Lengthy, Vague, and Inactionable:

Issues with Data Breach Notifications and Implications for Public Policy

Yixin Zou, Shawn Danino, Kaiwen Sun, Abraham H. Mhaidli, Austin McCall, Florian Schaub

Jun. 27, 2019

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

PRIVACYCON

The research presented was partially funded by the Mozilla Corporation.

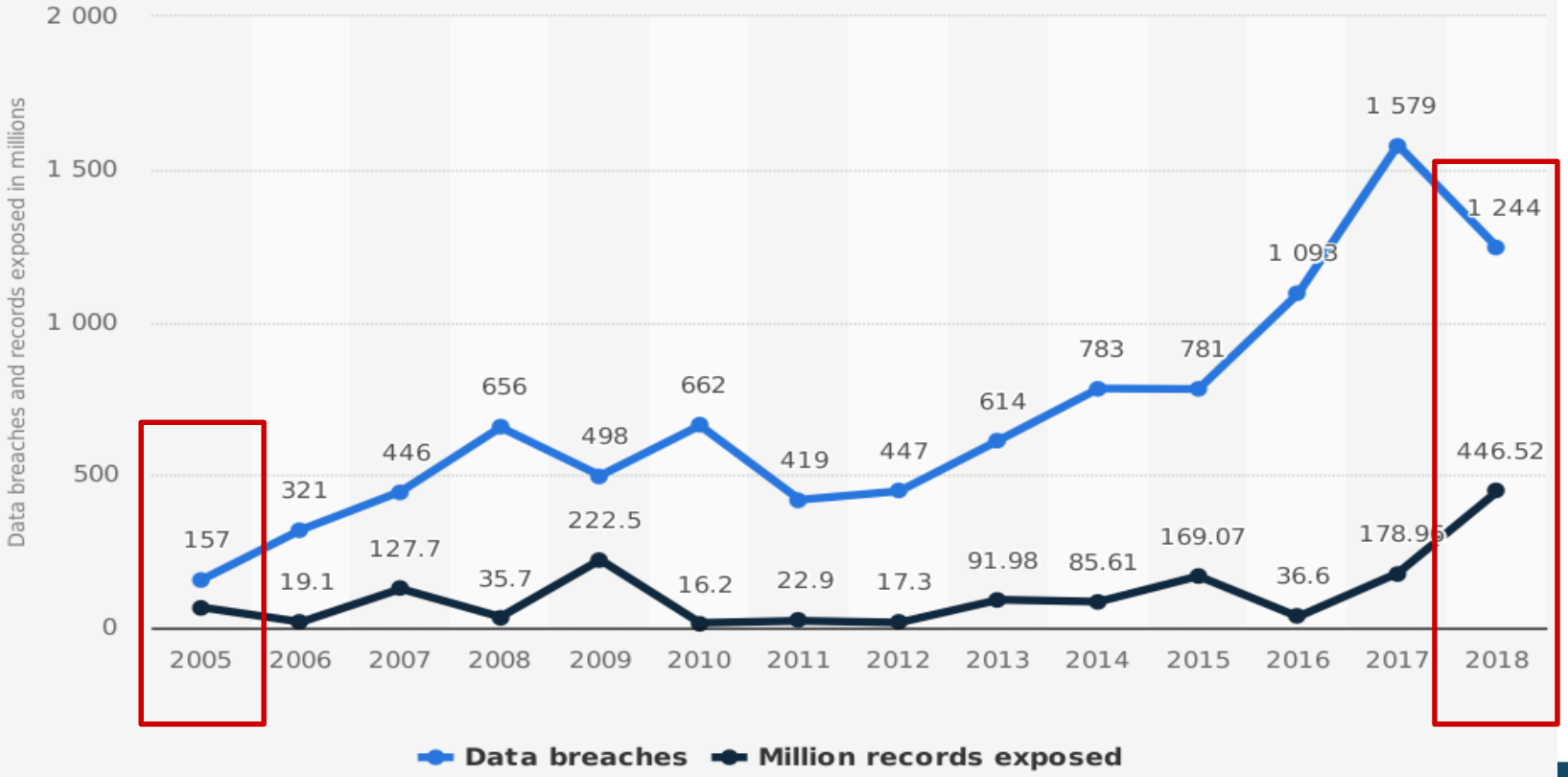
Security Incidents

Sensitive information

Data Breach

Unauthorized access

Annual number of data breaches and exposed records in the United States from 2005 to 2018 (in millions)



