Center for Democracy & Technology

TOWARDS PRIVACY-AWARE RESEARCH AND DEVELOPMENT IN WEARABLE HEALTH

WEARABLES

STATS

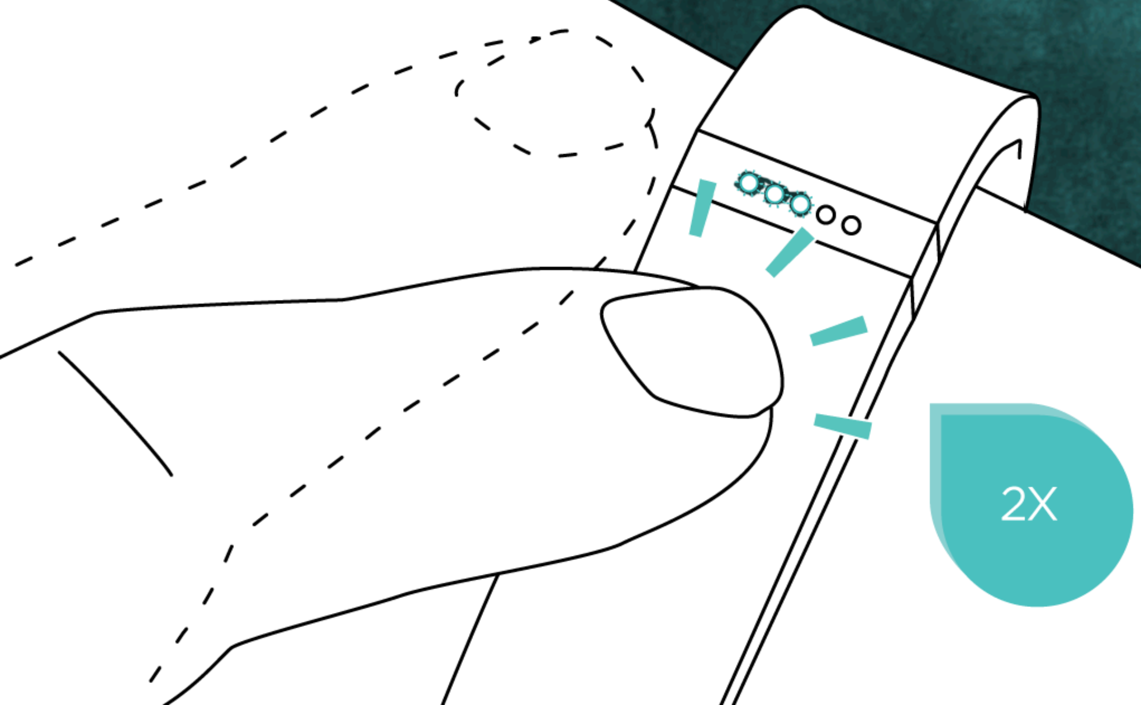
there are 211 million wearables being used worldwide today

