

# Security & Privacy for Existing and Emerging Technologies

Franziska (Franzi) Roesner

Assistant Professor

University of Washington

[franzi@cs.washington.edu](mailto:franzi@cs.washington.edu)



PAUL G. ALLEN SCHOOL  
OF COMPUTER SCIENCE & ENGINEERING



UNIVERSITY of WASHINGTON

SECURITY AND PRIVACY  
RESEARCH LAB

What security & privacy issues  
are we facing **today**?

This talk: secure communication for journalists (etc.)

What security & privacy issues will arise in  
the **future**, with emerging technologies?

This talk: security & privacy for augmented reality



# Part 1: Computer Security for Journalists

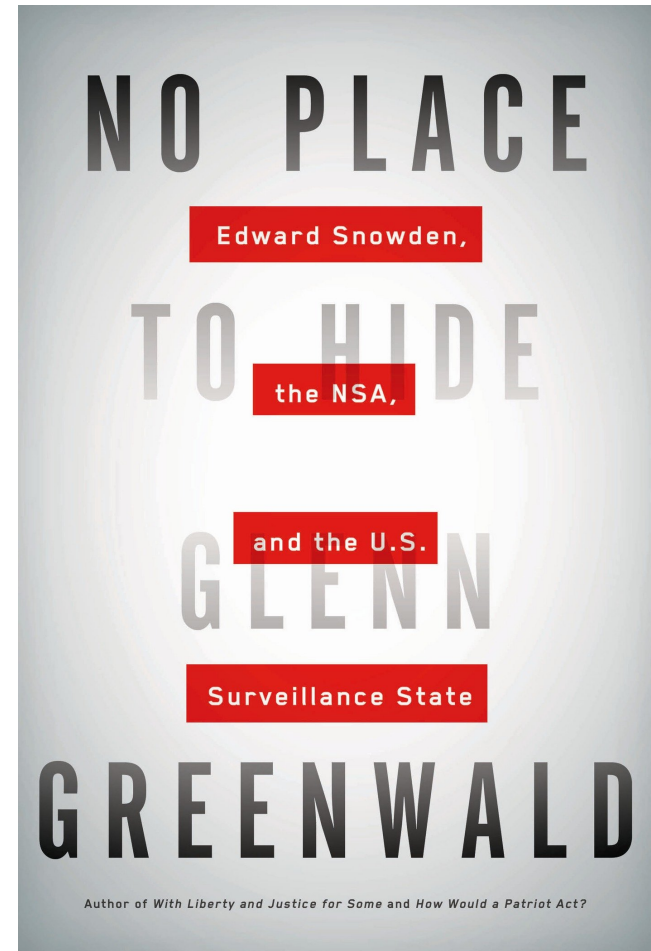




Using encryption software was something I had long intended to do...

**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.**

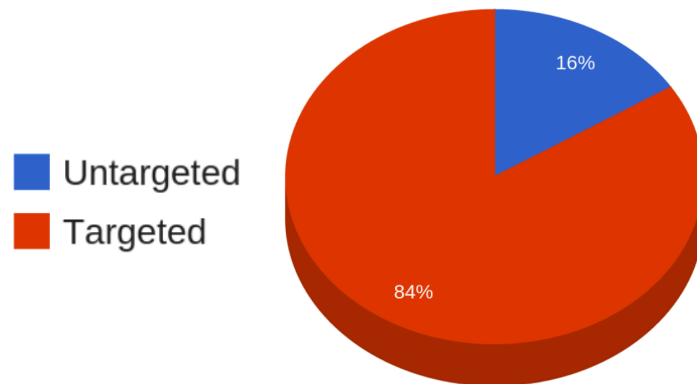




# Journalists can benefit from security tools...

## Top 25 New Sites

Targeted by State Sponsored Groups



\*From Alexa Top 25 New as of 03/23/2014 by @ashk4n

Source: Huntley & Marquis-Boire, BlackHat Asia 2014

### 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

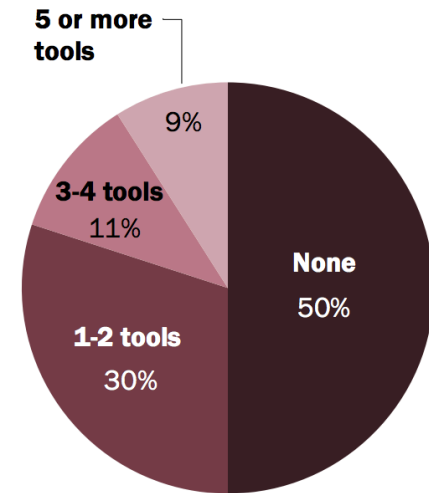
... but don't often use these tools in practice.



Why not?!

### Use of Digital Security Tools Varies

*% of IRE journalists who use \_\_\_ of the eight security tools asked about*



IRE Journalists Survey. Dec. 3 - 28, 2014. Q24, Q25.

