Research Group
Cooperative Systems

universität wien

# Human Factors in Anonymous Mobile Communications

Svenja Schröder
Research Group „Cooperative Systems“, University of Vienna

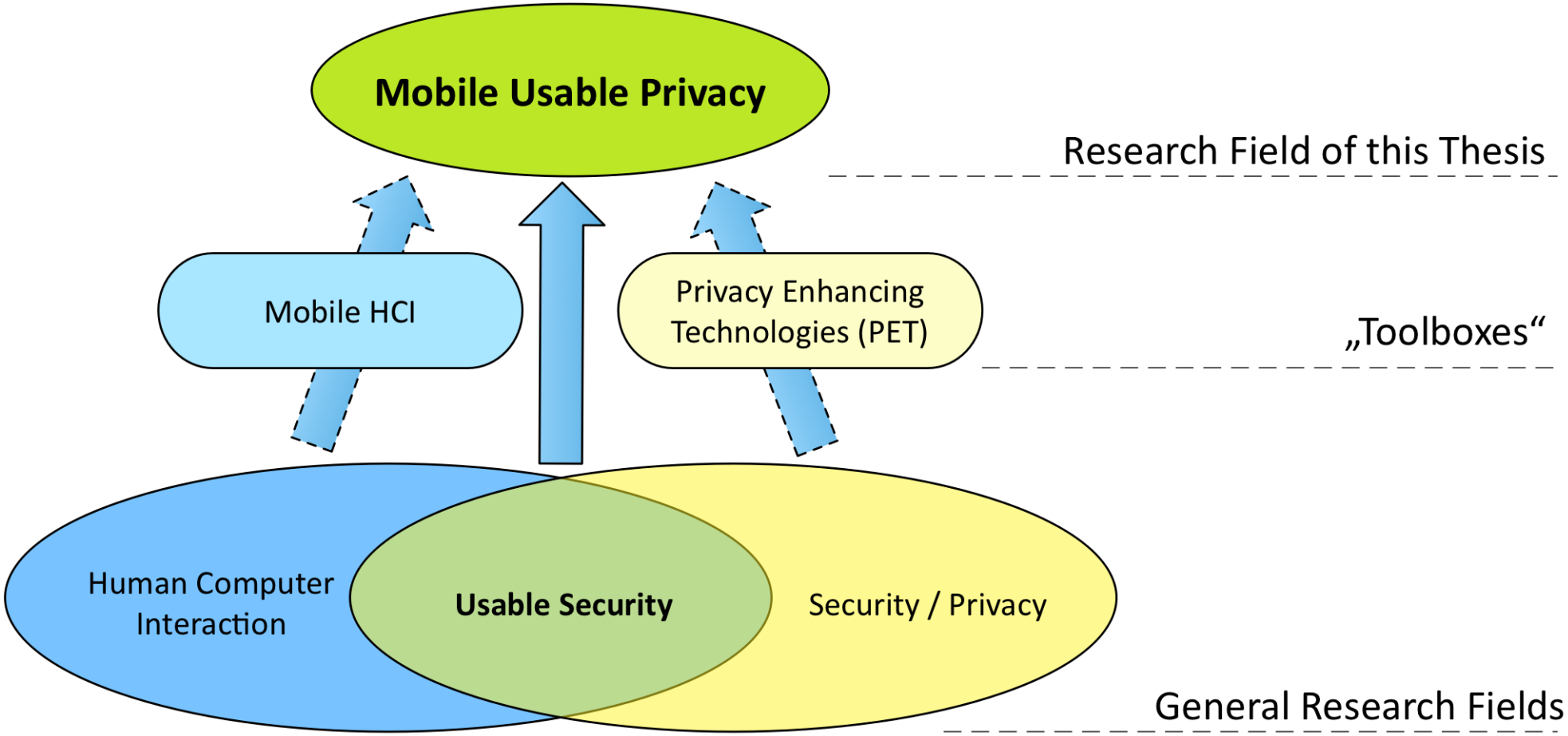
Talk at the PhD School at the Android Security Symposium,
September 9th, 2015 in Vienna

# Motivation

- Recent events like uncovering of global surveillance by the NSA have led to strong increase in popularity of the Tor network
- **Problems**:
  - » Usability problems hinder users in participating in the Tor network, which decreases the anonymity for all users
  - » Significant body of related research on usability of Tor programs on desktop computers, but not on mobile devices
- **Contribution of this PhD project:** Increase usability of Tor apps on mobile devices in order to increase overall anonymity


Source: „Uncle Sam Listens In" by Jeff Schuler - https://secure.flickr.com/photos/jeffschuler/2585181312/in/set-72157604249628154

