



SOUPS 2018

Using Data from Breaches

What is Users Level of Comfort?



Sowmya Karunakaran, Google

/ Kurt Thomas, Elie Bursztein, Oxana Comanescu

/ Google

Let's start with a pop quiz...

Roughly, how many online accounts have been compromised through data breaches?

5,371,008,023

What happens to the data that was compromised during the breach?

Most times becomes available in the black market for free/paid download


Several Uses for Data from Breaches

RESEARCH

[Innovations in Computer Science and Engineering](#) pp 199-210 | [Cite as](#)

Password Reuse Behavior: How Massive Online Data Breaches Impacts Personal Data in Web

Authors [Authors and affiliations](#)

Prabakaran Poornachandran , M. Nithun, Soumajit Pal, Aravind Ashok, Aravind Ajayan

Conference paper

BREACH LOOKUP SERVICE

';--have i been pwned?

Check if you have an account that has been compromised in a data breach

email address

pwned?

INVESTIGATIVE JOURNALISM

2.6TB The Panama Papers, 2016

1.4TB
The Paradise Papers

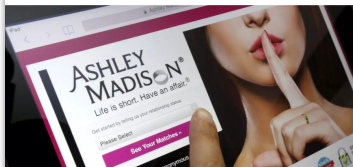
1.7GB WikiLeaks, 2010

3.3GB HSBC files, 2015

4.4GB Luxembourg tax files,
2014

260GB
Offshore secrets,
2013

Will the media name Ashley Madison users? It may not matter – we're all the media now



PROACTIVE SECURITY

Google Security Blog

Cleaning up after password dumps

September 10, 2014

One of the unfortunate realities of the Internet today is a phenomenon known in security circles as “credential dumps”—the posting of lists of usernames and passwords on the web. We’re always monitoring for these dumps so we can respond quickly to protect our users. This week, we identified several lists claiming to contain Google and other Internet providers’ credentials.

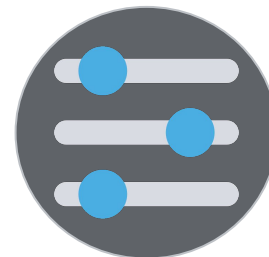
Research Questions

Do users understand breaches?



Comprehension

What according to users are acceptable uses for breached data?



Level of Comfort

Users understand risk of breaches

93%

of participants understand
meaning of data breach

Top user fears

Identity theft

Personal data loss

Monetary loss

What is their level of comfort with various uses of breached data?



Research design considerations

N=10,000

US, IN, DE, UK, AU, CA

2 scenarios per participant

Minimize Availability bias

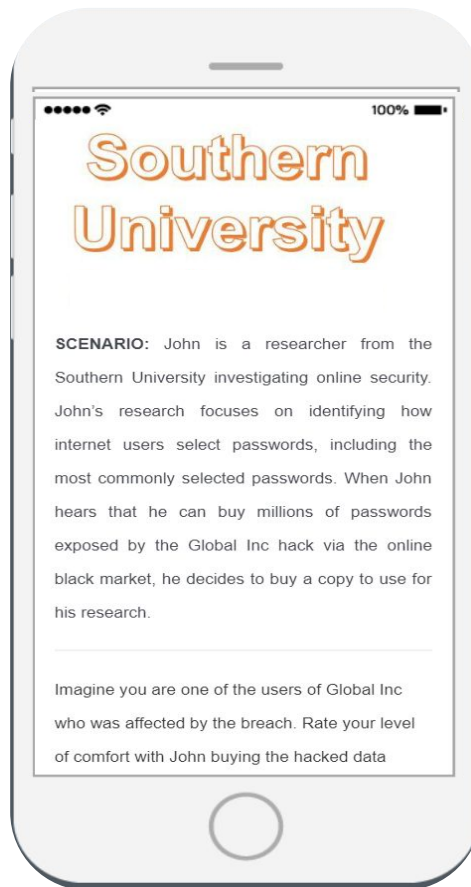
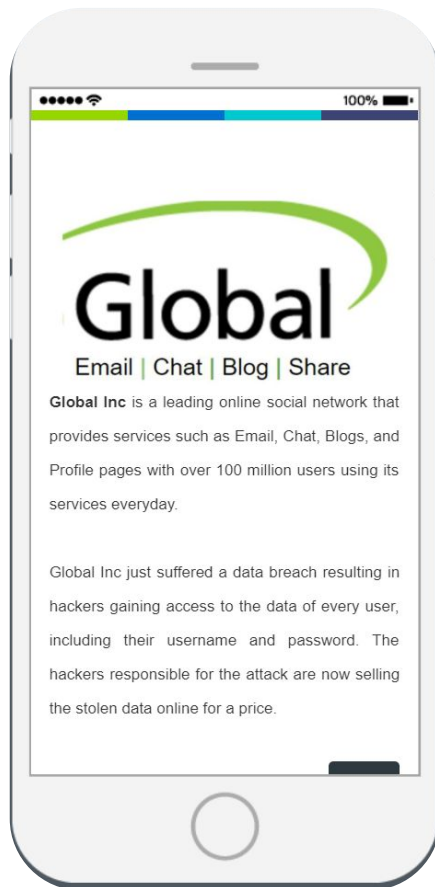