Source: Pew Research Center



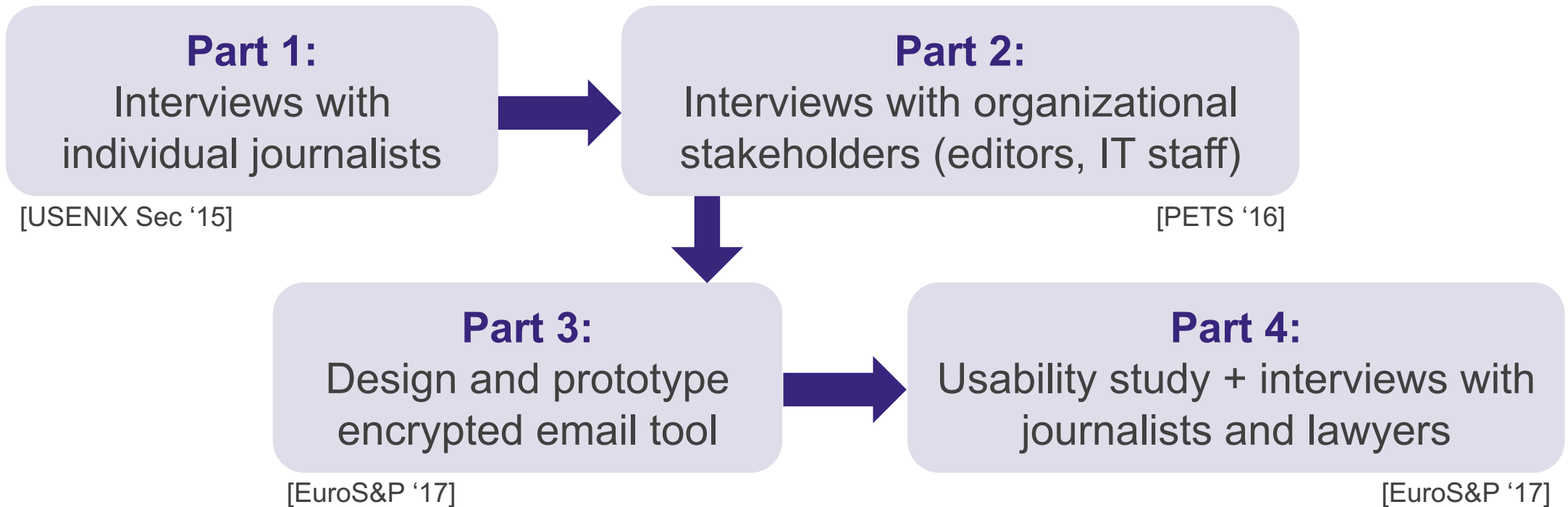
**Goals:** (1) **Study** the practices, constraints, and needs of journalists & lawyers, to guide (2) the **design** of new technical security/privacy **tools**.

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.





# 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.**



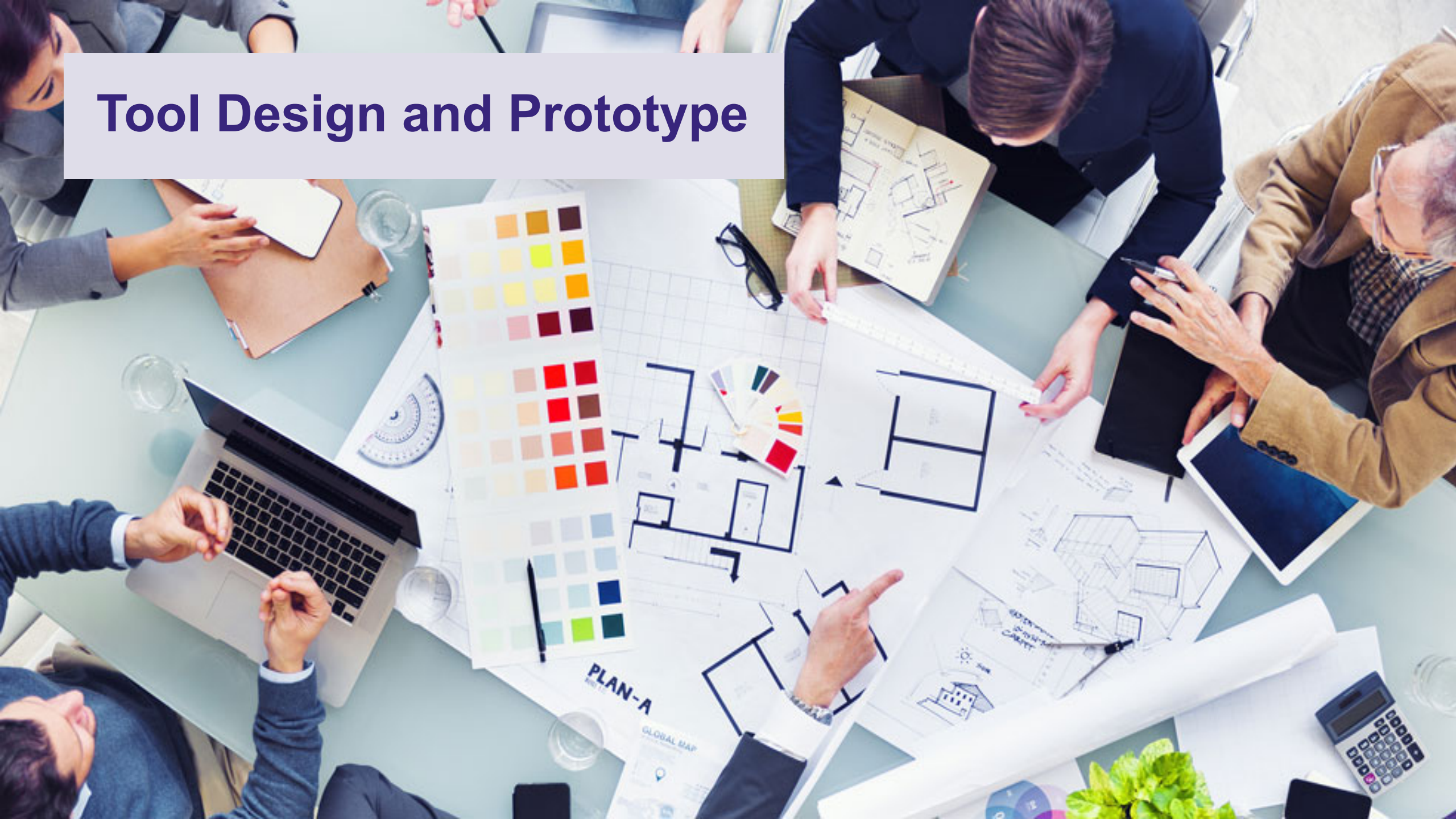


Long-term sources are common, with trust built over time; **truly anonymous sources are rare.**

