPS

Findings: System Design

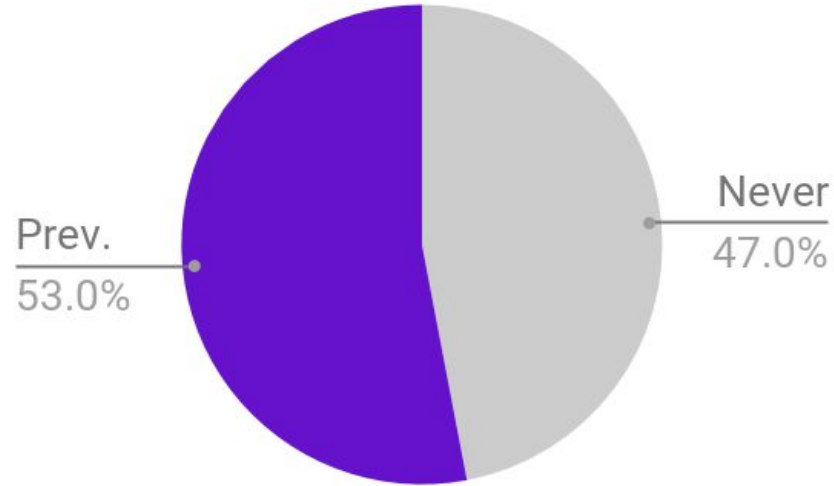
- Though designers considered approaches like **CryptDB** they had concerns about its efficacy for their use case, *and* about the maturity/support for the system
- Keeping **system URLs secret** was essential, as they lacked the resources to handle DDoS attacks.

Findings: Security Technology Use

At the start of the project



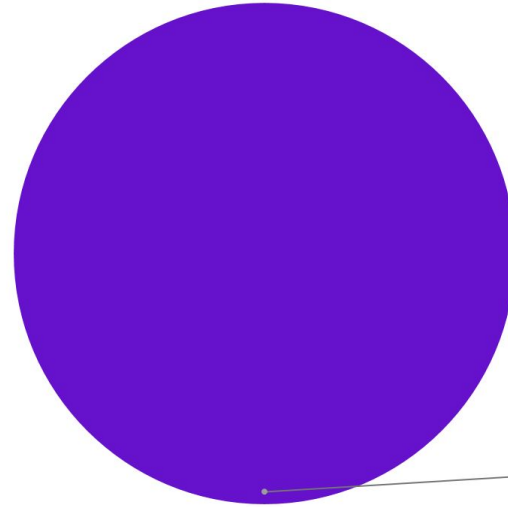
45% had never used two-factor



47% had never used PGP

Findings: Security Technology Use

By the end of the project



100% were using two-factor and PGP

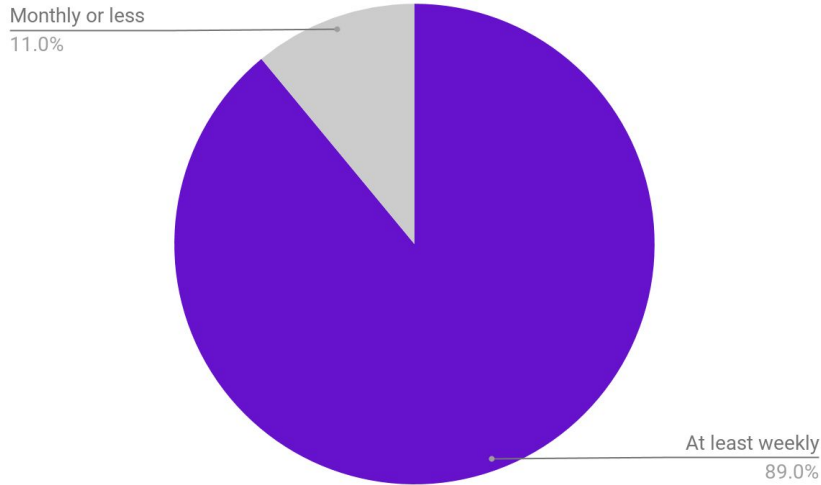
Findings: System Design

Multiple forms of two-factor were considered, including:

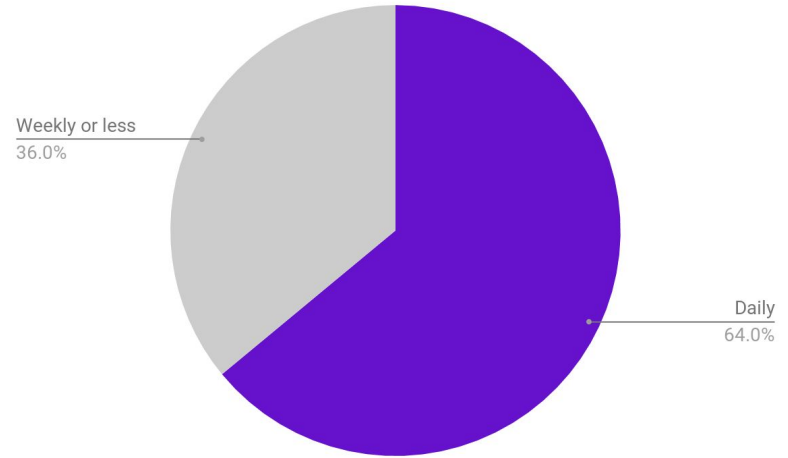
- Virtual machines
- Browser extensions
- Smartphone app

Findings: ICIJ Technology Use

In the 3 months prior to publication



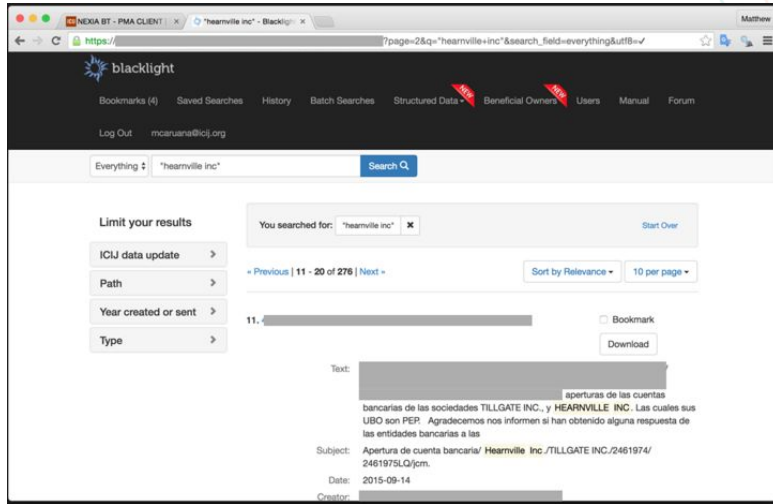
89% were using the Global I-Hub at least weekly



