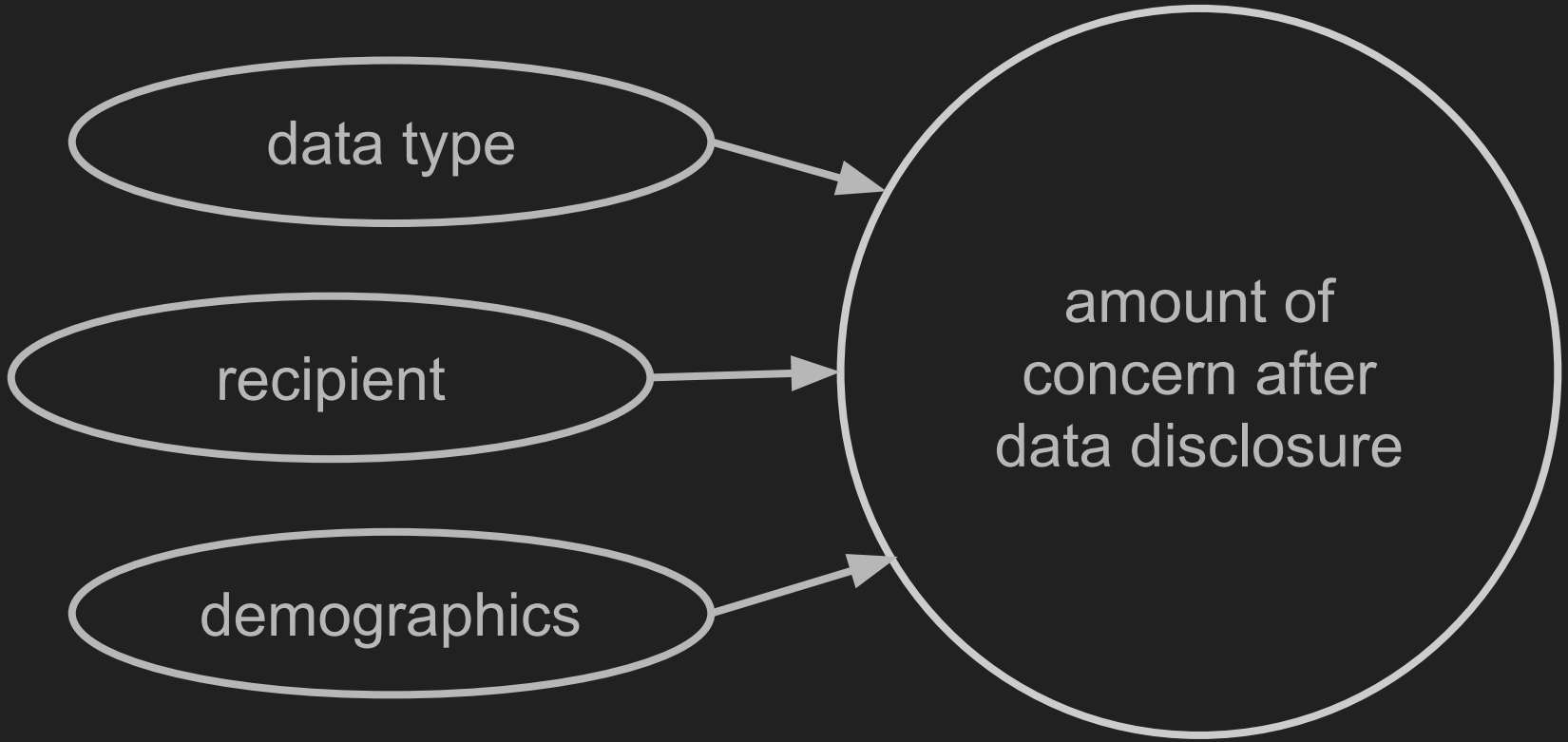
Information Disclosure Concerns in the Age of Wearable Computing

Linda Lee, JoongHwa Lee, Serge Egelman, David Wagner


15:55
5321
00:24:55
1080P
HD
11:42
GPS
118
John
120
122
70
01♥66
5.2
11:35


data type
recipient
demographics
amount of concern after data disclosure

The Survey

2 reading comprehension questions

6 wearables data disclosure questions

1 open ended risk question

14 demographic questions


135


5:30
SFO - JFK
Departs 8:05

Data Type

1. Video, Photo, Audio
2. Device-Stored Information
3. Personal Information
4. Biometric Measurements
5. Behavioral Inferences

Recipient Type

1. Public
2. Friends
3. Work contacts
4. An application’s server


Cubetastic3000

Using a Fictional Device

“Imagine that you are the proud owner of the Cubetastic3000. You wear this device all the time, because it is very lightweight, durable, and convenient.

The Cubetastic3000 has the capability to capture video, photos, audio, and biometrics (biological data about you, such as heart rate). Just like other devices, you can install third-party applications from an app store, and these applications can use the information from the Cubetastic3000.”

Every once in a while, an app might do something on your *Cubetastic3000* without asking you first. Depending on what the app does, your feelings could range from indifference (you don't care) to being very upset.