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

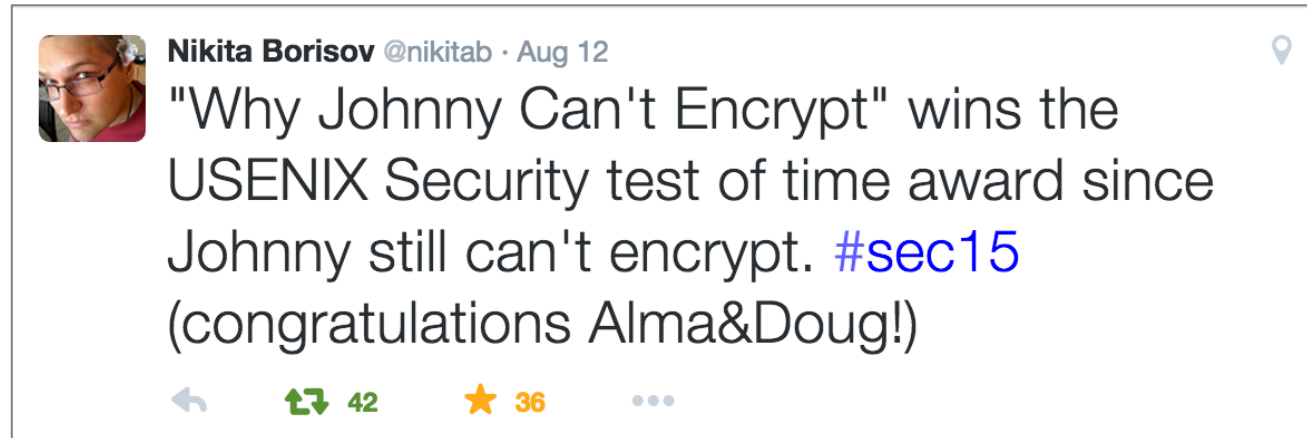


# Tool Design and Prototype



# Usable Encrypted Email?

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





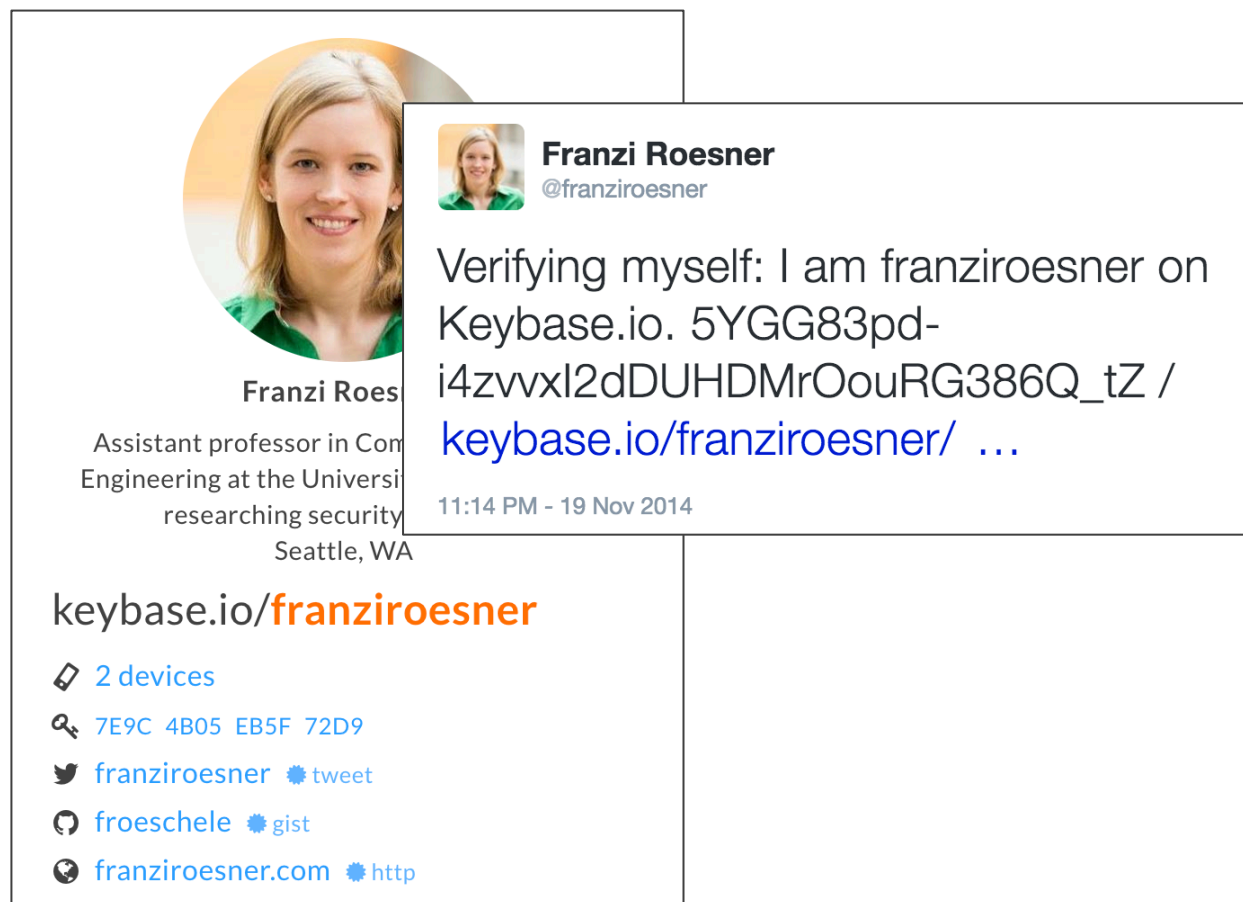
# Towards (More) Usable Encrypted Email

## 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>



The image shows a screenshot of a Keybase profile for Franz Roesner. The profile includes a circular profile picture of a woman with blonde hair, a bio identifying her as an assistant professor in Computer Engineering at the University of Washington, and a list of verifiable links to her social media profiles. A tweet from her is also visible, where she verifies her identity on Keybase.io.