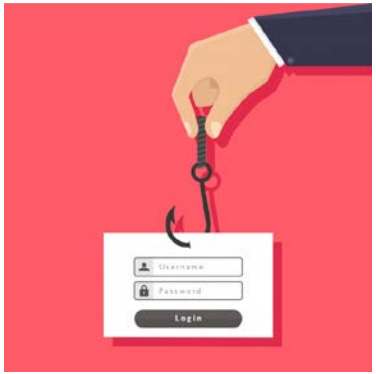
Source
Identity Theft Resource Center
© Statista 2019

Additional Information:
United States; Identity Theft Resource Center; 2005 to 2018

Potential harms of data breaches

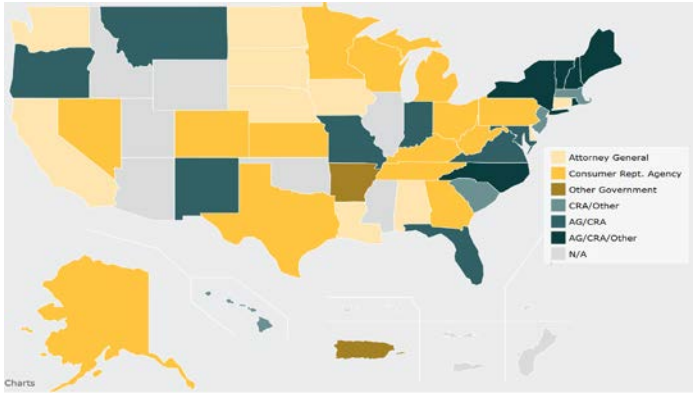
Data leaked to the dark web

Phishing attacks



Identity theft

U.S. regulations for data breach notifications



Each state has their own law, with large inconsistencies in between.[1]

HIPAA
Health Insurance Portability & Accountability Act

A few industry-specific laws (e.g., HIPPA).

[1] https://www.dwt.com/statedatabreachstatutes/

Consumers' inaction to data breaches

32% Ignored the notification(s) and did nothing.[2]

56% Used the same password for multiple online accounts.[3]

[2] **The Aftermath of A Data Breach: Consumer Sentiment.** Ponemon Institute. 2014.
[3] **Data Breaches and Customer Loyalty.** Gemalto. 2017.

Data breaches pose significant **security risks**.

Data breach notifications DO NOT trigger consumer reactions effectively.

How to make data breach notifications useful?

PRIVACYCON

Consumer Reactions to the EQUIFAX Data Breach

PRIVACYCON

Research questions

1. How did consumers **perceive the risks** of the Equifax data breach?

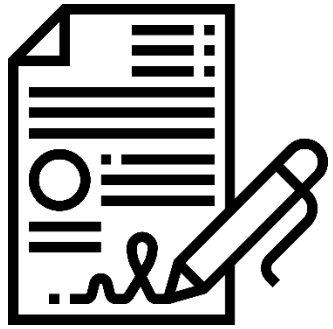
2. What **protective actions** did consumers take in response, and what are the reasons behind (in)action?

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.
Zou et al. (2018). In *Fourteenth Symposium on Usable Privacy and Security,* p.197-216.

Method

24 **semi-structured interviews** between Jan. and Feb. 2018.

Use **social media** and **email lists** for recruitment.



Thematic coding for analysis (κ = 0.79).

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.
Zou et al. (2018). In *Fourteenth Symposium on Usable Privacy and Security*, p.197-216.