5. How would you feel if an app on your Cubetastic3000 learned when, how, and how much you exercise and shared that with your work contacts, without asking you first?

Indifferent	-	-	-	Very Upset
○	○	○	○	○

Open-Ended Question

“What do you think are the most likely risks associated with wearable devices?”

Demographics

1,782 valid responses:

57.9% male, 41.0% female, rest declined to state genders.

Ages from 18 to 73, with a μ = of 32.1 (σ = 10.37).

49.2% had completed a college degree or more.

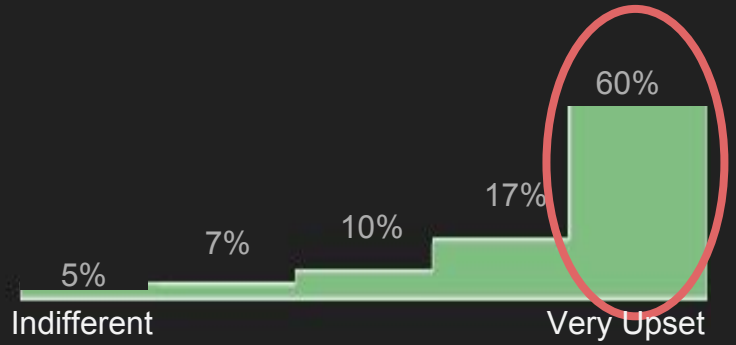
Responses

At least: 35 responses per data type/recipient combination

141 responses per data type

2,779 responses per recipient

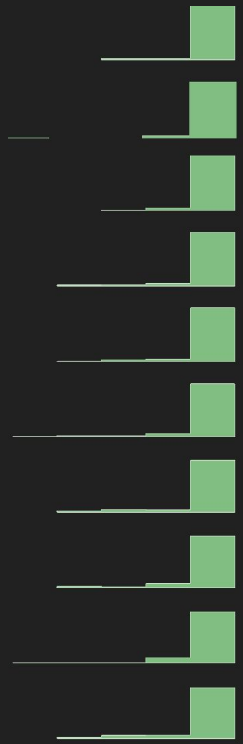
Distribution:



VUR = Very Upset Rate (% of people who answered “very upset” on Likert scale)

Most Concerning Data

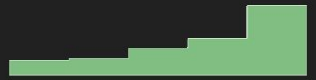
1. video of you unclothed
2. bank account information
3. social security number
4. video entering in a PIN
5. photo of you unclothed
6. photo of you (embarrassing)
7. username and password
8. credit card information
9. video of you (embarrassing)
10. photo of you at home



Least Concerning Data

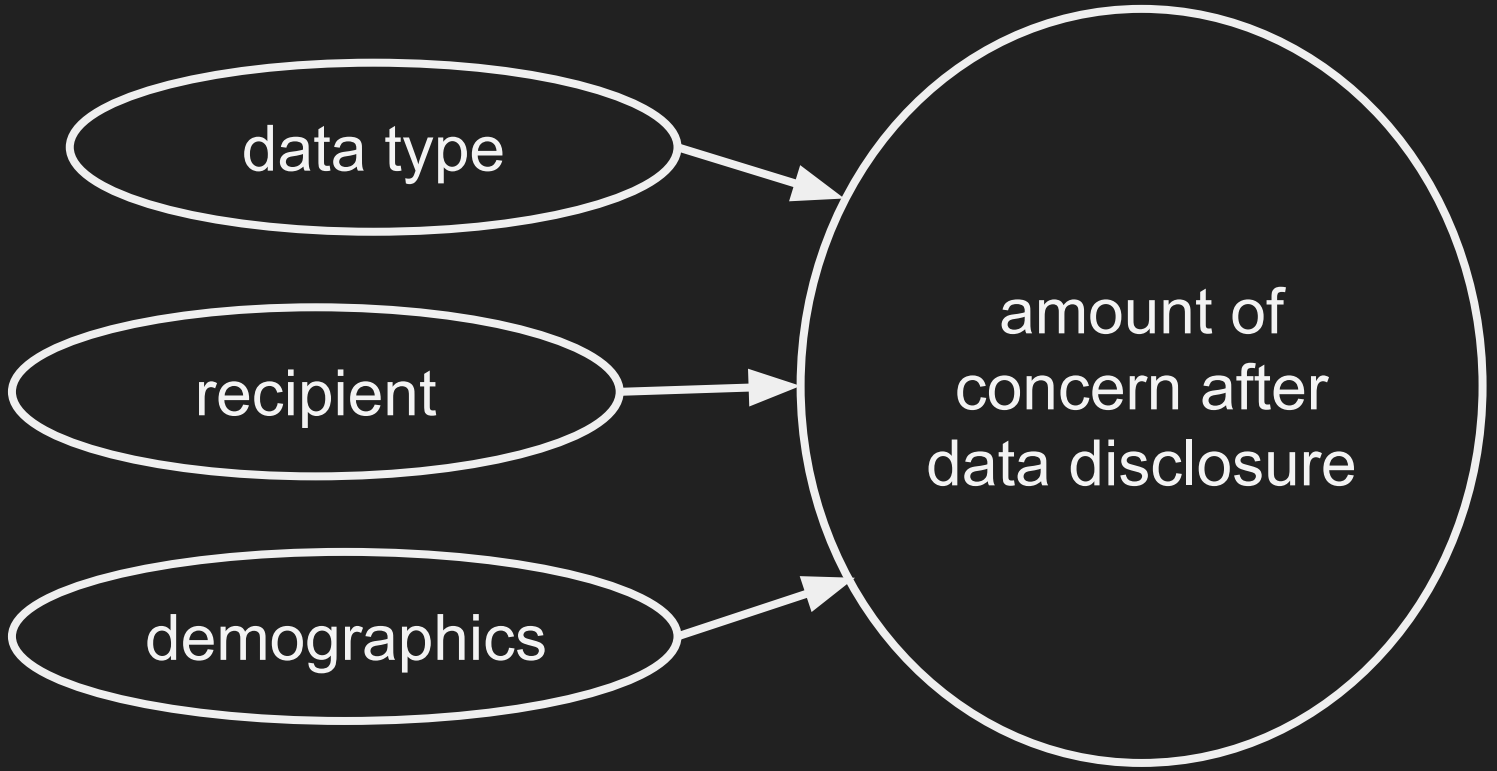
63. eye movements
64. exercise patterns
65. when you are happy
66. television shows watched
67. when you are busy or not
68. music on your device
69. your heart rate
70. age
71. language spoken
72. gender