**Franzi Roesner**  
Assistant professor in Computer Engineering at the University of Washington, researching security in Seattle, WA

keybase.io/**franziroesner**

- 2 devices
- 7E9C 4B05 EB5F 72D9
- franziroesner tweet
- froschele gist
- franziroesner.com http

**Franzi Roesner** @franziroesner  
Verifying myself: I am franziroesner on Keybase.io. 5YGG83pd-i4zvxl2dDUHDMrOouRG386Q\_tZ / [keybase.io/franziroesner/](https://keybase.io/franziroesner/) ...  
11:14 PM - 19 Nov 2014

# Our Tool: Confidante

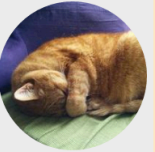
### Compose Email


To:

Alice Johnson <alice.johnson.campaign2016@gmail.com>

Keybase Username of Recipient:

alicejohnson2016

 **Alice Johnson** Keybase Profile


 @alicej\_2016

Meow meow :)

**Encrypt and Send**

### [MEOW] Meow meow meow

Inbox x

 **john.doe.campaign2016@gmail.com** 2:09 PM (2 minutes ago) ☆

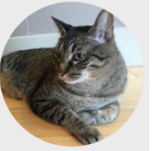
to me ▾



-----BEGIN PGP MESSAGE-----  
Version: Keybase OpenPGP v2.0.54  
Comment: <https://keybase.io/crypto>

wcBMA9jR3syKJ+zUAQf+JuqNh67APbSVXyZHIEbKpJr1zXrzX4H3QQmgdwmbwX1t  
egSIKaFAu9AbXnHhImDH0QHlrLeEGIPU0V2MHnflW6TjaUUcdQKRWGM1tDoqbmkw  
LxbJKN/epkOvt3ik#krmkeAxyV/fcS+I7/M859dLp8kIQ80L+87CJ7Veb0uL8L+BV

Meow,  
Meow meow

Message was signed by:

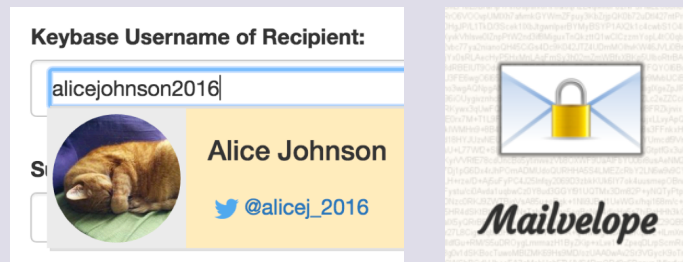
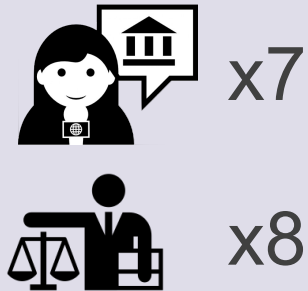
 **John Doe** Keybase Profile

 @jdoe\_campaign16  johndoecampaign

**Reply**

# 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.



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 to 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.**

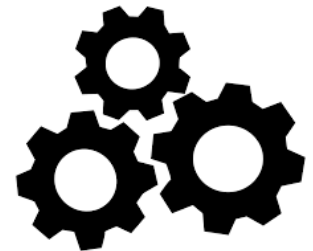
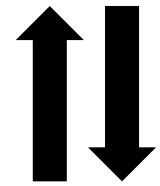


# Conclusions (Part 1)

**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.



## Part 2: Security & Privacy for Augmented Reality



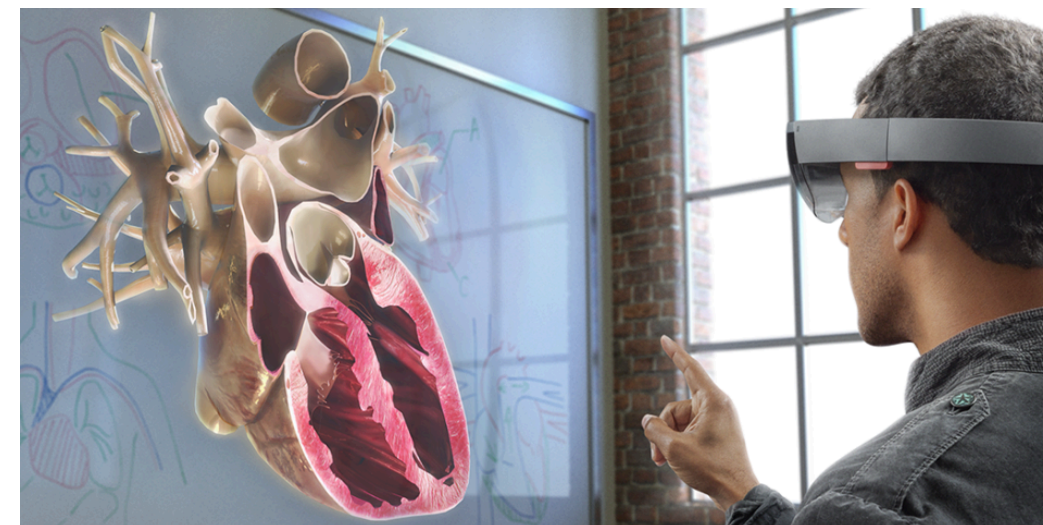


# Augmented Reality (AR)

## Our definition:

Computer-generated **audio, visual, and/or haptic feedback** is **overlaid on the user's perception** of the **real world** in **real-time**.

