

Hacking Your Thoughts:
Batman Forever meets Black Mirror

Katherine Pratt

DEFCON 27

10 Aug 19

The Standard Disclaimer

The work in this presentation was done at the University of Washington as part of a PhD dissertation. The results and views presented here do not necessarily represent those of my funding sources or my current employer.

Summary of Presentation

- Separating hype from reality
- Some experimental result
- Do consumers care about their neural privacy?
- Thoughts about proactive policy solutions:
  what do I want all of you to do?

Things NOT Covered by This Presentation

- Aliens are not involved
- I know nothing about any chips that the government has implanted

Definitions Before We Get Started

- **Brain Computer Interfaces (BCIs)**: can record brain activity while an individual is performing different actions (for example, blinking their eyes, playing a video game, or texting on a phone). BCIs are often used to give a user control of a computer using their brain activity.

Definitions Before We Get Started

- **Brain Computer Interfaces (BCIs)**: can record brain activity while an individual is performing different actions (for example, blinking their eyes, playing a video game, or texting on a phone). BCIs are often used to give a user control of a computer using their brain activity.
- **Targeted elicitation**: showing specific stimuli in order to obtain a particular response

What do you think of when you hear “Brain Hacking”?


VAL KILMER
TOMMY LEE JONES
JIM CARREY
BATMAN FOREVER
NICOLE KIDMAN
CHRIS O'DONNELL
JUNE 16

IMDb



You've sucked Gotham's brain waves and now you've devised a way to read minds!

You betcha! Soon my little "Box" will be on countless TVs around the world. Feeding me, credit card numbers, bank codes, sexual fantasies, and little white lies.



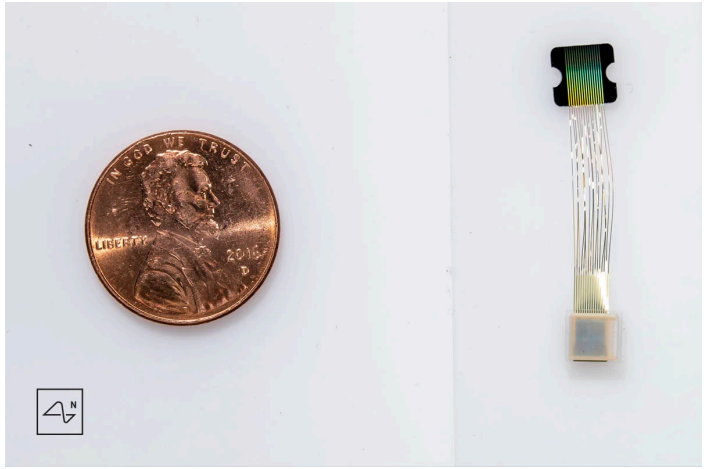

IMDb

This means that some of what you expect… isn't really possible.

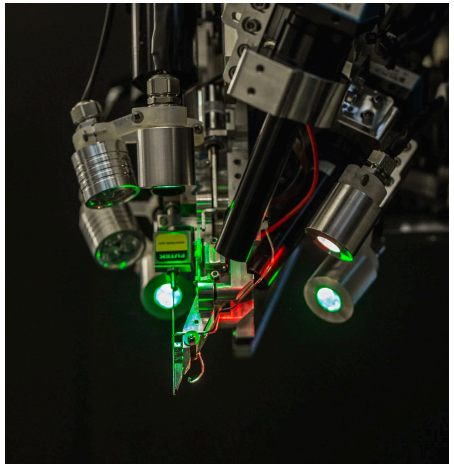
Separating Hype from Reality: Neuralink

AN INTEGRATED BRAIN-MACHINE INTERFACE PLATFORM WITH THOUSANDS OF CHANNELS

Elon Musk & Neuralink



Neuralink via Scientific American



- No feedback loop for information to return to brain from "reanimated" limbs
- Unclear how this implantation technique will work for deeper brain structures
- Possibility of profound side effects by stimulating brain tissue (Deep Brain Stimulator literature)

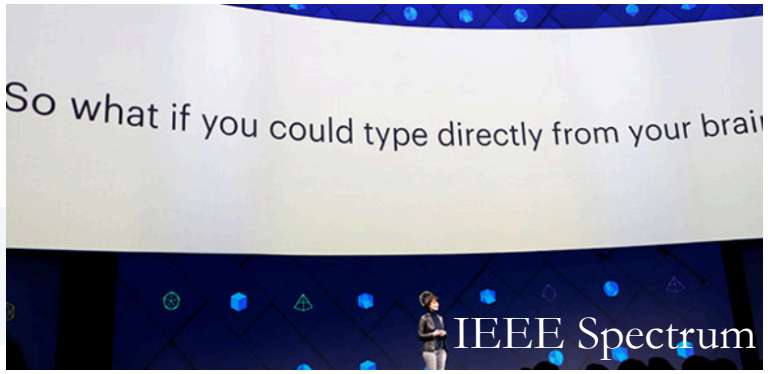
Separating Hype from Reality: Facebook

20 Apr 2017 | 17:30 GMT

Facebook Announces "Typing-by-Brain" Project

Facebook promises 100 words per minute, but doesn't detail the technology that can pull that off

By **Eliza Strickland**



nature COMMUNICATIONS

Article | OPEN | Published: 30 July 2019

Real-time decoding of question-and-answer speech dialogue using human cortical activity

David A. Moses, Matthew K. Leonard, Joseph G. Makin & Edward F. Chang

Nature Communications **10**, Article number: 3096 (2019) | Download Citation

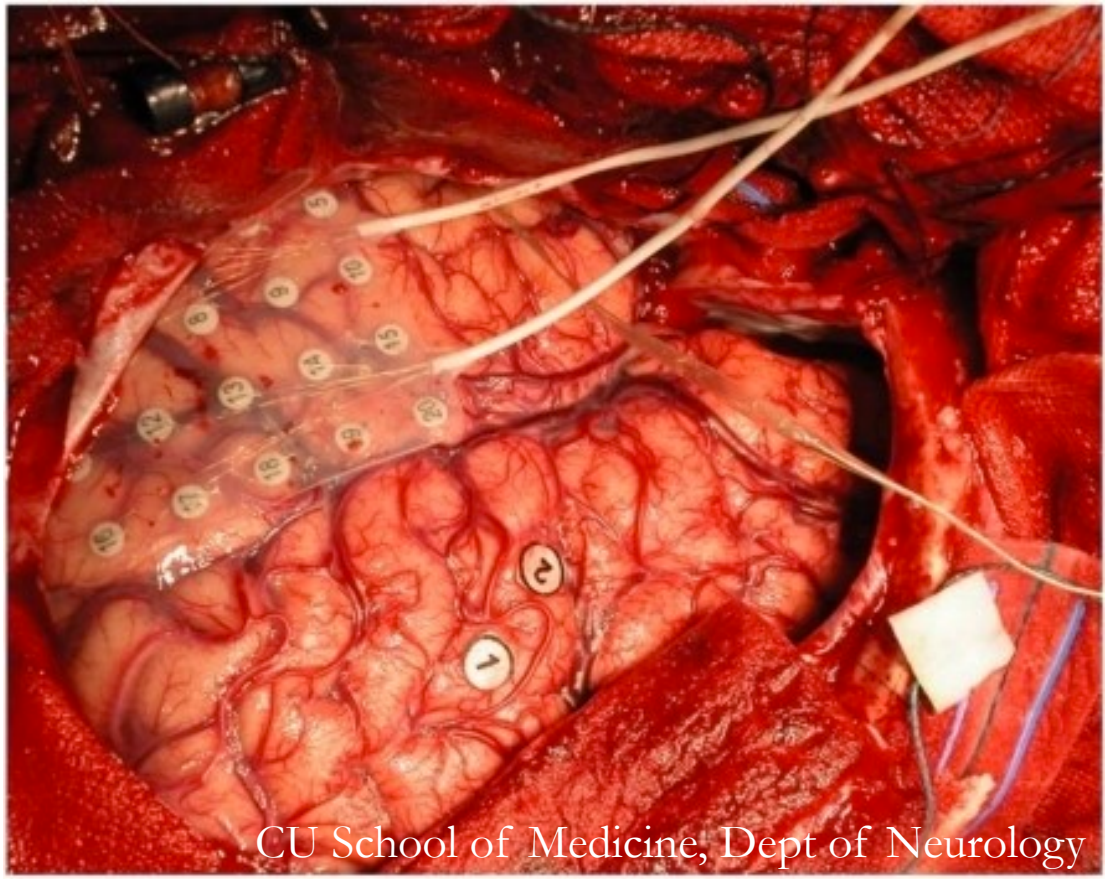
- Current gold standard for "typing-by-brain" is ~1 word per minute
- Published research study only done with 3 subjects, using incredibly invasive surgically placed electrodes
- Do you really want Facebook to have direct access to all of your thoughts and reactions?


Mark Stone/University of Washington



CAUTION: GORY PICTURE NEXT


Mark Stone/University of Washington

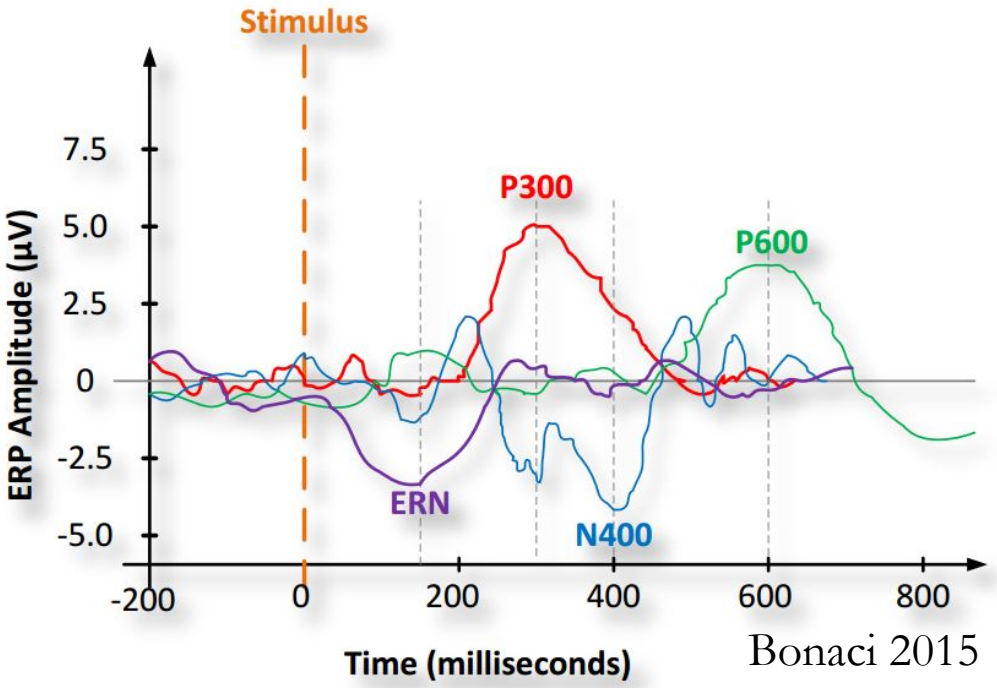

CU School of Medicine, Dept of Neurology

So What's Currently Feasible?

How do you get the information out?

Electroencephalography (EEG): No Surgery Needed





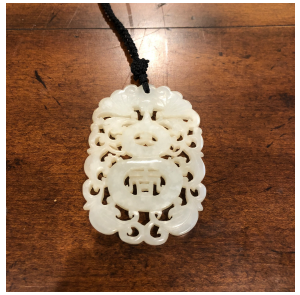
Bonaci 2015

Guilty Knowledge Test: P300 "Oddball" Response

Guilty Knowledge Test: P300 “Oddball” Response



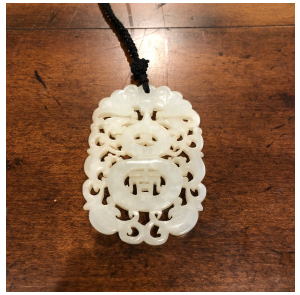




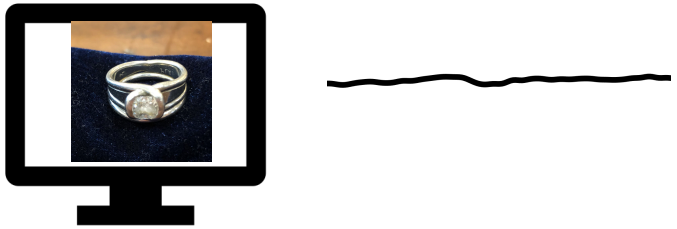

Guilty Knowledge Test: P300 "Oddball" Response








Guilty Knowledge Test: P300 “Oddball” Response

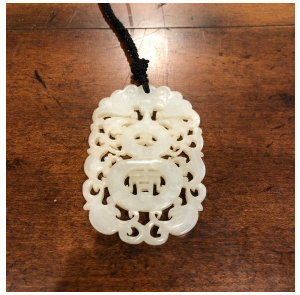


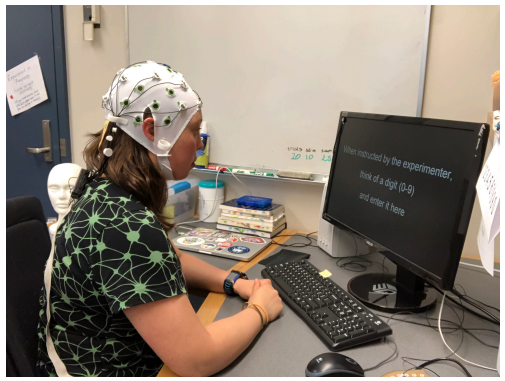














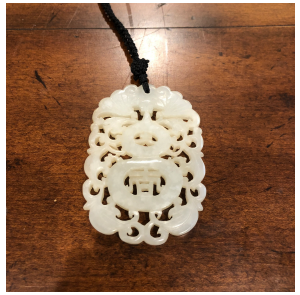
Guilty Knowledge Test: P300 "Oddball" Response

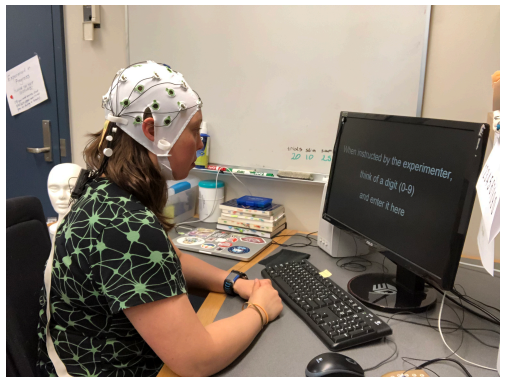




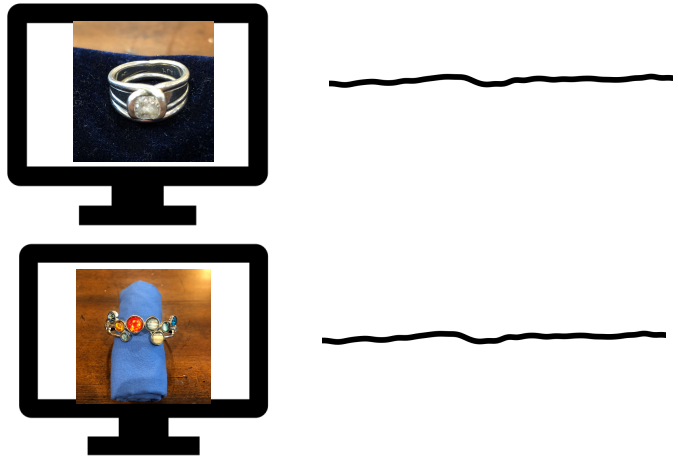












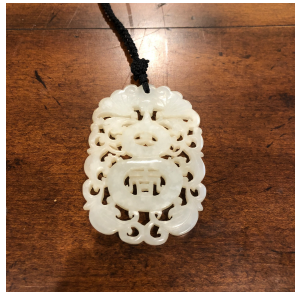
Guilty Knowledge Test: P300 "Oddball" Response