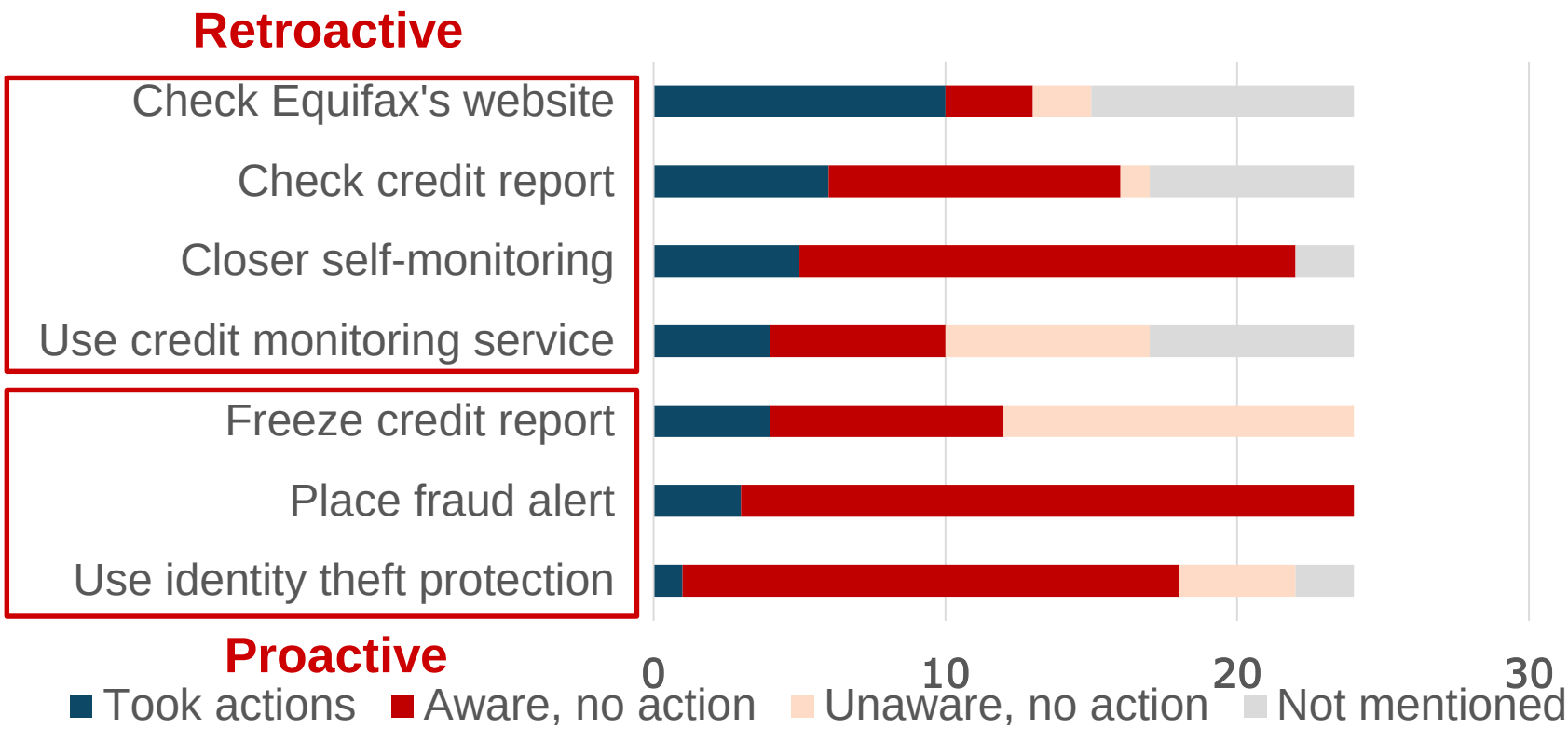
Little action despite high concern

20 out of 24 were **aware** of the breach.

Identity theft and **privacy invasion** were conceived as major risks.

14 participants **DID NOT** take any protective measures.

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.
Zou et al. (2018). In *Fourteenth Symposium on Usable Privacy and Security*, p.197-216.



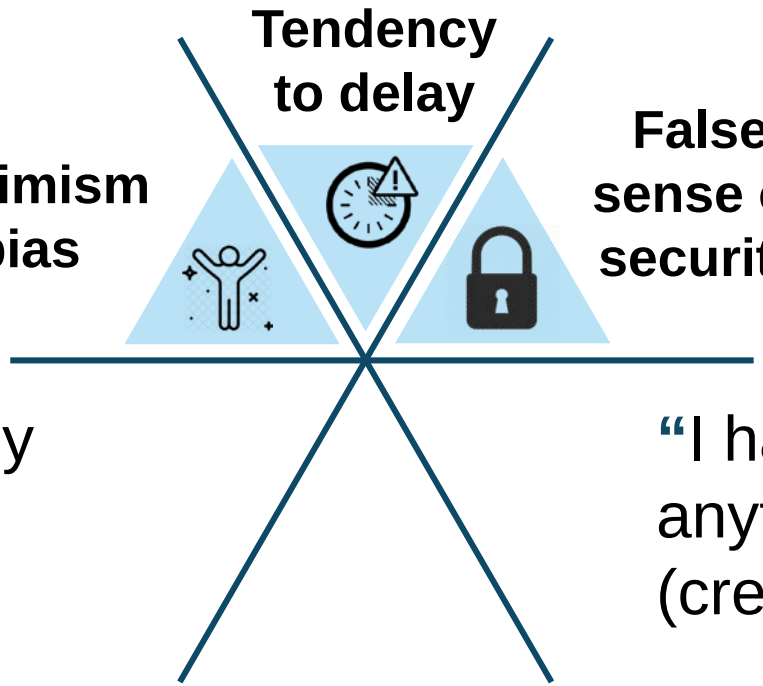
[4] https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

