Improving Mental Models of End-to-End Encrypted Communications

Omer Akgul • Wei Bai

SP² SECURITY. PRIVACY. PEOPLE

UNIVERSITY OF MARYLAND

MARYLAND CYBERSECURITY CENTER

In collaboration with

Shruti Das Michael Pearson

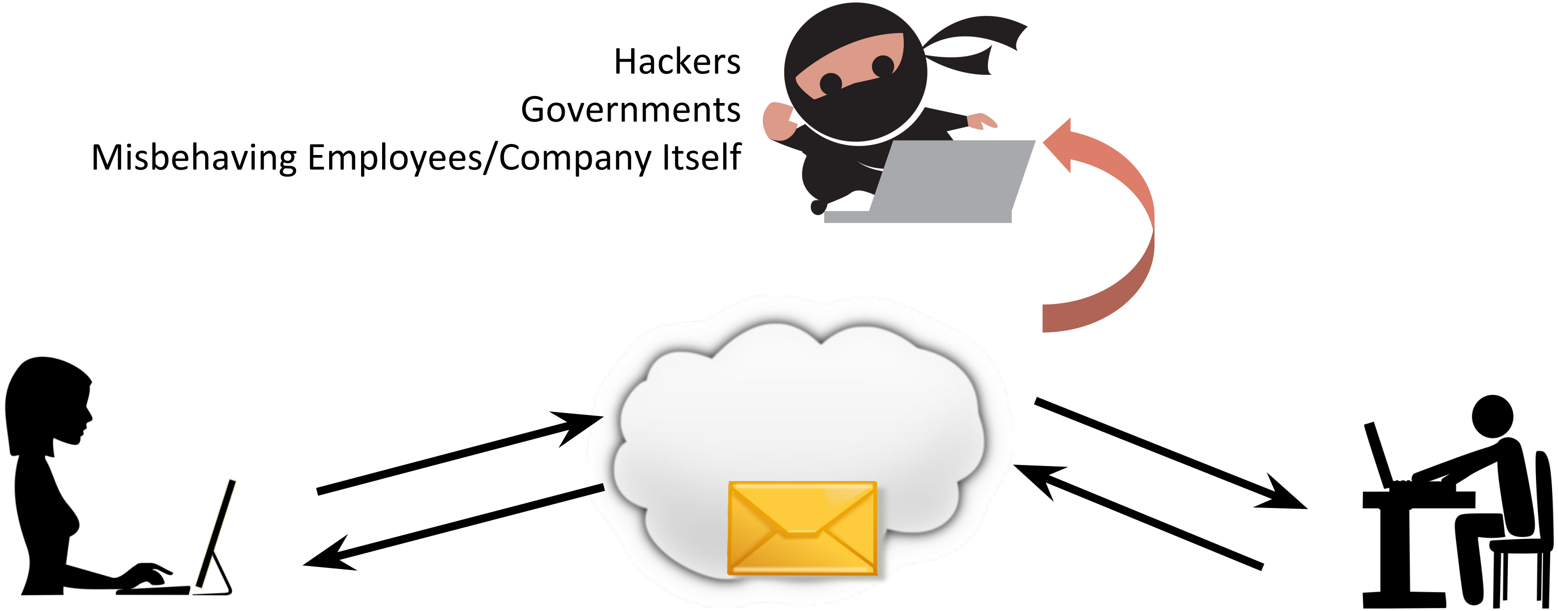
Dr. Michelle Mazurek

Dr. Patrick Gage Kelley

UNIVERSITY OF MARYLAND

Google

End-to-End Encryption (E2EE)



Hackers
Governments
Misbehaving Employees/Company Itself

Cartoon cloud made by egyninja from http://www.publicdomainfiles.com/show_file.php?id=13946016618385.
Envelope from https://freesvg.org/rg1024-yellow-mail
Attacker from https://pixabay.com/illustrations/ninja-laptop-hacker-cyber-security-4983545/
Person in the left from https://freesvg.org/computer-access-available-vector-sign11006#
Person in the right from https://en.wikipedia.org/wiki/File:Computer_user_icon.svg

Adoption of E2EE **Not By**

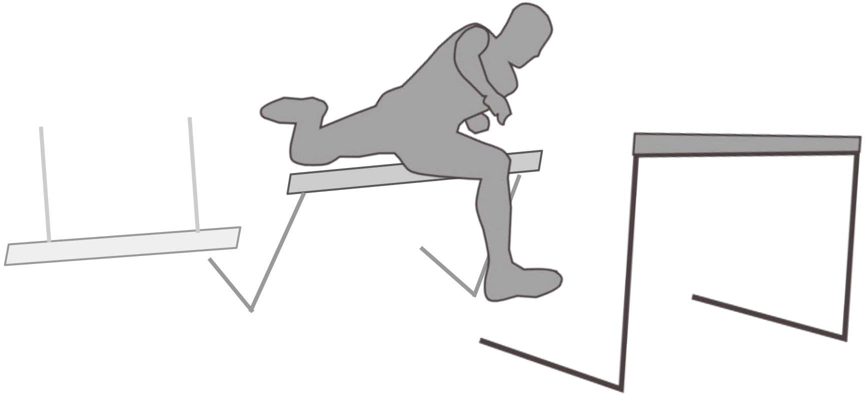
- Security Experts & People with High Computer Literacy
- Special Needs of Security and Privacy: lawyers, journalists, activists …

Adoption of E2EE **By General Users**

Icon from https://pixabay.com/illustrations/inclusion-group-wheelchair-5249903/

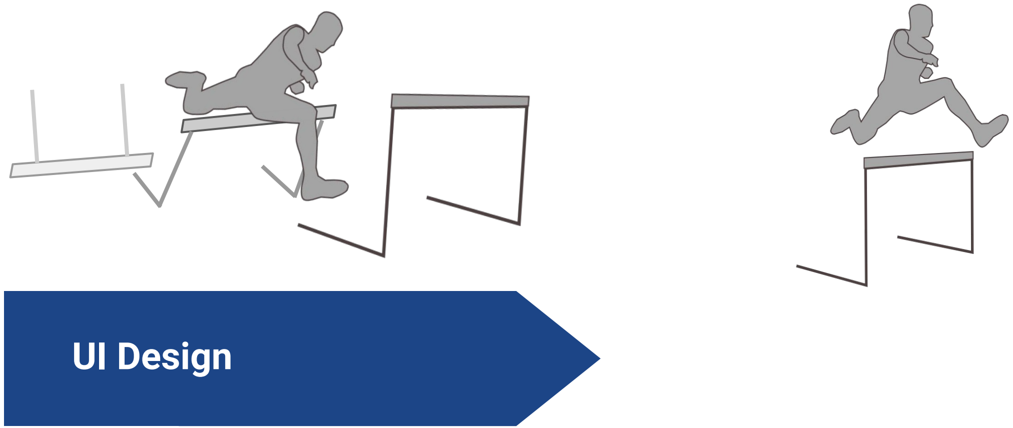
Adoption of E2EE By **General Users**?

Many hurdles impede their adoption!



Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

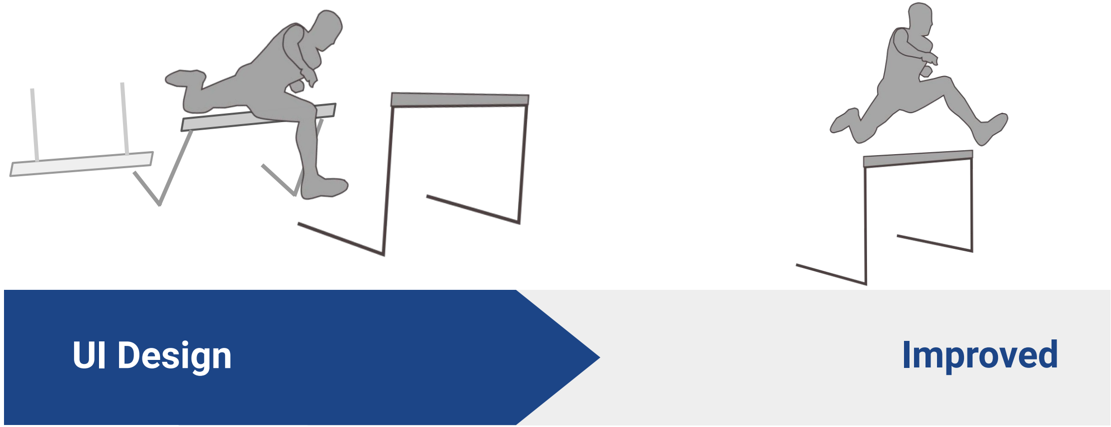
Many Hurdles Impede Adoption



UI Design

Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

Many Hurdles Impede Adoption

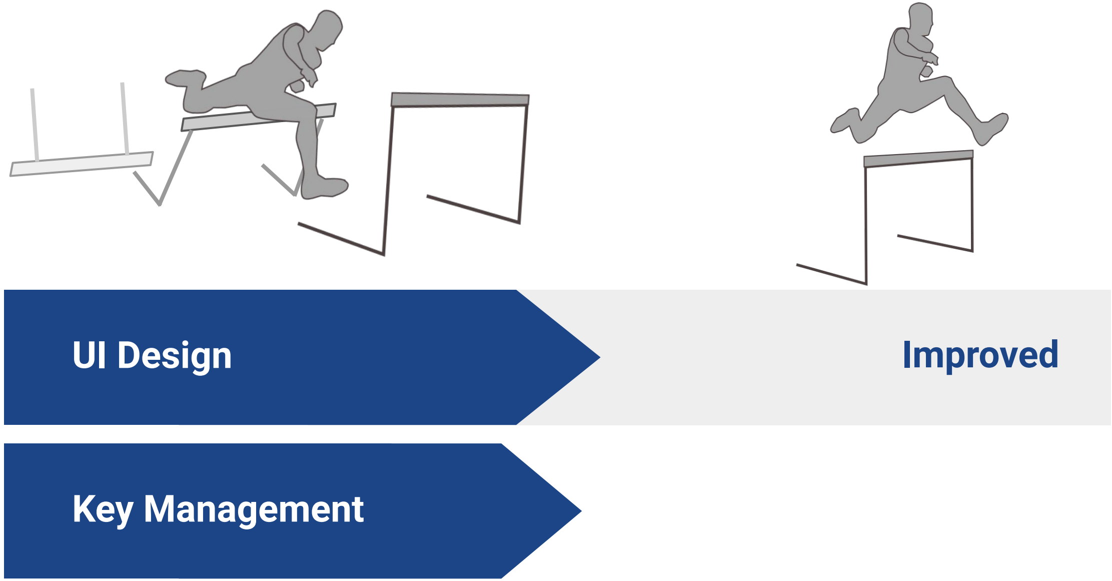


UI Design

Improved

Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

Many Hurdles Impede Adoption



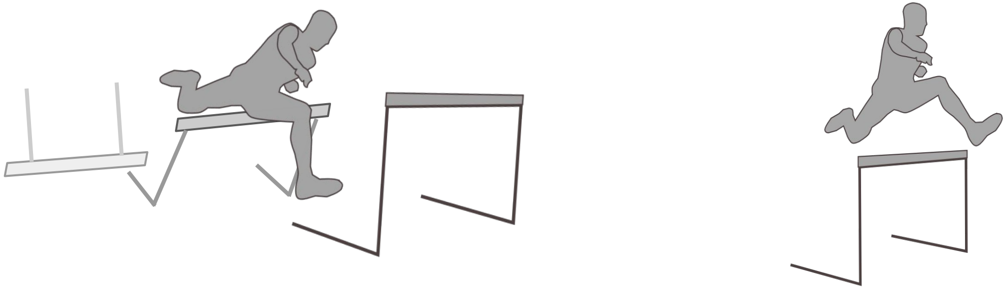
UI Design

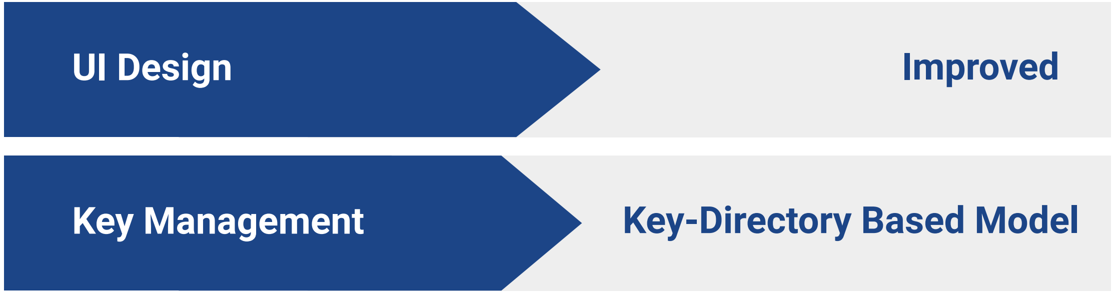
Improved

Key Management

Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

Many Hurdles Impede Adoption





UI Design

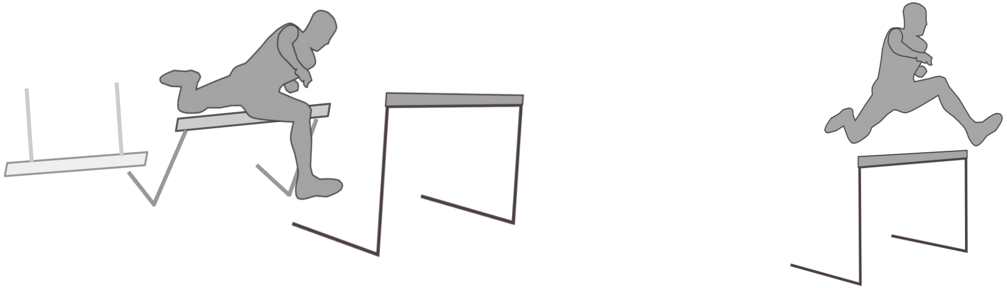
Improved

Key Management

Key-Directory Based Model

Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

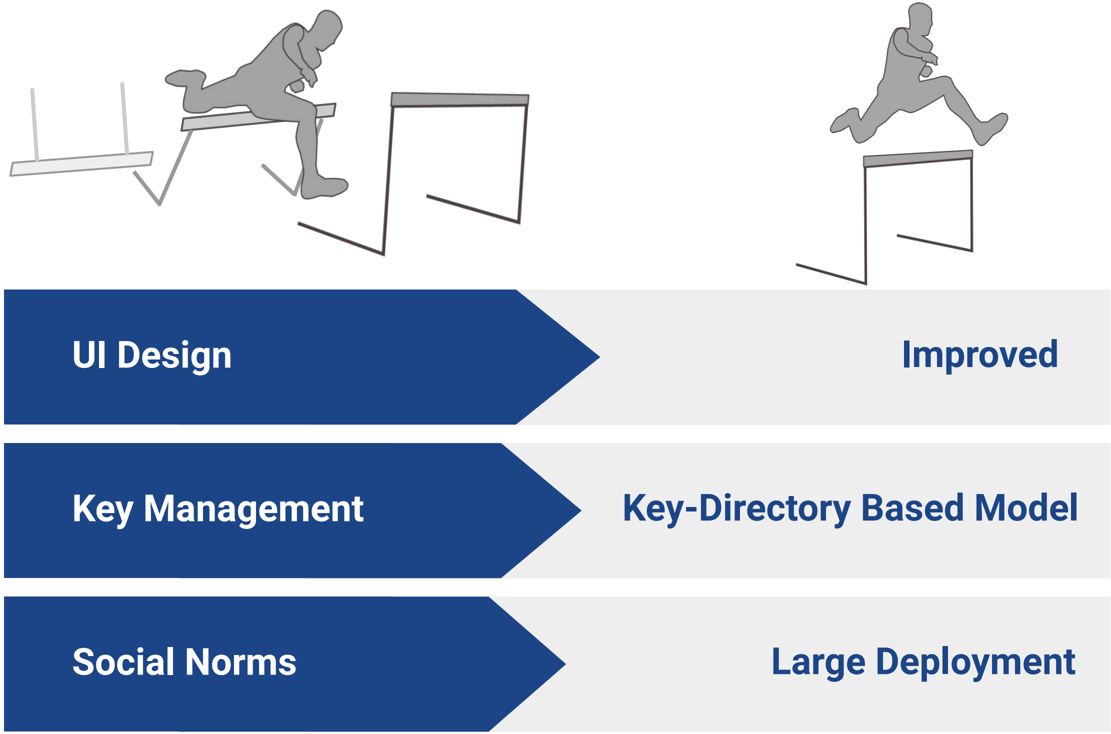
Many Hurdles Impede Adoption



UI Design	Improved
Key Management	Key-Directory Based Model
Social Norms	

Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

Many Hurdles Impede Adoption



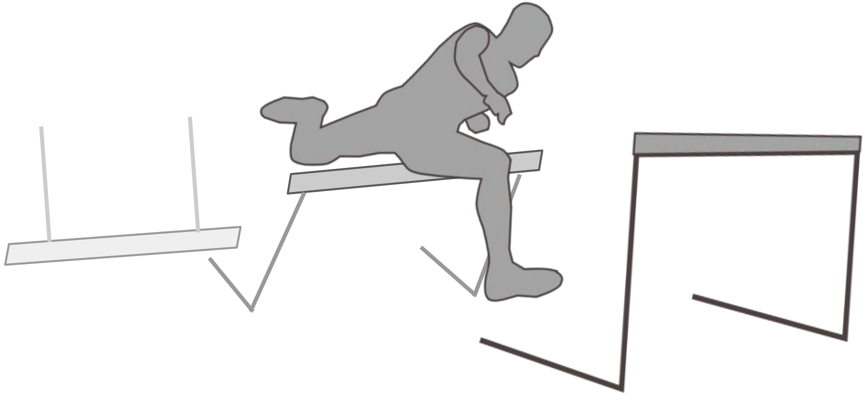
UI Design → Improved

Key Management → Key-Directory Based Model

Social Norms → Large Deployment

Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

Mental Models - **Big Hurdle**!