Challenge

Individuals' behavior in context of ethical dilemmas cannot be studied through observation or by asking respondents about the behavior directly.

Scenario-based assessment

Sample scenario



Scenarios

Security

LOOKUP SERVICES
(ex: HAVE I BEEN PWNEED)

PROACTIVE PROTECTION - SCANNING
OF BREACHED DATA DUMPS

THREAT INTELLIGENCE: NOTIFIES
SOCIAL NETWORK SERVICE

THREAT INTELLIGENCE: NOTIFIES
PAYMENT SERVICES

Investigative Journalism

REVEALING A TAX EVASION SCAM

REVEALING DATING SITE PRIVATE
PROFILES

Marketing

COMPETITOR USING BREACHED
DATA FOR MARKETING TO HACKED
USERS

Researcher

RESEARCHER USING THE BREACHED
DATA FOR SECURITY RESEARCH

2 sub scenarios covering source of hacked data: Buy from hacker vs Free download

SCENARIO

Threat Intelligence Sharing | 40% reported comfort

“

I don't have any issue with hacked firm contacting them. It is probably the best thing to do. They can **reset my password before anyone has a chance to try and hack my account.**

”

“

Global Inc has already **failed in securing my data, and I do not trust them** to make any efforts to secure my data elsewhere in the future.

”

SCENARIO

Security Research

A mere **15%** reported comfort

“

If John is a genuine researcher, then no problem. His work would benefit us in the long run.

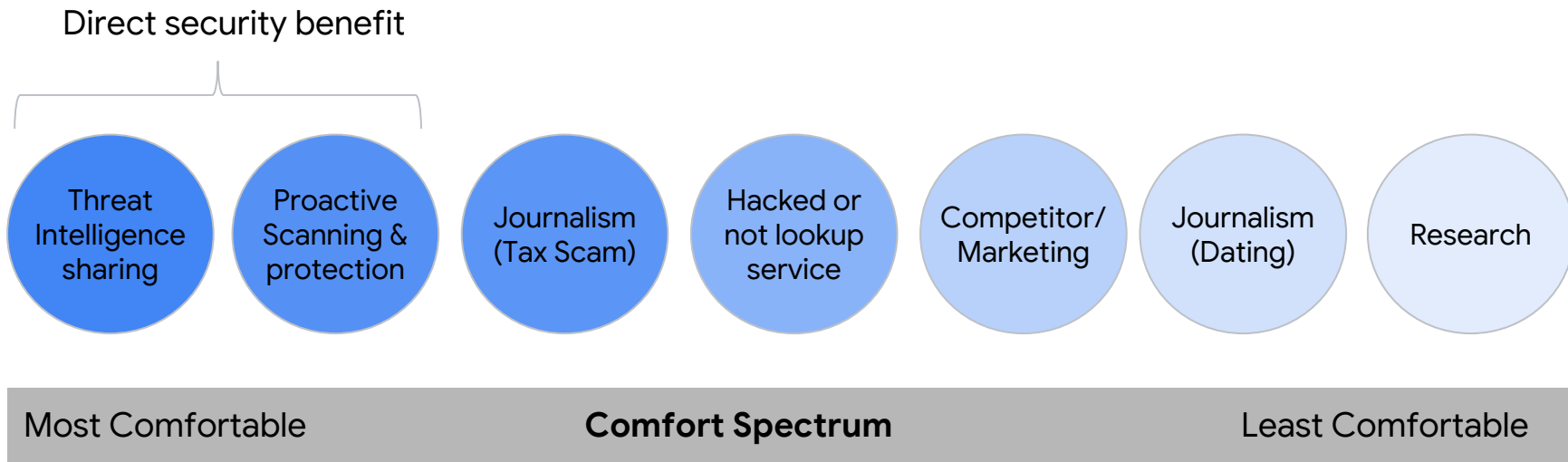
”