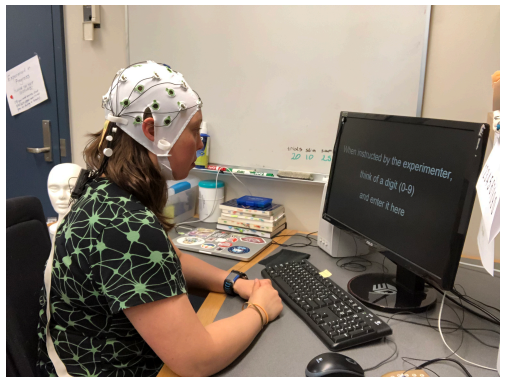




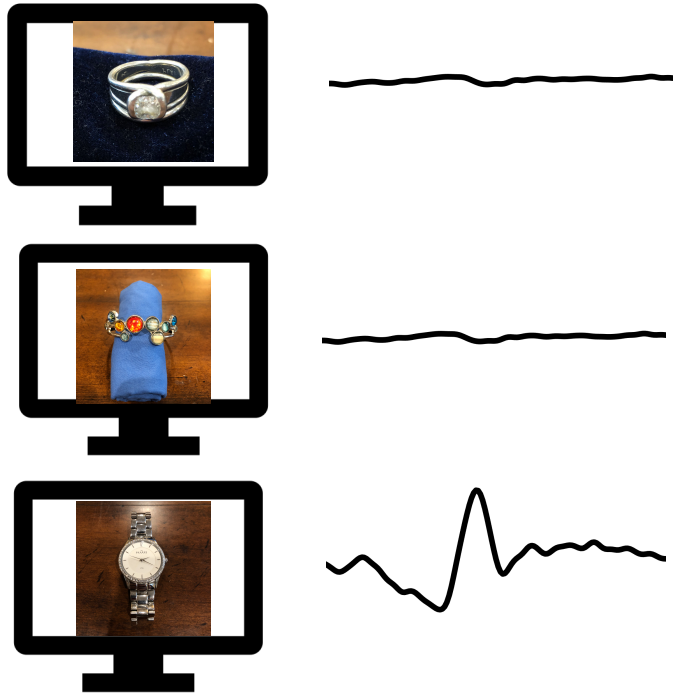












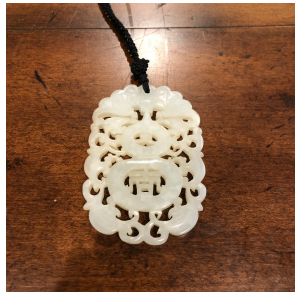
Guilty Knowledge Test: P300 "Oddball" Response