Icons from https://freesvg.org/vector-silhouette-of-an-athlete with modification

What are mental models?

Mental models describe how a user thinks about a problem; it is the model in the person's mind of how things work. People use these models to make decisions about the effects of various actions [1].

It helps to understand how users make security decisions, and to characterize the security problems that result from these decisions [2].

[1] P. Johnson-Laird, V. Girotto, , and P. Legrenzi. Mental models: a gentle guide for outsiders
[2] R. Wash. Folk models of home computer security. In Symposium of Usable Privacy and Security (SOUPS 2010).

Icon from https://www.needpix.com/photo/596351/brain-business-credit-intelligence-icon-mental-health-presentation-presentation-clipart-presentation-graphic-work

Why do (incorrect) mental models matter?

People perceive E2EE incorrectly in both directions [1-2]:

- Encryption protects from anything
- Encryption can be trivially broken by anyone who works in IT

[1] Abu-Salma et al. Obstacles to the adoption of secure communication tools. In IEEE Security & Privacy, 2017
[2] Wu et al. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In USENIX SOUPS 2018

Icon from https://pixabay.com/illustrations/question-question-mark-response-1015308/

Why do (incorrect) mental models matter?

People perceive E2EE incorrectly in both directions [1-2]:

- Encryption protects from anything
- Encryption can be trivially broken by anyone who works in IT

Difficult for users to make thoughtful decisions:

- “SMS is the most secure messaging service.” [1]

[1] Abu-Salma et al. Obstacles to the adoption of secure communication tools. In IEEE Security & Privacy, 2017
[2] Wu et al. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In USENIX SOUPS 2018

Icon from https://pixabay.com/illustrations/question-question-mark-response-1015308/

Why do (incorrect) mental models matter?

People perceive E2EE incorrectly in both directions [1-2]:

- Encryption protects from anything
- Encryption can be trivially broken by anyone who works in IT

Difficult for users to make thoughtful decisions:

- “SMS is the most secure messaging service.” [1]

Struggled to complete some E2EE tasks

[1] Abu-Salma et al. Obstacles to the adoption of secure communication tools. In IEEE Security & Privacy, 2017
[2] Wu et al. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In USENIX SOUPS 2018

Icon from https://pixabay.com/illustrations/question-question-mark-response-1015308/

Why do (incorrect) mental mo

People perceive E2EE incorrectly in both di

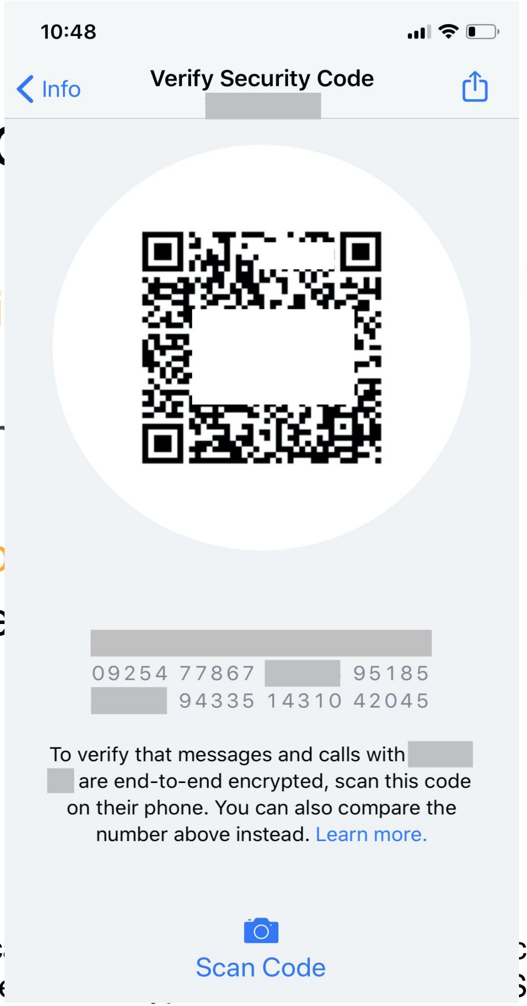
- Encryption protects from anything
- Encryption can be trivially broken by ar

Difficult for users to make thoughtful decisio

- “SMS is the most secure messaging se

Struggled to complete some E2EE tasks

*Screenshot taken from presenters’ devices



[redacted]

[redacted]

09254 77867 [redacted] 95185
[redacted] 94335 14310 42045

To verify that messages and calls with [redacted] [redacted] are end-to-end encrypted, scan this code on their phone. You can also compare the number above instead. Learn more.

[1] Abu-Salma et al. Obstacles to the adoption of secure communic cy, 2017
[2] Wu et al. When is a Tree Really a Truck? Exploring Mental Mode S 2018

Icon from https://pixabay.com/illustrations/question-question-mark-response-1015308/

Why do (incorrect) mental models matter?

People perceive E2EE incorrectly in both directions [1-2]:

- Encryption protects from anything
- Encryption can be trivially broken by anyone who works in IT

Difficult for users to make thoughtful decisions:

- “SMS is the most secure messaging service.” [1]

Struggled to complete some E2EE tasks

Because they inhibit

Confident, Proactive, and Correct usage

[1] Abu-Salma et al. Obstacles to the adoption of secure communication tools. In IEEE Security & Privacy, 2017

[2] Wu et al. When is a Tree Really a Truck? Exploring Mental Models of Encryption. In USENIX SOUPS 2018

Icon from https://pixabay.com/illustrations/question-question-mark-response-1015308/

Improve mental models **Naturally**

Goal: Help people grok basic understanding and threats

- **Enough** to make judgments about how to communicate
- **Without** turning everyone into crypto experts
- **Without** requiring people to sign up for training modules

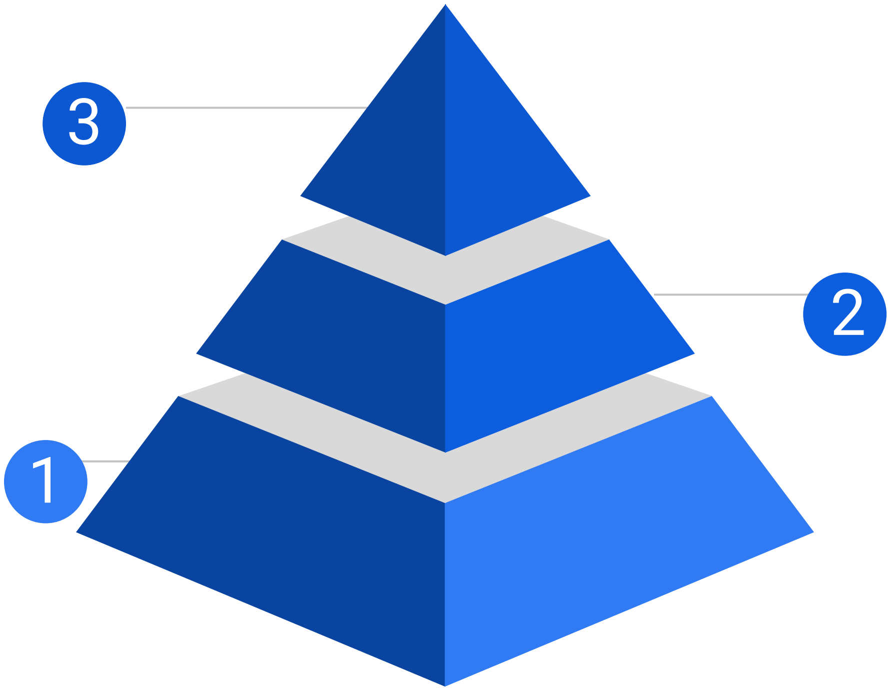
Multi-Stage Efforts: From Lab to Field

Field(ish) Study

- Fit messages to an app
- Daily use for 3 weeks

Lab Study

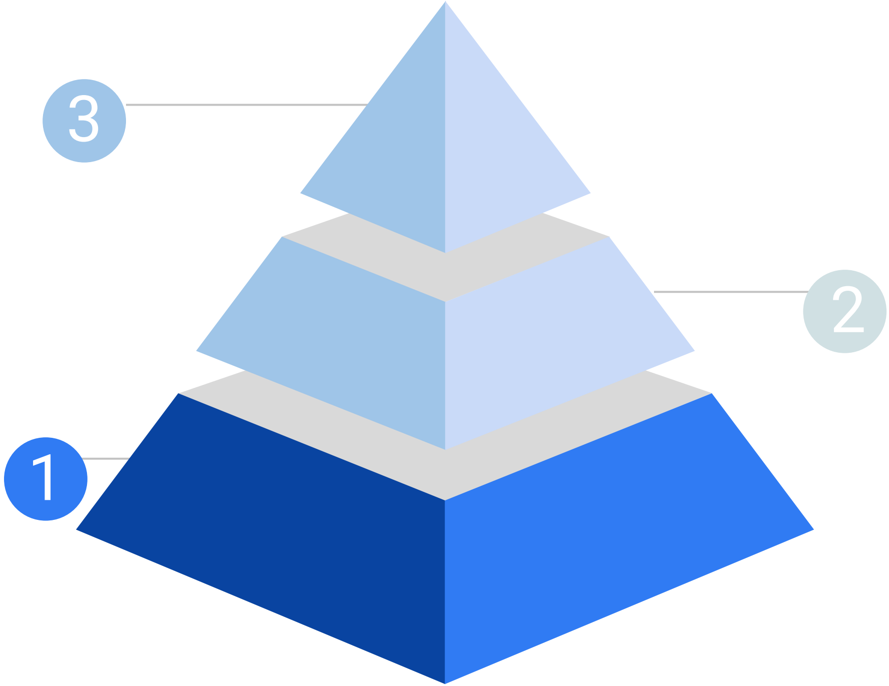
- In-depth tutorial



Online Survey

- Test different messages varying in length and contents

Multi-Stage Efforts: From Lab to Field



Field(ish) Study

- Fit messages to an app
- Daily use for 3 weeks

Online Survey

- Test different messages varying in length and contents

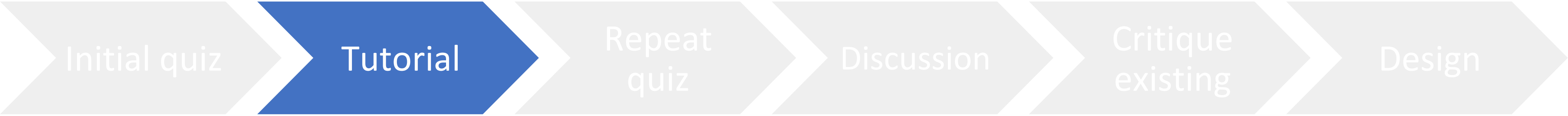
Lab Study

- In-depth tutorial

Study 1: Lab Study

Focus: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area



Initial quiz

Tutorial

Repeat quiz

Discussion

Critique existing

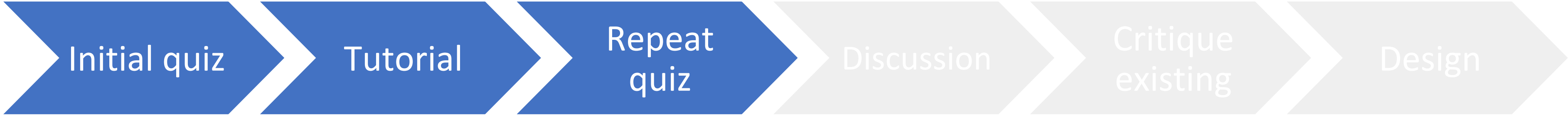
Design

[1] Bai et al. Improving Non-Experts’ Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Study 1: Lab Study

Focus: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area



Initial quiz

Tutorial

Repeat quiz

Discussion

Critique existing

Design

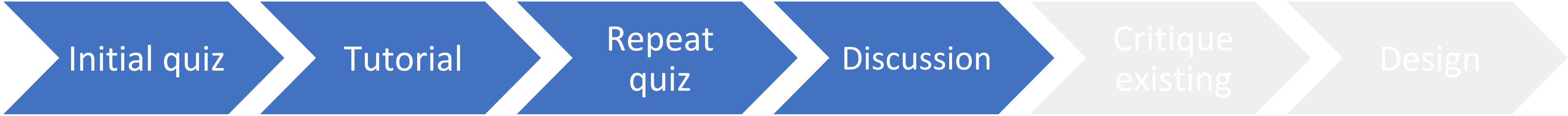
Reasons behind quiz answers

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Study 1: Lab Study

Focus: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area



Initial quiz

Tutorial

Repeat quiz

Discussion

Critique existing

Design

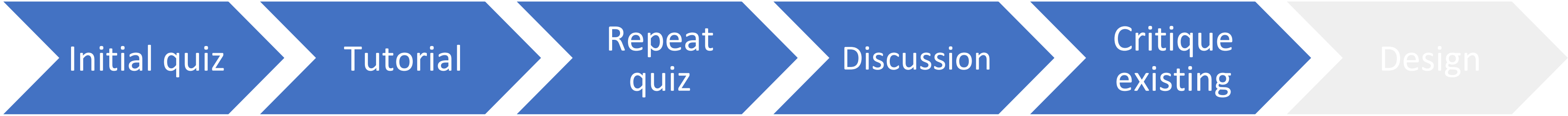
Important, surprising, worth conveying

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Study 1: Lab Study

Focus: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area



Initial quiz → Tutorial → Repeat quiz → Discussion → Critique existing → Design

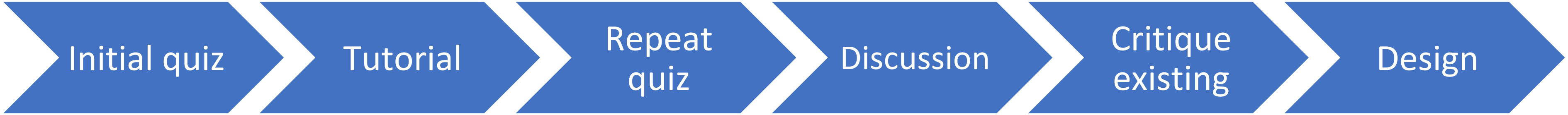
Critique two existing explanations

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Study 1: Lab Study

Focus: What is important, what is surprising, what to convey to others

- 25 non-expert participants, DC area



Initial quiz

Tutorial

Repeat quiz

Discussion

Critique existing

Design

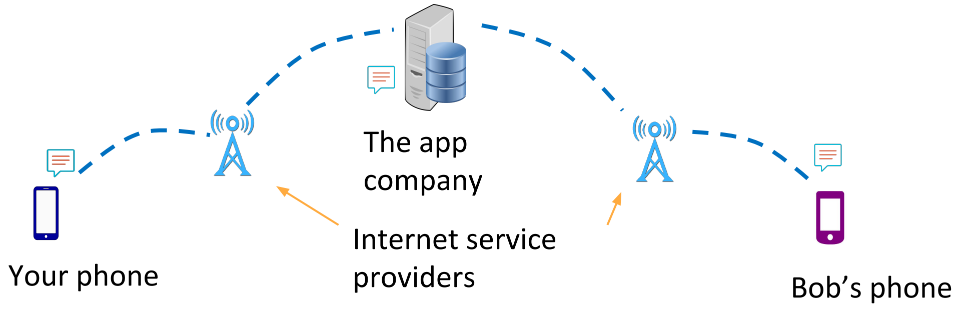
Sample message of E2EE educational intervention

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Modular Tutorial

- High-level overview
- Risks
- Common misconceptions
- High-level description of how it works

- Not trying to develop a tutorial



Tutorial screenshot taken from [1]

[1] Bai et al. Improving Non-Experts’ Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Confidentiality: Most significant

- Even though less surprising, participants found it important
- Some subtleties were surprising
    - ISPs are in the message path?

> *". . . the internet service provider and the app company . . . may still get a copy of the message, that is protected by this wall, that is nearly impossible to break. So they can see you sent a message, but they can't see what the message says."*

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Explaining risks clearly is useful

- Particularly like comparison of E2EE vs. non-E2EE
- Important to clarify weakness of E2EE as well as benefits

"Knowing the risks of the non-E2EE and then really comparing it to how is this better… that's really the most important."

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

Integrity & authenticity still confusing

- Authenticity is conflated with username/password

“E2EE protects against message modification and impersonation. Not even usernames and/or passwords can be stolen or guessed.”

[1] Bai et al. Improving Non-Experts’ Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

How E2EE works - can create confusion

- Concern about forging private keys

"… if you work in a 'locksmith office'…, you might not have somebody's key but you would be able to get into their house because you are an expert and you know how to manipulate systems."