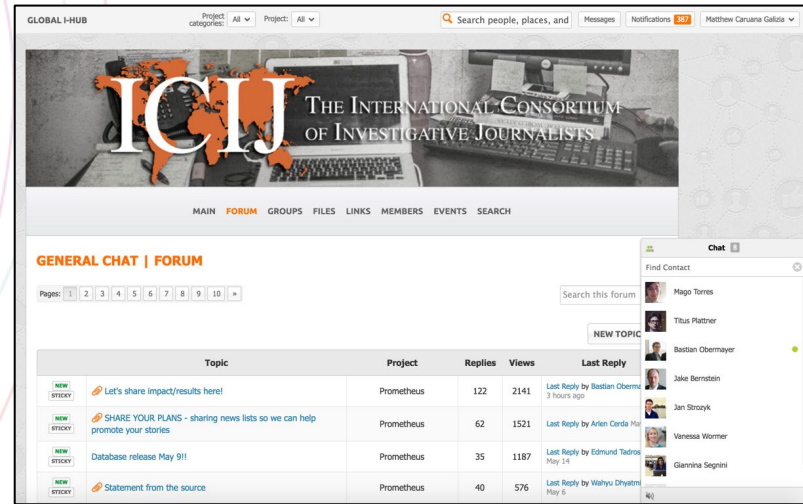
64% were using Blacklight daily

Findings: ICIJ Technology Use

Blacklight document search platform



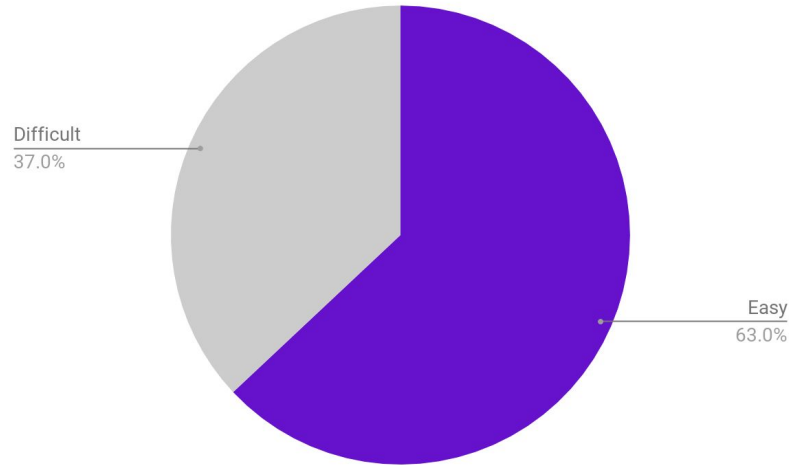
Global I-Hub forum



Both platforms required two-factor for every sign-on!

Findings: Security Technology Use

And yet...



63% rated security compliance "easy"

Takeaway

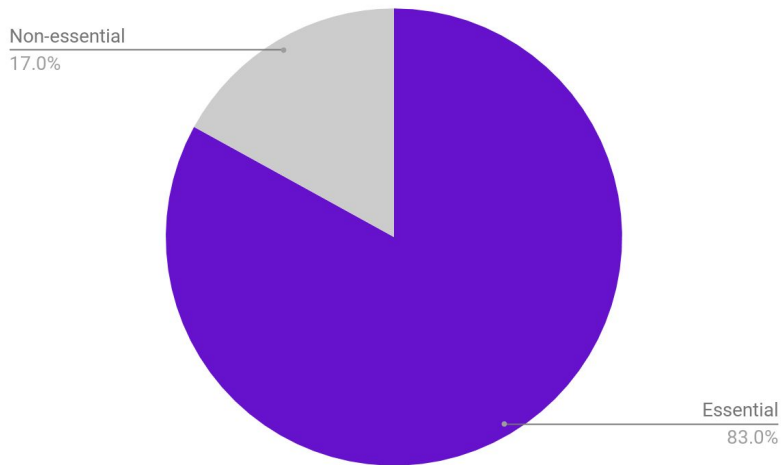
Usable, flexible security protocols can help minimize the use of workarounds

For colleagues who are not that experienced with PGP or Signal or whatever...[the I-Hub is] a good way to write secure emails or messages to each other.

Takeaway

The fact that these tools **helped journalists complete core job tasks** made the relatively stringent security requirements an acceptable tradeoff.

Findings: ICIJ Technology Use

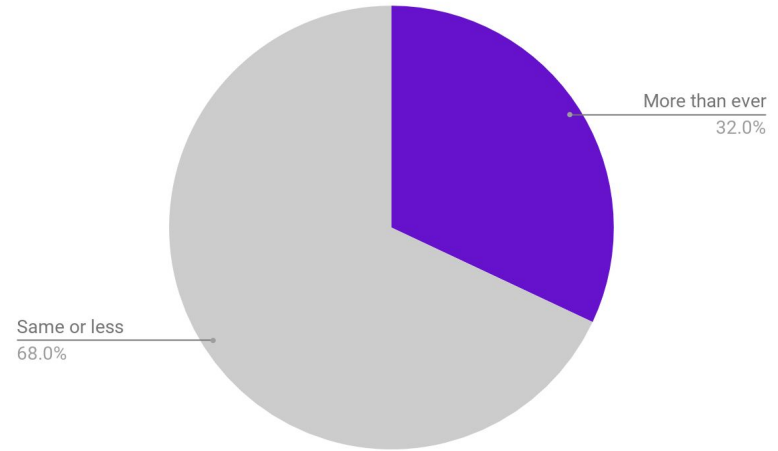


83% found ICIJ's data tools
"essential"