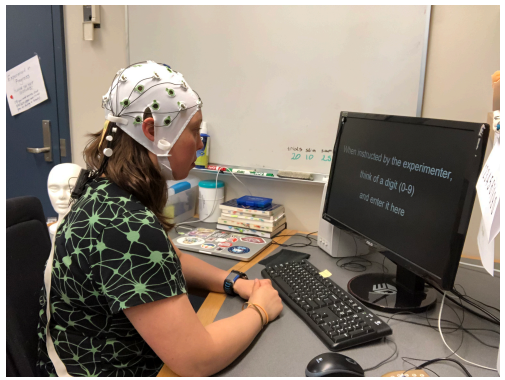




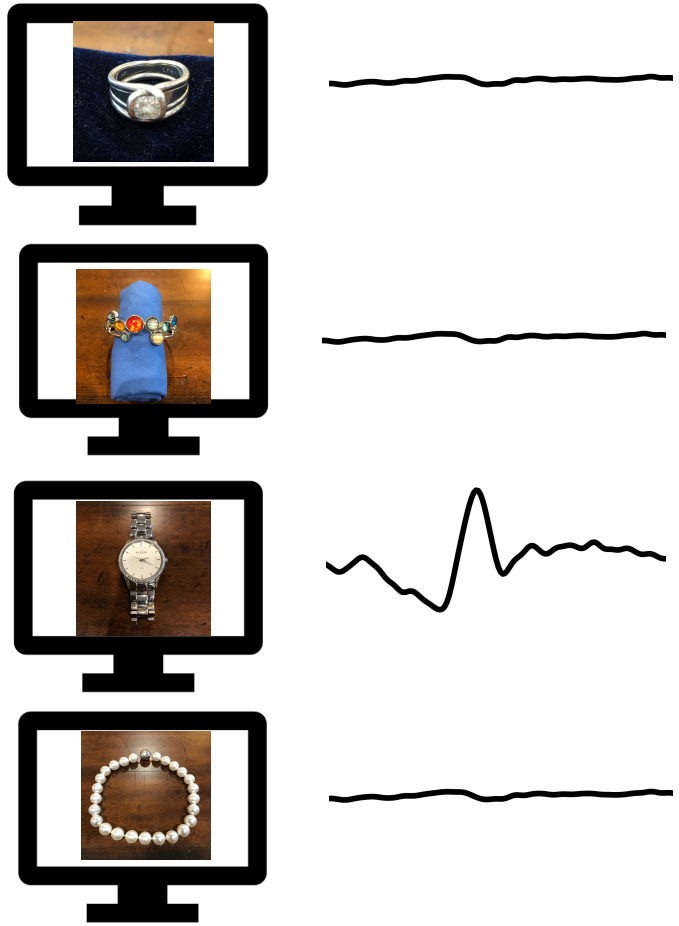








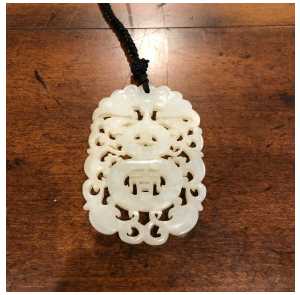


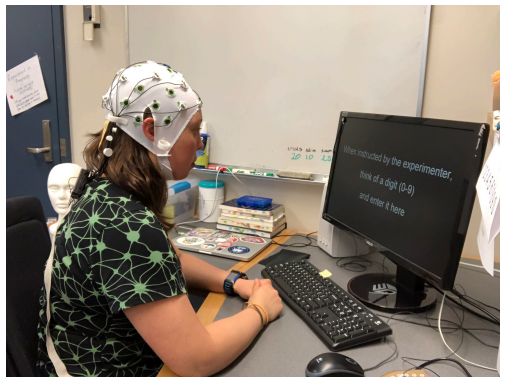


Guilty Knowledge Test: P300 "Oddball" Response

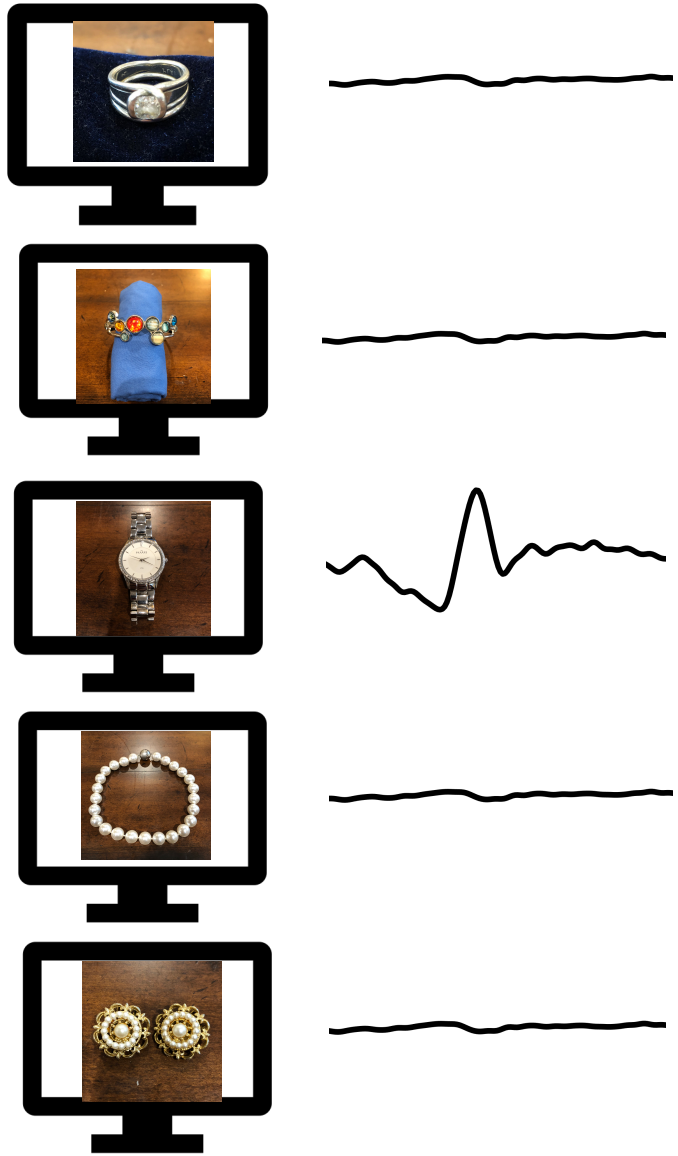








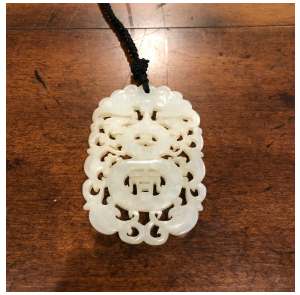


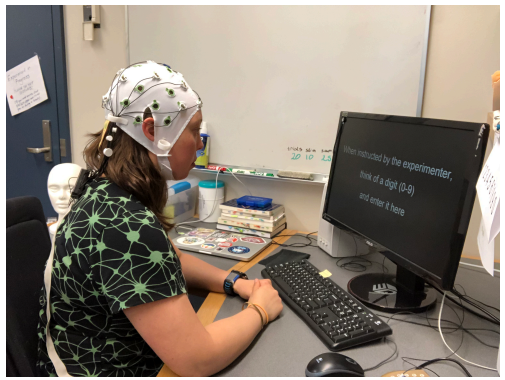


Guilty Knowledge Test: P300 "Oddball" Response

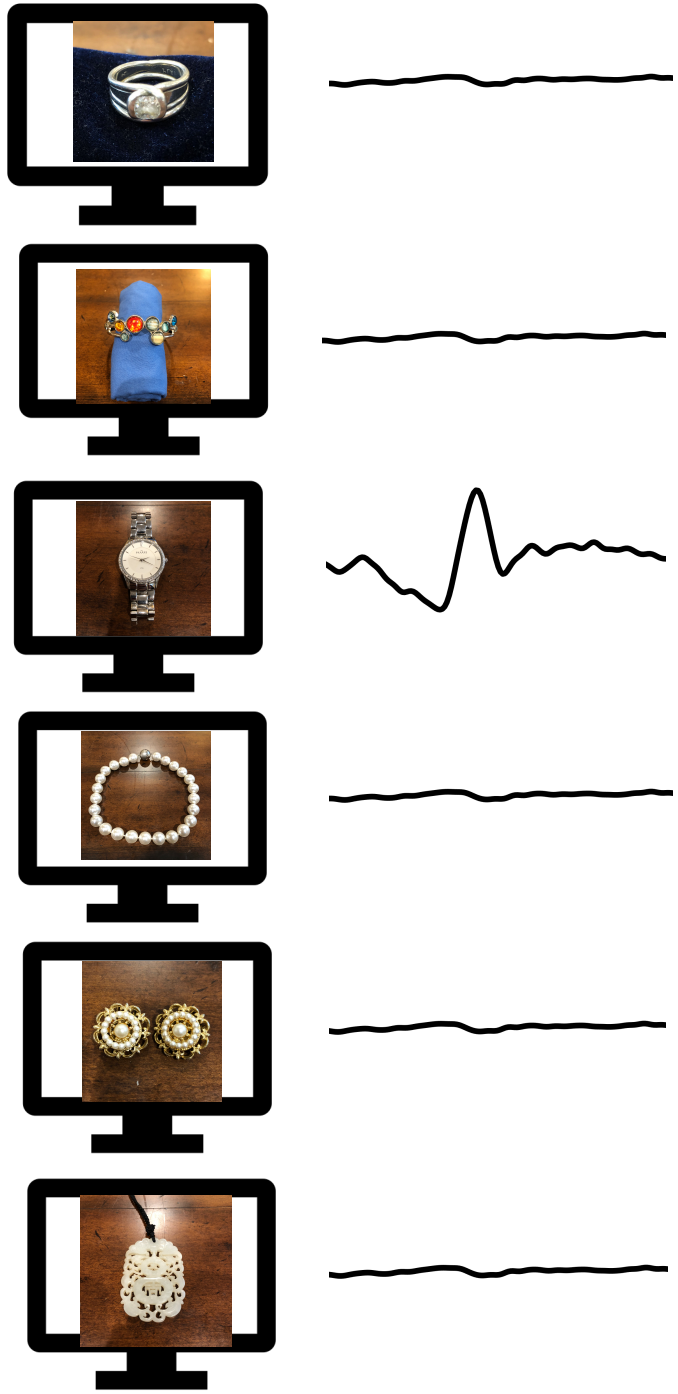








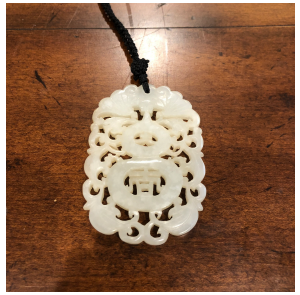


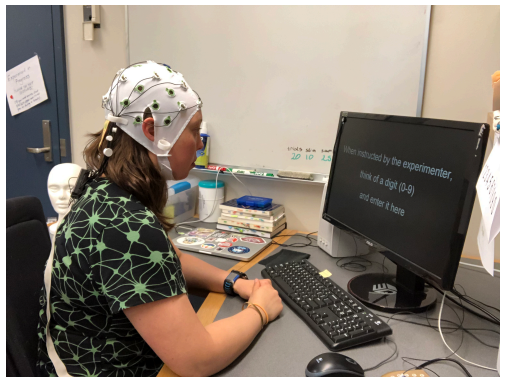


Guilty Knowledge Test: P300 "Oddball" Response

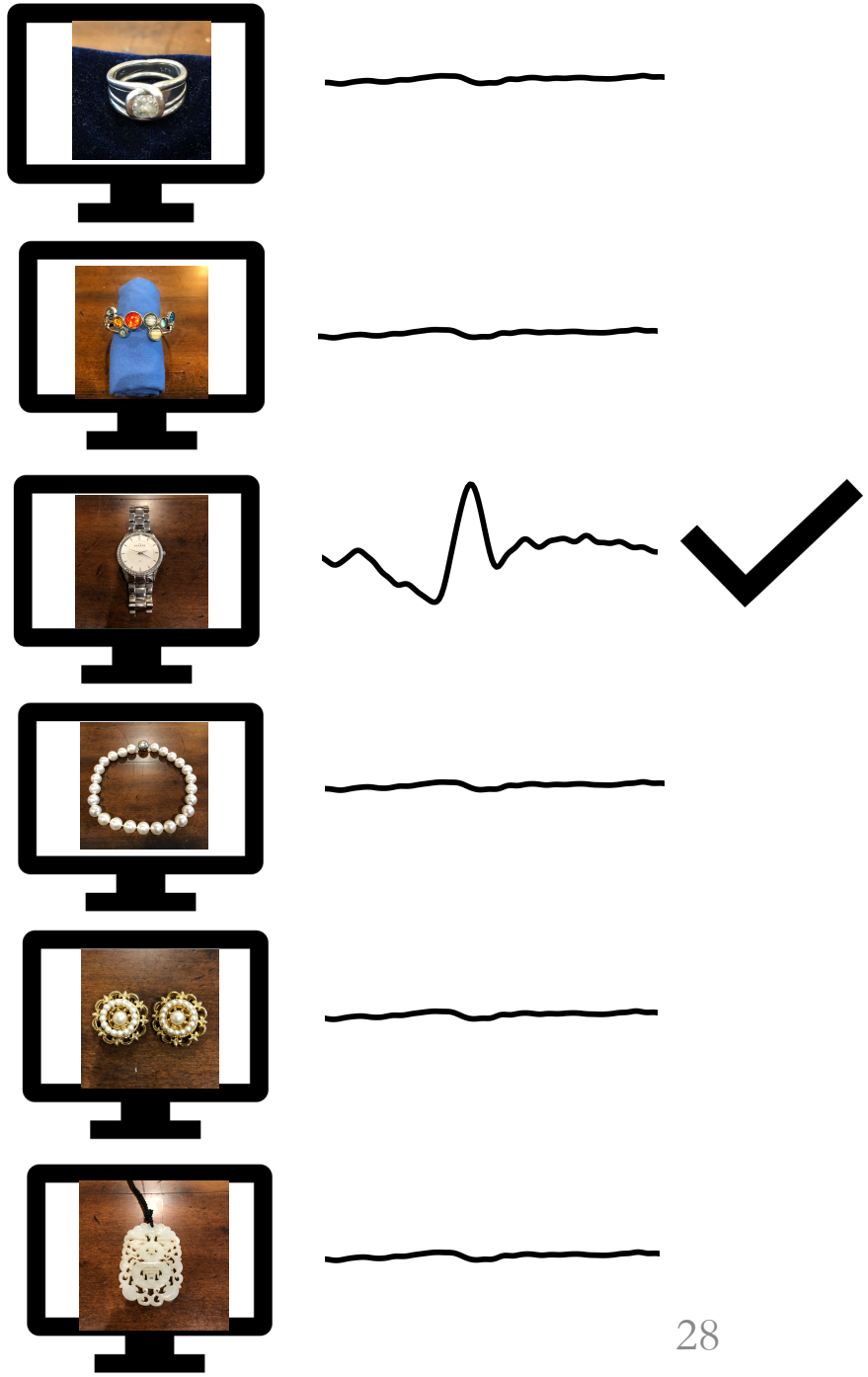






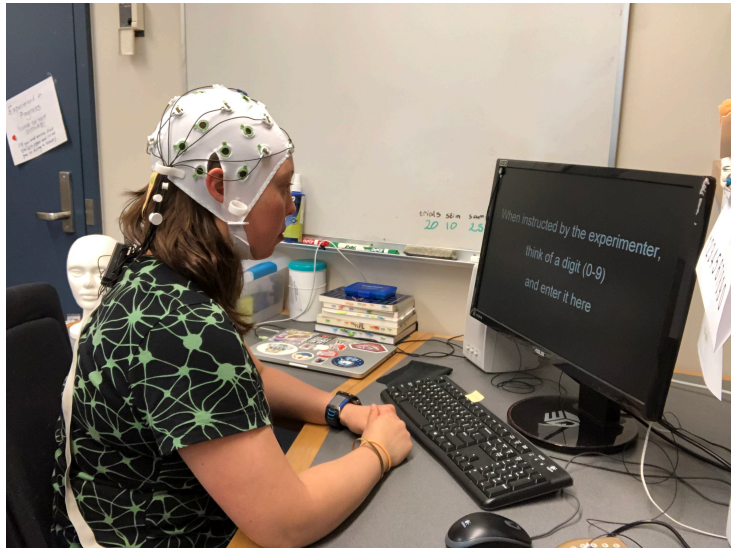


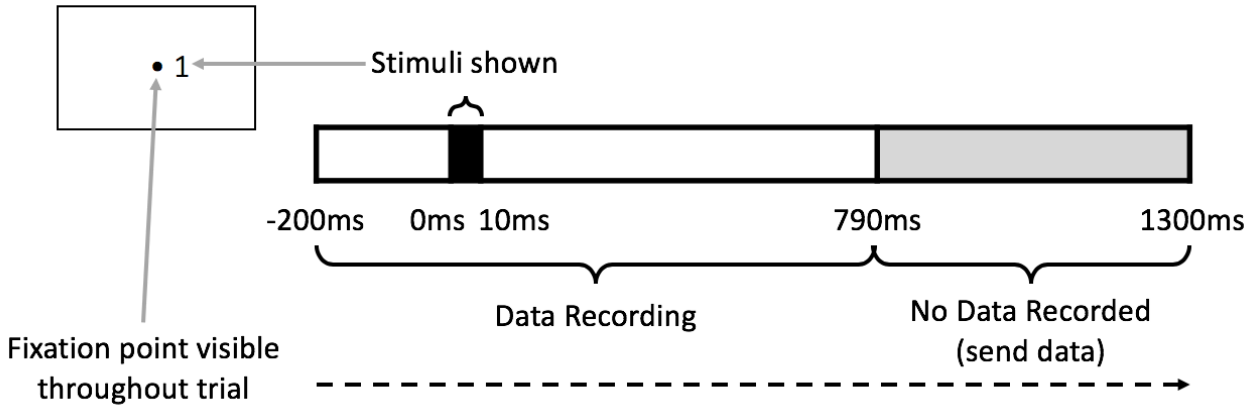




Experimental Paradigm: Single Digit Guessing Game

- Prior literature uses overt (conscious) and subliminal ("unconscious") stimuli, and results almost entirely rely on training data
- My research involved "guessing" a subject's pre-selected digit, without any prior data about the subject





Three Different Kinds of Results

- Overall effectiveness in identifying subject's chosen digit
- Effect of *attention* on correctly identifying subject's digit
- Determining current versus *future* digits (intention)

1. Overall effectiveness in identifying subject's chosen digit

For all but one subject, the computer correctly calculated the correct digit 2-3 times for the 10 experimental sessions.

1. Overall effectiveness in identifying subject's chosen digit

For all but one subject, the computer correctly calculated the correct digit 2-3 times for the 10 experimental sessions.

Human	Guess
3	2
8	6
0	8
2	1
5	**5**
1	**1**
8	9
9	4
6	**6**
6	3

2. Effect of *attention* on correctly identifying subject's digit

Percentage wise, the correct digit was calculated more often for spacebar rounds (attention) than non-spacebar rounds (passive).

3. Determining current versus *future* digits (intention)

- The number the subject was going to pick *for the next round* was calculated almost as many times as the number for the current round (13 vs 14)
- The number of correct future guesses varied by subject (not consistent)

3. Determining current versus *future* digits (intention)

- The number the subject was going to pick *for the next round* was calculated almost as many times as the number for the current round (13 vs 14)
- The number of correct future guesses varied by subject (not consistent)

Human	Guess
6	9
3	**3**
8	9
2	7
0	9
7	9
4	2
9	4
6	**6**
5	8

Human	Guess
3	5
7	5
5	1
5	7
9	**9**
9	2
2	8
2	4
4	**4**
4	1



What do Consumers Think of Neural Privacy?

What Is Being Protected?

- What I'm interested in: quantifiable information that is determined from a combination of EEG and relevant environmental stimuli
- Raw, original neural signals without context are much less informative

HARVARD

LAW REVIEW.

VOL. IV. DECEMBER 15, 1890. NO. 5.

THE RIGHT TO PRIVACY.

> "It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."
>
> WILLES, J., in Millar *v.* Taylor, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the "right to life" served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man's spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession—intangible, as well as tangible.

Issues to Consider in Defining Neural Privacy

1. Is privacy a right or an interest?

Issues to Consider in Defining Neural Privacy

1. Is privacy a right or an interest?
2. Do we own our own thoughts?

Issues to Consider in Defining Neural Privacy

1. Is privacy a right or an interest?
2. Do we own our own thoughts?
3. What relationship do we have with those who elicit information neutrally?

Issues to Consider in Defining Neural Privacy

1. Is privacy a right or an interest?
2. Do we own our own thoughts?
3. What relationship do we have with those who elicit information neutrally?
4. The importance of trust

Defining Neural Privacy

- We all should have an interest in protecting our neural privacy, but require additional legal frameworks to make it a right

Defining Neural Privacy

- We all should have an interest in protecting our neural privacy, but require additional legal frameworks to make it a right
- Defining and ascribing ownership is necessary to provide value to what is being elicited (controlling a video game vs monitoring emotions)

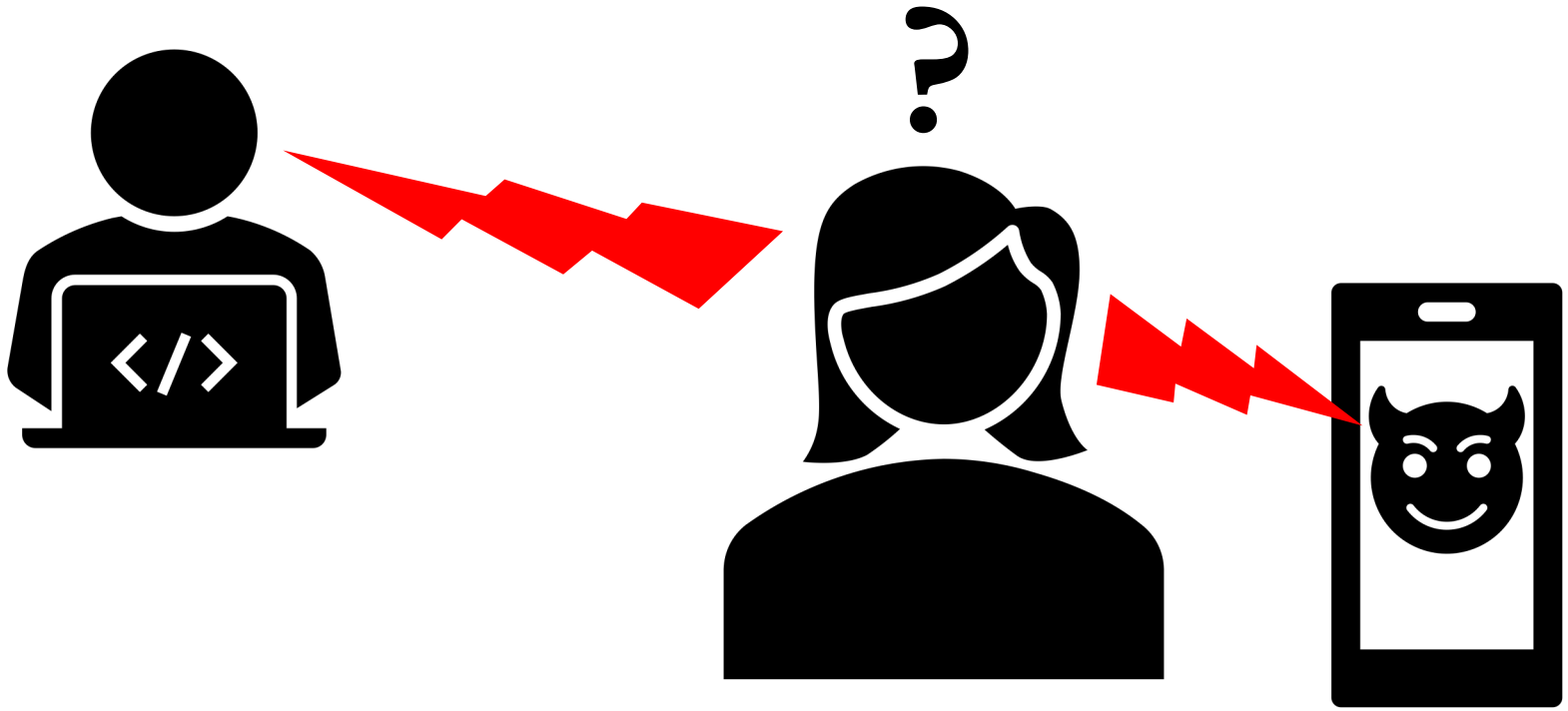
Defining Neural Privacy

- We all should have an interest in protecting our neural privacy, but require additional legal frameworks to make it a right
- Defining and ascribing ownership is necessary to provide value to what is being elicited (controlling a video game vs monitoring emotions)
- Users should be able to trust that the information taken from elicited neural signals by a company will be used and interpreted properly, making the relationship between user and company an intimate one

Neuroethics Survey

- Is there a difference in perceived privacy violation between a person intercepting BCI signals versus a phone app?
- What are the differences in trust and willingness to share neural information with a range of entities?
- Is neural information more important that other data that's already available about us?