[1] Bai et al. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE EuroUSEC, 2020

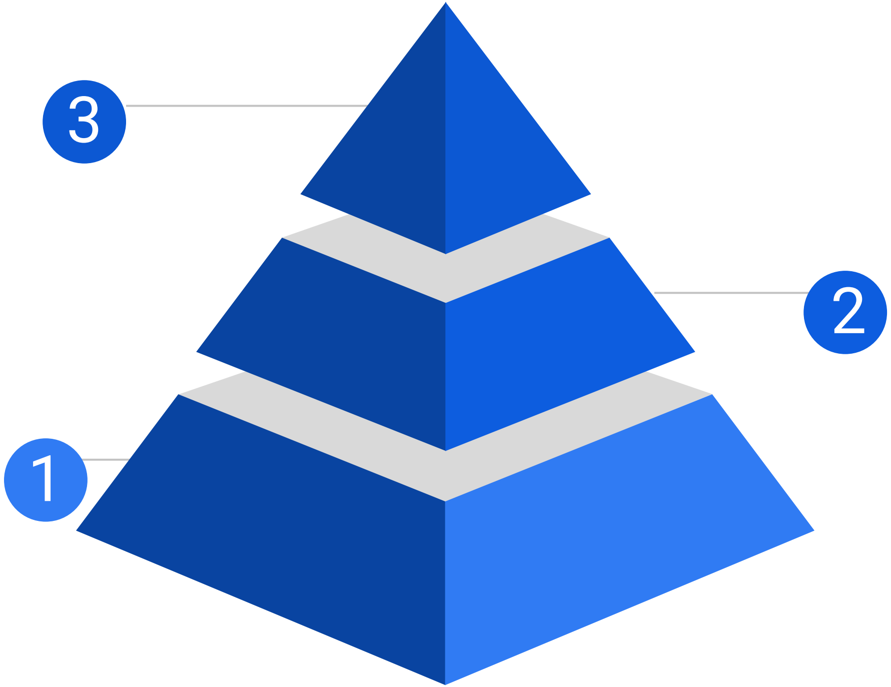
Study 1 - Takeaways

- Confidentiality: Most significant

- Explaining risks clearly is useful
  - Comparing E2EE vs Non-E2EE
  - Weakness

- Some pieces may not worth mentioning
  - Integrity & authenticity
  - How E2EE works

Multi-Stage Efforts: From Lab to Field



Field(ish) Study

- Fit messages to an app
- Daily use for 3 weeks

Online Survey

- Test different messages varying in length and contents

Lab Study

- In-depth tutorial

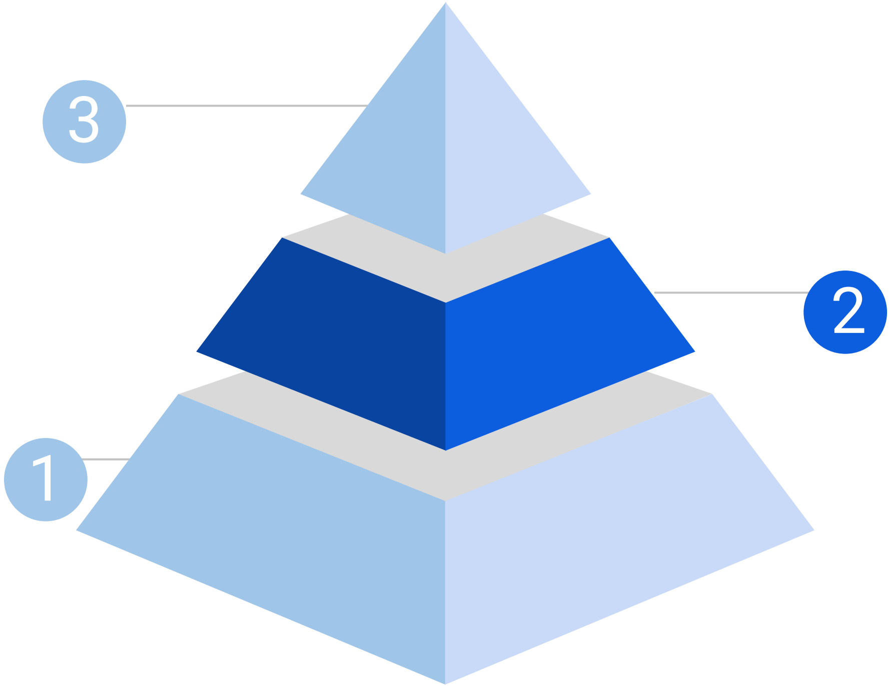
Multi-Stage Efforts: From Lab to Field

Field(ish) Study

- Fit messages to an app
- Daily use for 3 weeks

Lab Study

- In-depth tutorial



Online Survey

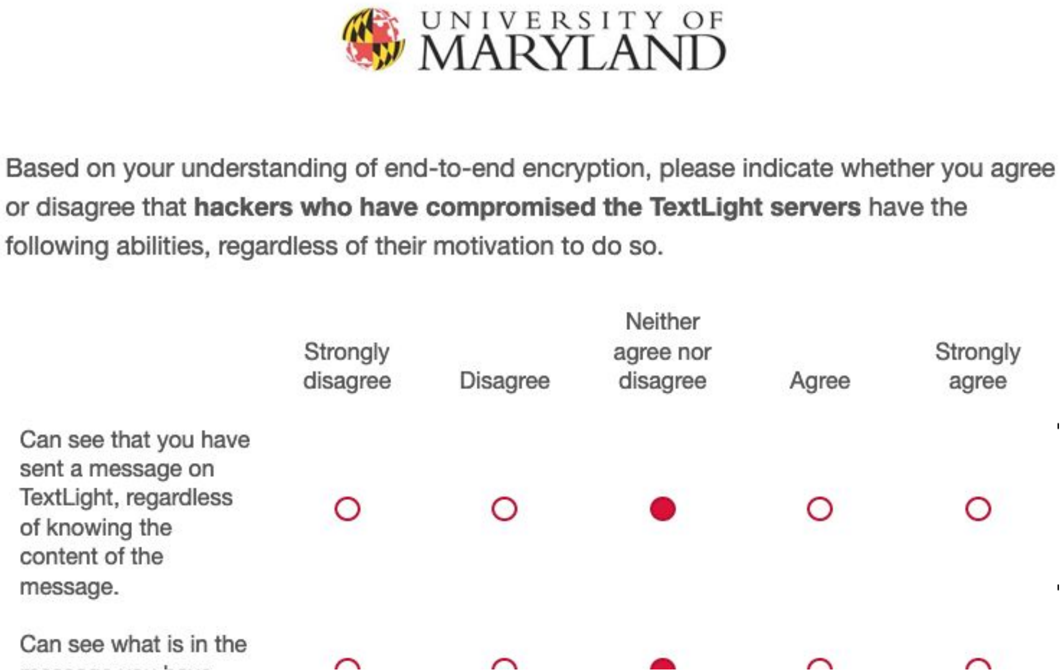
- Test different messages varying in length and contents

Feeds Into Study 2

- Can we **shift** user mental model on E2EE with short messages in text?
- How much is lost in **short**, **medium** vs. **long** messages?
  - Long: App’s info webpage, complete coverage of things we want to convey
  - Short: Messages during loading, tooltips etc., concise single talking point
  - Medium: “Click here for more” in app, etc.
- Which short, medium messages are most effective (for what)?
- Don’t want to **oversell** security

Study 2: Setup

- Online study via a crowdsourcing platform (Prolific, n=461)
- 1 Long, 5 short, 2 medium, 1 control message
  - Hypothetical app called TextLight (to remove brand bias)
- Between subjects design
- Quiz before, read message, quiz after
  - Quiz asks about adversaries and their capabilities
  - Measure change in scores



UNIVERSITY OF MARYLAND

Based on your understanding of end-to-end encryption, please indicate whether you agree or disagree that **hackers who have compromised the TextLight servers** have the following abilities, regardless of their motivation to do so.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Can see that you have sent a message on TextLight, regardless of knowing the content of the message.	○	○	●	○	○
Can see what is in the	○	○	●	○	○

Pre survey

Read Message

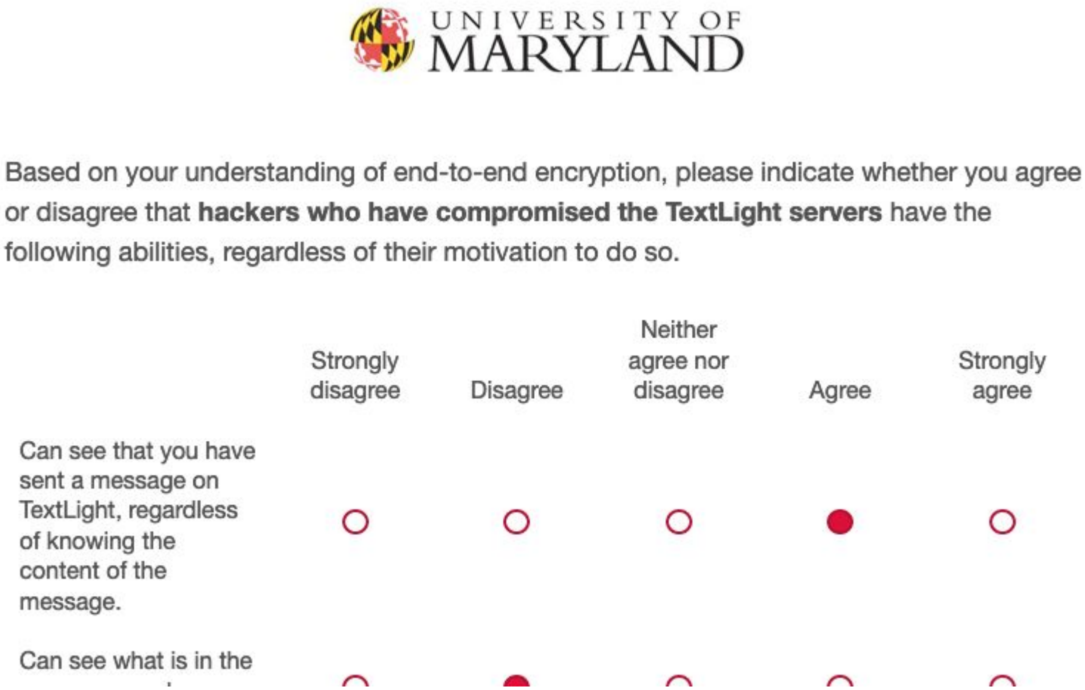
Exit survey

> “Messages in TextLight are end-to-end encrypted. This ensures that only you and the person you’re communicating with can read the messages you send and receive. Nobody in between can see the content of your messages.”

Pre survey

Read Message

Exit survey



UNIVERSITY OF MARYLAND

Based on your understanding of end-to-end encryption, please indicate whether you agree or disagree that **hackers who have compromised the TextLight servers** have the following abilities, regardless of their motivation to do so.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Can see that you have sent a message on TextLight, regardless of knowing the content of the message.	○	○	○	●	○
Can see what is in the	○	●	○	○	○

Pre survey

Read Message

Exit survey

Message types

Short	
Medium	
Long	
Control	

Message types

Short	(1) Nobody but you and recipient
Medium	
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks
Medium	
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks
Medium	
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks (4) Lock/key metaphor
Medium	
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks (4) Lock/key metaphor (5) E2EE vs. other
Medium	
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks (4) Lock/key metaphor (5) E2EE vs. other
Medium	(1) Lock/key for your device, E2EE vs. other, endpoint risks, metadata risks
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks (4) Lock/key metaphor (5) E2EE vs. other
Medium	(1) Lock/key for your device, E2EE vs. other, endpoint risks, metadata risks (2) Nobody but you and recipient, lock/key for your device, E2EE vs. other, metadata risks
Long	
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks (4) Lock/key metaphor (5) E2EE vs. other
Medium	(1) Lock/key for your device, E2EE vs. other, endpoint risks, metadata risks (2) Nobody but you and recipient, lock/key for your device, E2EE vs. other, metadata risks
Long	All key points, extra emphasis
Control	

Message types

Short	(1) Nobody but you and recipient (2) Metadata risks (3) Endpoint risks (4) Lock/key metaphor (5) E2EE vs. other
Medium	(1) Lock/key for your device, E2EE vs. other, endpoint risks, metadata risks (2) Nobody but you and recipient, lock/key for your device, E2EE vs. other, metadata risks
Long	All key points, extra emphasis
Control	Describes non-security/privacy features

Short messages

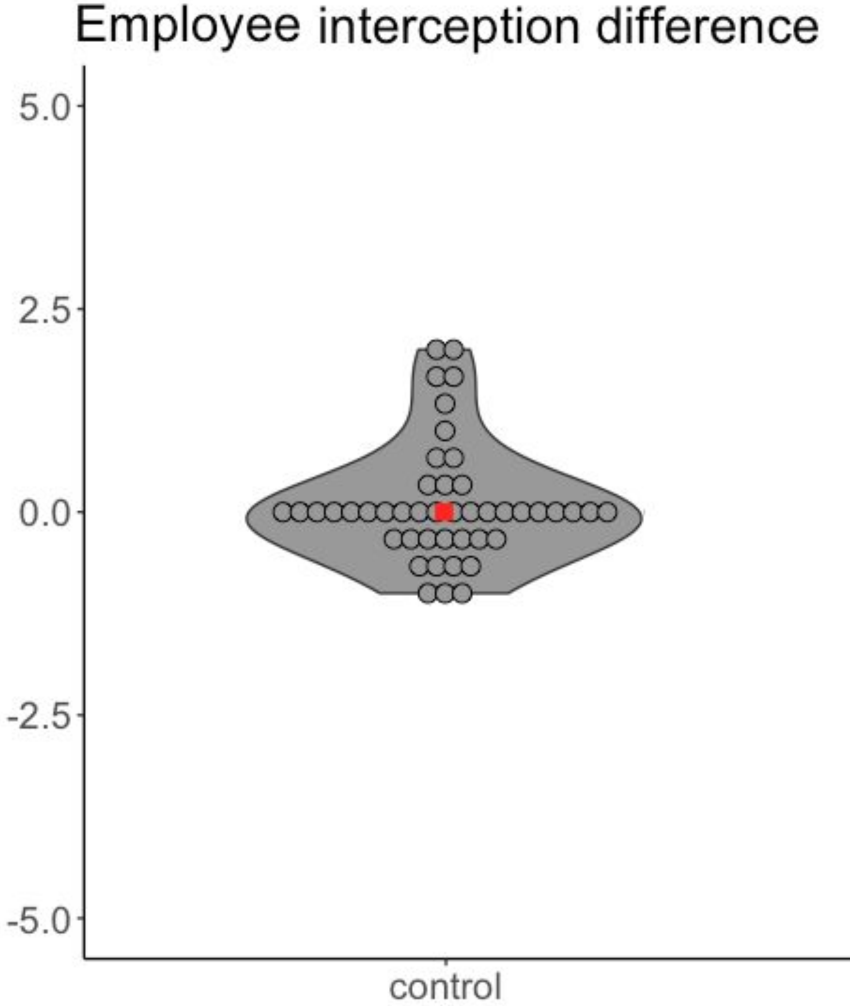
Short v1

“Messages in TextLight are end-to-end encrypted. This ensures that only you and the person you’re communicating with can read the messages you send and receive. Nobody in between can see the content of your messages.”