Findings: Collaboration

Collaboration and community-building was an **explicit goal** for the system designers

- Adapted I-Hub from the open-source social network Oxwall in part because of its community-oriented features



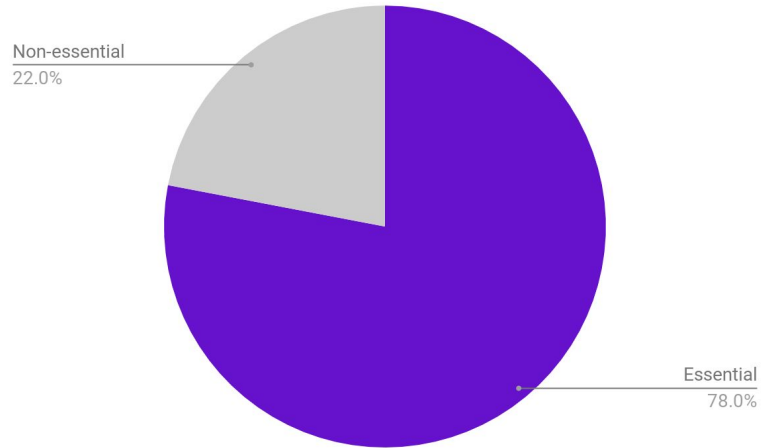
32% collaborated
"more than ever"

As one ICIJ editor described it:

You cannot collaborate on email, or encrypted email, or Signal. You need a real space that feels comfortable and friendly and it's colorful, and [I-Hub] was.

You can upload files, you can “like” a topic...that simple kind of “liking” thing also helped reporters bond together and encourage one another.... it just helped tremendously with providing a sense of team.

Findings: ICIJ Technology Use



78% found ICIJ's coordination efforts "essential"

Findings: Ongoing Emphasis on Security

In every editorial note I would write, I would remind [contributors] about some security measure, how it takes one of us to make a mistake for the whole thing to basically fall to hell, and you would lose an entire year of work, and we would be—a joke basically. Nobody would ever come to us again with any confidential information. So, I would remind them so they didn't feel comfortable and too confident.

Takeaway

Normalize security practices and establish secure defaults

In this project we just routinely encrypted everything we wrote...Because we were just used to doing it and that helped us a lot as a team, that we understood that it's not such a big thing, it's not such a pain in the ass—but you're always on the safe side of it.

Findings: User Involvement

One of the most-valued system features -- batch search on Blacklight -- was suggested by a user.

Takeaway

Open communications between technologists and users is key

It's great, it's just software that is designed for journalists. . . and that's all we care about.

Takeaway

Cultivate organizational commitment to sustainable technology solutions

There is a tendency... to have this kind of quick solution and where it puts the load of the problem onto staff....Selling [long-term technical solutions] is a little difficult to directors... But when you do implement it, it works beautifully I think, and becomes an example to other organizations.


Summary

We worked closely with ICIJ to understand the systems and processes they used to achieve support & adoption for strong security protocols in the Panama Papers project through:

- Building **security buy-in and resource dedication** from both editorial *and* technology personnel
- Actively engaging with users to **ensure secured systems were as useful as possible**
- **Normalizing secure, flexible defaults** with applicability beyond the immediate project
- Seeking **professional security advice** and treating **security as an ongoing effort**

Thanks

This work would not have been possible without the support of the following:

- ICIJ editors and Data Team
- The Panama Papers journalists and survey participants
- Paper shepherd and session chair Adrienne Porter Felt
-  NSF Awards CNS-1513575, CNS-1513875, and CNS-1513663
- Advisory board for NSF project:
 - Sarah Cohen, Bryan Ford, Roxana Geambasu, Angela Sasse and Trevor Timm

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

USENIX Security 2017

Susan E. McGregor

Columbia Journalism School
Elizabeth Anne Watkins
Columbia University



Kelly Caine

Clemson University
Mahdi Nasrullah Al-Ameen
Clemson University



Franziska Roesner

University of Washington



This work is supported in part by the National Science Foundation under Awards CNS-1513575, CNS-1513875, and CNS-1513663.