1. Who/What is Taking Your Information?

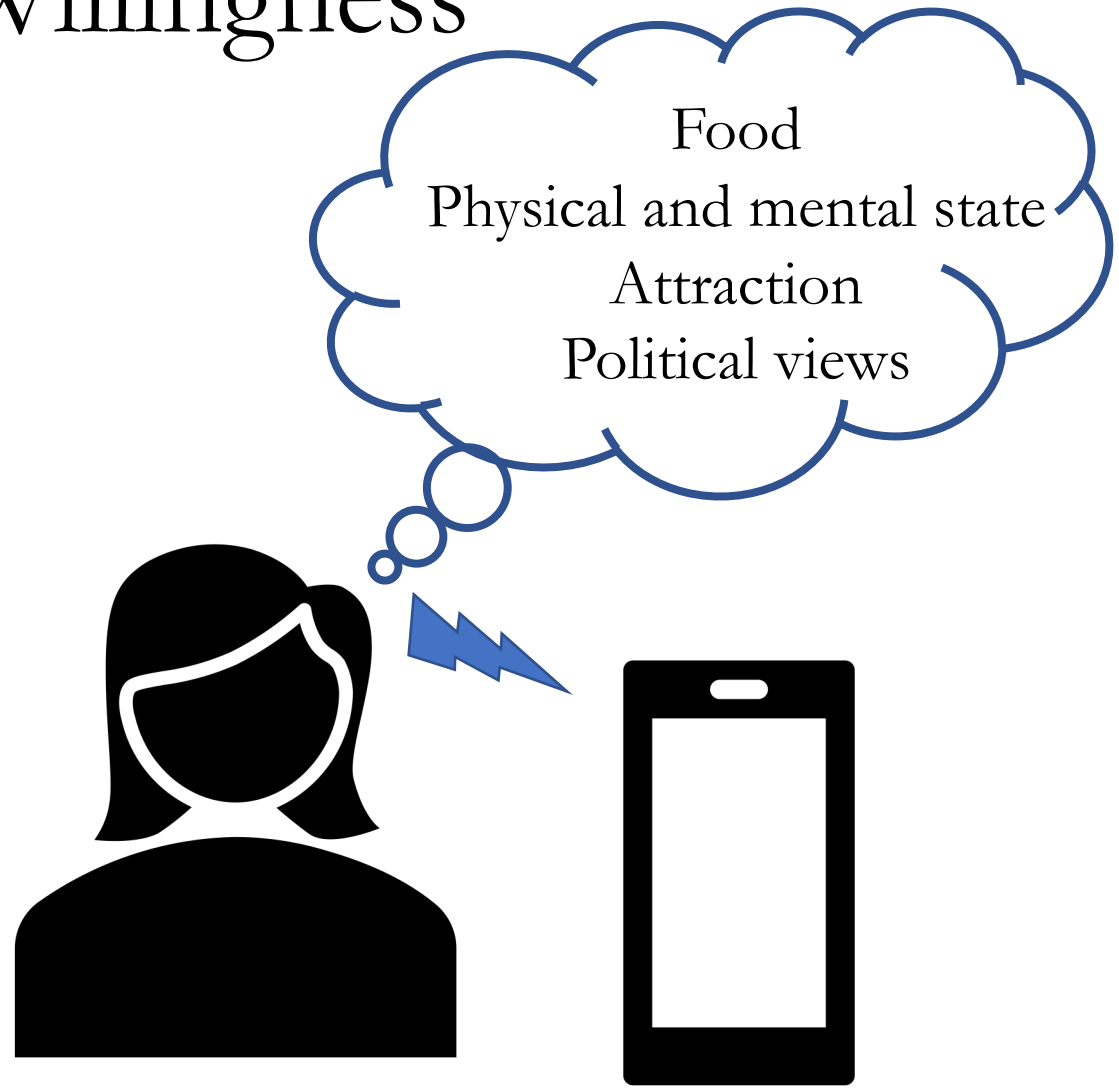


Content
Video
Brain Activity
Neural Planning
Emotions

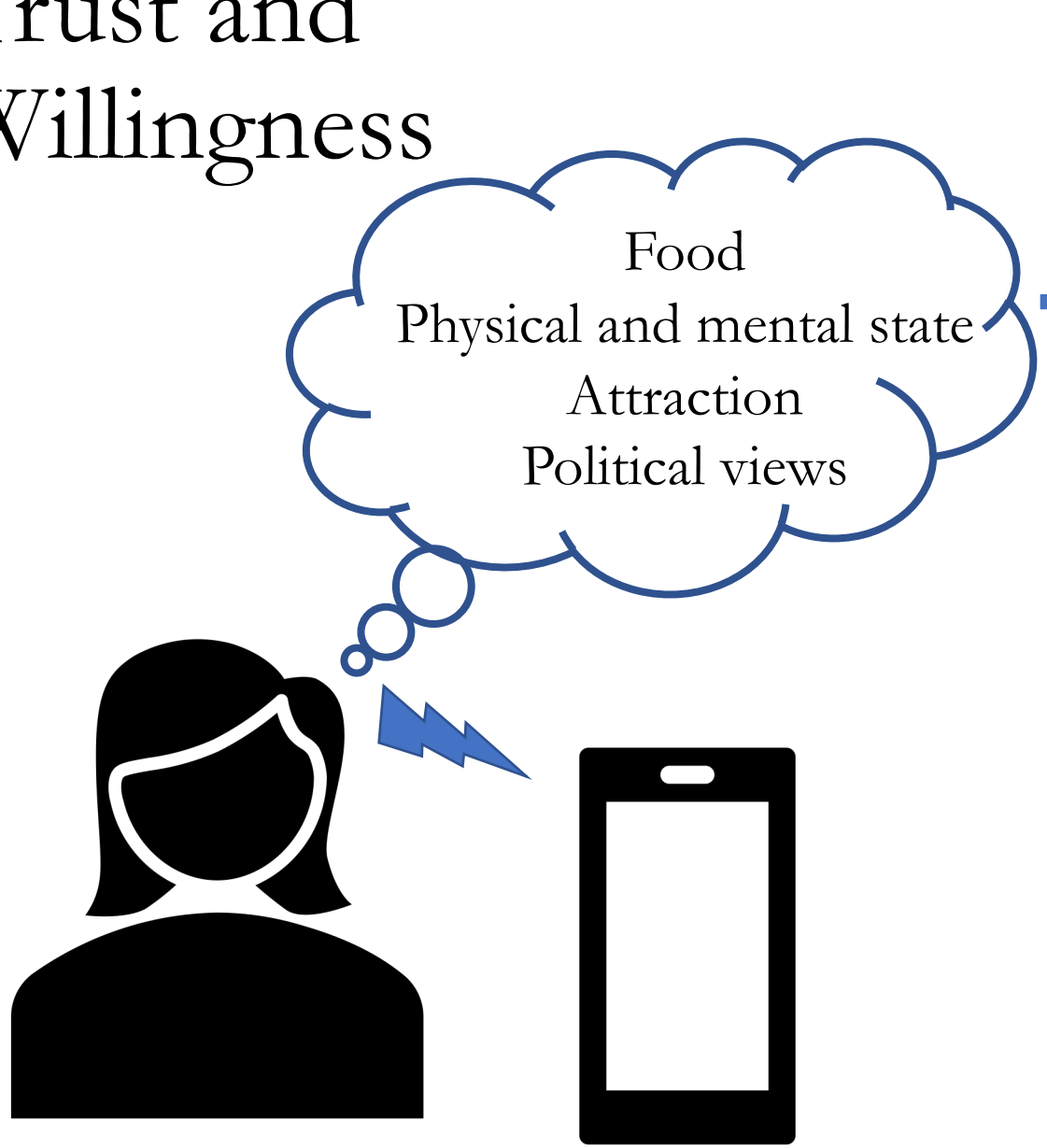
Summary of Results:
Who/What is Taking Your Information

- Person procurement of neural planning information is a statistically significant privacy violation over the app
- Mobility status does not statistically impact perceptions of neural privacy in these scenarios

Trust and Willingness



Trust and Willingness



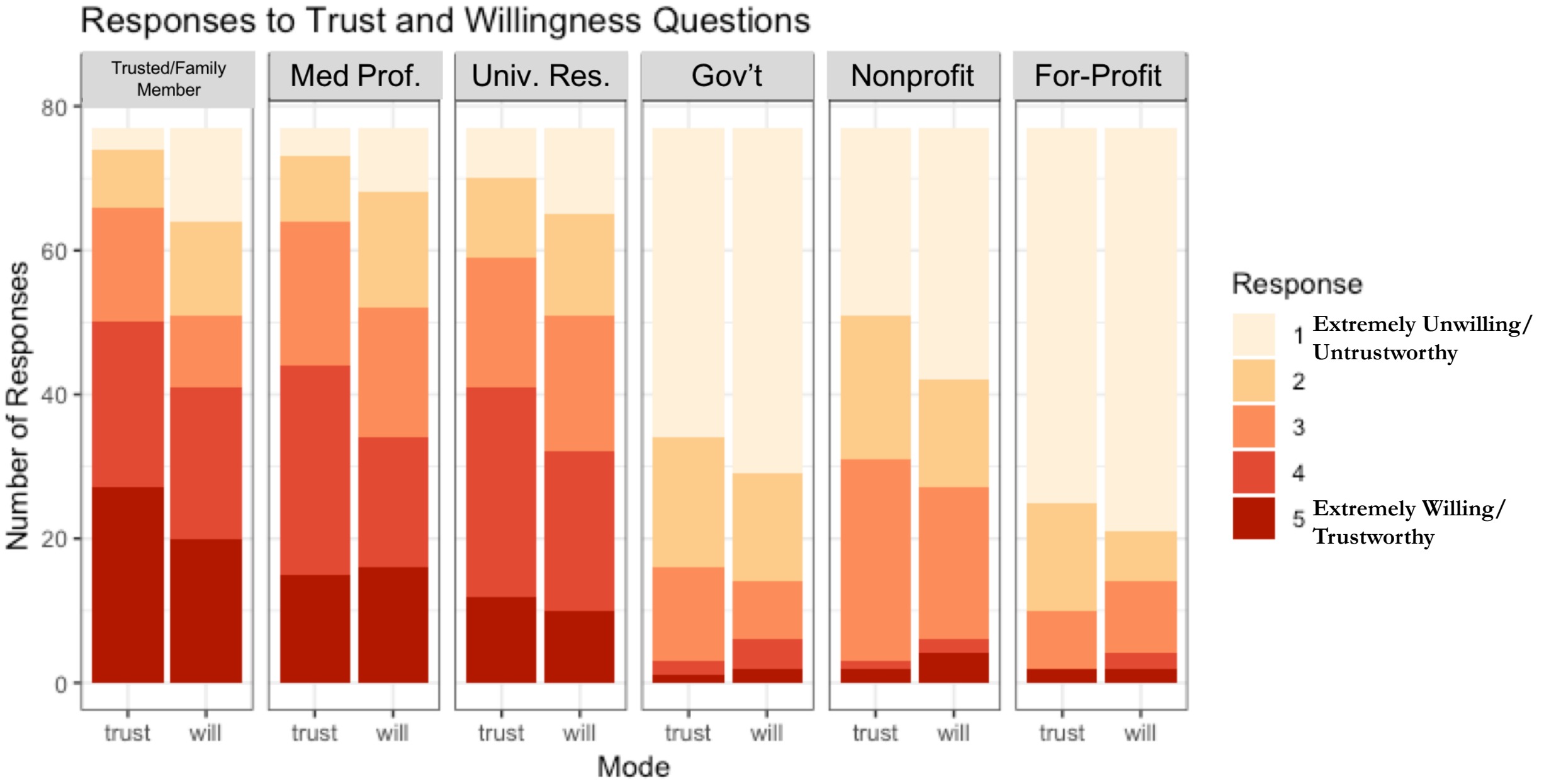


Trustworthiness?
Willingness?

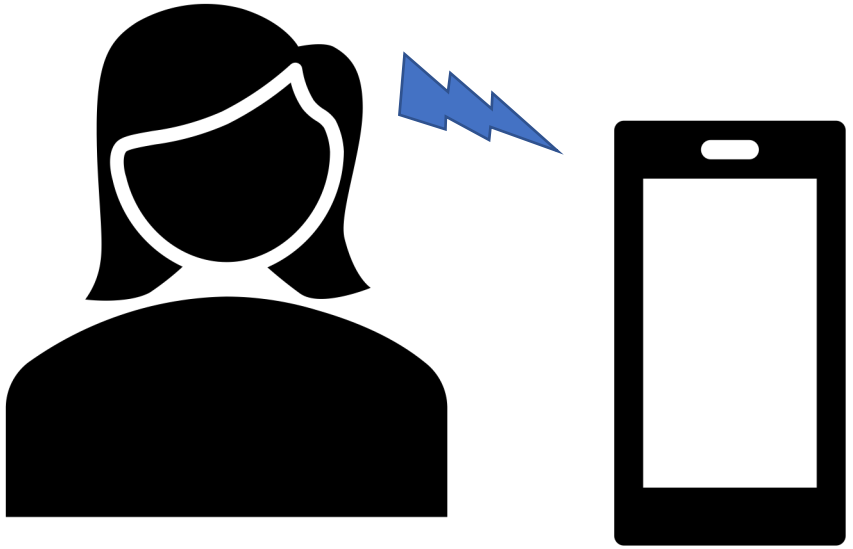
Government

Non-profit

For-profit


Responses to Trust and Willingness Questions
Trusted/Family Member
Med Prof.
Univ. Res.
Gov't
Nonprofit
For-Profit
Number of Responses
0
20
40
60
80
trust
will
Mode
Response
1 Extremely Unwilling/ Untrustworthy
2
3
4
5 Extremely Willing/ Trustworthy

What's More Important?



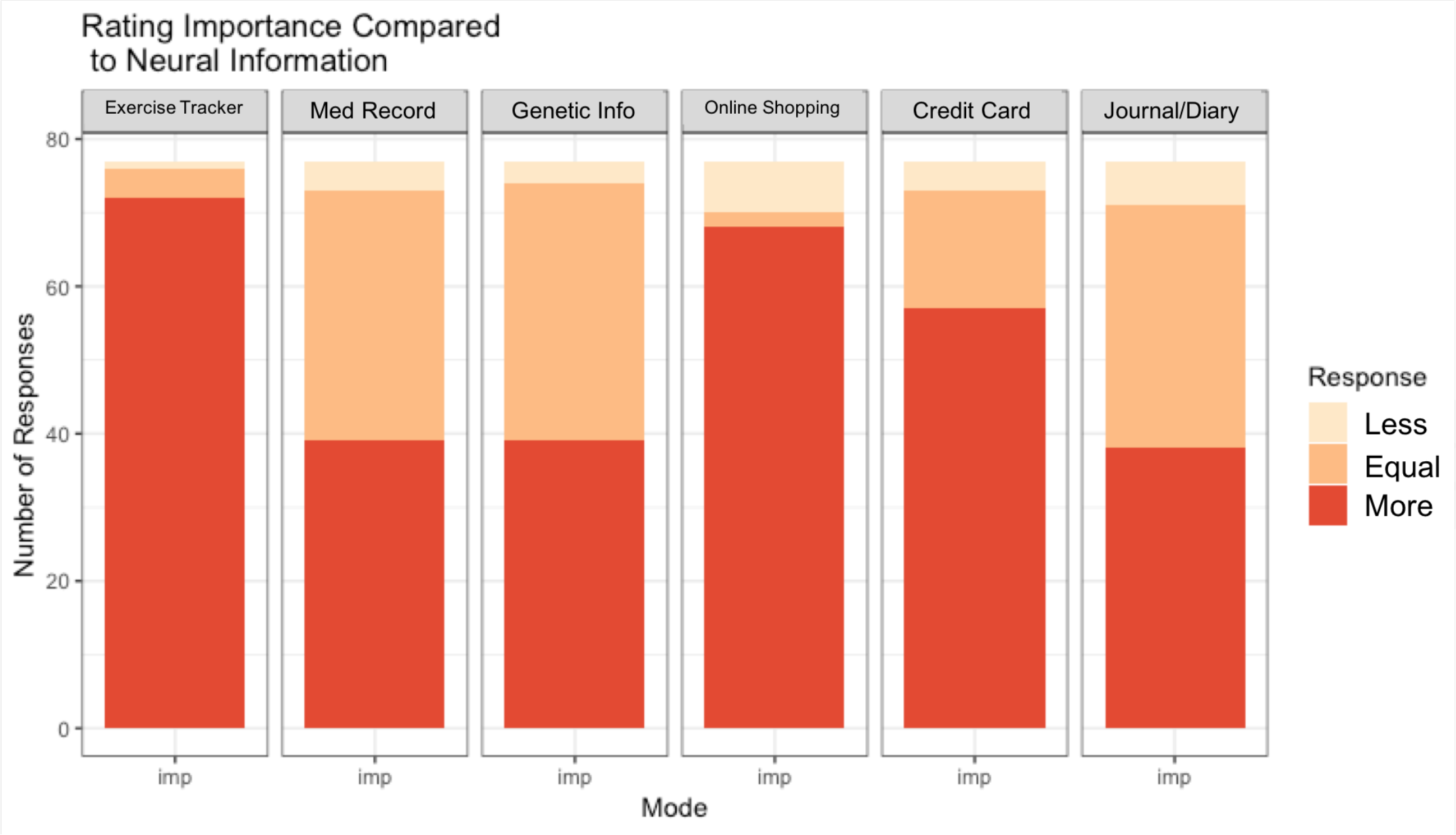
Is your neural information…

>

=

<

- Fitbit or similar exercise tracker
- Record of my personal medical history (e.g. at your doctor's office)
- Genetic information from a company like 23andMe
- Online shopping history
- Monthly credit card statement
- Journal/diary


Rating Importance Compared
to Neural Information
Exercise Tracker
Med Record
Genetic Info
Online Shopping
Credit Card
Journal/Diary
Number of Responses
80
60
40
20
0
imp
Mode
Response
Less
Equal
More

What are potential policy and regulatory implications?