Short v4

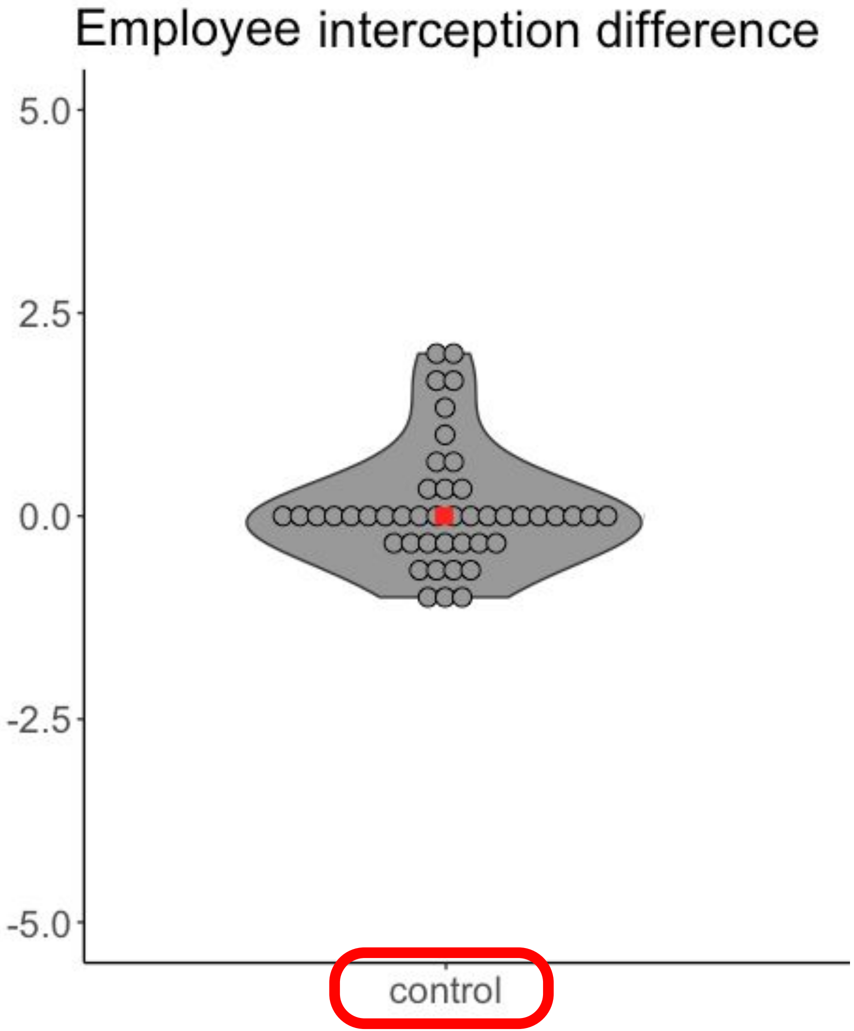
“Messages in TextLight are end-to-end encrypted. Before a message ever leaves your device, it’s secured with a lock, and only you and your recipients have the keys to open the message and read it.”

better

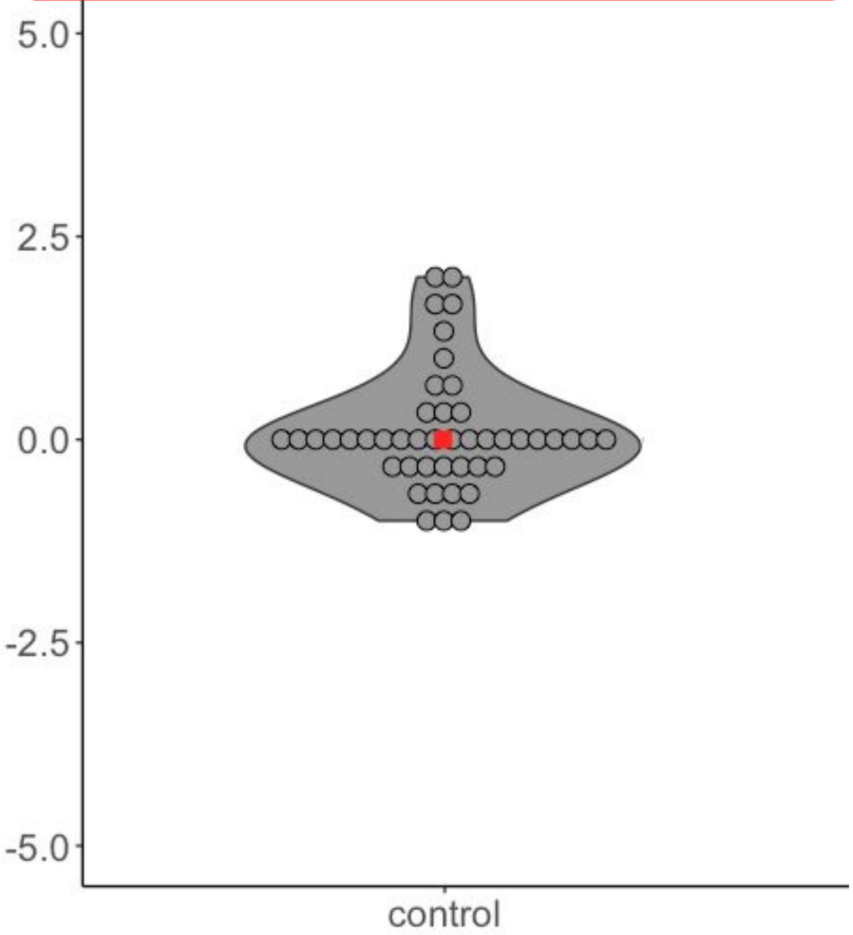


Employee interception difference

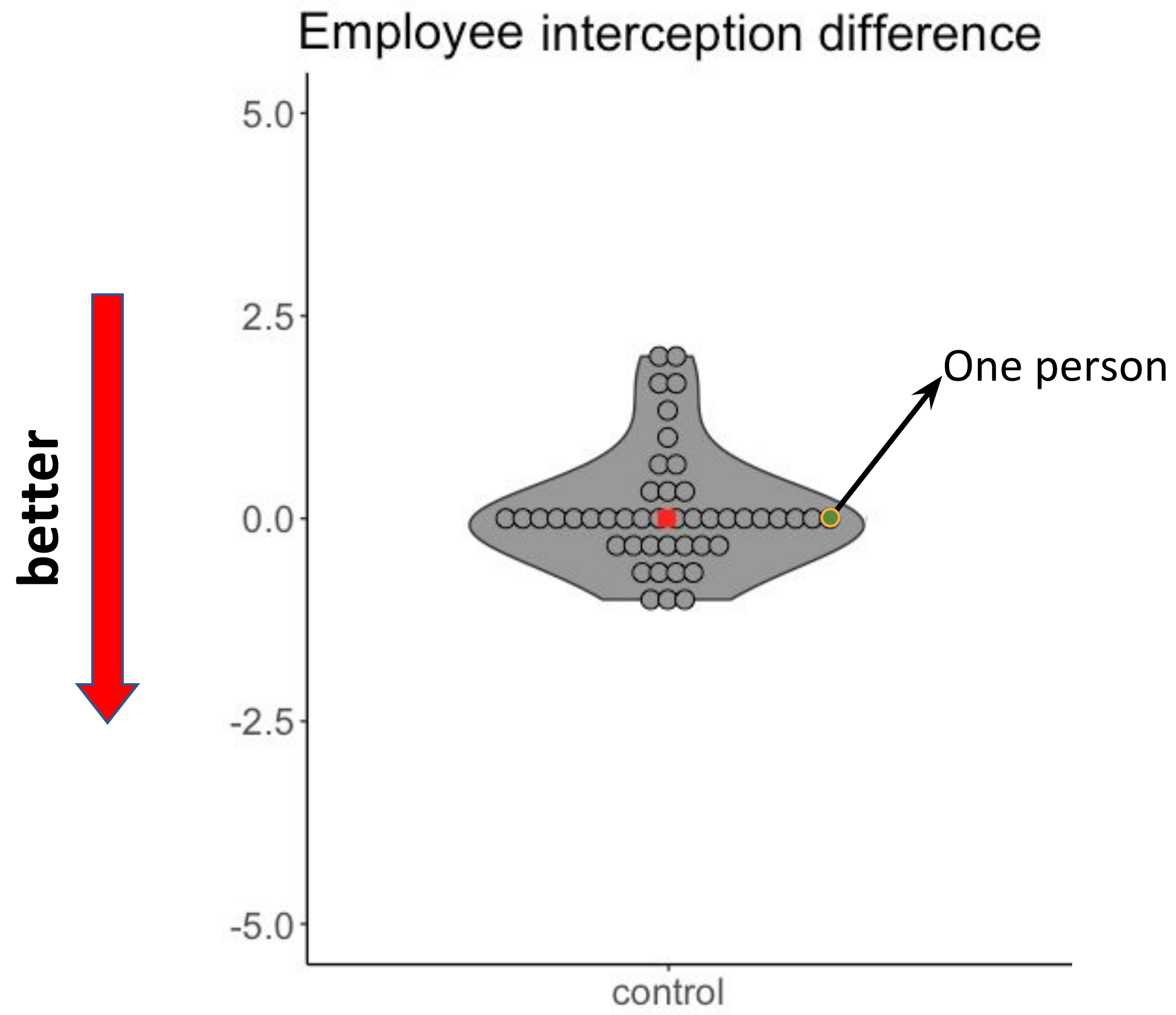
better



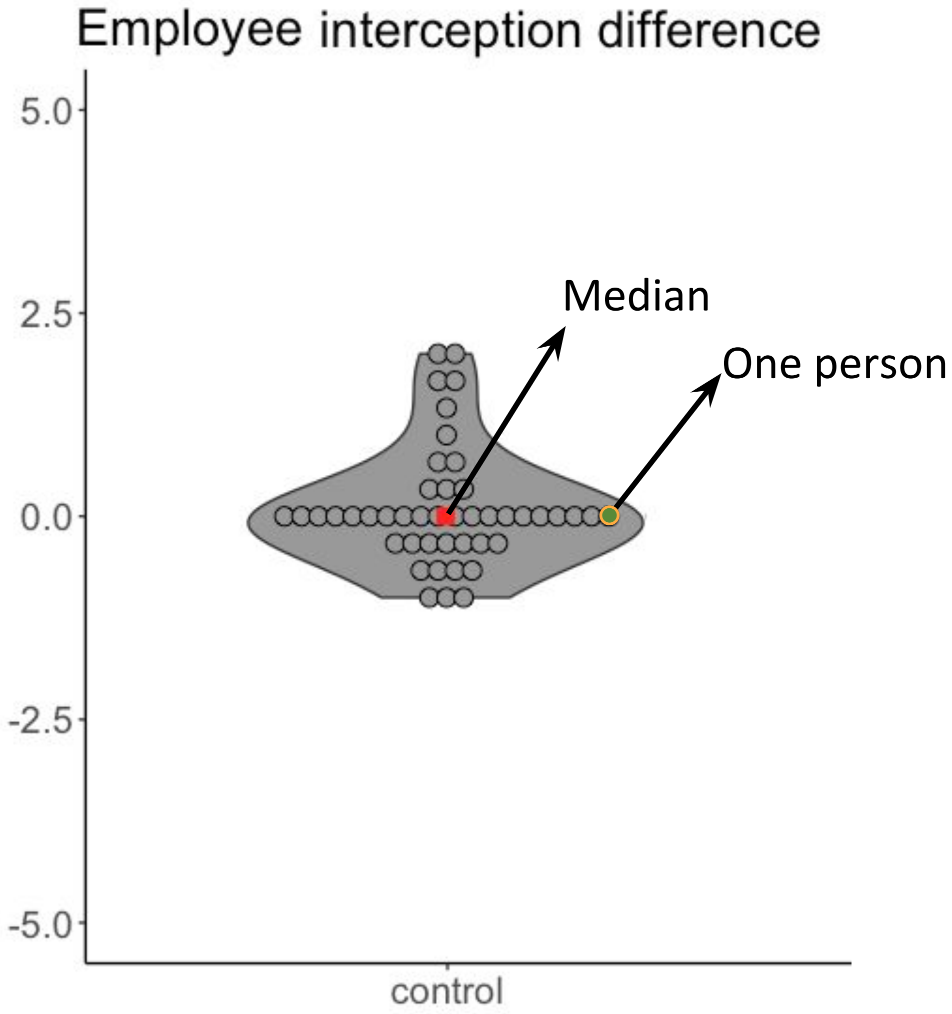
Employee interception difference



better

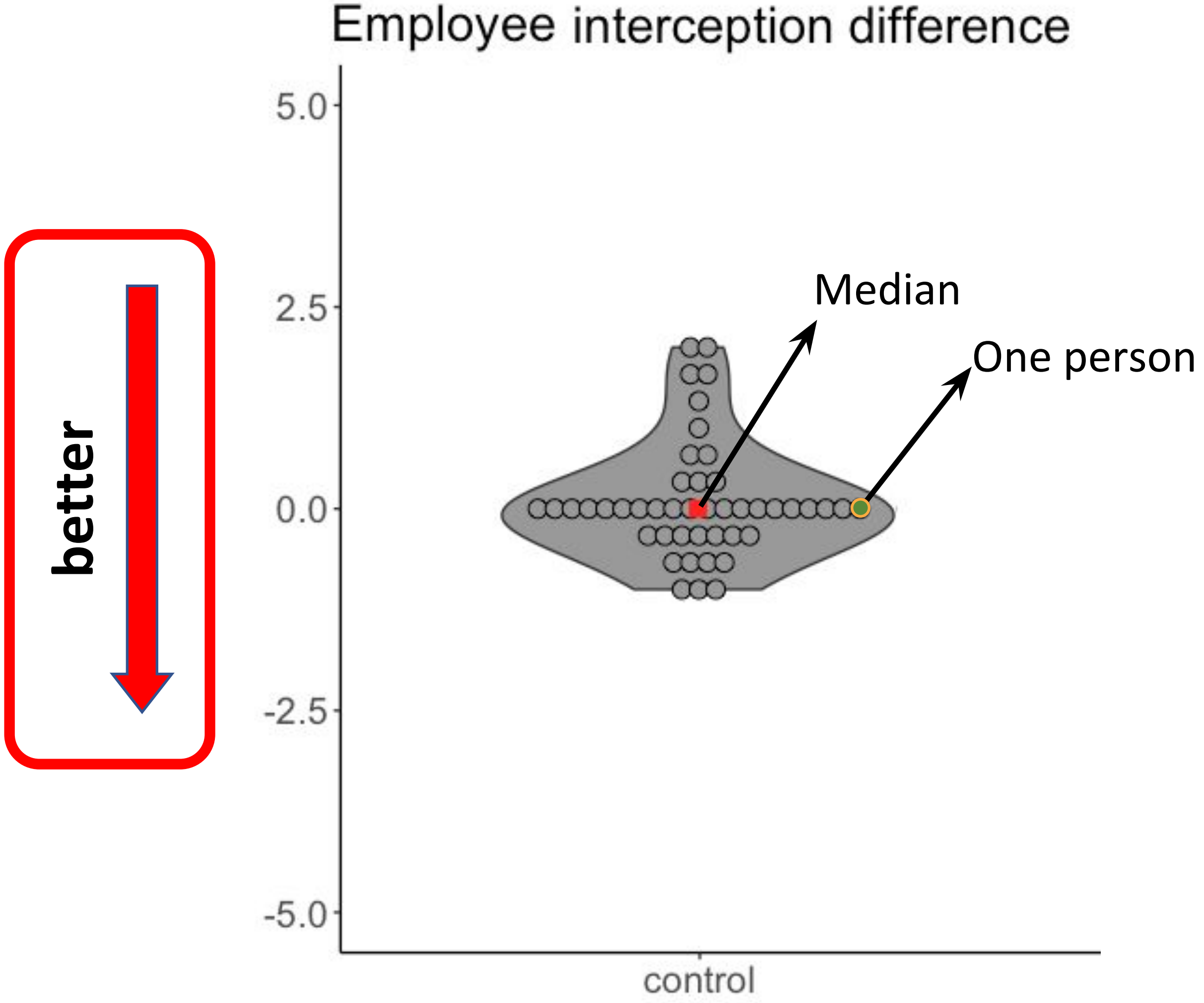

Employee interception difference
5.0
2.5
0.0
-2.5
-5.0
control
better
One person

better



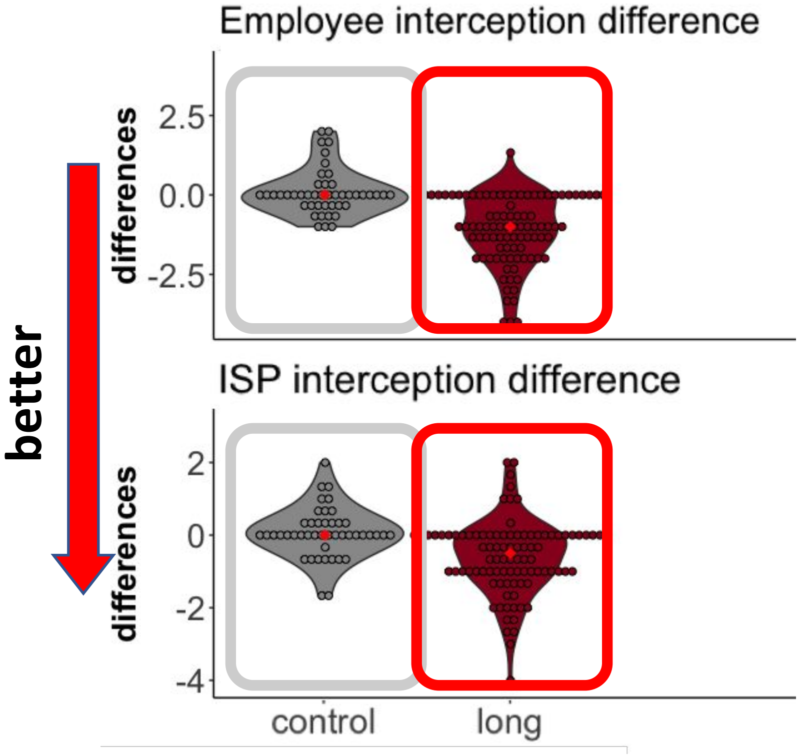
Median

One person


Employee interception difference
5.0
2.5
0.0
-2.5
-5.0
control
Median
One person
better