# Current and Emerging AR



# Future AR Systems

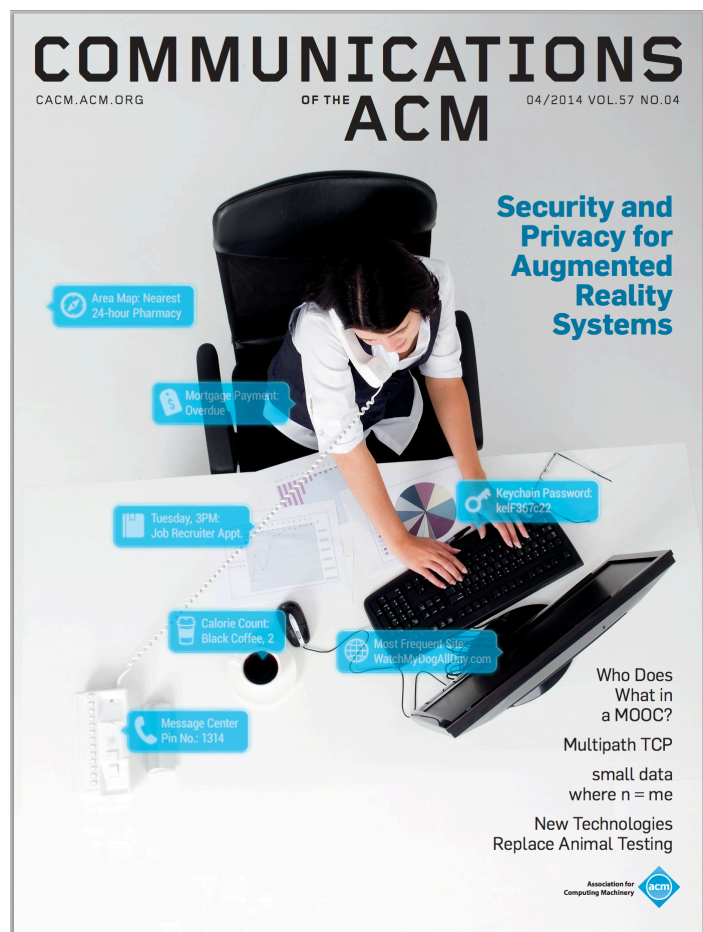
## Today vs. Tomorrow

One app at a time **vs.** Many concurrent apps  
Few, trusted developers **vs.** Tons of third-party apps  
App on by command **vs.** Background apps  
2D annotations **vs.** 3D virtual objects  
Synthetic annotations **vs.** Virtual object interactions

Security and privacy?



# Identifying Security & Privacy Challenges



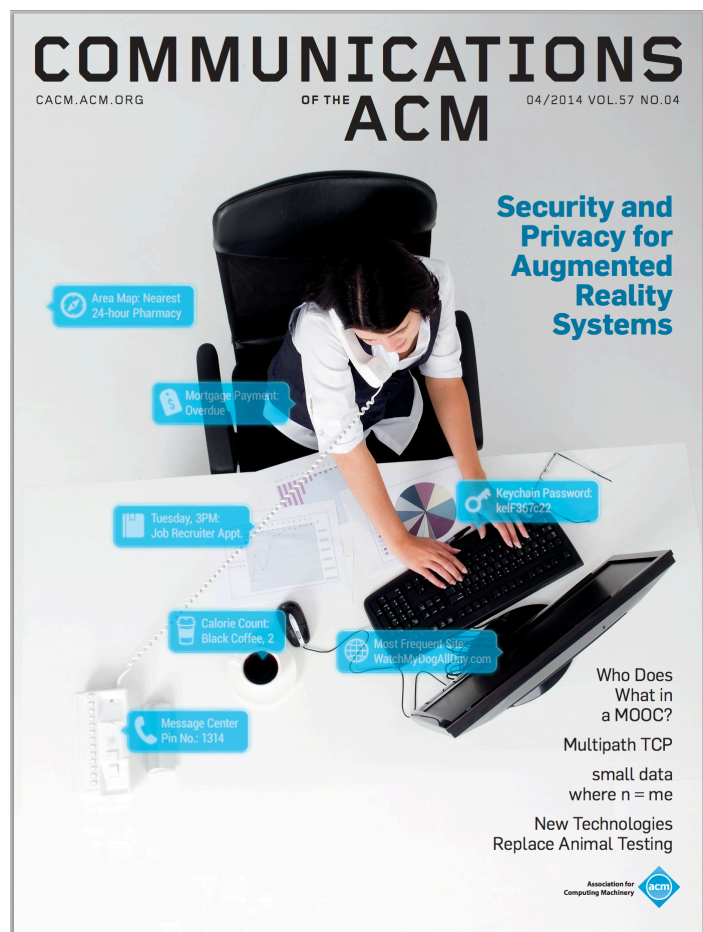
## Challenges along two axes:

1. Single AR app, Multiple apps, Multiple systems
2. Input, Output, Data access

F. Roesner, T. Kohno, D. Molnar. "Security and Privacy for Augmented Reality Systems." *Communications of the ACM*, April 2014.