“

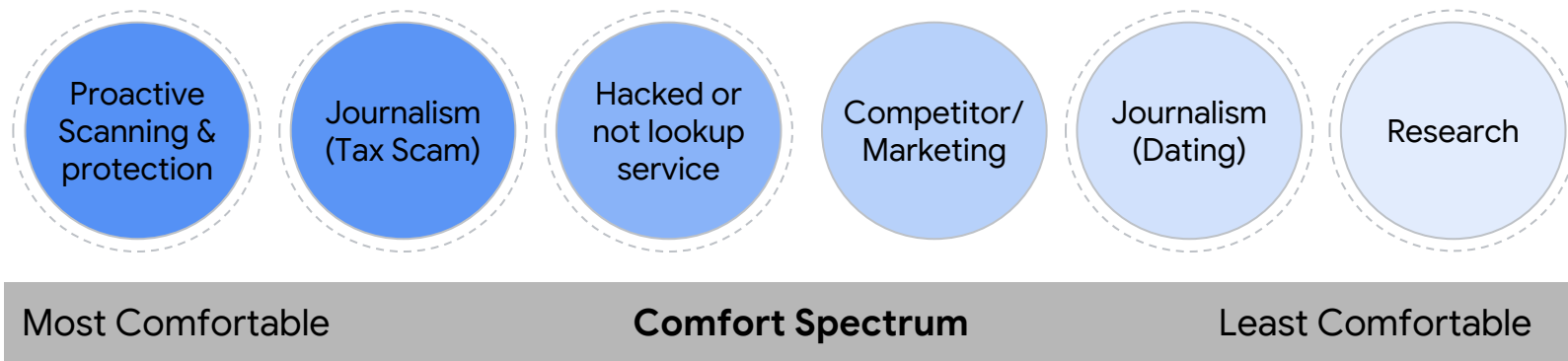
It's incredibly unethical for John to buy passwords from hackers. It's no different than someone buying a car that was stolen.

”