68.1 million wearables will be shipped this year

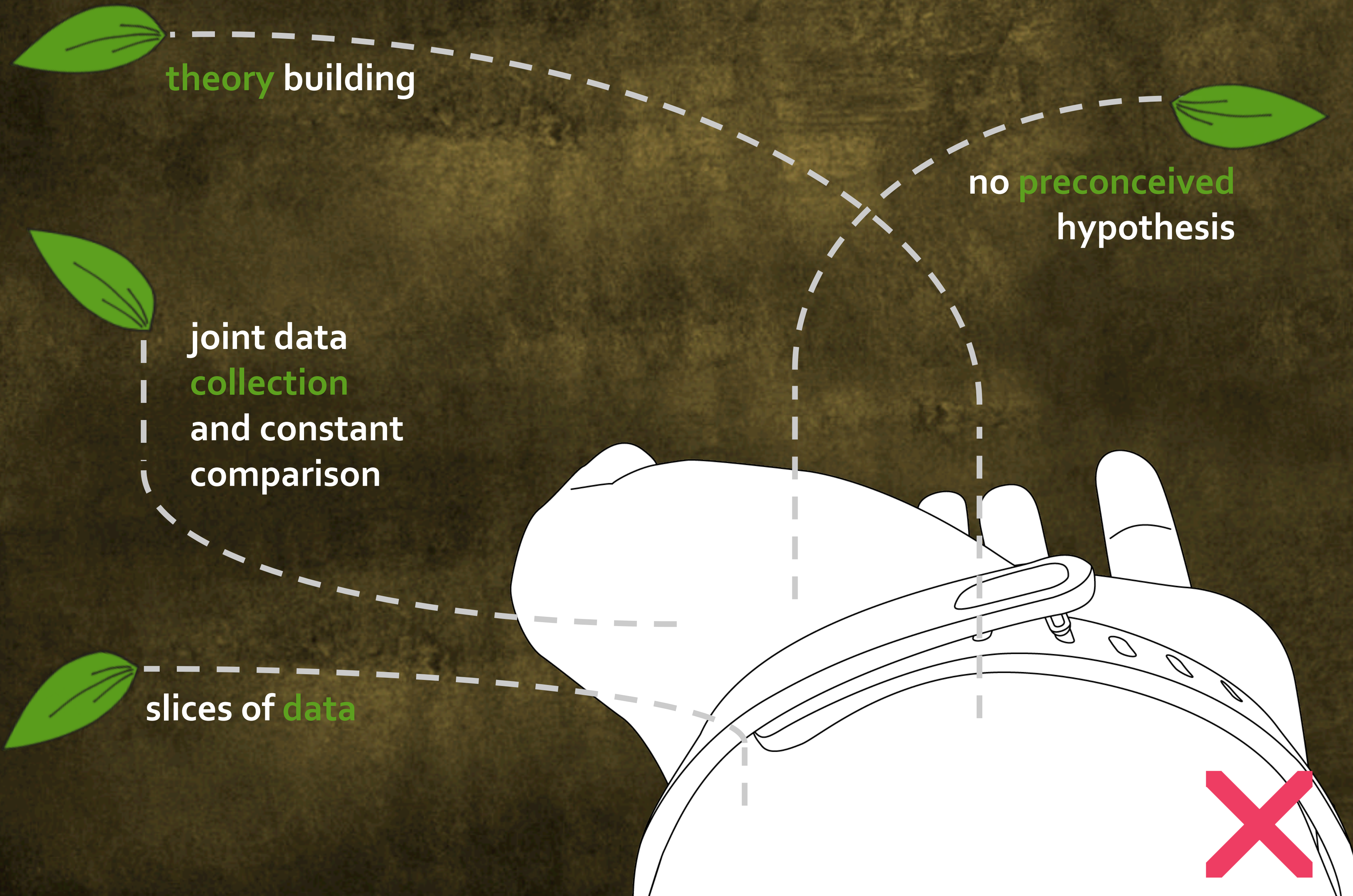
one survey found that around one-third of internet users in the U.S., Australia, and the UK expressed serious concerns about the privacy of their data

34% of those using wearables for fitness tracking share their data using social settings

wearable users generate an average of 15 petabytes of data traffic on networks each month