# Identifying Security & Privacy Challenges

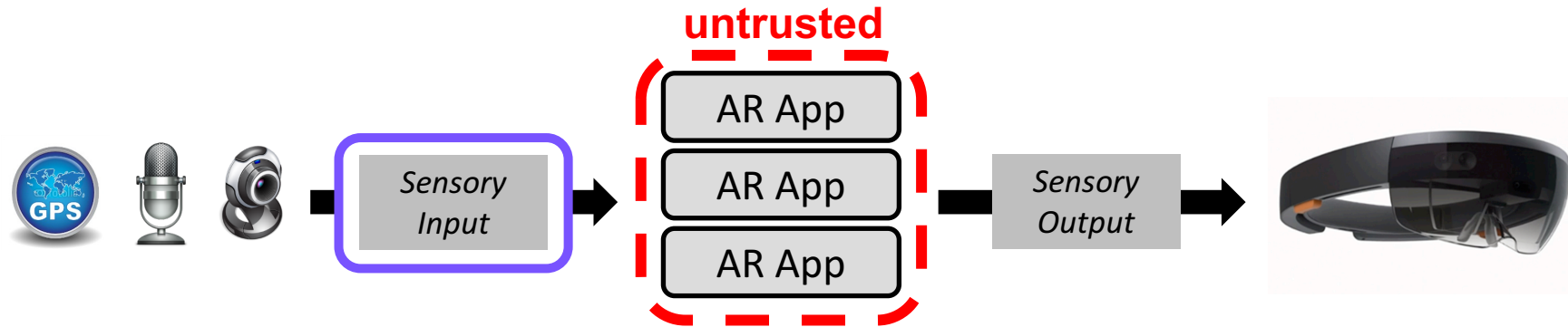


**Challenges along two axes:**

1. **Single AR app, Multiple apps**, Multiple systems
2. **Input, Output**, Data access

F. Roesner, T. Kohno, D. Molnar. “Security and Privacy for Augmented Reality Systems.” *Communications of the ACM*, April 2014.