# Research Fields



**Usable Security**

*Main research field*

- Bringing the user more into focus during security design → more secure systems
- "Human in the Loop": security failures often originate in unintentional mistakes of the users (Cranor 2008)

Privacy-Enhancing Technologies

*In particular: Tor onion routing network*

- Technology and Apps for accessing the Tor network to ensure users' anonymity
- Increasing the user base at the same time leads to an enhanced anonymity for all users, due to network effects (Dingledine & Mathewson 2005)

Mobile HCI

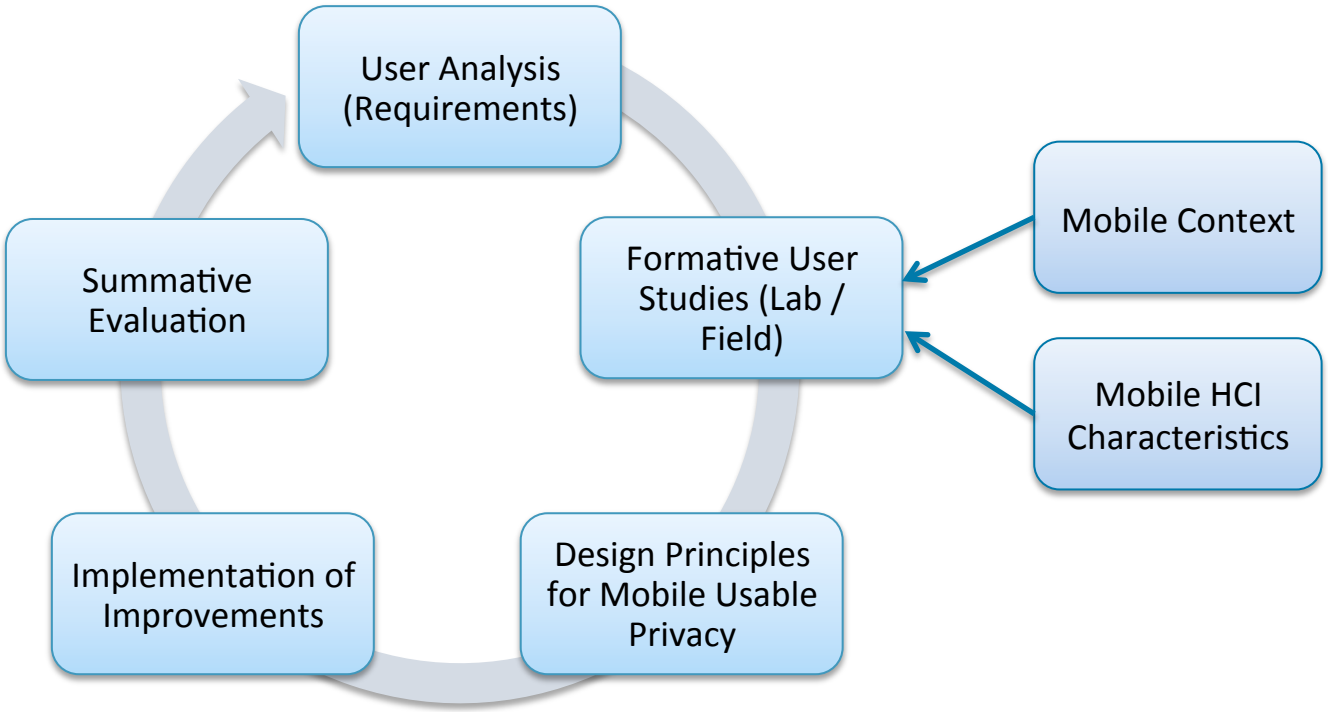
*Mobile interaction, sensors, device specs, …*

- Human Computer interaction with mobile devices, e.g. Smartphones, Tablets and Smartwatches

# Research Questions

- Which **usability problems** hinder users to participate in the Tor network? How can they be overcome?
  - » Are there special usability problems during installation / setup?
- How does the **mobile context** influence the usage of the Tor network?
  - » Are there any special characteristics of the mobile context in which the Tor network is used? (E. g. perceived risk? Quiet/loud surroundings?)
  - » In which ways does this context influence the Tor app usage? How does this reflect in the users' behavior?
- Which special **mobile characteristics** can help to **enhance** the functionality and usability of mobile Tor apps in a reasonable way?
  - » Which mobile HCI characteristics can be drawn on without compromising the users' anonymity? (Sensors? Device specifics?)