Is there anything we can do about this?

Existing Biometric Precedents: Protecting and Profiting Off of You

- 2008 Genetic Information Non-Discrimination Act
- Life Insurance
- Rosenbach v Six Flags

Who Should Be In Charge of Regulation and When?

(Final questions from last section's neuroethics survey)

Who…

- User
- University Researcher
- Independent Regulatory Organization
- Legislators
- Device Manufacturers

…for BCIs, compared to current involvement

- Development oversight
- Use
- Reparations for malicious elicitation or misuse

Summary of Results: Policy and Responsibility

- Independent Regulatory Organizations, Legislators, and Device Manufacturers should be more involved going from development to reparations for misuse
- Users should be least involved in reparations from misuse, while Device Manufacturers should be the most involved

Examples of Policy Solutions

- Increased involvement by legislators with reparations for malicious elicitation or misuse
  - Federal or state-level right to neural privacy legislation (or broader generic/biometric data privacy legislation)
  - Provide reparations by statute (monetary, private right of action, etc.)
  - Empower regulatory agencies like the FTC

Examples of Policy Solutions

- Increased involvement by legislators with reparations for malicious elicitation or misuse
  - Federal or state-level right to neural privacy legislation (or broader generic/biometric data privacy legislation)
  - Provide reparations by statute (monetary, private right of action, etc.)
  - Empower regulatory agencies like the FTC
- Involving Independent Regulatory Organizations

Examples of Policy Solutions

- Increased involvement by legislators with reparations for malicious elicitation or misuse
  - Federal or state-level right to neural privacy legislation (or broader generic/biometric data privacy legislation)
  - Provide reparations by statute (monetary, private right of action, etc.)
  - Empower regulatory agencies like the FTC
- Involving Independent Regulatory Organizations
- Accountability for device manufacturers

Examples of Policy Solutions

- Increased involvement by legislators with reparations for malicious elicitation or misuse
  - Federal or state-level right to neural privacy legislation (or broader generic/biometric data privacy legislation)
  - Provide reparations by statute (monetary, private right of action, etc.)
  - Empower regulatory agencies like the FTC
- Involving Independent Regulatory Organizations
- Accountability for device manufacturers
- Overall, how do consumers understand the risks of using a device?

Here's My Ask of You

The Main Takeaways

You Are Here



Gunshow Comic, KC Green

To the Developers in the Room

- Just because you can doesn't mean you should

To the Developers in the Room

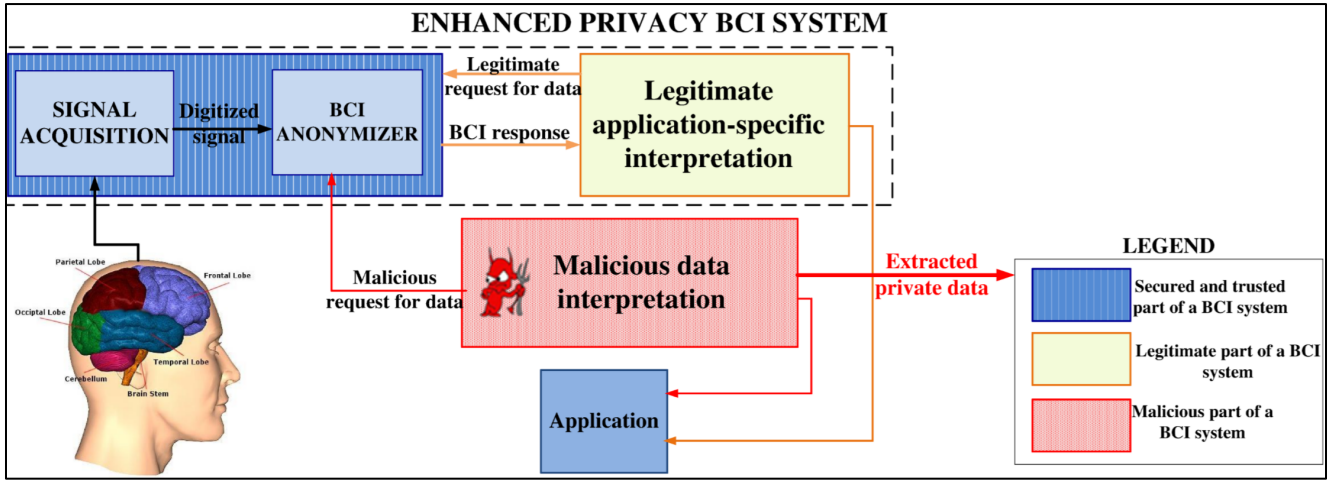
- Just because you can doesn't mean you should
- Ask yourself what problem you're solving, how else you can obtain that information, and what is the least amount of information you need to complete a particular task

To the Developers in the Room

- Just because you can doesn't mean you should
- Ask yourself what problem you're solving, how else you can obtain that information, and what is the least amount of information you need to complete a particular task
- Do as much processing as possible locally/on device

To the Developers in the Room

- Just because you can doesn't mean you should
- Ask yourself what problem you're solving, how else you can obtain that information, and what is the least amount of information you need to complete a particular task
- Do as much processing as possible locally/on device



Bonaci, Calo, Chizeck (2014)

To the Privacy-Conscious in the Room

- Just don't use these kinds of devices

To the Privacy-Conscious in the Room

- Just don't use these kinds of devices
- You may feel better with a slower screen refresh rate to prevent subliminal elicitation

To the Privacy-Conscious in the Room

- Just don't use these kinds of devices
- You may feel better with a slower screen refresh rate to prevent subliminal elicitation
- Ask for comprehensive US federal data privacy legislation:

contactingcongress.org

  - Call/email their DC offices
  - Go to town halls and ask for their positions on data privacy
  - Be involved in the democratic process!

To the Privacy-Conscious in the Room

- Just don't use these kinds of devices
- You may feel better with a slower screen refresh rate to prevent subliminal elicitation
- Ask for comprehensive US federal data privacy legislation:

contactingcongress.org

  - Call/email their DC offices
  - Go to town halls and ask for their positions on data privacy
  - Be involved in the democratic process!
- Read the terms of service to find out what is happening to your biometric information

To the 3-Letter Agencies in the Room

- (Yes, I know you're here)

To the 3-Letter Agencies in the Room

- (Yes, I know you're here)
- If you're even thinking about using this kind of technique for interrogation, you must come to terms with some serious ethical and legal questions
  - 1st Amendment: Freedom of Speech/Expression
  - 4th Amendment: Reasonable expectation of privacy
  - 5th Amendment: Self-incrimination

To the 3-Letter Agencies in the Room

- (Yes, I know you're here)
- If you're even thinking about using this kind of technique for interrogation, you must come to terms with some serious ethical and legal questions
  - 1st Amendment: Freedom of Speech/Expression
  - 4th Amendment: Reasonable expectation of privacy
  - 5th Amendment: Self-incrimination
- These are the results from compliant, willing participants

To the 3-Letter Agencies in the Room

- (Yes, I know you're here)
- If you're even thinking about using this kind of technique for interrogation, you must come to terms with some serious ethical and legal questions
  - 1st Amendment: Freedom of Speech/Expression
  - 4th Amendment: Reasonable expectation of privacy
  - 5th Amendment: Self-incrimination
- These are the results from compliant, willing participants
- This technology is still in its infancy and should not be considered the ultimate solution to any problem

So In Summary…

This is One Potential Future…



… But We Can Create a Different One



But if there's one thing I need you to remember from this talk…



There is a difference between telepathy and targeted elicitation of information.



There is a difference between telepathy and targeted elicitation of information.



Time for Questions?

@GattaKat

Backup Slides

1. Is Privacy a Right or an Interest? Part 1

- The term "right" is often synonymous with a guarantee, even if there is no legal remedy for an infraction or harm

1. Is Privacy a Right or an Interest? Part 1

- The term "right" is often synonymous with a guarantee, even if there is no legal remedy for an infraction or harm
- There is renewed interest in a right to privacy given our current internet ecosystem and the lack of control over our information

1. Is Privacy a Right or an Interest? Part 1

- The term "right" is often synonymous with a guarantee, even if there is no legal remedy for an infraction or harm
- There is renewed interest in a right to privacy given our current internet ecosystem and the lack of control over our information
- Without appropriate remedies, there is no right

1. Is Privacy a Right or an Interest? Part 1

- The term "right" is often synonymous with a guarantee, even if there is no legal remedy for an infraction or harm
- There is renewed interest in a right to privacy given our current internet ecosystem and the lack of control over our information
- Without appropriate remedies, there is no right
- Is there different language we can use to describe what we are owed, if anything, with respect to our privacy?

1. Is Privacy a Right or an Interest? Part 2

- Thomson: There is no right to privacy—rather, what we think of as a right to privacy is just a collection of different, but related, rights

1. Is Privacy a Right or an Interest? Part 2

- Thomson: There is no right to privacy—rather, what we think of as a right to privacy is just a collection of different, but related, rights
- DeCew: If privacy is instead an interest, it can still be protected or invaded, and discussed without justifying why or how it should be observed

1. Is Privacy a Right or an Interest? Part 2

- Thomson: There is no right to privacy—rather, what we think of as a right to privacy is just a collection of different, but related, rights
- DeCew: If privacy is instead an interest, it can still be protected or invaded, and discussed without justifying why or how it should be observed
- The fact that there is no overarching and defined statutory right to privacy means it will continue to be infringed upon like an interest, or ignored

2. Do We Own Our Own Thoughts?

- Is ownership necessary to assert privacy claim? Inness says no

2. Do We Own Our Own Thoughts?

- Is ownership necessary to assert privacy claim? Inness says no
- The construct of ownership may only be necessary if there is a value (monetary or otherwise) to the thought

2. Do We Own Our Own Thoughts?

- Is ownership necessary to assert privacy claim? Inness says no
- The construct of ownership may only be necessary if there is a value (monetary or otherwise) to the thought
- It may be difficult to know the value of a "thought" until something is done with it

2. Do We Own Our Own Thoughts?

- Is ownership necessary to assert privacy claim? Inness says no
- The construct of ownership may only be necessary if there is a value (monetary or otherwise) to the thought
- It may be difficult to know the value of a "thought" until something is done with it
- If ownership is assigned:
  - It's easier to create a legal construct to protect the person eliciting information, and the company receiving it
  - But it's also more difficult of the wrong information is elicited

2. Do We Own Our Own Thoughts?

- Is ownership necessary to assert privacy claim? Inness says no
- The construct of ownership may only be necessary if there is a value (monetary or otherwise) to the thought
- It may be difficult to know the value of a "thought" until something is done with it
- If ownership is assigned:
  - It's easier to create a legal construct to protect the person eliciting information, and the company receiving it
  - But it's also more difficult of the wrong information is elicited
- The purpose for eliciting information should be important to questions of ownership

3. What Relationship Do We Have With Those Who Elicit Information Neurally?

- Defining the relationship between the user and the company

3. What Relationship Do We Have With Those Who Elicit Information Neurally?

- Defining the relationship between the user and the company
- Intimacy: specification that choice is involved on the part of the agent providing information, and that the value comes from the original relationship one has with the information (Inness)

3. What Relationship Do We Have With Those Who Elicit Information Neurally?

- Defining the relationship between the user and the company
- Intimacy: specification that choice is involved on the part of the agent providing information, and that the value comes from the original relationship one has with the information (Inness)
- When information is elicited not by choice, the violation of privacy can be linked to a lack of acknowledging that the sharing of information is in fact a relationship

4. The Importance of Trust

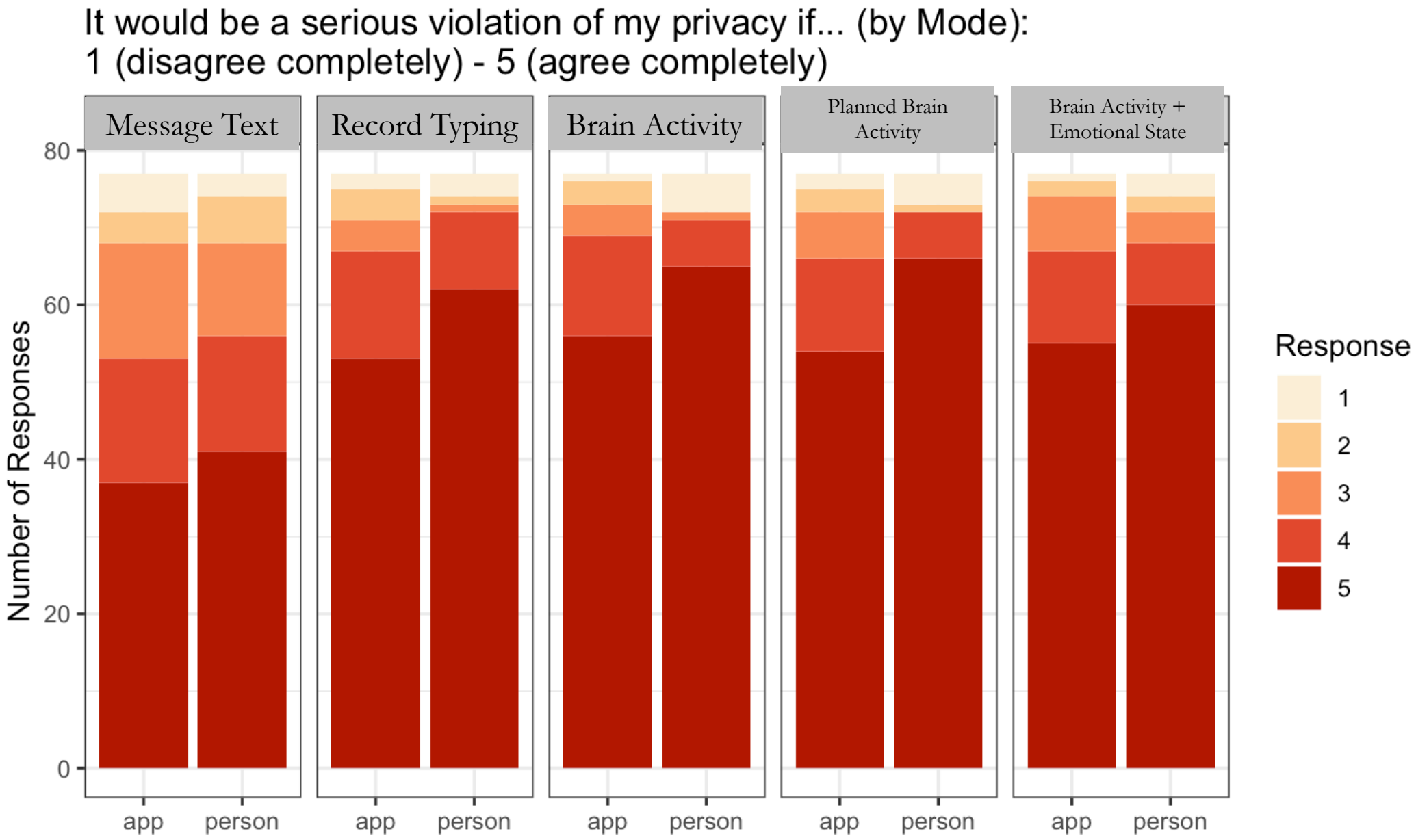
- Lack of trust may no longer be an adequate deterrent to a company's malevolent behavior
  - 91% of Americans in 2016 agreed or strongly agreed that users had lost control over the collection and use of of their information
  - 2/3rd of those surveyed in 2017 said that existing legislation is inadequate in protecting private information