GROUNDED THEORY METHOD



theory building

no preconceived hypothesis

joint data collection and constant comparison

slices of data

FINDINGS

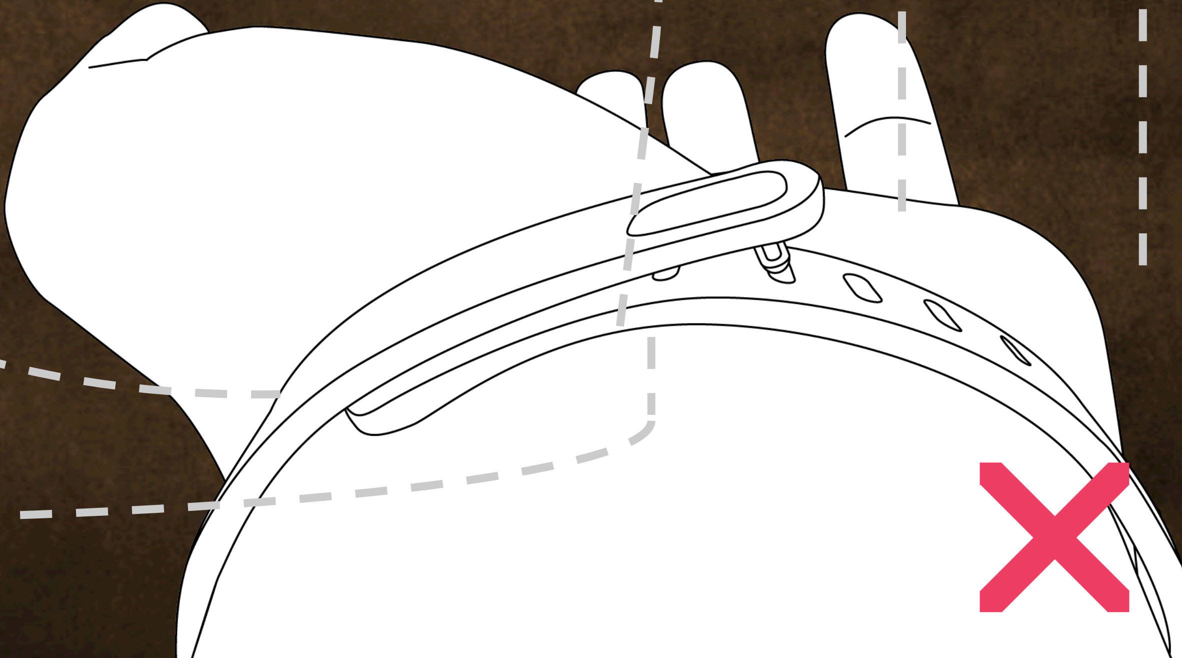
researchers most often **use themselves and their colleagues** as test subjects