# Research Approach




- User Trials:
  - » Lab Study to identify major usability issues
  - » Field study to explore influence of mobile context
- In total: 3 user studies planned
- User studies will be conducted in the COSY user trial lab

# Related Work: Usability Evaluation of Tor Applications (1/2)

- 2007: Examination of usability of different Tor application setups for traditional PCs (Clark et al, 2007)
  - » Most usable configuration: All-in-one browser
  - » Resulted in development of Tor Browser Bundle (TBB)
- 2012/2014: Several flaws found in Tor Browser Bundle (Norcie et al., 2012 & 2014)
  - » Resulted in usability improvement of TBB (shorter launch time, less delay, distinguishable browser windows, etc.)
  - » Subsequent study evaluated improvements from former study and resulted in design guidelines

# Related Work: Usability Evaluation of Tor Applications (2/2)

- 2012: Usability focused on network metrics revealed high user frustration potential due to delay (Müller et al., 2012)
- 2014: Usability of Tor on Android devices tested in a cognitive walkthrough study with 3 experts (Assal and Chiasson, 2014)
  - »Several usability flaws found:
    - Unintuitive feel of the apps
    - Technical language
    - Insecure options that risk the users' security and privacy

# Generalized heuristics for anonymity systems by Norcie et al. (2014)

- "*Installation precedes operation*" (the developers should ensure that the app installation and setup succeeds)
- "*Ensure users are aware of trade-offs*" (for example increased network latency as a price for increased anonymity)
- "*Say why, not how*" (security measures should be explained to the users in a jargon free language)

# Starting point: apps on Android and iOS

- **Orbot**[1] (*Android*): Tor proxy app, works with a list of specific Android apps

- **Orweb**[1] (*Android*): Browser working with Orbot

- Currently in development: **Orfox**[2](*Android*), Tor-enabled Firefox as long-term substitute for Orweb

- **Onion Browser**[3] (*iOS*): Tor-enabled browser

*Sources*:
[1]https://guardianproject.info
[2]https://guardianproject.info/2015/06/30/orfox-aspiring-to-bring-tor-browser-to-android/
[3]https://mike.tig.as/onionbrowser/

# Outline of the planned studies

- **Online questionnaire**: User analysis to identify requirements
- **Laboratory study**: User study of Tor usage
  - » Installation, setup, usage
  - » Identify major usability problems
- **Field study**: Studying mobile Tor usage in the field
  - » Identify usability problems specific to the field
- **Summative study**: Ensure overall quality of improvements

# Lab Studies vs. Field Studies

| | Lab Studies | Field Studies |
|---|---|---|
| Advantages | • Equipment available<br>• No interruptions | • Natural environment (realism)<br>• Context retained |
| Disadvantages | • Lack of realism<br>• Difficult to observe user collaboration | • Distractions / noise |