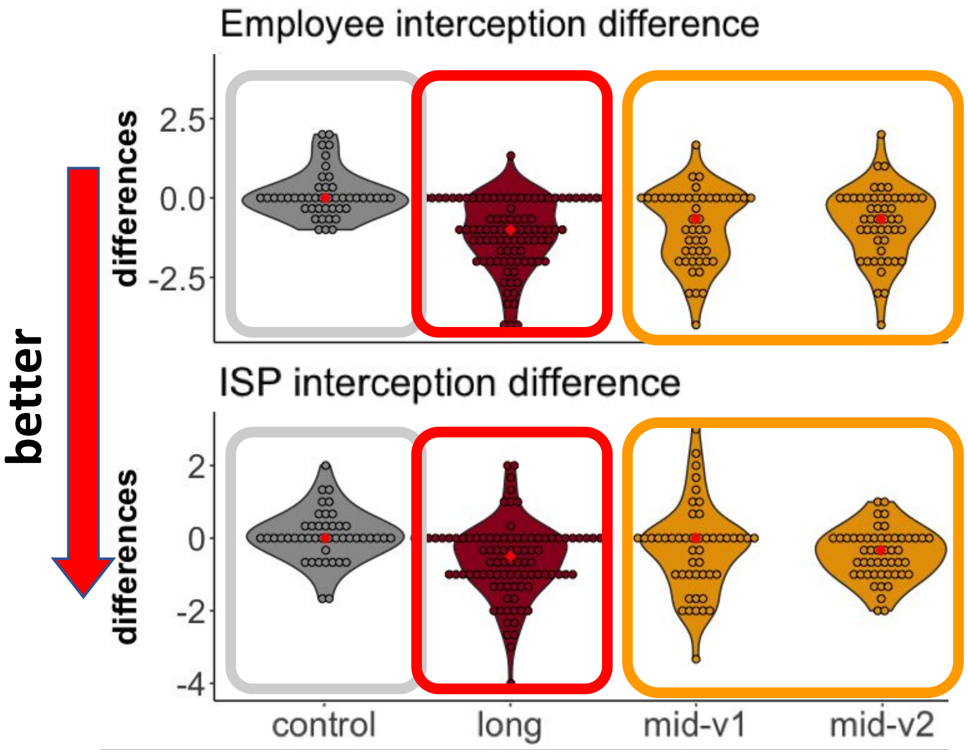
Study 2: Results Highlights

- Long message is generally better than control



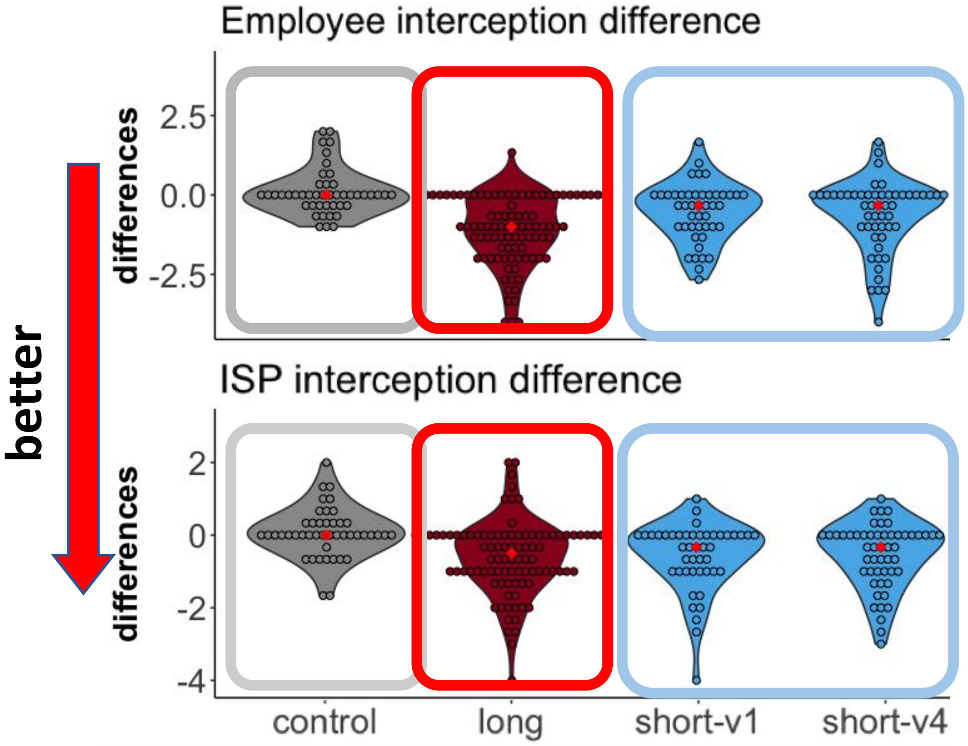
Mediums?

- Mostly better than control
- Mostly not worse than long



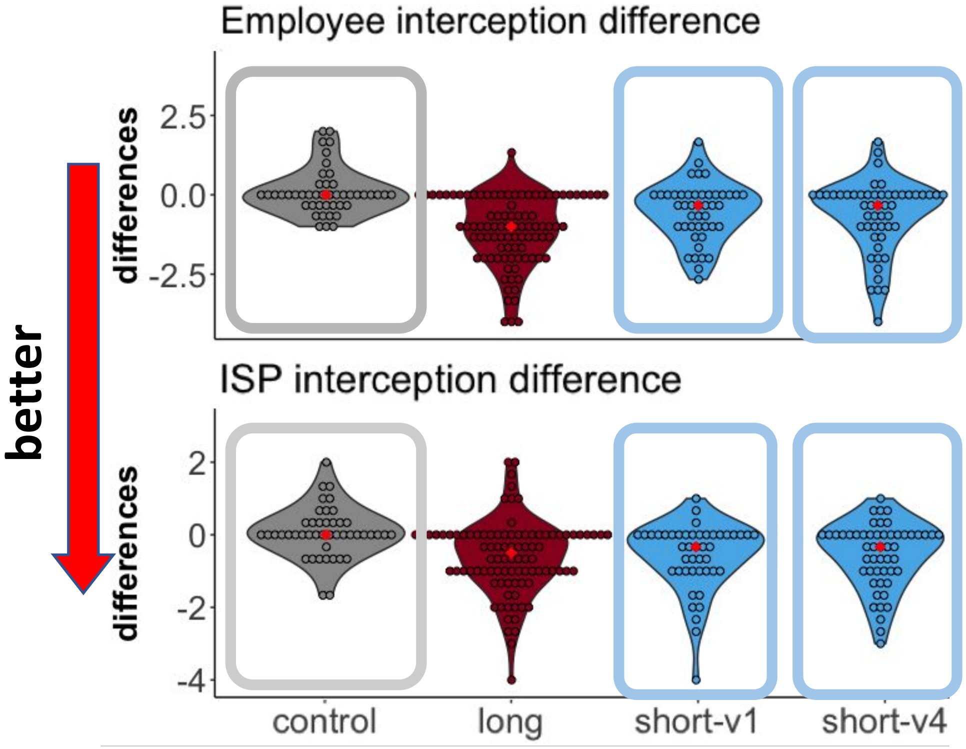
Short messages?

- Similar case to mids



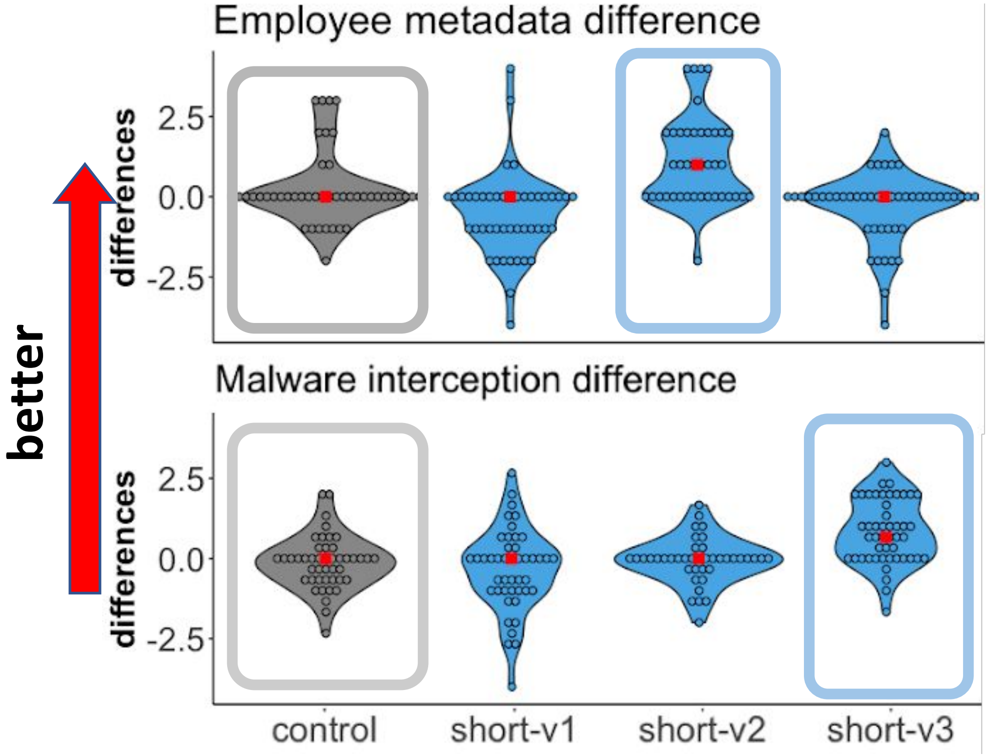
Short messages?

- Similar case to mids
- Some perform better than others generally
  - Only you and the recipient
  - Lock/Key work



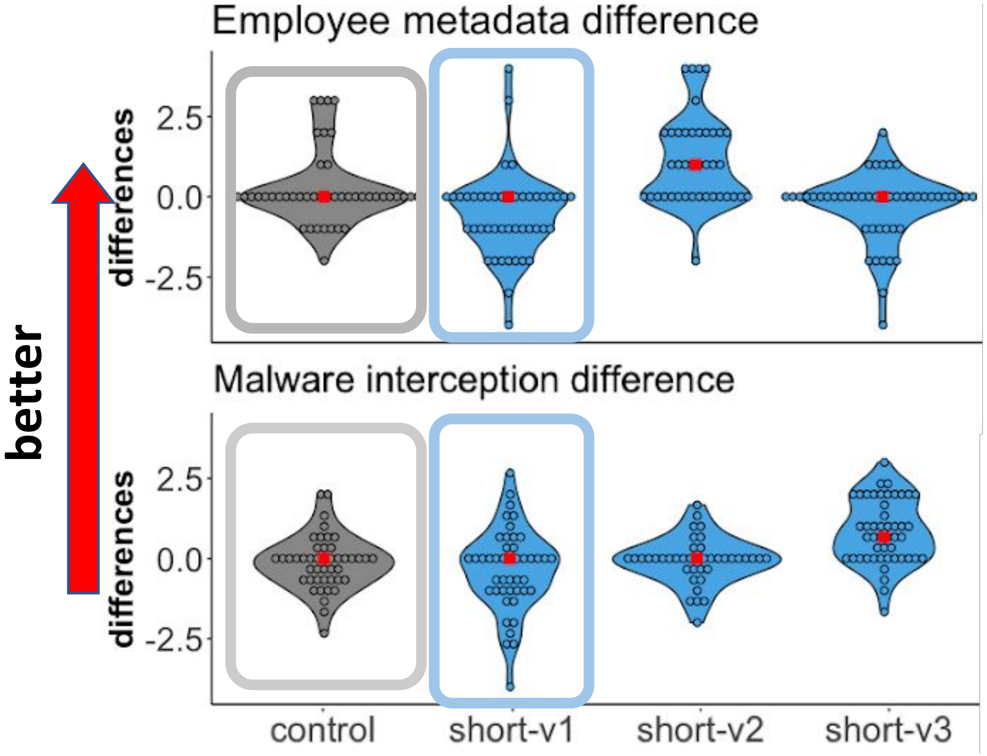
Shorts messages?

- When message is topical, mostly better than all messages



Shorts messages?

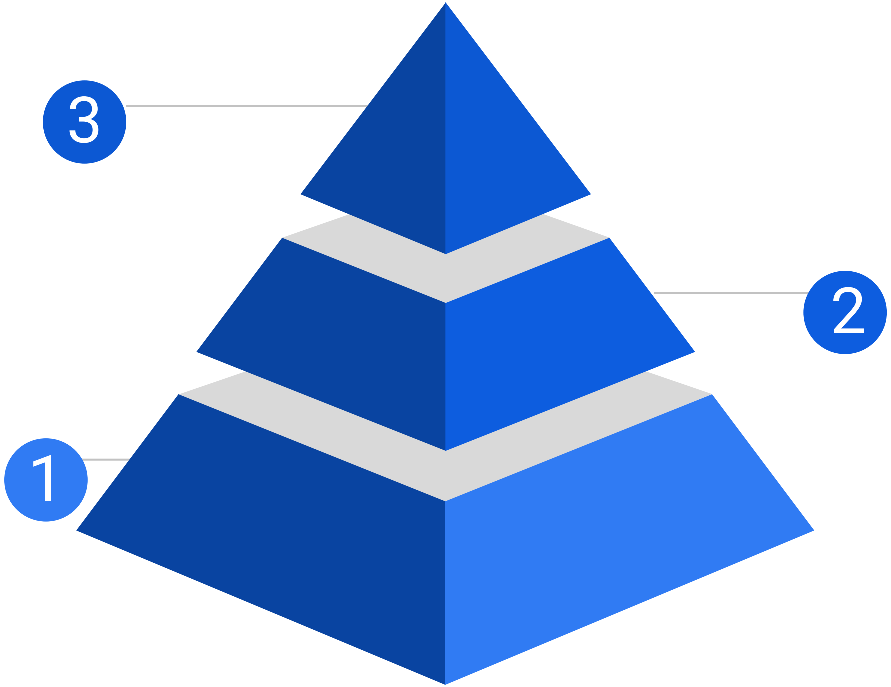
- When message is topical, mostly better than all messages
- But, some additional risk of overcorrecting!



Study 2: Takeaways

- The messages work! (in a controlled environment)
- Short messages work surprisingly well
  - Can be shown one by one to not overwhelm
  - Form a complete mental model

Multi-Stage Efforts: From Lab to Field



Field(ish) Study

- Fit messages to an app
- Daily use for 3 weeks

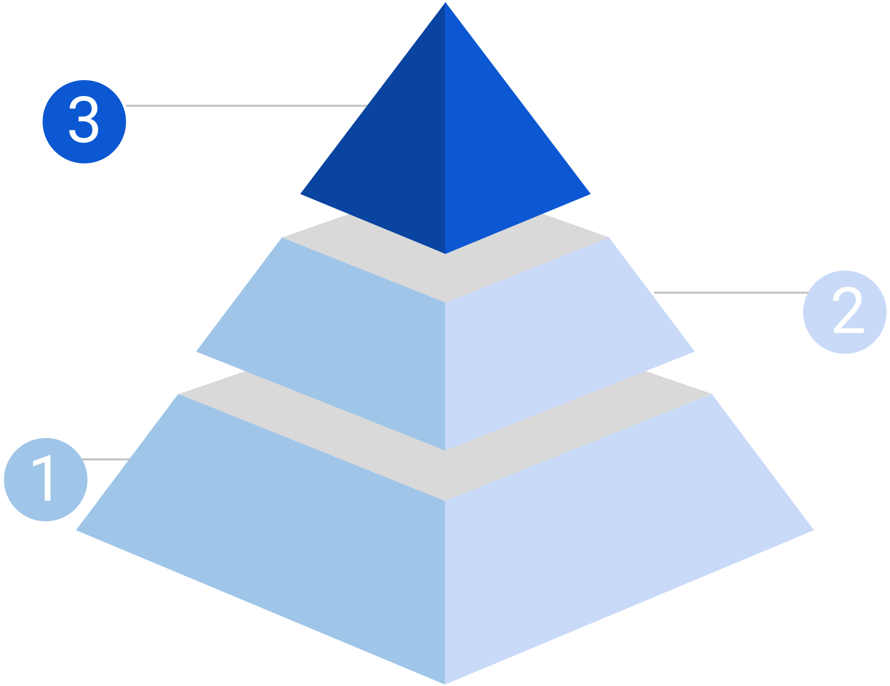
Online Survey

- Test different messages varying in length and contents

Lab Study

- In-depth tutorial

Multi-Stage Efforts: From Lab to Field



Field(ish) Study

- Fit messages to an app
- Daily use for 3 weeks

Online Survey

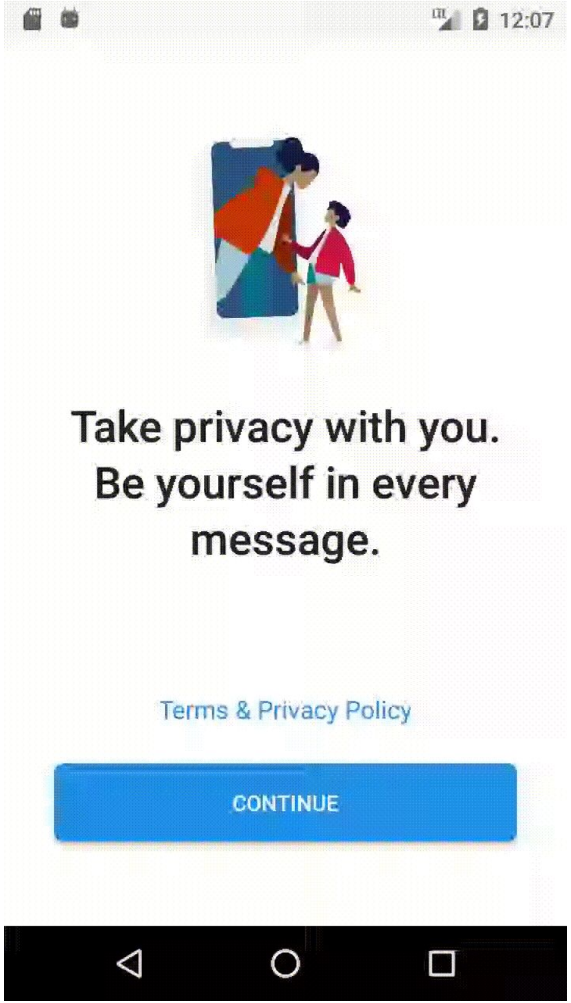
- Test different messages varying in length and contents

Lab Study

- In-depth tutorial

Feeds Into Study 3

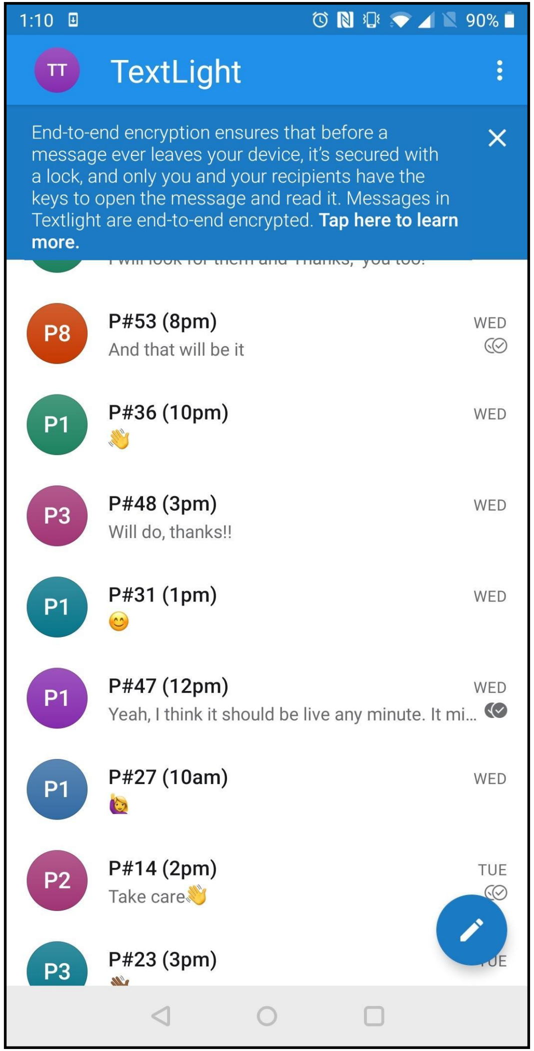
- How well would messages from study 2 work in the real world?
  - (integrated in an app)
- Why does it or why doesn't it work?
  - How can we improve it further?