# Input Privacy

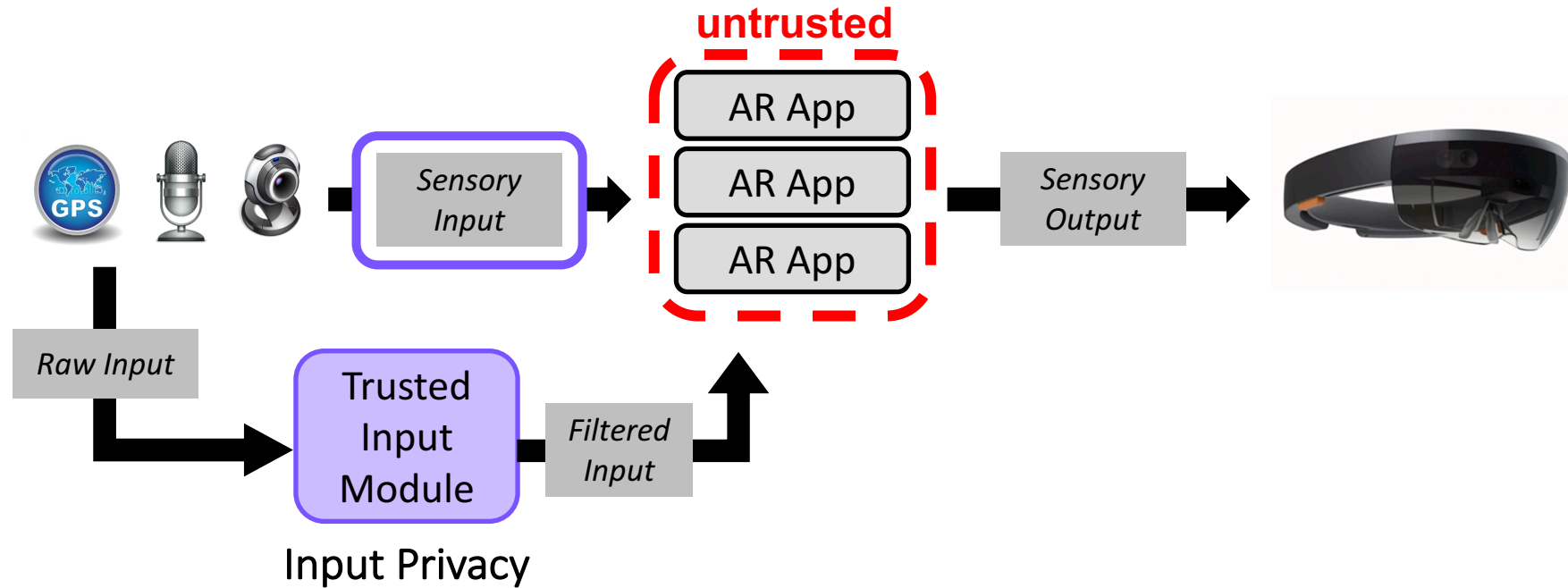


## Seattle dive bar becomes first to ban Google Glasses over privacy fears

By NINA GOLGOWSKI

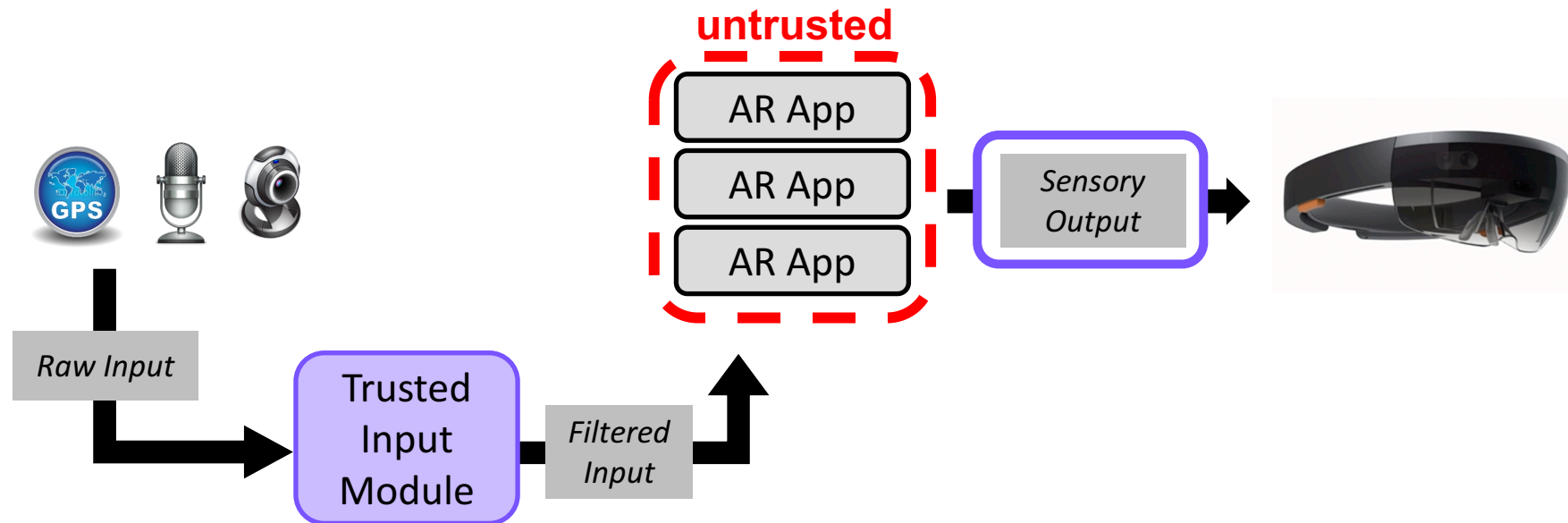
PUBLISHED: 00:43 EST, 10 March 2013 | UPDATED: 02:16 EST, 10 March 2013

# Input Privacy



- *Jana et al., USENIX Security '13*
- *Roesner et al., CCS '14*
- *Templeman et al., NDSS '14*
- *Raval et al., MobiSys '16*

# Output Security







Hyper Reality (<https://www.youtube.com/watch?v=YJg02ivYzSs>)

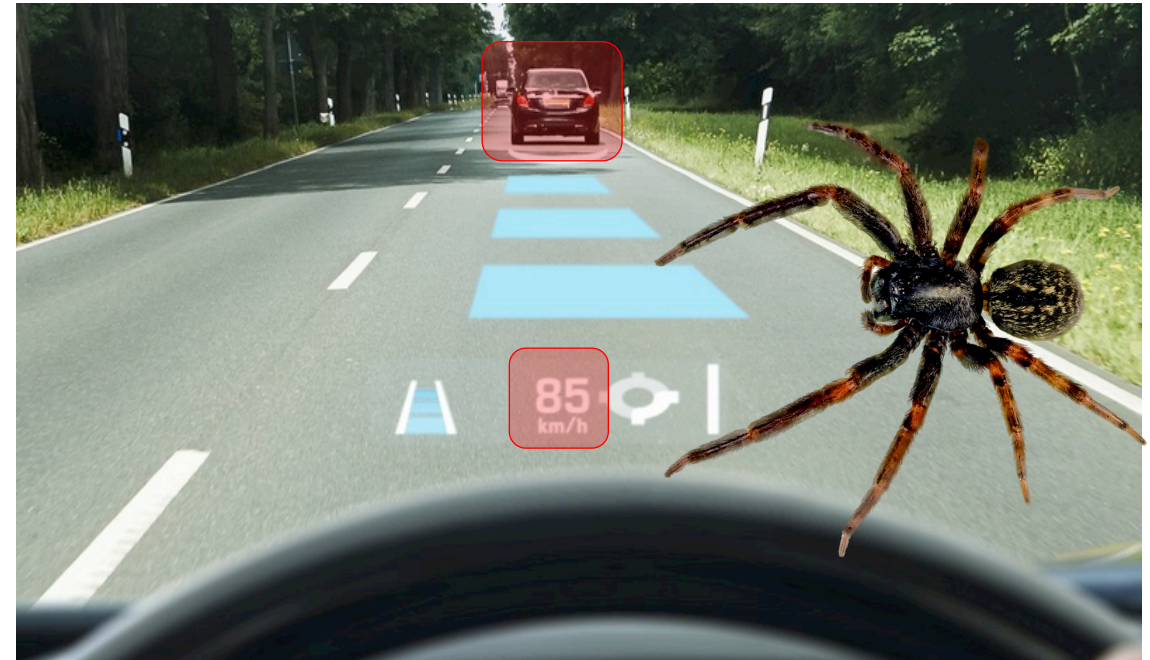
# Output Security

A buggy or malicious app might...