Level of comfort highest for scenarios with direct security benefit

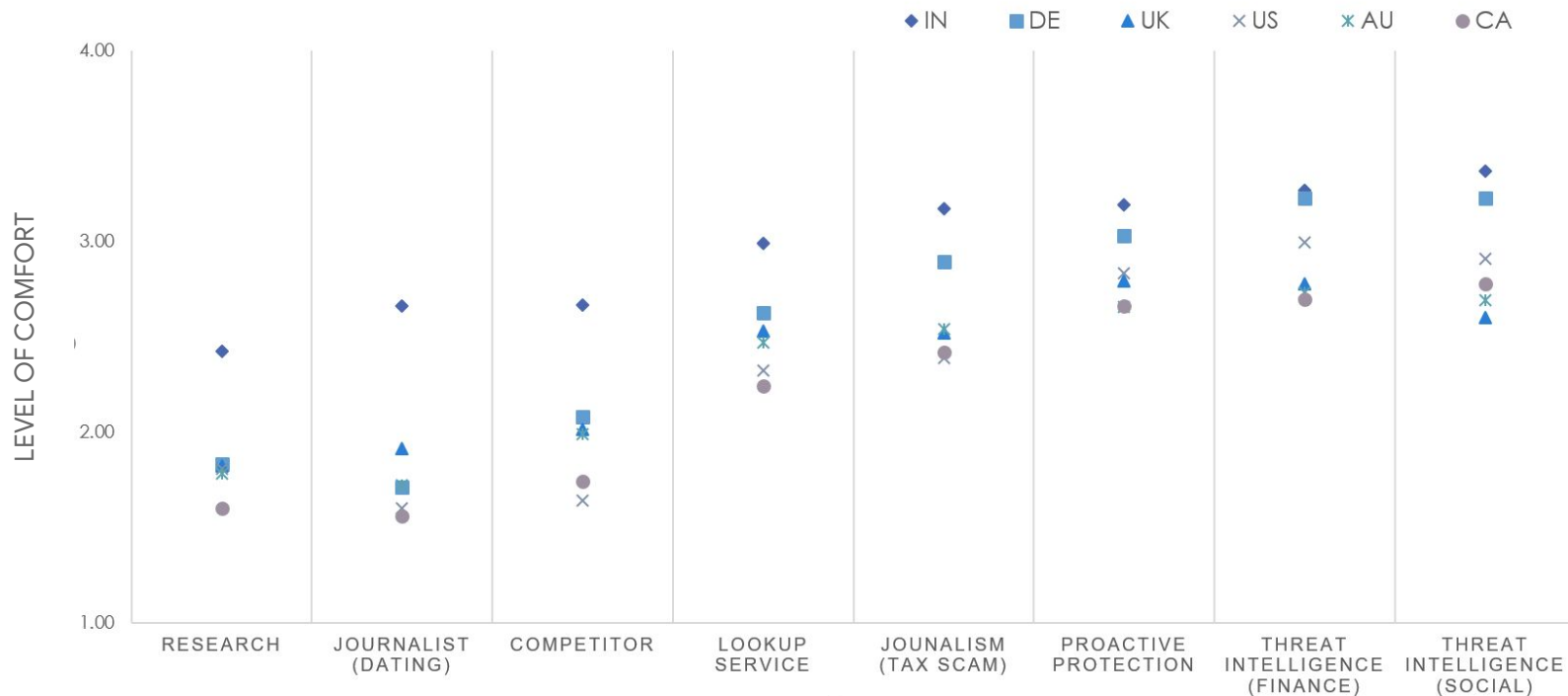


Order preserved regardless of buy vs free download



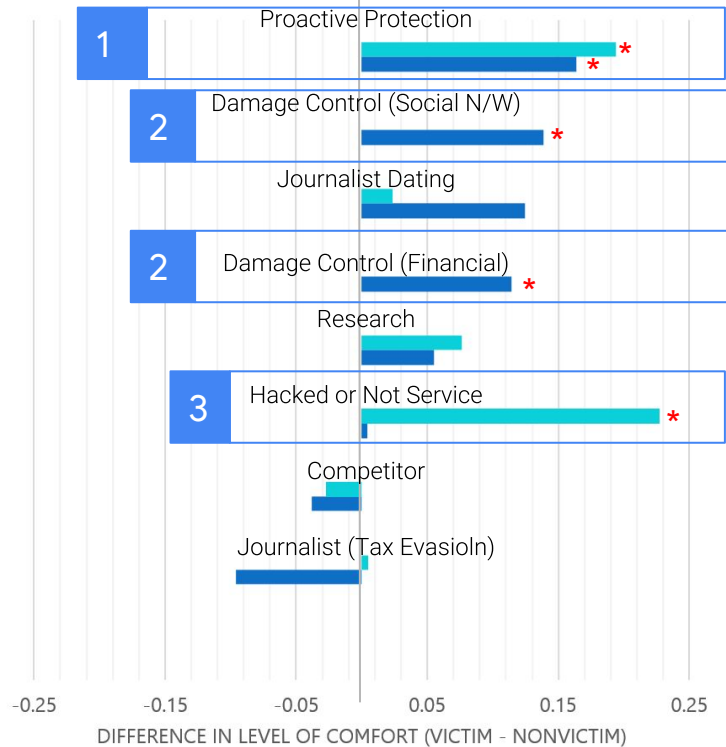
Significant differences in level of comfort between buy vs free download

Comfort spectrum consistent across countries



Prior victims of data breach expressed significantly higher level of comfort

← Non-Victims more comfortable Victims more comfortable →



* Significant Difference

Victims more comfortable

1. Proactive measures
(Irrespective of method of procurement - buy vs free download)
2. Damage control measures
(Both financial and social networking data)
3. Hacked or not service
(Only if method of procurement is free)

Implications

Key expectations and remediation steps

Breached companies need to be transparent and notify victims.

“

I think it's imperative for the company to tell the people whose data has been accessed. Companies should not control but rather empower

”

Proactively reset passwords and lock down accounts from further damage

“

This is a proactive step from [the company], and one that they are not actually obligated to do. This makes me feel like the company cares about protecting my identity

”

Articulate how any security service can provide a direct benefit to the victims.

“

I have faith that this action will ultimately contribute to making the general population less vulnerable in the long run.

”

Address security & privacy concerns



Clarify the skepticism surrounding security actions that would help secure their accounts.



Match user's strong expectations about privacy and ethical behavior while using breached datasets.

Thank You

sowmyakaru@google.com

 @Sowmya_Karu