Take privacy with you. Be yourself in every message.

Study 3 Setup

- Incorporate successful messages from online study into an app (experimental)
  - Show short messages



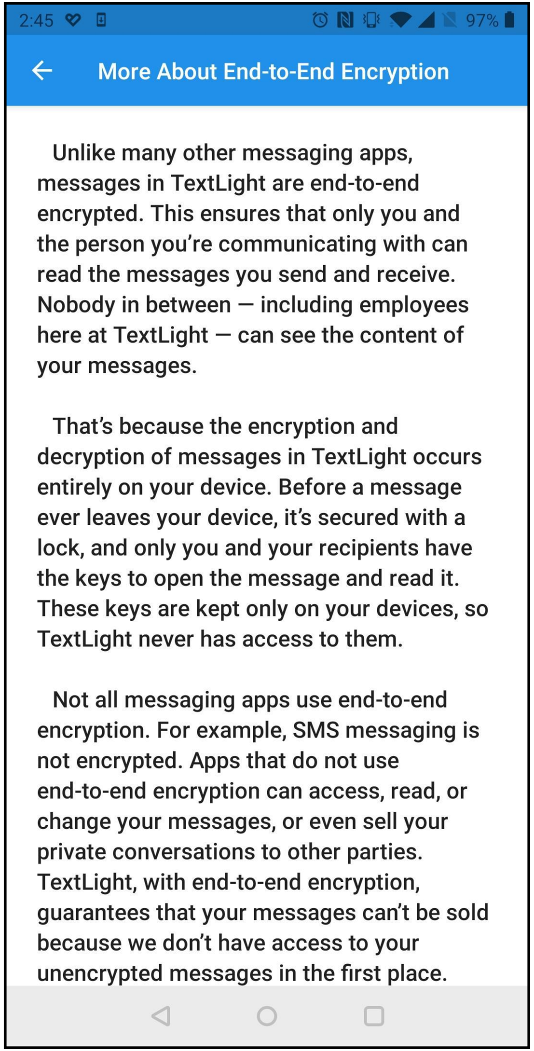
End-to-end encryption ensures that before a message ever leaves your device, it's secured with a lock, and only you and your recipients have the keys to open the message and read it. Messages in Textlight are end-to-end encrypted. **Tap here to learn more.**

I will look for them and Thanks, you too!

P8	P#53 (8pm) And that will be it	WED
P1	P#36 (10pm) 👋	WED
P3	P#48 (3pm) Will do, thanks!!	WED
P1	P#31 (1pm) 😊	WED
P1	P#47 (12pm) Yeah, I think it should be live any minute. It mi...	WED
P1	P#27 (10am) 🙋	WED
P2	P#14 (2pm) Take care👋	TUE
P3	P#23 (3pm)	TUE

Study 3 Setup

- Incorporate successful messages from online study into an app (experimental)
  - Show short messages
  - Clickable to open long message



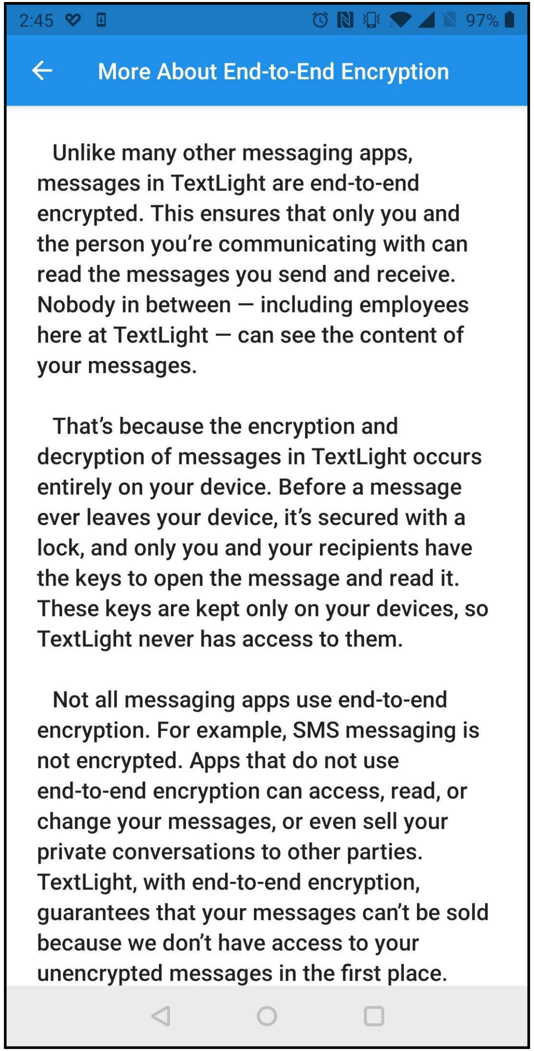
Unlike many other messaging apps, messages in TextLight are end-to-end encrypted. This ensures that only you and the person you're communicating with can read the messages you send and receive. Nobody in between — including employees here at TextLight — can see the content of your messages.

That's because the encryption and decryption of messages in TextLight occurs entirely on your device. Before a message ever leaves your device, it's secured with a lock, and only you and your recipients have the keys to open the message and read it. These keys are kept only on your devices, so TextLight never has access to them.

Not all messaging apps use end-to-end encryption. For example, SMS messaging is not encrypted. Apps that do not use end-to-end encryption can access, read, or change your messages, or even sell your private conversations to other parties. TextLight, with end-to-end encryption, guarantees that your messages can't be sold because we don't have access to your unencrypted messages in the first place.

Study 3 Setup

- Incorporate successful messages from online study into an app (experimental)
    - Show short messages
    - Clickable to open long message
    - Re-brand Signal to TextLight



Unlike many other messaging apps, messages in TextLight are end-to-end encrypted. This ensures that only you and the person you're communicating with can read the messages you send and receive. Nobody in between — including employees here at TextLight — can see the content of your messages.

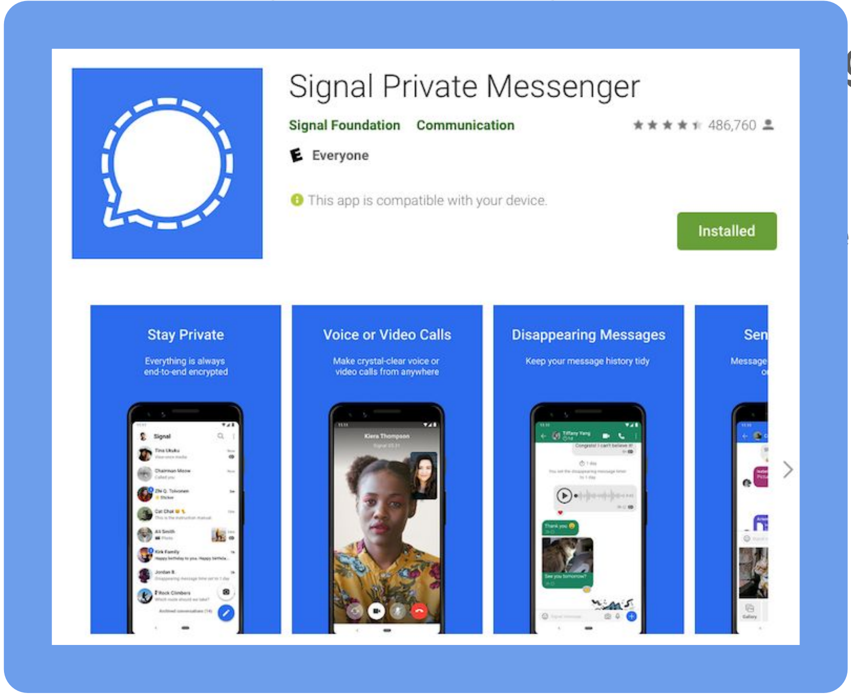
That's because the encryption and decryption of messages in TextLight occurs entirely on your device. Before a message ever leaves your device, it's secured with a lock, and only you and your recipients have the keys to open the message and read it. These keys are kept only on your devices, so TextLight never has access to them.

Not all messaging apps use end-to-end encryption. For example, SMS messaging is not encrypted. Apps that do not use end-to-end encryption can access, read, or change your messages, or even sell your private conversations to other parties. TextLight, with end-to-end encryption, guarantees that your messages can't be sold because we don't have access to your unencrypted messages in the first place.

Study 3 Setup

ges fro

rimenta



Signal Private Messenger

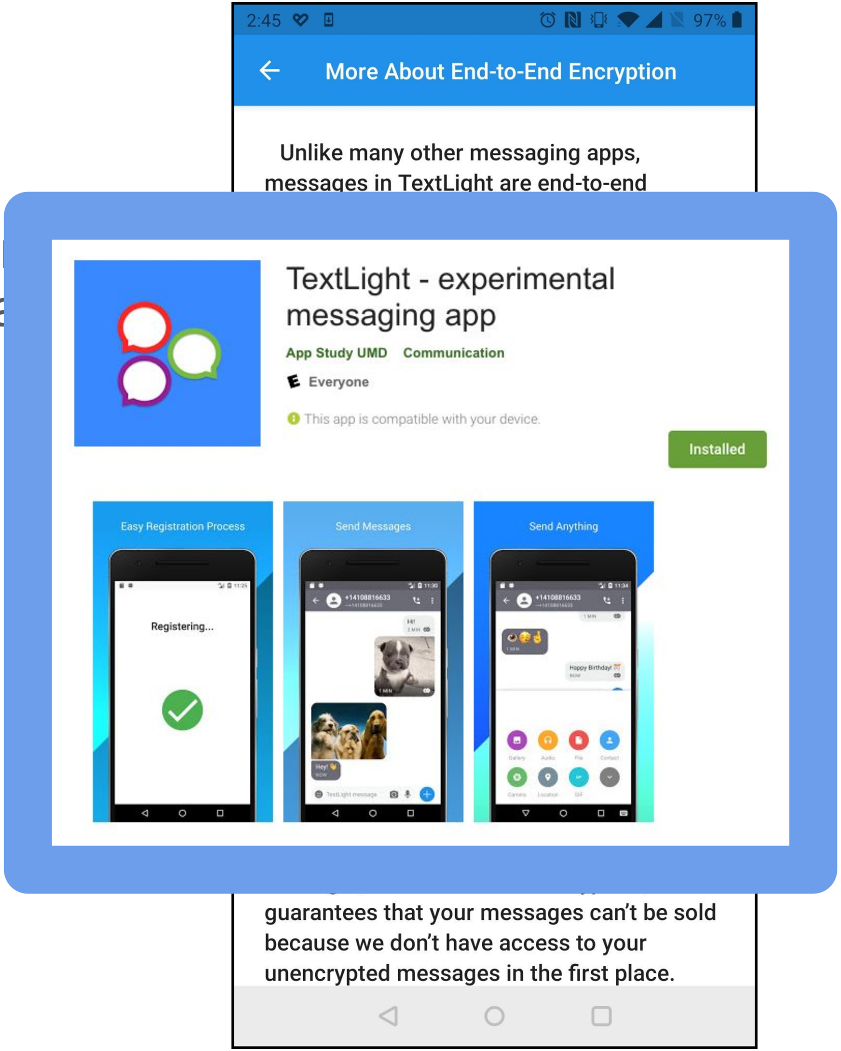
Signal Foundation Communication ★★★★½ 486,760

Everyone

This app is compatible with your device.

Installed

Stay Private
Everything is always end-to-end encrypted
Voice or Video Calls
Make crystal-clear voice or video calls from anywhere
Disappearing Messages
Keep your message history tidy
Sen
Message



2:45 97%

More About End-to-End Encryption

Unlike many other messaging apps, messages in TextLight are end-to-end

TextLight - experimental messaging app

App Study UMD Communication

Everyone

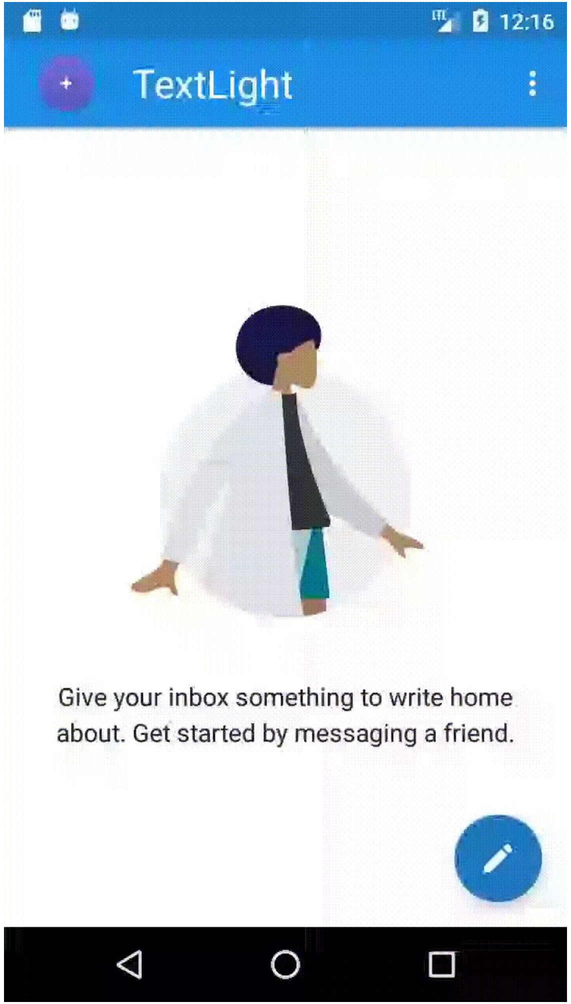
This app is compatible with your device.

Installed

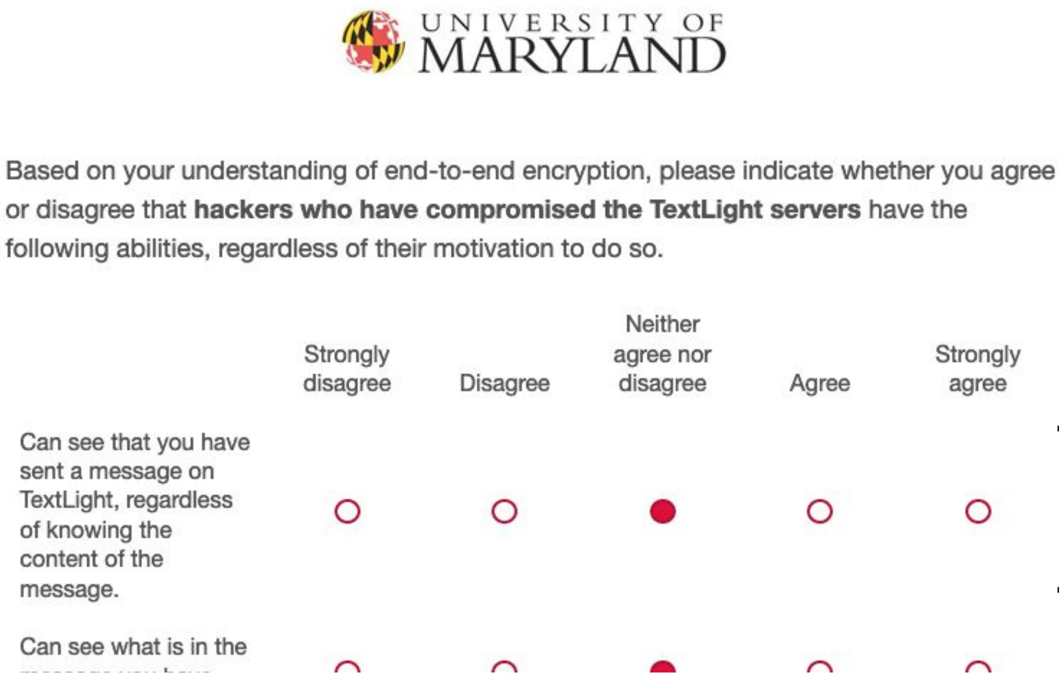
guarantees that your messages can't be sold because we don't have access to your unencrypted messages in the first place.