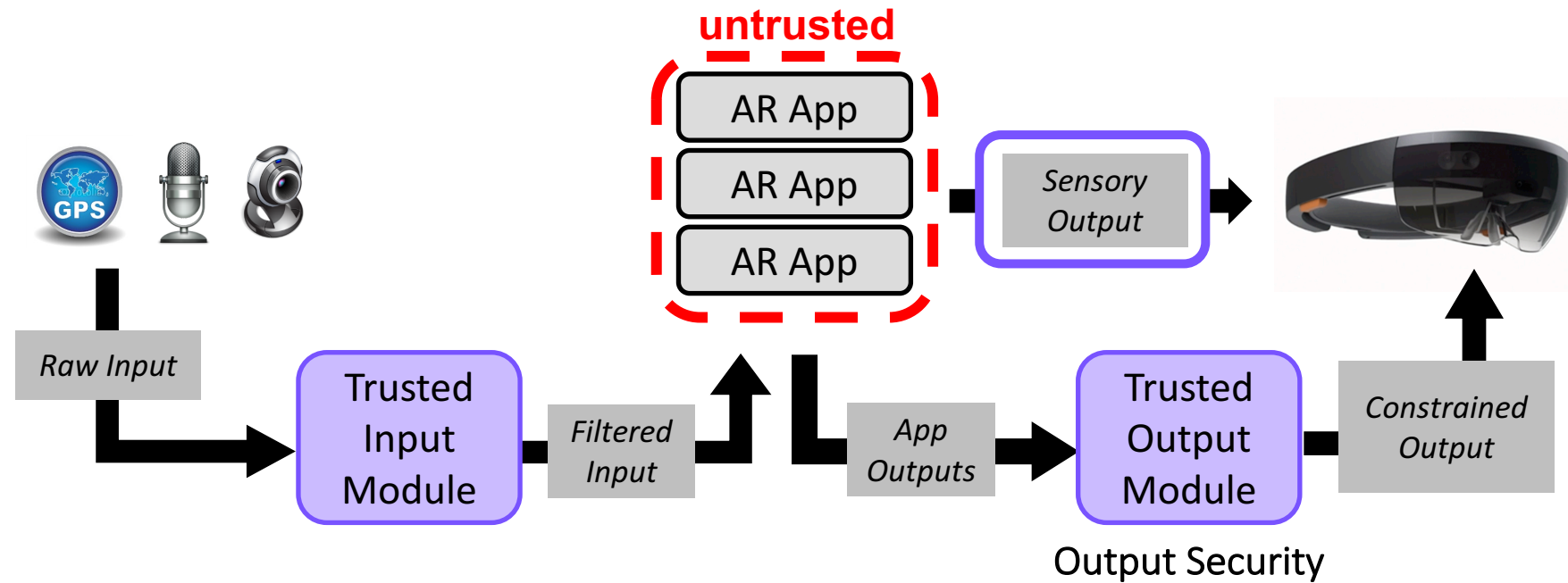
**Obscure another app's virtual content**  
to hide or modify its meaning

**Obscure important real-world content,**  
such as traffic signs or cars

**Disrupt the user physiologically,**  
such as by startling them



# Output Security



- *Lebeck et al., HotMobile '16*
- *Lebeck et al., IEEE S&P '17*



“Real world”



# Arya: AR Objects and Output Policies in Action

K. Lebeck, K. Ruth, T. Kohno, F. Roesner.  
“Securing Augmented Reality Output.” *IEEE Symposium on Security and Privacy*, May 2017.

← “Real world” in our AR simulator



"Real world"

Buggy or malicious apps

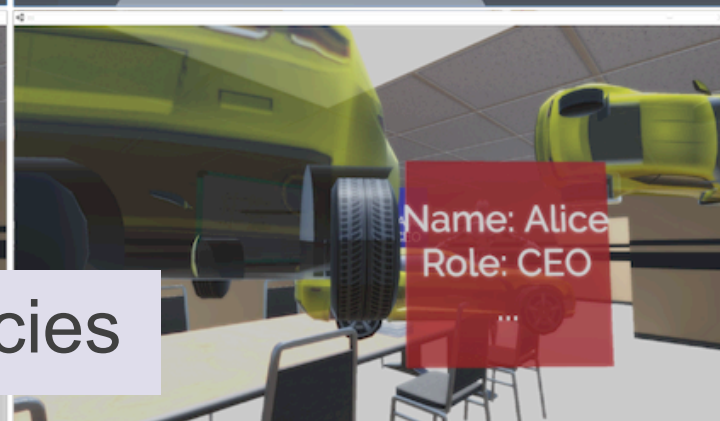
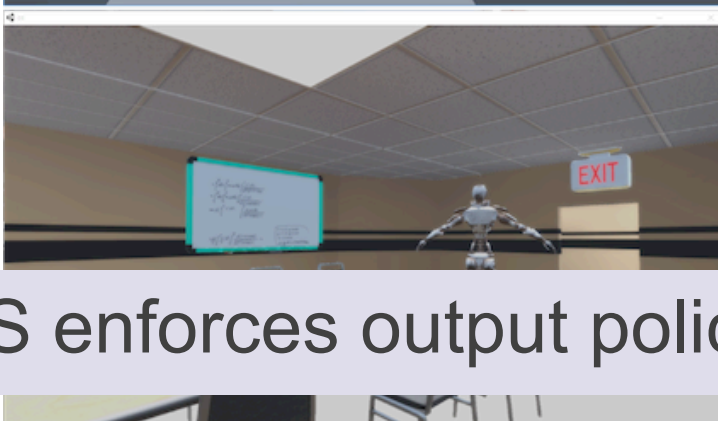


← Buggy or malicious apps

"Real world"

Buggy or malicious apps

Policies enforced



OS enforces output policies



# Conclusion (Part 2)

Emerging AR platforms raise new security and privacy risks, including **input privacy** and **output security**.

Our **Arya prototype** introduces an output security module to constrain output from buggy or malicious AR applications.

We must (and can still!) address security & privacy challenges in AR technologies **before these platforms become widespread and entrenched.**

<https://ar-sec.cs.washington.edu>

# Thanks to many collaborators!



**Ada Lerner**  
(UW)



**Eric Zeng**  
(UW)



**Mitali Palekar**  
(UW)



**Kelly Caine**  
(Clemson)



**Susan McGregor**  
(Columbia)



**Kiron Lebeck**  
(UW)



**Kimberly Ruth**  
(UW)



**Yoshi Kohno**  
(UW)



What security & privacy issues  
are we facing **today**?

What security & privacy issues will arise in  
the **future**, with emerging technologies?



[franzi@cs.washington.edu](mailto:franzi@cs.washington.edu)



[@franziroesner](https://twitter.com/franziroesner)



<https://www.franziroesner.com>