data aggregation and reviews by managers are key privacy processes

much of the research is focused on new **sensors and applications**

some projects are dreamed up using **“hacks”**

a culture of privacy exists that can be **harnessed**

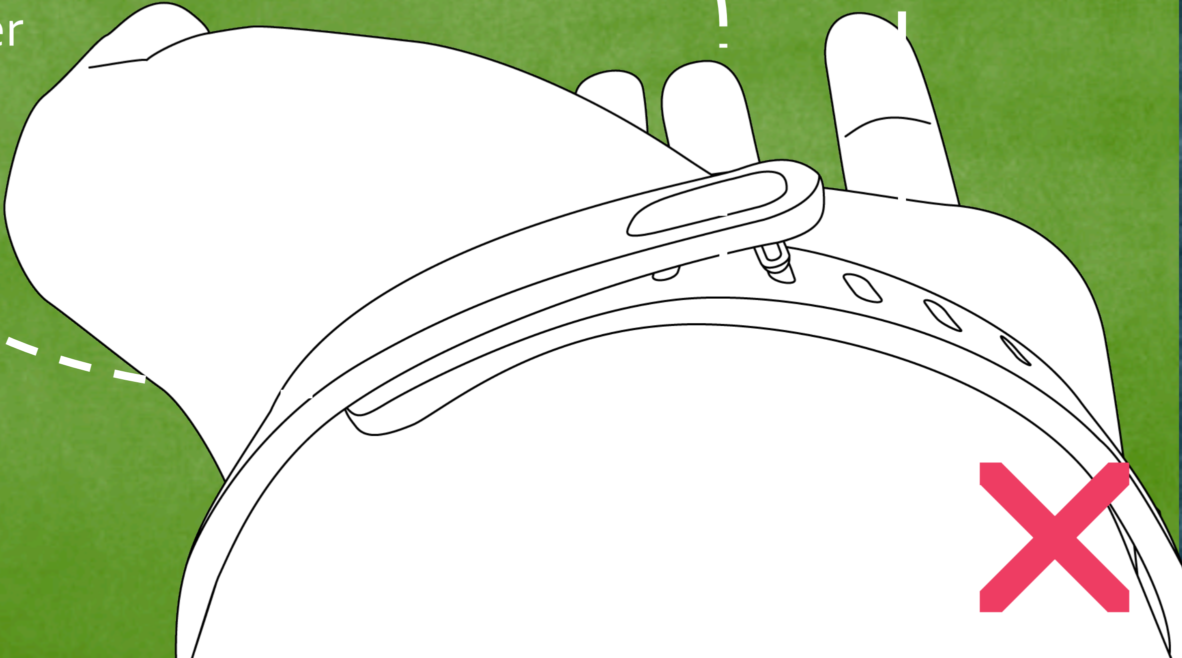


FINDINGS

pilot studies use research employee data and are not anonymized unless sensitive

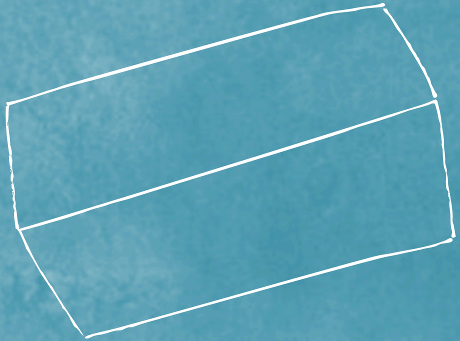
internal studies use data on employees oustide of the research team and all data is anonymized except to researcher

user studies examine data from non-employees – data is anonymized even to researcher though they may access demographic data if needed



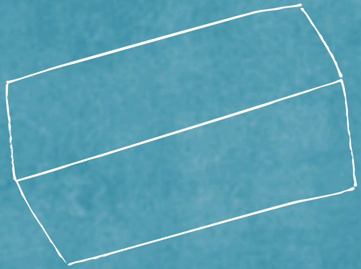
ANALYSIS

research done on employees poses possible benefits and risks



start-ups need flexibility and nimbleness in processes to produce effective and innovative research

the rapid growth of a successful start-up poses risks as investigations accelerate in size and scope and data sets that are typically separated become co-mingled



informal processes rely on the background of the researcher (experience with IRBs, HIPAA)

PRIVACYPIVOTPOINTS

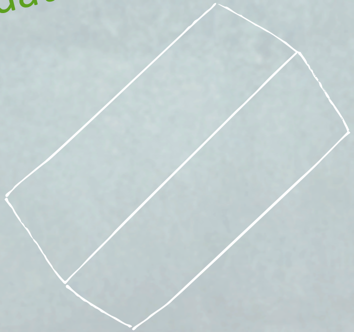
> when the **project lead** is identified

> when projects **use employee** test subjects

> when projects **expand** to bigger user populations

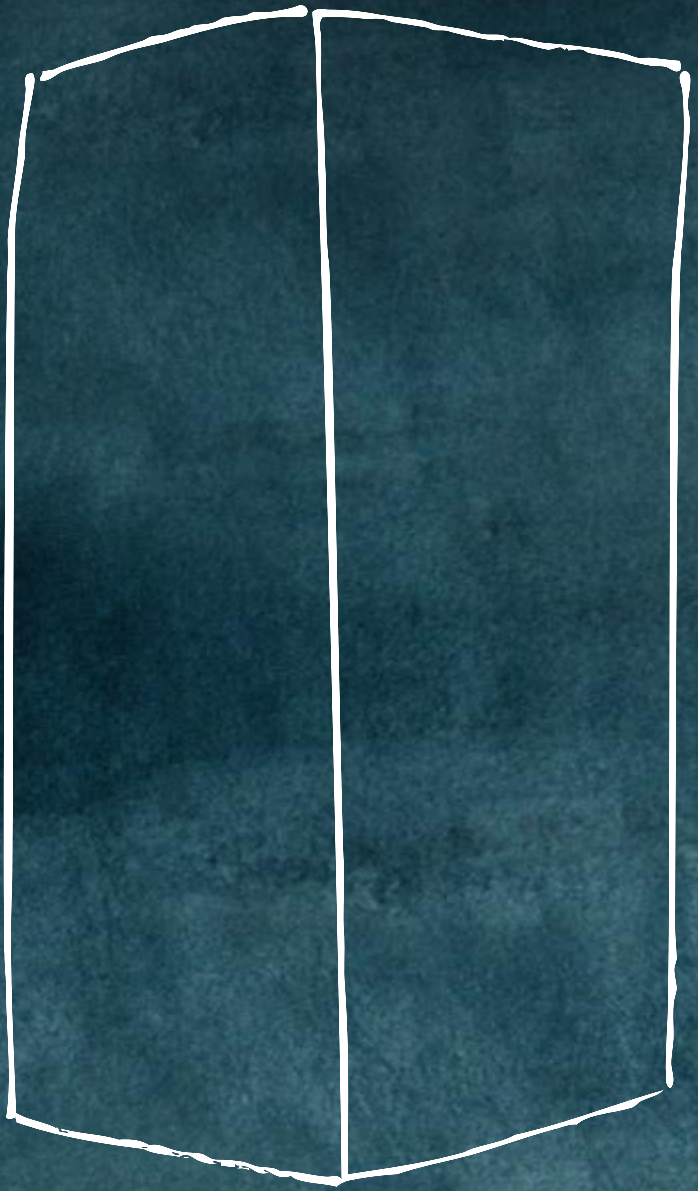
> when **reporting on projects** using employee data, regardless of sensitivity