Study 3 Setup

- Incorporate successful messages from online study into an app (experimental)
    - Show short messages
    - Clickable to open long message
    - Re-brand Signal to TextLight
- Control version that doesn't have the messages
- Use the app for 3 weeks
    - Short texting sessions daily
- Measure change like in study 2



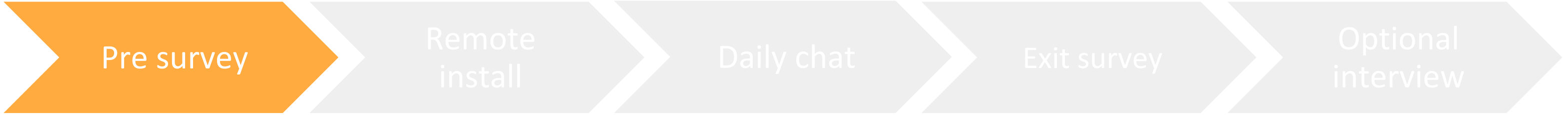
Give your inbox something to write home about. Get started by messaging a friend.

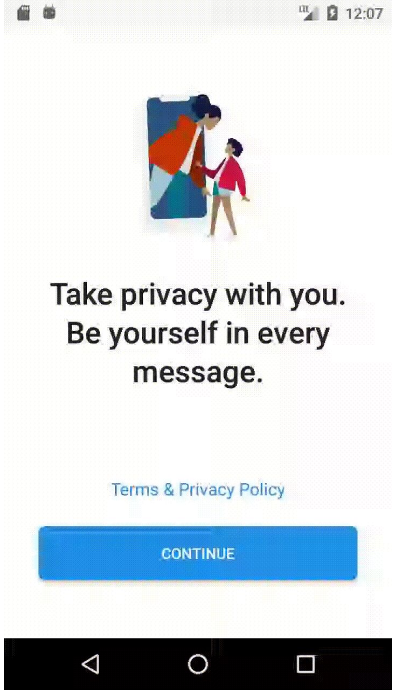


UNIVERSITY OF MARYLAND

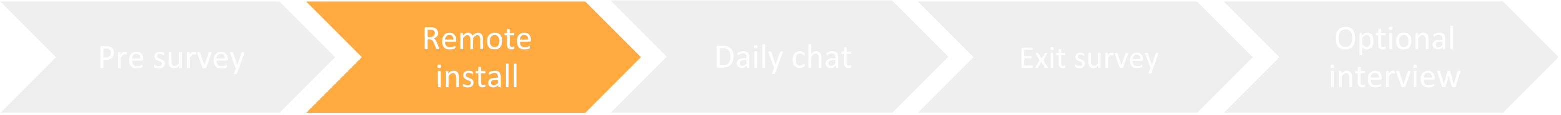
Based on your understanding of end-to-end encryption, please indicate whether you agree or disagree that **hackers who have compromised the TextLight servers** have the following abilities, regardless of their motivation to do so.

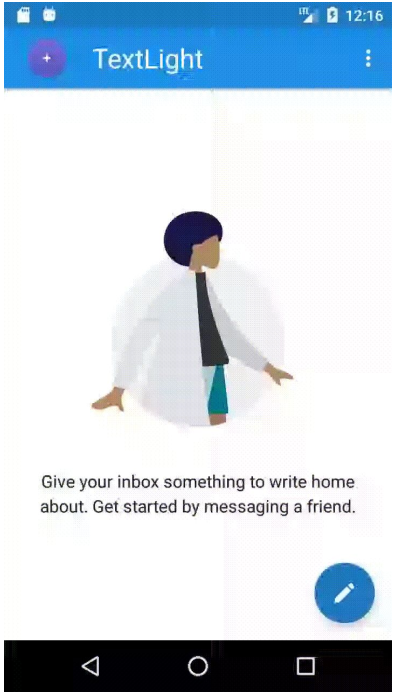
	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Can see that you have sent a message on TextLight, regardless of knowing the content of the message.	○	○	●	○	○
Can see what is in the	○	○	●	○	○



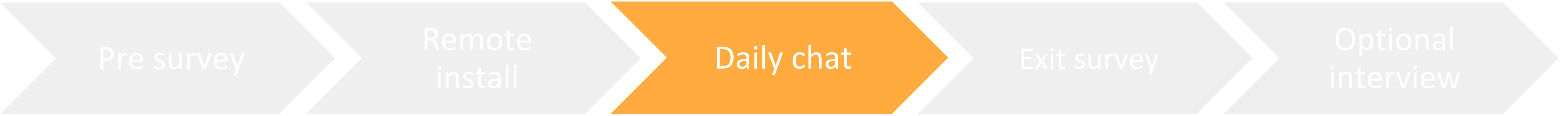


Take privacy with you. Be yourself in every message.





Give your inbox something to write home about. Get started by messaging a friend.



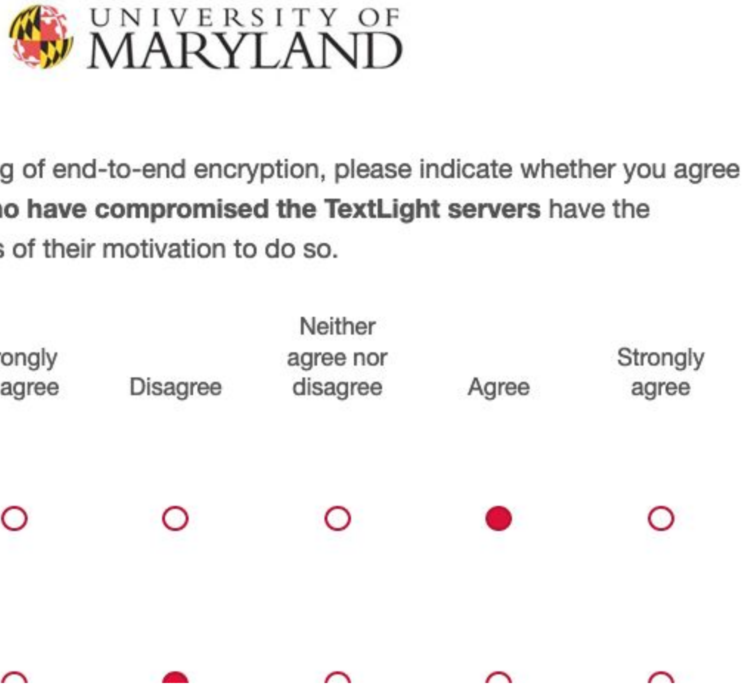
Pre survey

Remote install

Daily chat

Exit survey

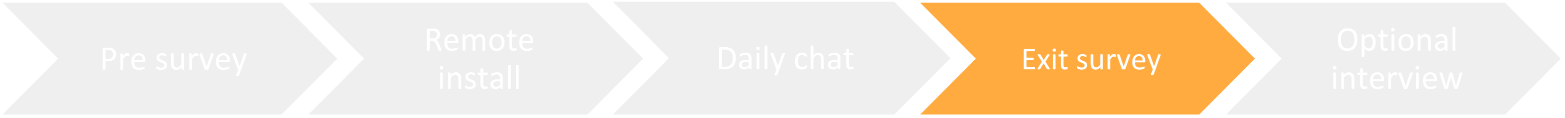
Optional interview



UNIVERSITY OF MARYLAND

Based on your understanding of end-to-end encryption, please indicate whether you agree or disagree that **hackers who have compromised the TextLight servers** have the following abilities, regardless of their motivation to do so.

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
Can see that you have sent a message on TextLight, regardless of knowing the content of the message.	○	○	○	●	○
Can see what is in the	○	●	○	○	○



Pre survey

Remote install

Daily chat

Exit survey

Optional interview

Pre survey

Remote install

Daily chat

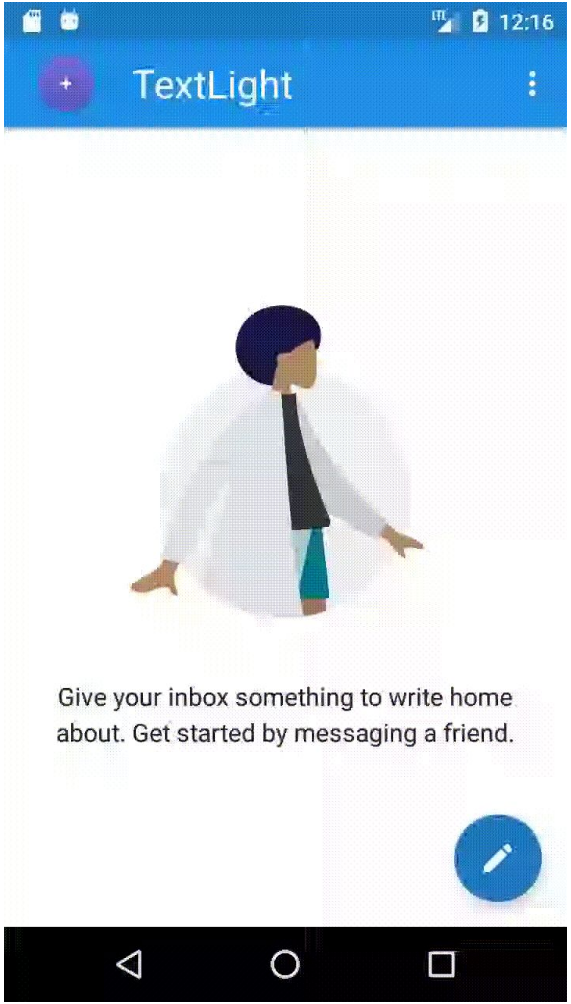
Exit survey

Optional interview

Icon made by Becris from flaticon.com

How did participants use it?

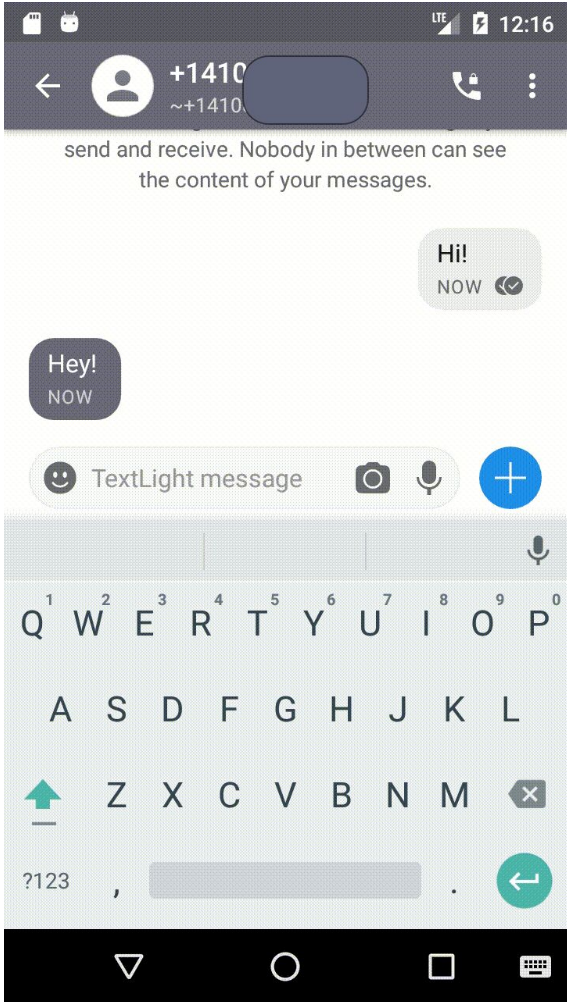
- 61 participants
  - 32 experimental
  - 29 control
  - No usability difference reported
- Days used?
  - median=20, mean=18.5
- Total screen time?
  - mean=2.6 hours, std dev. = 2.25
- Total messages sent?
  - required to send at least 5 a day (100 over 20 days)
  - median=124, mean=138.2



Give your inbox something to write home about. Get started by messaging a friend.

Study 3: Results overview

- Statistically, there is almost no difference between experimental and control groups
- Interviews tell us more



12:16

+1410[redacted]

~+1410.

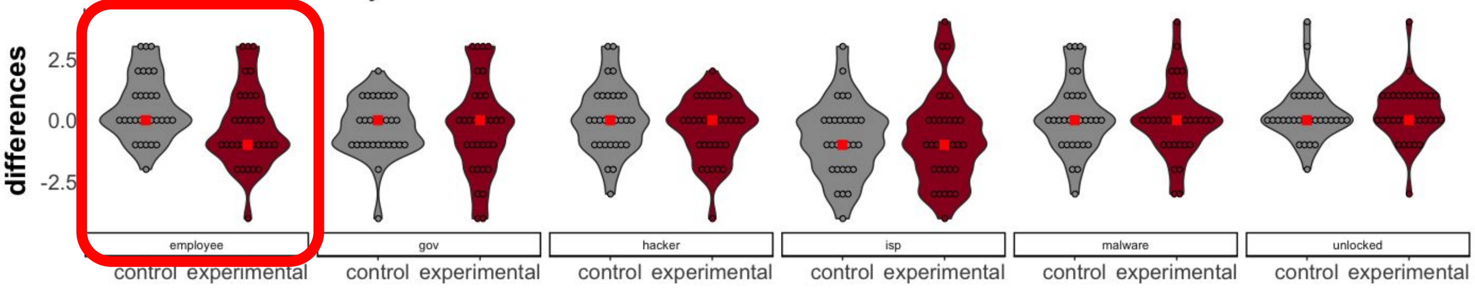
send and receive. Nobody in between can see the content of your messages.