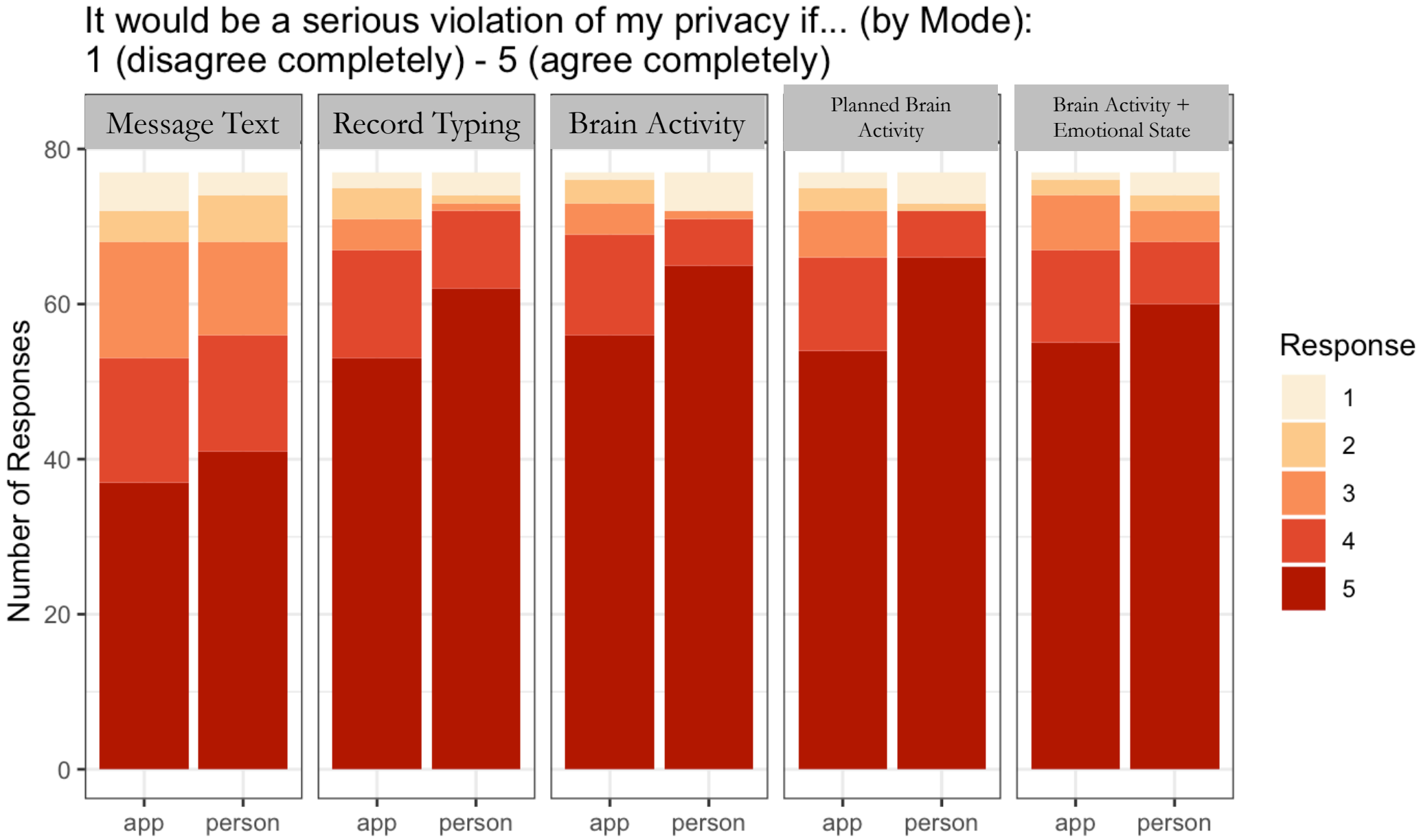
4. The Importance of Trust

- Lack of trust may no longer be an adequate deterrent to a company's malevolent behavior
  - 91% of Americans in 2016 agreed or strongly agreed that users had lost control over the collection and use of of their information
  - 2/3rd of those surveyed in 2017 said that existing legislation is inadequate in protecting private information
- Privacy as trust (Waldman): relationship through regulation of access, either restricting or openness

First Analysis: Person vs App

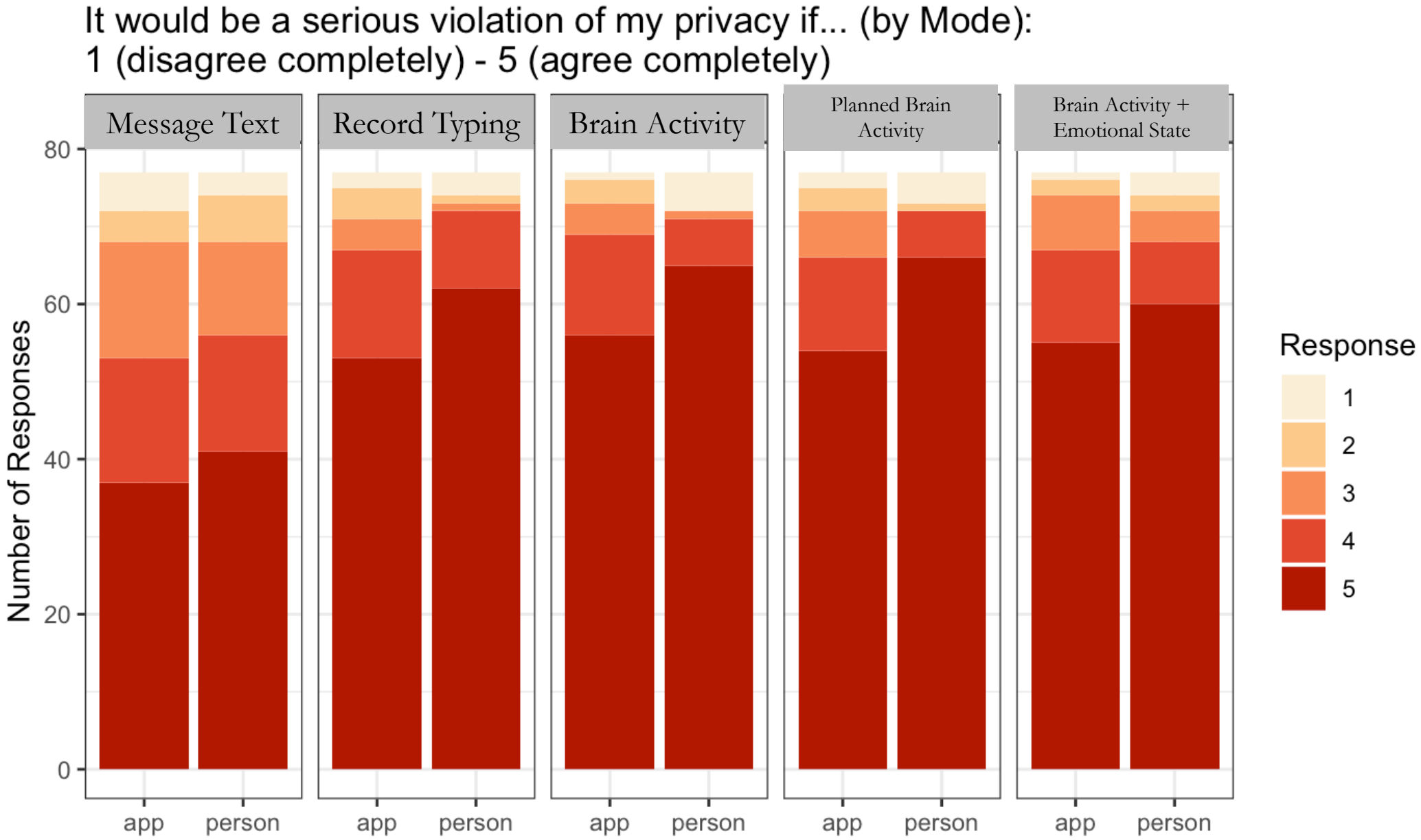
Odds ratio < 1 means respondents perceived the app collecting their neural information as LESS of a privacy issue than if it was collected by a person


It would be a serious violation of my privacy if... (by Mode):
1 (disagree completely) - 5 (agree completely)
Message Text
Record Typing
Brain Activity
Planned Brain Activity
Brain Activity + Emotional State
Number of Responses
0
20
40
60
80
app
person
Response
1
2
3
4
5