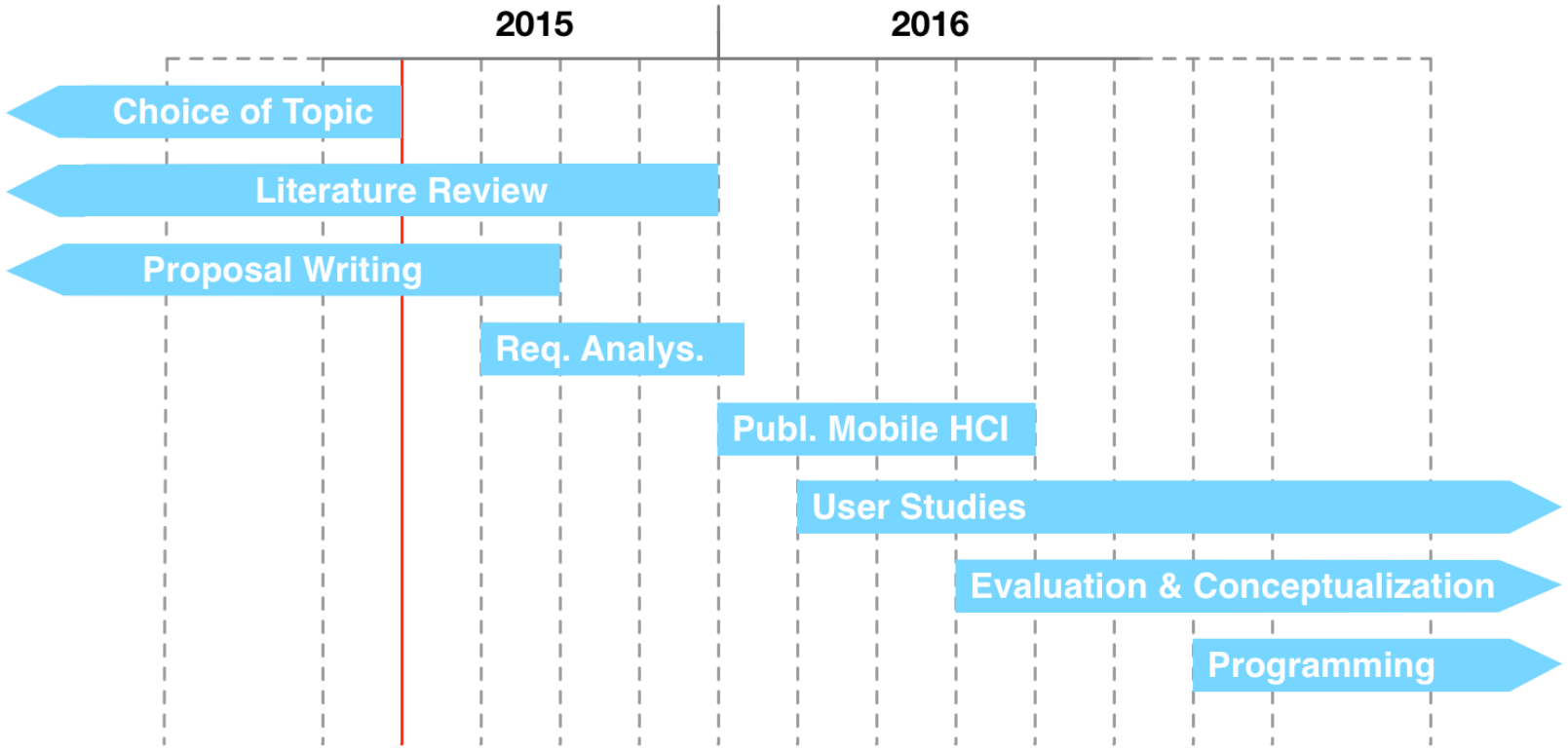
*Source*: Alan Dix „HCI 3e – Ch9: Evaluation techniques“ (http://de.slideshare.net/alanjohndix/hci-3e-ch-9-evaluation-techniques)

- Question “lab or field” → Depends!
  - » What’s more important? Ecological validity or control?
- “If” and “why” not as important as “when” and “how” (Kjeldskov, 2014)

# Expected Outcome

- List of **requirements** for mobile Tor usage
- Increased **usability** of apps
- **Insights about role of context** in mobile usable privacy
- **Guidelines / heuristics** for developers

# Status of the thesis (2014-2017)



# Issues to tackle

- Target group?
  - » Experts / non-experts / both?
  - » Motivation and goals? Usage scenarios?
- "Context"?
  - » Only surroundings / noise / other distractions, or also specific situations (e.g. with a high risk)?

# Thank you!

Questions?

# Literature


- Assal, H. & Chiasson, S. (2014). *Will this onion make you cry? A Usability Study of Tor-enabled Mobile Apps*. Poster presented at the 10th Symposium on Usable Privacy and Security (SOUPS).
- Clark, J. & Van Oorschot, P.C. & Adams, C. (2007). *Usability of anonymous web browsing: an examination of tor interfaces and deployability*. In: Proceedings of the 3rd symposium on Usable privacy and security (SOUPS). ACM.
- Cranor, L. F.: „A Framework for Reasoning About the Human in the Loop“. In: Proceedings of the 1st Conference on Usability, Psychology, and Security. USENIX Association, 2008.
- Dingledine. R. & Mathewson, N. (2005). *Anonymity loves company: usability and the network effect*. In Cranor, L. & Garfinkel, S. (editors): *Security and Usability*. O'Reilly.
- Kjeldskov, J. and Skov, M.B.: „Was it Worth the Hassle? Ten Years of Mobile HCI Research Discussions on Lab and Field Evaluations“. In: Proceedings of Mobile HCI 2014, Toronto, CA, 2014.
- Müller, S. & Brecht, F. & Fabian, B. & Kunz, S. & Kunze, D. (2012). *Distributed performance measurement and usability assessment of the tor anonymization network*. *Future Internet*, *4*(2).
- Norcie, G. & Caine, K. & Camp, L.J. (2012). *Eliminating Stop-Points in the Installation and Use of Anonymity Systems: a Usability Evaluation of the Tor Browser Bundle*. In: Proceedings of the 5th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETS). 2012.
- Norcie, G. & Blythe, J. & Caine, K. & Camp, L. J. (2014). *Why Johnny Can't Blow the Whistle: Identifying and Reducing Usability Issues in Anonymity Systems*. In Proceedings of the 2014 Workshop on Usable Security (USEC).