Hi!
NOW

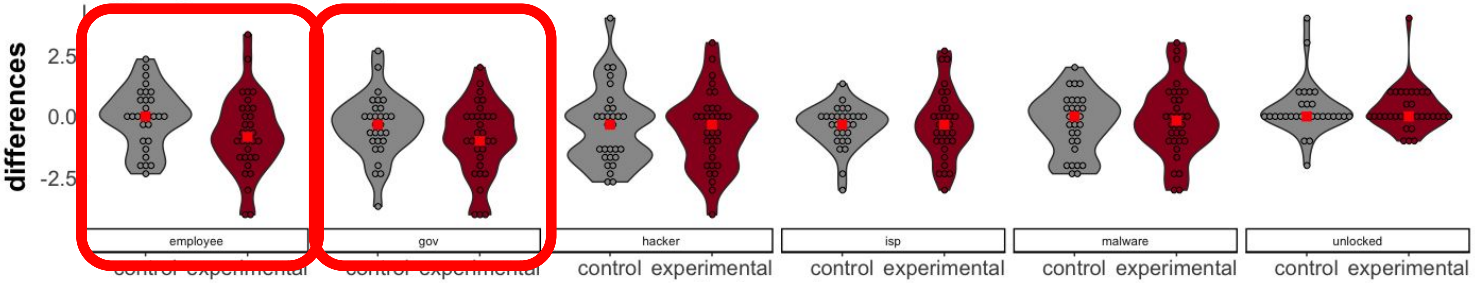
Hey!
NOW

TextLight message

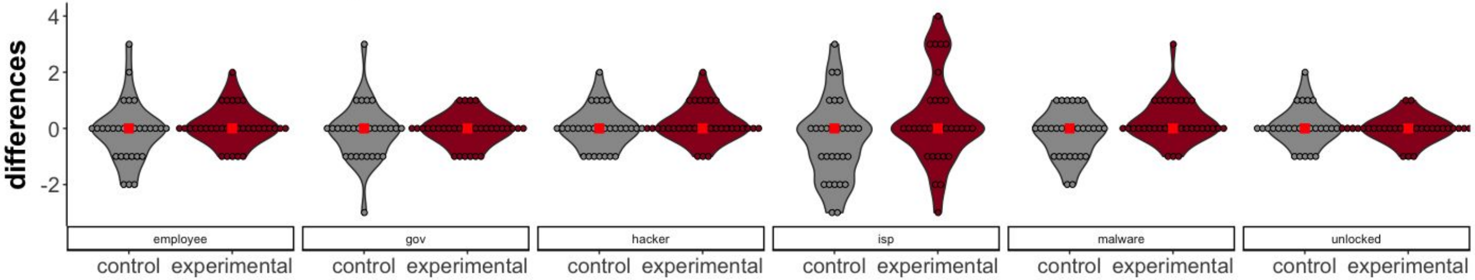
Metadata Capability Differeces



Aggregate Capability Differeces

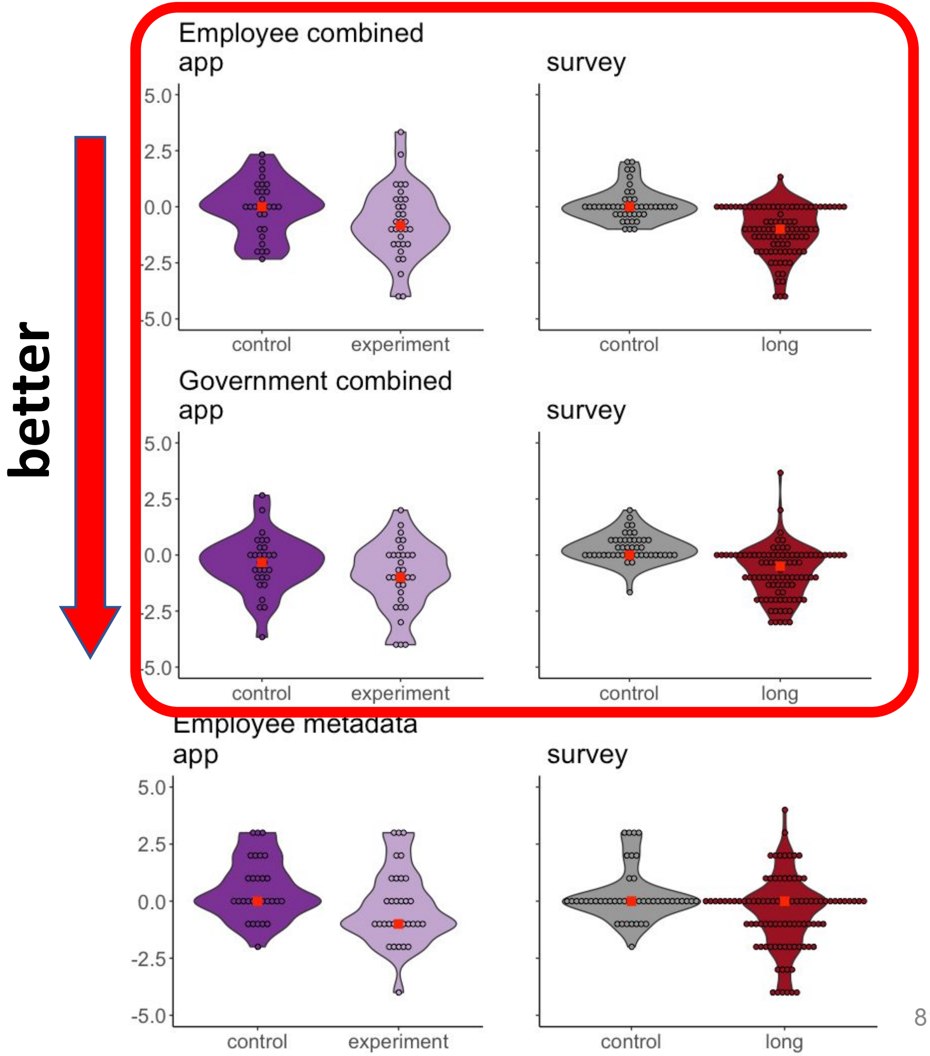


Not-e2ee Capability Differeces



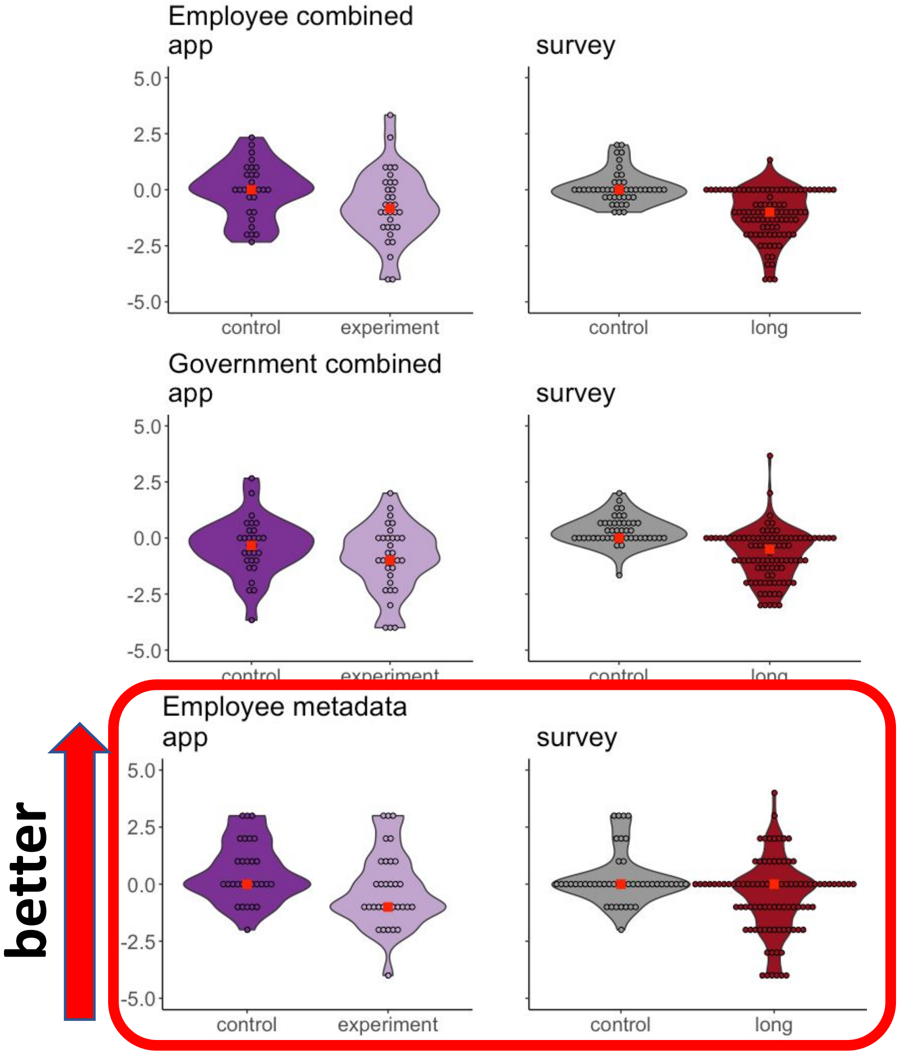
Reminiscent of study 2

- Employee and government shift in the right direction
  - These adversaries had the largest effect sizes in the survey study



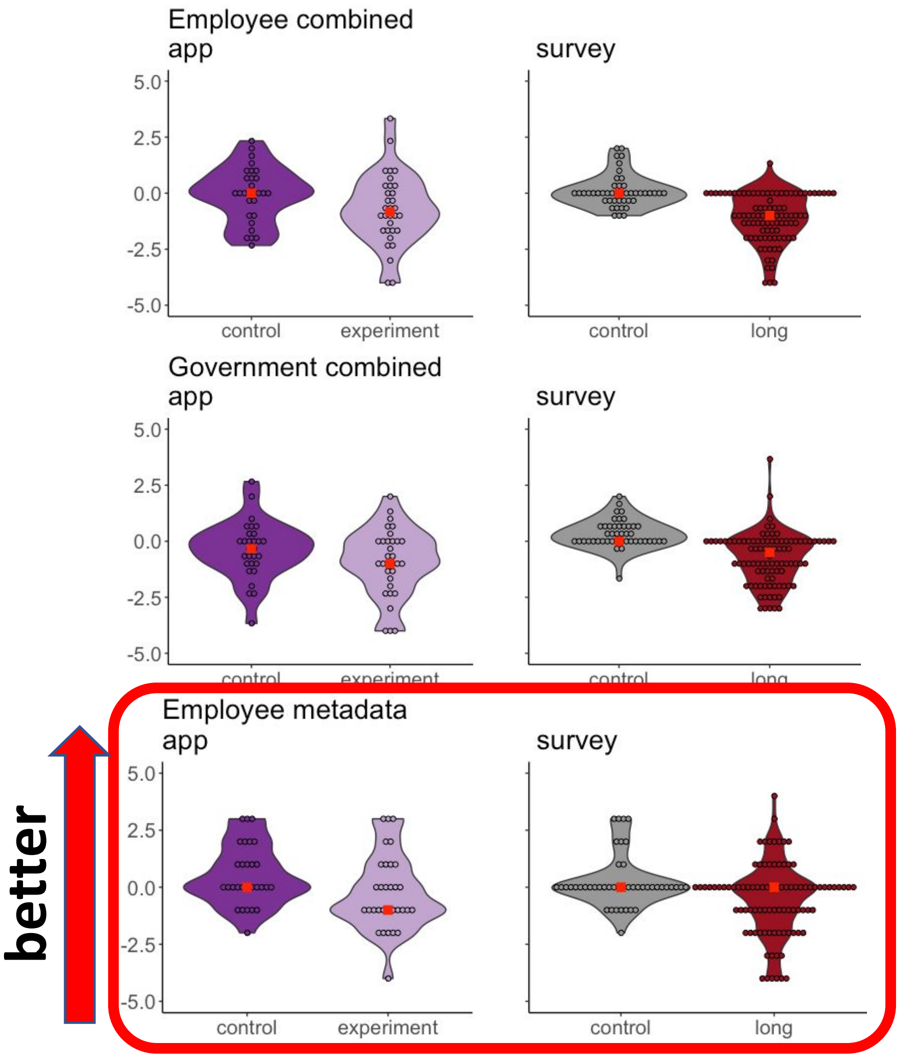
Reminiscent of study 2

- Employee and government shift in the right direction
  - These adversaries had the largest effect sizes in the survey study



Reminiscent of study 2

- Employee and government shift in the right direction
  - These adversaries had the largest effect sizes in the survey study
- Some shift the wrong way
  - (like in the survey study)



Interviews:

- We interviewed 19/32 experimental participants
  - 10/19 participants were able to generalize the concept
    - “ [it protects from] *Probably anyone who would interrupt or interfere in between the messaging, in between where you sent it and someone else received it.*”
  - 14/19 knew the unlocked phone adversary was powerful
  - 9/19 participants got at least something wrong about E2EE
    - “ [it protects from] *people … hacking into your phone … from either reading the messages or altering the contents of the message.*”
  - 9/19 said they didn’t read the messages or weren’t interested in them.
    - “*I obviously didn't pay a lot of attention to it.*”

Study 3 takeaways

- No statistically significant changes in mental models, but;
  - The strongest effects seen in study 2 show themselves
  - There is some overselling
  - Some had decent mental models when interviewed
- The messages might have to be made more obvious
  - Even if it sacrifices some usability.
  - Some users simply ignored the messages

Summary

Questions? → akgul@cs.umd.edu |@_oakgul
wbai@umiacs.umd.edu

- Mental models of secure communication: not **functional** enough
- Can **small nudges** and user-centered design improve things?
  - Initial qualitative study to identify topics, messages
  - Online study to examine specific messages
  - Longitudinal study to measure real-world effectiveness

- We identify key items to teach users.
- They work well when we **control external factors**.
- **Integration** to applications might need to be more obvious.
  - Perhaps by sacrificing usability a little bit.

References

1. W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek. An inconvenient trust: User attitudes toward security and usability tradeoffs for key-directory encryption systems. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), pages 113–130, Denver, CO, June 2016. USENIX Association.
2. W. Bai, D. Kim, M. Namara, Y. Qian, P. G. Kelley, and M. L. Mazurek. Balancing security and usability in encrypted email. IEEE Internet Computing, 21(3):30–38, May 2017.
3. Wei Bai, Michael Pearson, Patrick Gage Kelley, and Michelle L. Mazurek. Improving Non-Experts' Understanding of End-to-End Encryption: An Exploratory Study. In IEEE 5th European Workshop on Usable Security (EuroUSEC), 2020.
4. W. Diffie and M. E. Hellman. New directions in cryptography. Information Theory, IEEE Transactions on, 22(6):644–654, Nov 1976.
5. S. Fahl, M. Harbach, T. Muders, and M. Smith. Confidentiality as a Service – usable security for the cloud. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on, pages 153–162, June 2012.
6. S. Fahl, M. Harbach, T. Muders, M. Smith, and U. Sander. Helping johnny 2.0 to encrypt his facebook conversations. In Proceedings of the Eighth Symposium on Usable Privacy and Security, SOUPS '12, pages 11:1–11:17. ACM, 2012.
7. S. L. Garfinkel and R. C. Miller. Johnny 2: a user test of key continuity management with S/MIME and Outlook Express. In Proceedings of the 2005 Symposium on Usable Privacy and Security, SOUPS '05, pages 13–24. ACM, 2005.
8. S. Gaw, E. W. Felten, and P. Fernandez-Kelly. Secrecy, flagging, and paranoia: Adoption criteria in encrypted email. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '06, pages 591–600, New York, NY, USA, 2006. ACM.

References

9. S. E. McGregor, P. Charters, T. Holliday, and F. Roesner. Investigating the Computer Security Practices and Needs of Journalists. In 24th USENIX Security Symposium (USENIX Security 15), pages 399–414. USENIX Association, 2015.
10. M. S. Melara, A. Blankstein, J. Bonneau, E. W. Felten, and M. J. Freedman. CONIKS: Bringing key transparency to end users. In 24th USENIX Security Symposium (USENIX Security 15), pages 383–398. USENIX Association, Aug. 2015.
11. S. Ruoti, J. Anderson, S. Heidbrink, M. O'Neill, E. Vaziripour, J. Wu, D. Zappala, and K. Seamons. "We're on the same page": A usability study of secure email using pairs of novice users. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '16, pages 4298–4308, New York, NY, USA, 2016. ACM.
12. S. Ruoti, N. Kim, B. Ben, T. van der Horst, and K. Seamons. Confused Johnny: when automatic encryption leads to confusion and mistakes. In Proceedings of the Ninth Symposium on Usable Privacy and Securit, SOUPS '13, pages 5:1–5:12. ACM, July 2013.
13. M. D. Ryan. Enhanced certificate transparency and end-to-end encrypted mail. In 21st Annual Network and Distributed System Security Symposium, NDSS'14, 2014.
14. S. Sheng, L. Broderick, C. A. Koranda, and J. J. Hyland. Why Johnny still can't encrypt: evaluating the usability of email encryption software. In Proceedings of the Second Symposium on Usable Privacy and Security, SOUPS '06, 2006.
15. D. J. Solove. 'I've got nothing to hide' and other misunderstandings of privacy. San Diego Law Review, 44:745, 2007.

References

16. W. Tong, S. Gold, S. Gichohi, M. Roman, and J. Frankle. Why King George III can encrypt. http://randomwalker.info/teaching/spring-2014-privacy-technologies/king-george-iiiencrypt.pdf, 2014.
17. A. Whitten and J. D. Tygar. Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In Proceedings of the 8th Conference on USENIX Security Symposium - Volume 8, SSYM'99, pages 14–14, 1999.
18. R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the adoption of secure communication tools. In 2017 IEEE Symposium on Security and Privacy (SP), pages 137–153, San Jose, CA, May 2017. IEEE Computer Society.
19. F. Asgharpour, D. Liu, and L. J. Camp. Mental models of security risks. In Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security, FC'07/USEC'07, pages 367–377, Berlin, Heidelberg, 2007. Springer-Verlag.
20. S. Dechand, A. Naiakshina, A. Danilova, and M. Smith. In encryption we don't trust: The effect of end-to-end encryption to the masses on user perception. In 2019 IEEE European Symposium on Security and Privacy (EuroS&P), pages 401–415, Stockholm, Sweden, June 2019. IEEE Computer Society.
21. A. Demjaha, J. Spring, I. Becker, S. Parkin, and A. Sasse. Metaphors considered harmful? an exploratory study of the effectiveness of functional metaphors for end-to-end encryption. In Workshop on Usable Security. Internet Society, 2018.
22. Electronic Frontier Foundation. Secure Messaging Scorecard, 2016. https://www.eff.org/node/82654.
23. N. Gerber, V. Zimmermann, B. Henhapl, S. Emeröz, and M. Volkamer. Finally johnny can encrypt: But does this make him feel more secure? In Proceedings of the 13th International Conference on Availability, Reliability and Security, ARES 2018, pages 11:1–11:10, New York, NY, USA, 2018. ACM.

References

24. J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts. Trustworthy and effective communication of cybersecurity risks: A review. In 2011 1st Workshop on Socio-Technical Aspects in Security and Trust (STAST), pages 60–68, Sep. 2011.
25. S. Schröder, M. Huber, D. Wind, and C. Rottermanner. When Signal Hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging. In European Workshop on Usable Security (EuroUSEC), Darmstadt, Germany, 2016. Internet Society.
26. J. Tan, L. Bauer, J. Bonneau, L. F. Cranor, J. Thomas, and B. Ur. Can unicorns help users compare crypto key fingerprints? In Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI ’17, pages 3787–3798, New York, NY, USA, 2017. ACM.
27. E. Vaziripour, J. Wu, M. O’Neill, D. Metro, J. Cockrell, T. Moffett, J. Whitehead, N. Bonner, K. Seamons, and D. Zappala. Action needed! helping users find and complete the authentication ceremony in signal. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), pages 47–62, Baltimore, MD, August 2018. USENIX Association.
28. E. Vaziripour, J. Wu, M. O’Neill, J. Whitehead, S. Heidbrink, K. Seamons, and D. Zappala. Is that you, alice? A usability study of the authentication ceremony of secure messaging applications. In Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017), pages 29–47, Santa Clara, CA, July 2017. USENIX Association.
29. J. Warshaw, N. Taft, and A. Woodruff. Intuitions, analytics, and killing ants: Inference literacy of high school-educated adults in the US. In Twelfth Symposium on Usable Privacy and Security (SOUPS 2016), pages 271–285, Denver, CO, June 2016. USENIX Association.

References

30. J. Wu, C. Gattrell, D. Howard, J. Tyler, E. Vaziripour, D. Zappala, and K. Seamons. "something isn’t secure, but i’m not sure how that translates into a problem": Promoting autonomy by designing for understanding in signal. In Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019), pages 137–154, Santa Clara, CA, August 2019. USENIX Association.
31. J. Wu and D. Zappala. When is a tree really a truck? Exploring mental models of encryption. In Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018), pages 395–409, Baltimore, MD, August 2018. USENIX Association.
32. K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. Zezschwitz, “‘If HTTPS were secure, I wouldnt need 2FA’: End user and administrator mental models of HTTPS,” in IEEE Symposium on Security and Privacy, May 2019.