PRIVACYCON

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.

Zou et al. (2018). In *Fourteenth Symposium on Usable Privacy and Security,* p.197-216.

Cognitive and behavioral biases behind inaction



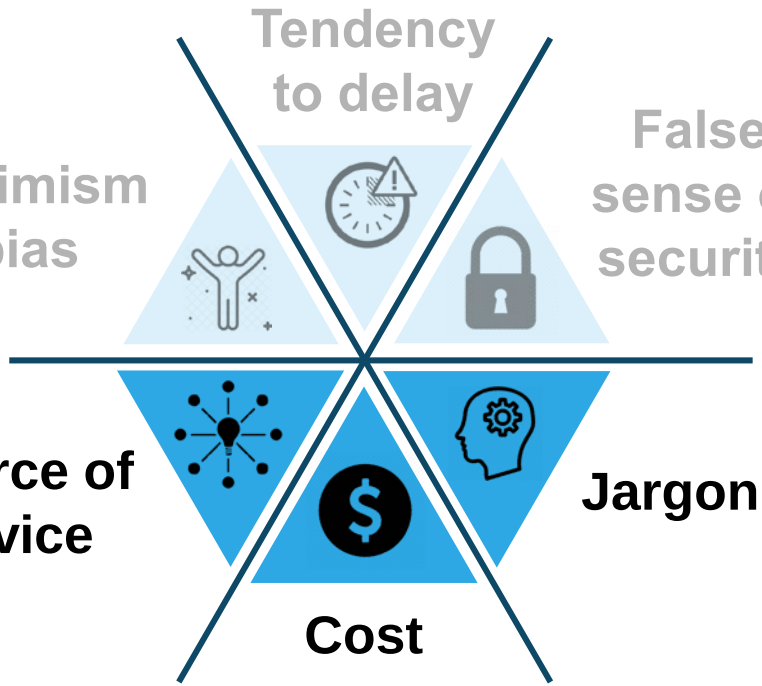
“Why would they go after me?”

“I haven’t done anything since the (credit) freeze.”

PRIVACYCON

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.
Zou et al. (2018). In *Fourteenth Symposium on Usable Privacy and Security*, p.197-216.

Extrinsic factors that motivate actions or inaction



PRIVACYCON

"I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach.

Zou et al. (2018). In *Fourteenth Symposium on Usable Privacy and Security*, p.197-216.

An Empirical Analysis of Data Breach Notifications

Dear [Driver Name]:

Our security teams detected unusual activity on your account that looked like it might not be from you. We want to make you aware of this incident, what we have done in response, and steps that you can take to help protect your information.

What Happened
Specifically, we detected a login between approximately December 10, 2018 22:00 UTC and December 11, 2018 01:00 UTC that may not have been you. We further detected activity accessing the "Waybill" functionality on your account between the time of the unusual login and the point when your password was reset. For your account, we identified the following Waybill access(es):

Date and time (UTC): [Timestamp] IP Address: [IP Address]

What Information Was Involved
The Waybill functionality in your jurisdiction displays information about your current or most recent trip, as well as your name and driver's license number.

What We Are Doing
We reset the password on your account to prevent additional unauthorized access. Furthermore, we have since removed the display of driver's license from the Waybill in your jurisdiction.

What You Can Do
If you accessed a Waybill at the time(s) above, then no further action is necessary. If you believe someone else may have been responsible for this access, we recommend that you take the steps below. In addition, remember to practice good password hygiene, including using complex and unique passwords for each of your online accounts. If you used the same password on any other online accounts, you should change it on those accounts too. A password manager and this useful guide from the Electronic Frontier Foundation (https://ssd.eff.org/en/node/23/) can help you create and safely keep track of strong passwords for every account.