Sensitivity to Various Recipients

Recipient Type	VUR	Distribution
Work Contacts	75%	
Public	72 %	
Friends	69 %	
App’s Server	42 %	

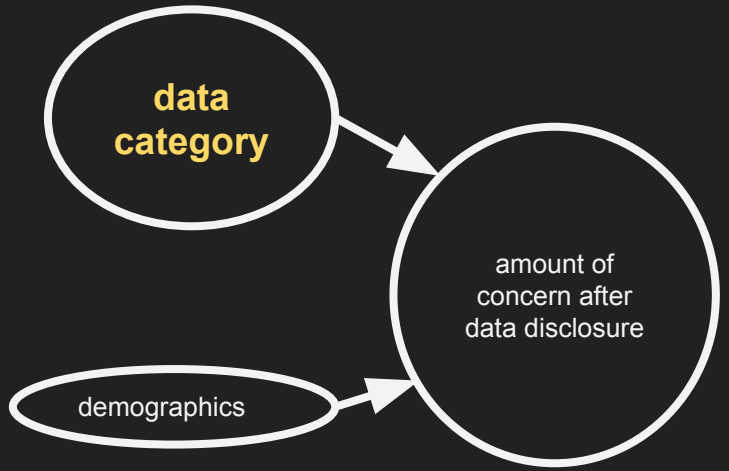
VUR = Very Upset Rate (% of people who answered “very upset” on Likert scale)

Data disclosure acceptance predictors



What data categories matter?

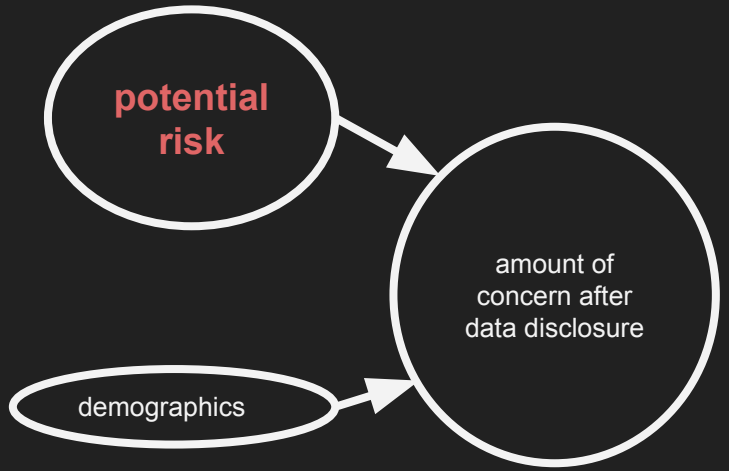
Data Categories	VUR
Video	78 %
Photo	76 %
Audio	67 %
Demographic	65 %
Behavioral	53 %
Biometric	46 %



VUR = Very Upset Rate (% of people who answered “very upset” on Likert scale)

What risks are most concerning?

Potential Risk	VUR
Financial	82 %
Relationships	69 %
Safety	66 %
Personal Image	66 %
Privacy Loss	47 %



VUR = Very Upset Rate (% of people who answered “very upset” on Likert scale)

Top self-reported risks of wearables

“What do you think are the most likely risks associated with wearable devices?”

Concern	Frequency
Privacy	25.32%
Being unaware	15.40%
Health risk	10.70%
Safety	10.42%
Social impact	8.80%
...	...

Limitations

Dependencies on external factors

Self-reported data

Takeaways

Understanding the user matters.

The type of data matters.

Privacy matters.

Context matters.