> when **correlating data** points or using historical data



> when projects **move from one phase** to another such as when hacks are given the green light

Recommendations

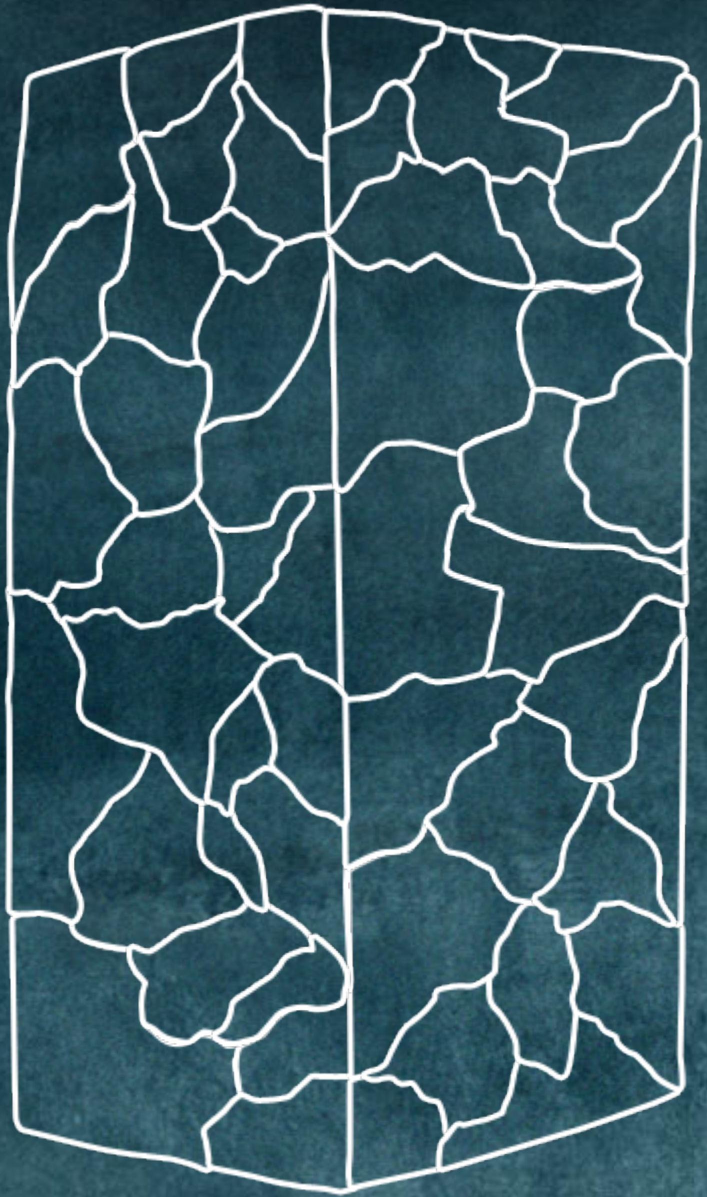


use the box: create formal privacy reviews and protocols

go outside the box: hire a Data Sociologist

investigate paying volunteers for data to avoid coercion

ask researchers to create their own privacy and security accountability measures assess map deploy tweak



use privacy as a tool for

innovation and brand awareness

Center for Democracy & Technology

TO LEARN MORE ABOUT THE INNOVATIVE AND IMPORTANT WORK BEING DONE AT CDT, VISIT WWW.CDT.ORG