Odds Ratios

0.83 0.55 0.77 0.56 0.97



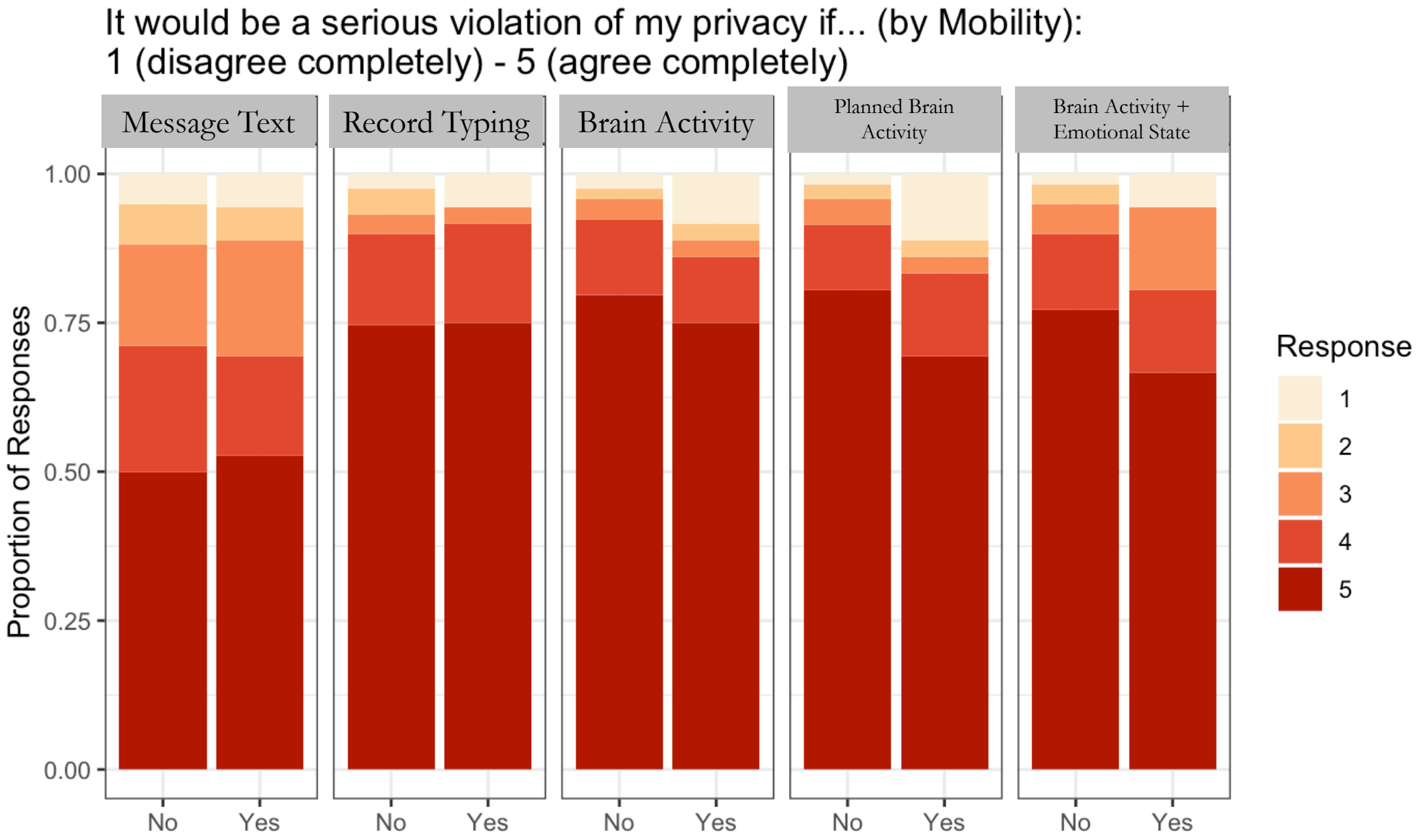
Odds Ratios

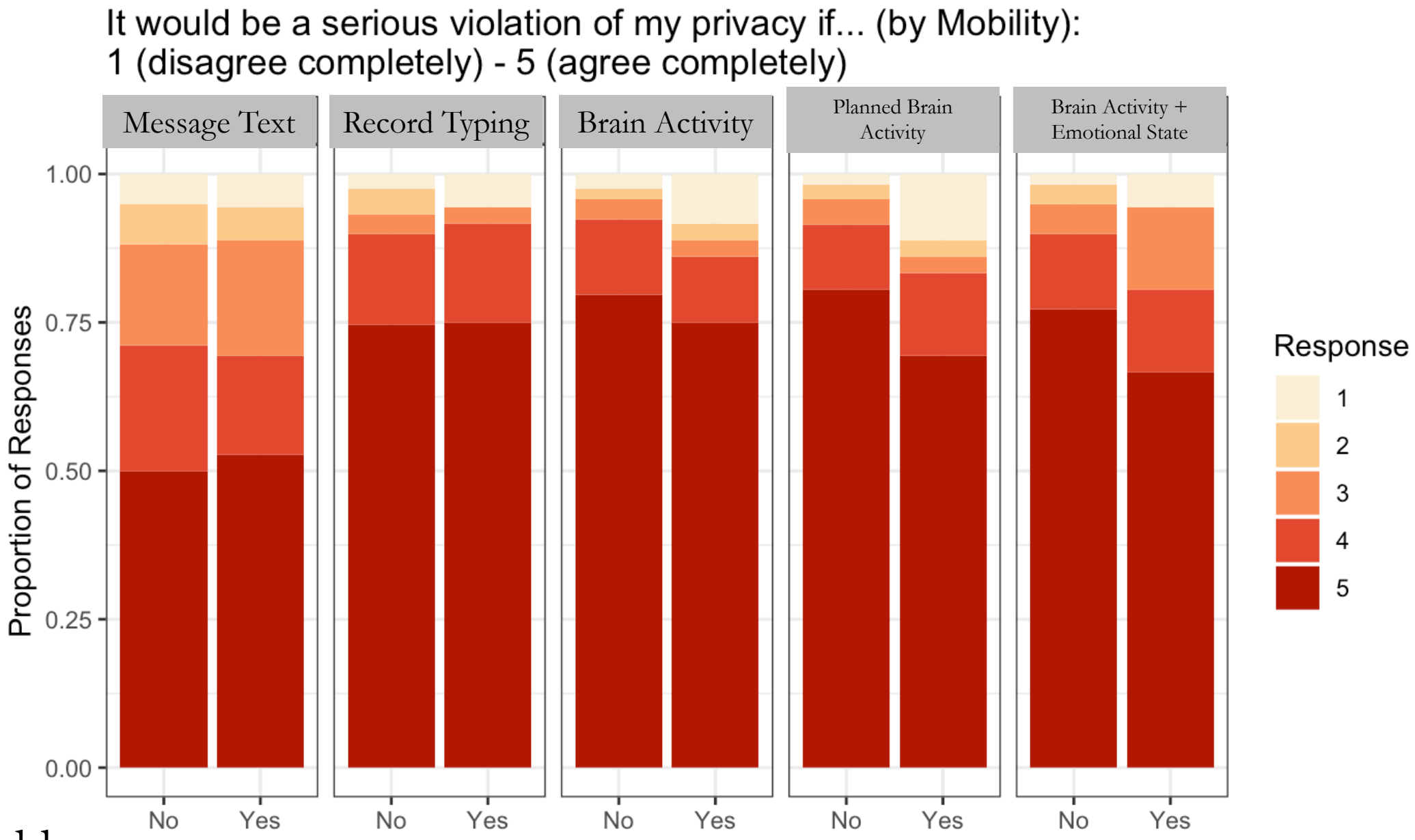
0.83 0.55 0.77 **0.56** 0.97

Second Analysis:
Mobility vs Non-Mobility Impaired

Odds ratio < 1: non-mobility impaired individuals perceive the data collected to be **less** of a privacy violation, compared to those who are

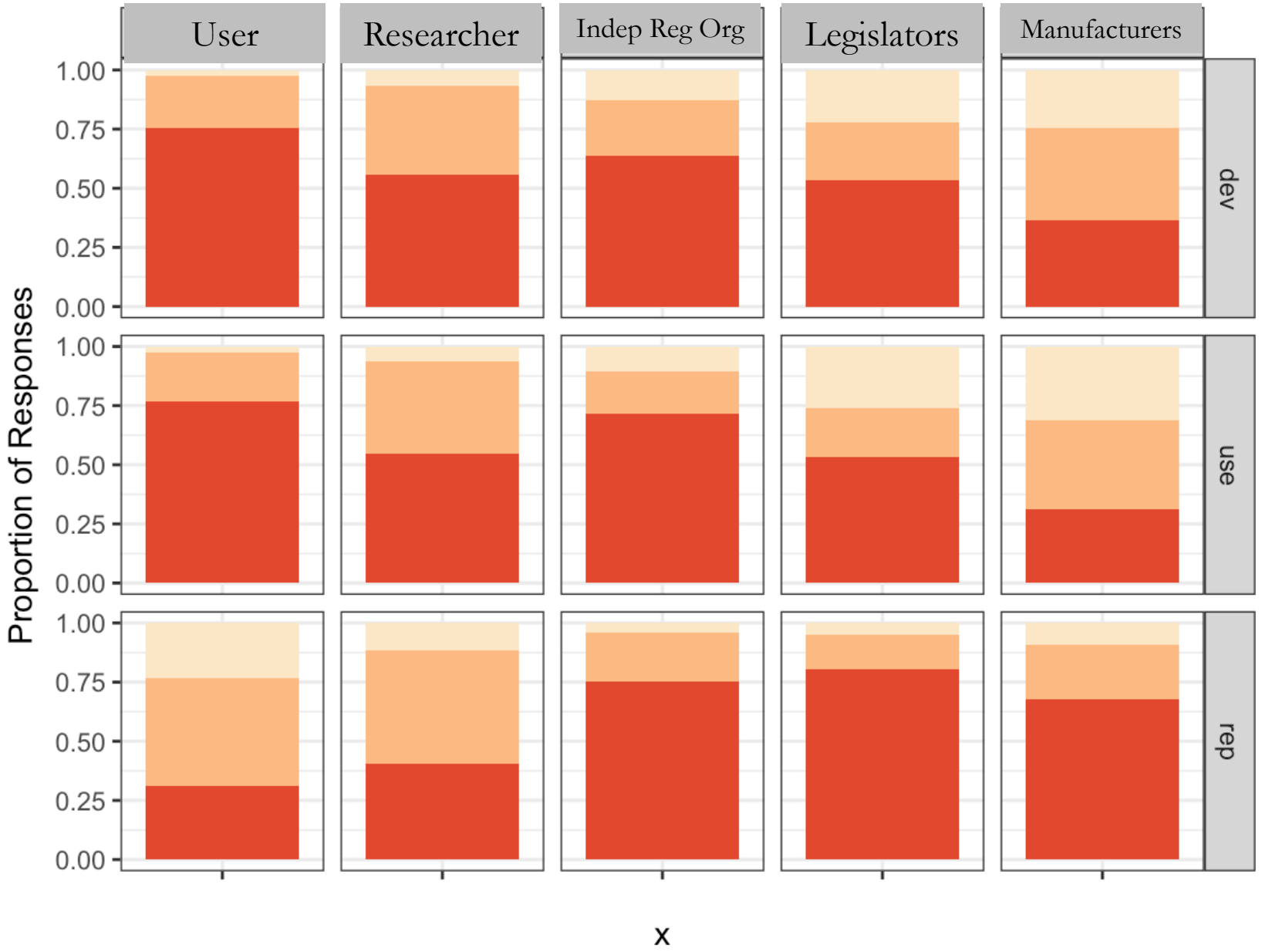
Odds ratio > 1: non-mobility impaired individuals perceived data collected to be **more** of a privacy violation, compared to those who are


It would be a serious violation of my privacy if... (by Mobility):
1 (disagree completely) - 5 (agree completely)
Message Text
Record Typing
Brain Activity
Planned Brain Activity
Brain Activity + Emotional State
Proportion of Responses
1.00
0.75
0.50
0.25
0.00
No
Yes
Response
1
2
3
4
5



Odds Ratios	0.95	0.96	1.24	1.76	1.70

Figure 2. Responses to Level of Involvement by Entity and Stage:
1 (less involved) - 3 (more involved)



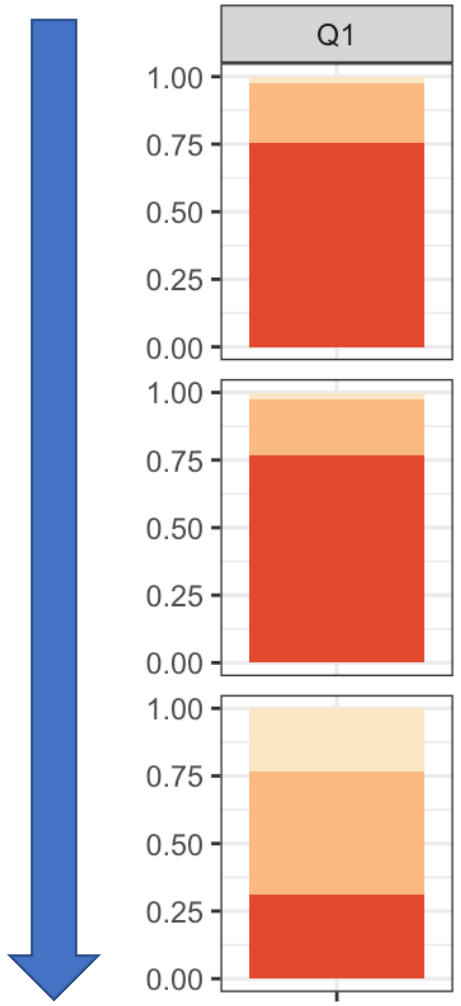
First Analysis: Involvement by Entity

How should each entity's involvement change through the BCI lifecycle

First Analysis: Involvement by Entity

How should each entity's involvement change through the BCI lifecycle

Odds ratio > 1 means less involvement through each stage



First Analysis: Involvement by Entity

How should each entity's involvement change through the BCI lifecycle

Odds ratio > 1 means less involvement through each stage

Odds ratio < 1 indicates the entity should be more involved through each stage

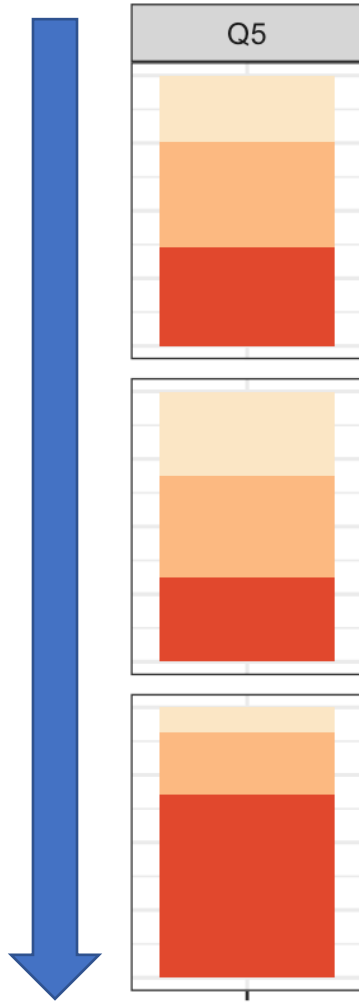
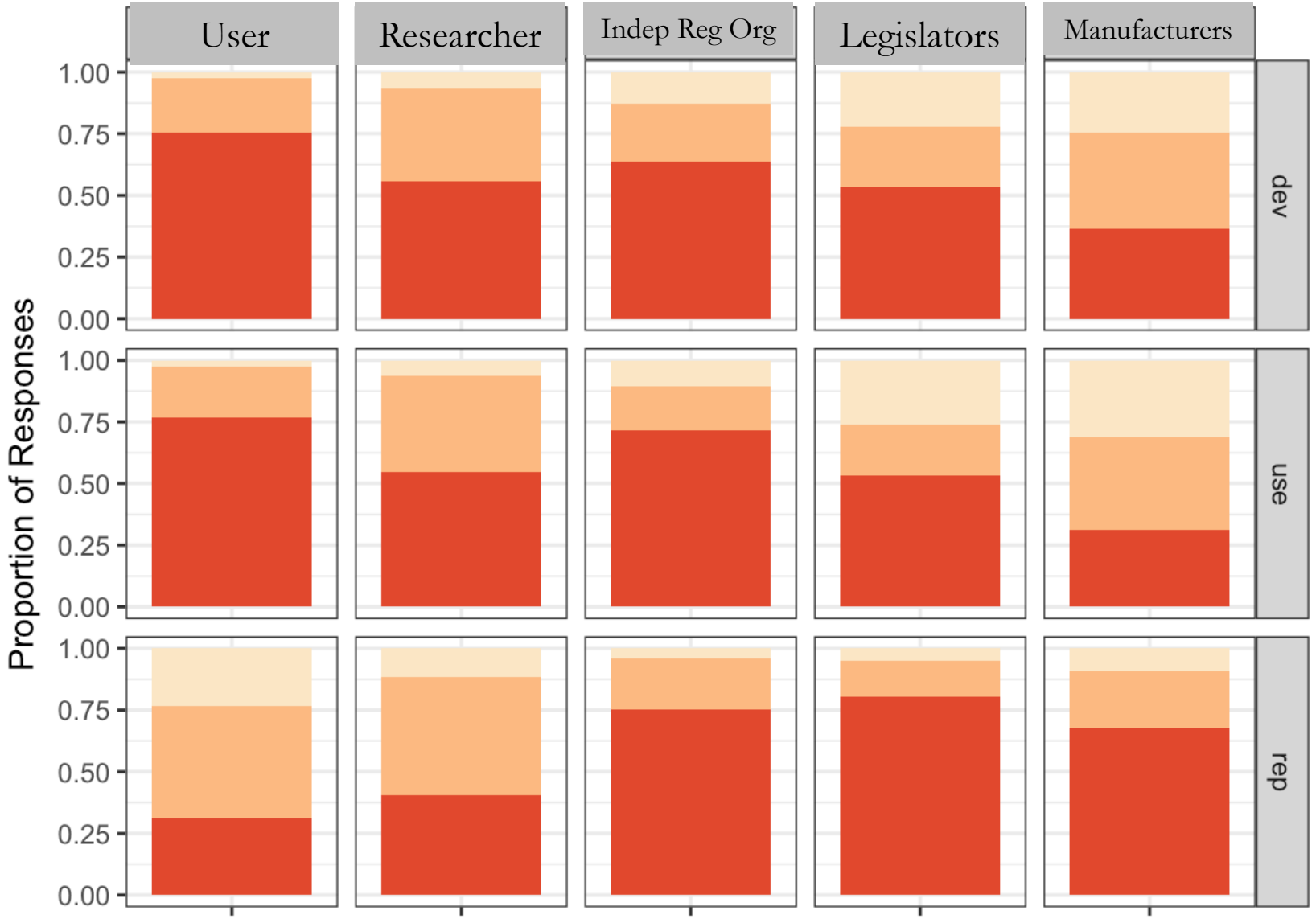


Figure 2. Responses to Level of Involvement by Entity and Stage:
1 (less involved) - 3 (more involved)

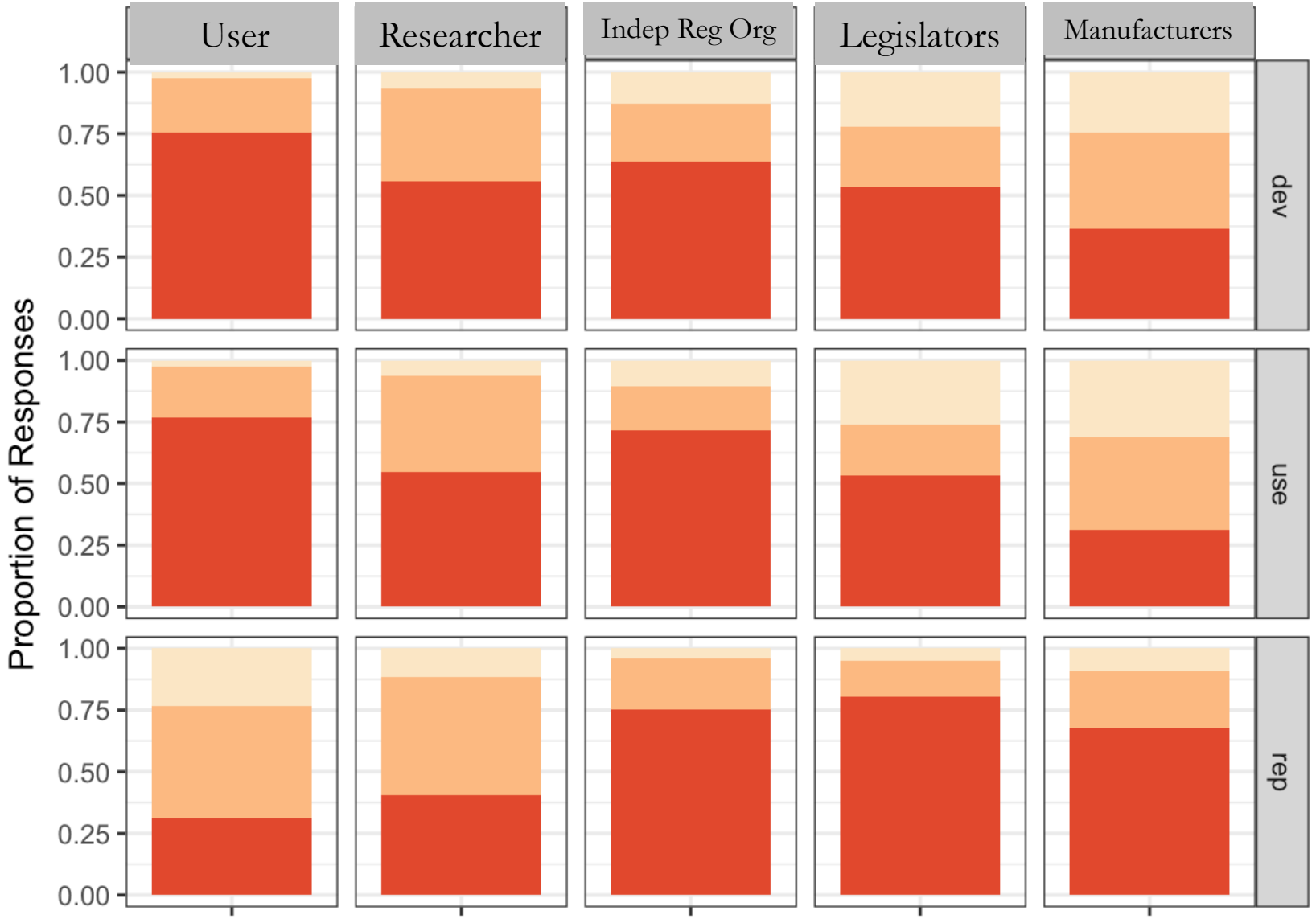


Compared to
Current Involvement

Response
1 Less Involved
2 Same
3 More Involved

	User	Researcher	Indep Reg Org	Legislators	Manufacturers
Odds Ratios	2.481	1.248	0.709	0.685	0.741

Figure 2. Responses to Level of Involvement by Entity and Stage:
1 (less involved) - 3 (more involved)



Compared to
Current Involvement

Response
1 Less Involved
2 Same
3 More Involved

	User	Researcher	Indep Reg Org	Legislators	Manufacturers
Odds Ratios	2.481	1.248	**0.709**	**0.685**	**0.741**

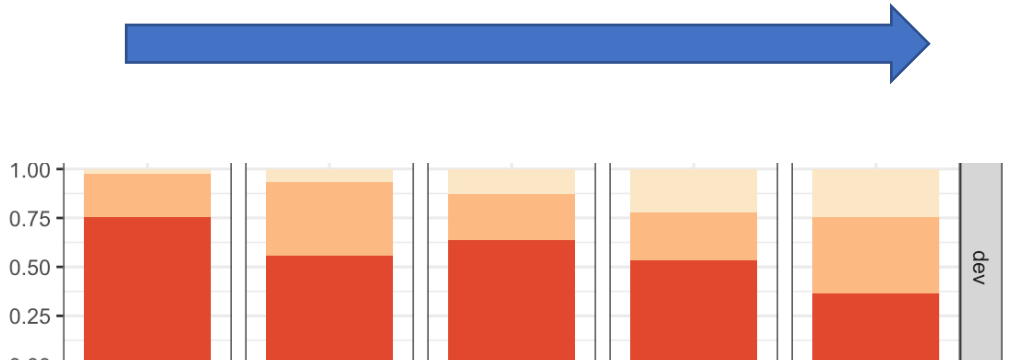
Second Analysis: Involvement by Stage

Who should be more involved at each stage?

Second Analysis: Involvement by Stage

Who should be more involved at each stage?

Odds ratios > 1 means involvement should decrease going from user to device manufacturer

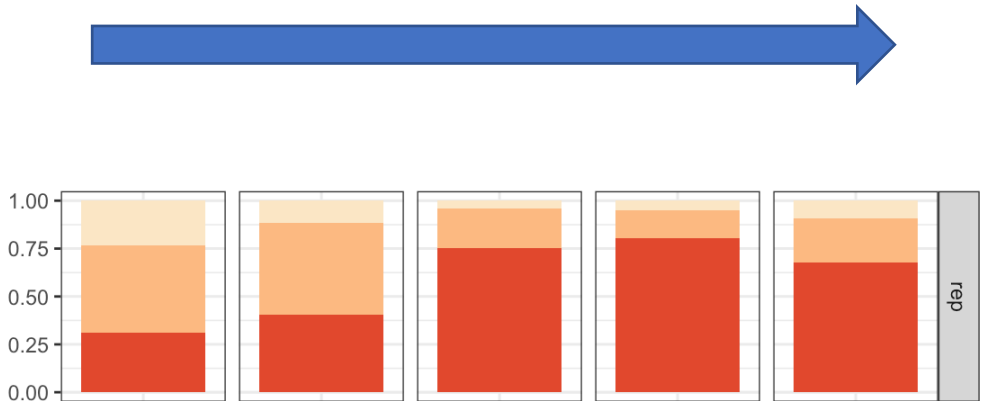


Second Analysis: Involvement by Stage

Who should be more involved at each stage?

Odds ratios > 1 means involvement should decrease going from user to device manufacturer

Odds ratios < 1, involvement should increase going from user to device manufacturer.



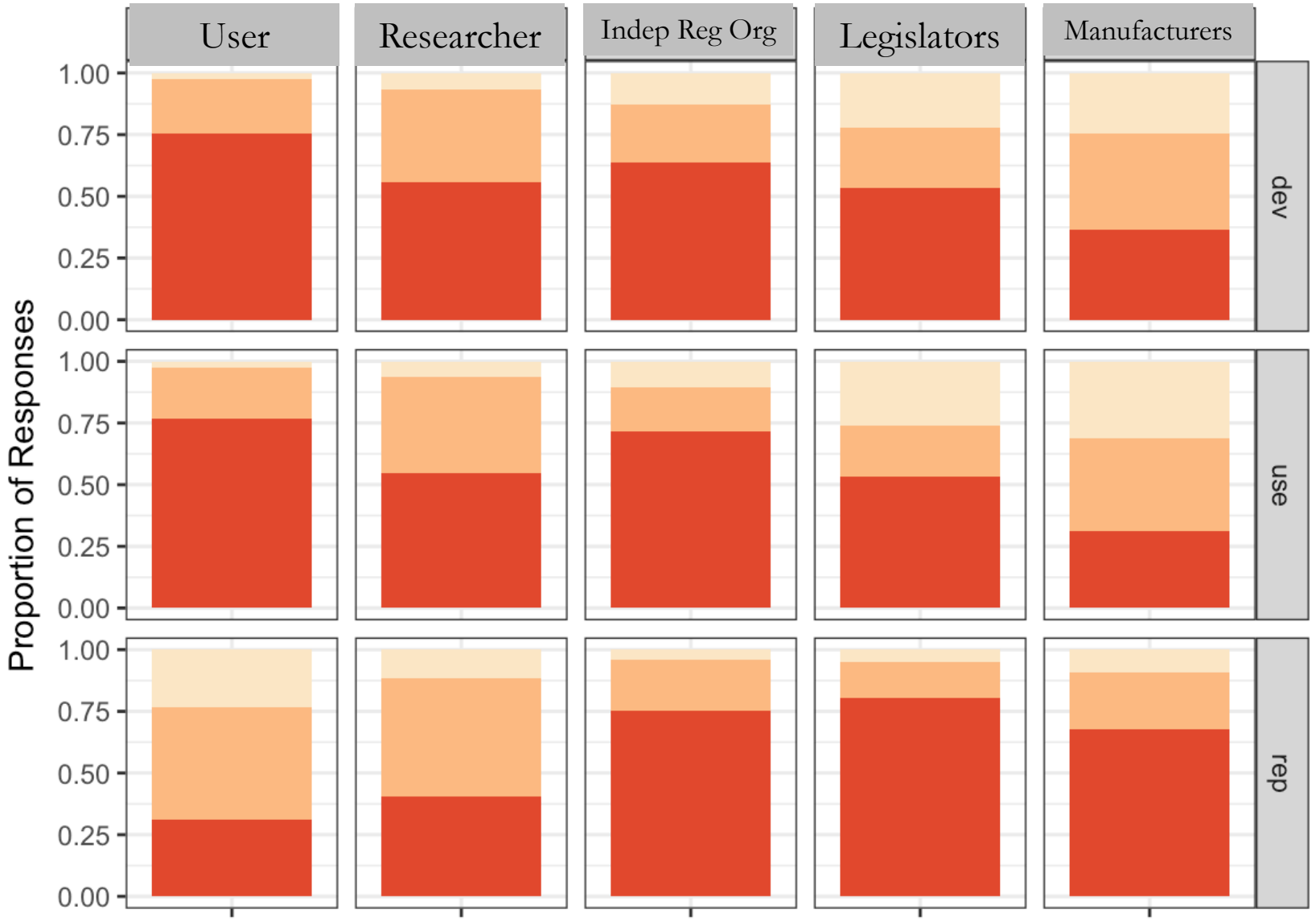
Odds Ratios

1.461

1.536

0.620

Figure 2. Responses to Level of Involvement by Entity and Stage:
1 (less involved) - 3 (more involved)



Compared to Current Involvement

Response

1 Less Involved

2 Same

3 More Involved

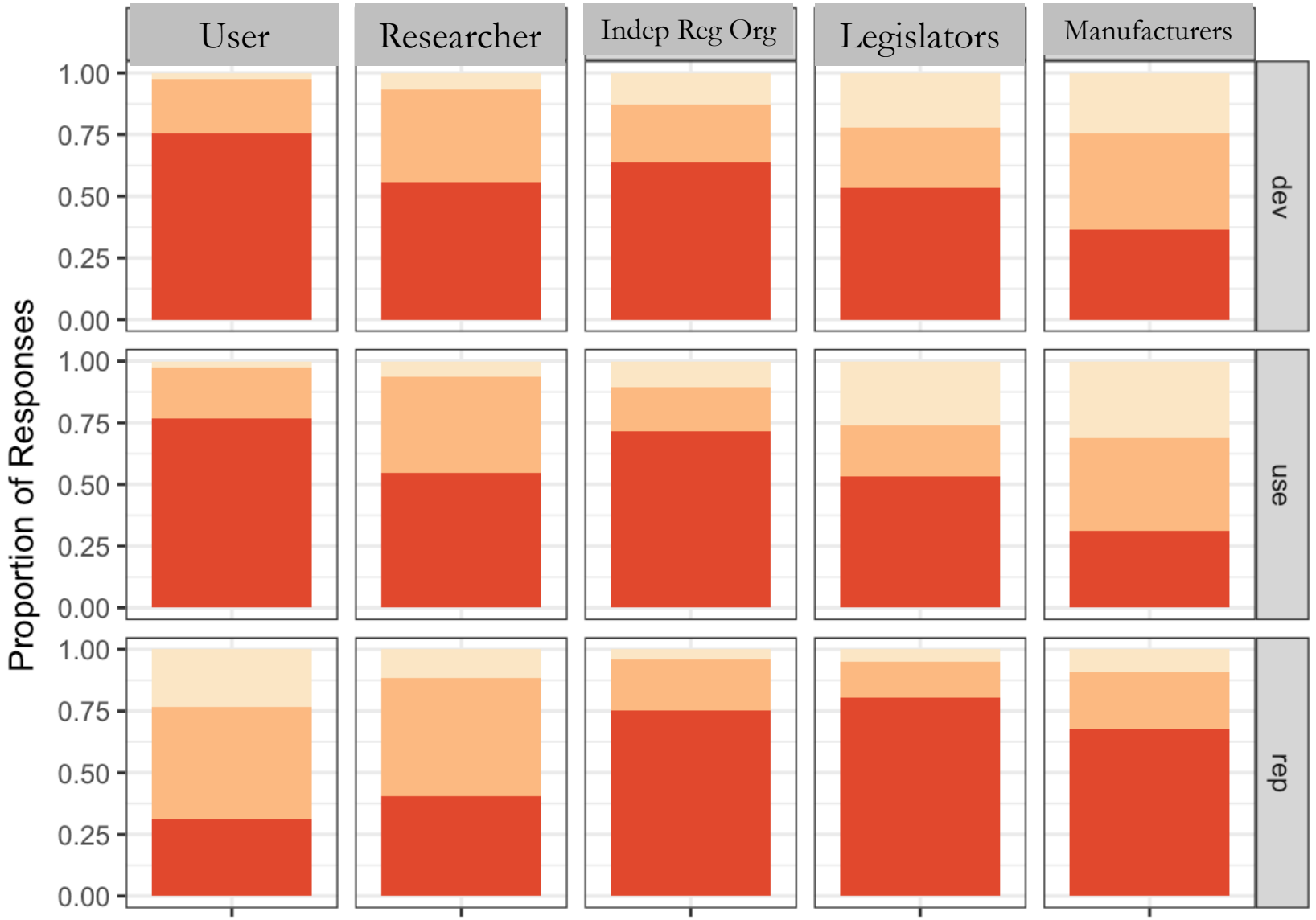
Odds Ratios

1.461

1.536

0.620

Figure 2. Responses to Level of Involvement by Entity and Stage:
1 (less involved) - 3 (more involved)



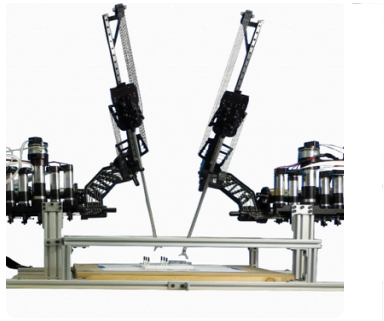
Compared to Current Involvement

Response
1 Less Involved
2 Same
3 More Involved

Sources of Funding

ELECTRICAL & COMPUTER ENGINEERING

Irene Peden Endowed Fellowship



UW BioRobotics Lab

TECH POLICY LAB

CENTER for NEUROTECHNOLOGY
a National Science Foundation Engineering Research Center

NSF EEC 1028725

NSF GRFP
NSF GRADUATE RESEARCH FELLOWSHIP PROGRAM

DGE-1256082
DGE-1762114