Activate Experian IdentityWorks
To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

What are the potential issues with current data breach notification?

- Readability
- Risk communication techniques
- Structure and format
- How recommended actions are presented

PRIVACYCON

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Method

161 notifications during the first half of 2018, sampled from the website of **Maryland Attorney General**.

Quantitative metrics

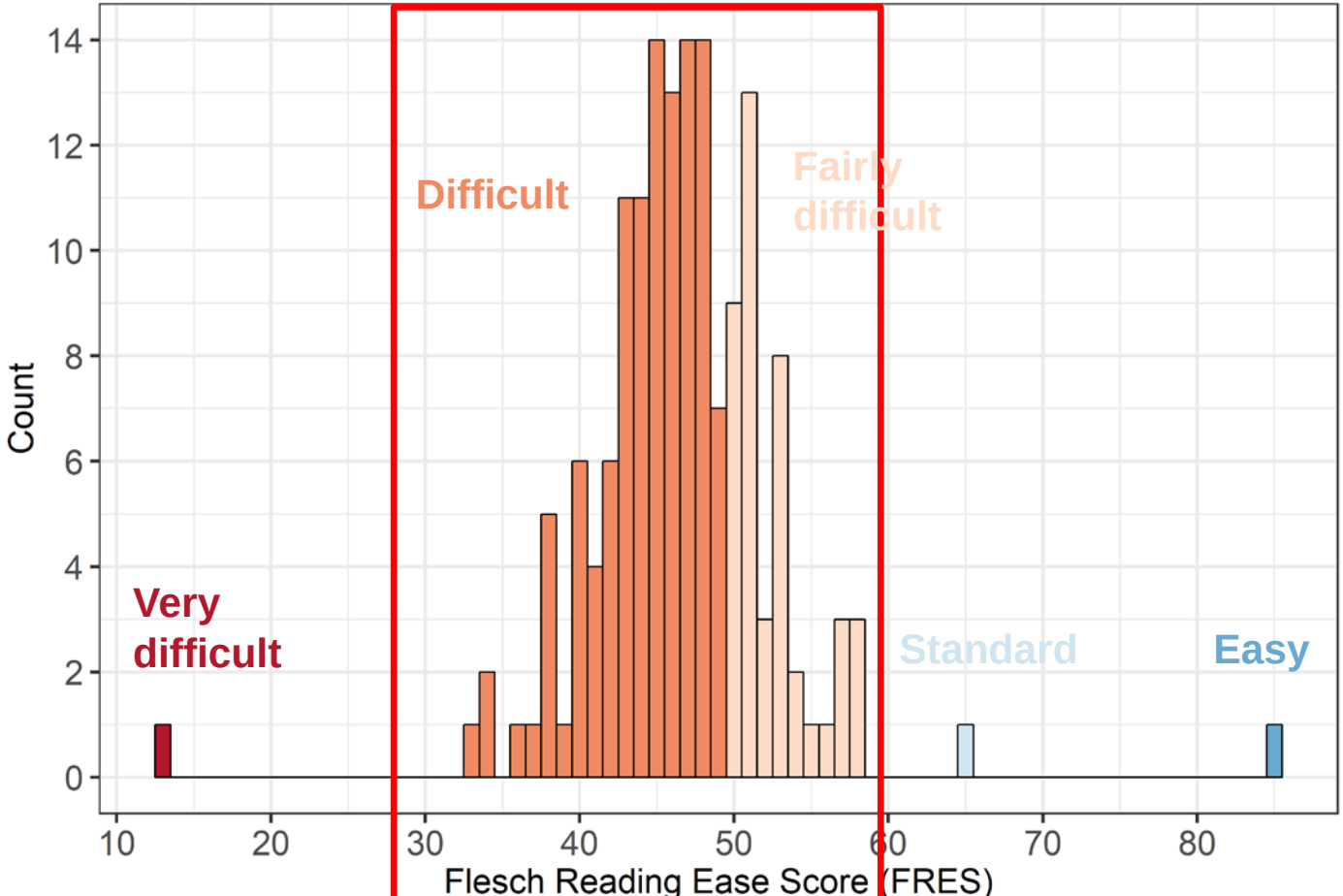
Readability Grade Levels	
Flesch-Kincaid Grade Level	9.8
Gunning Fog Index	13.2
Readability Scores	
Flesch Reading Ease	47.5

Qualitative coding

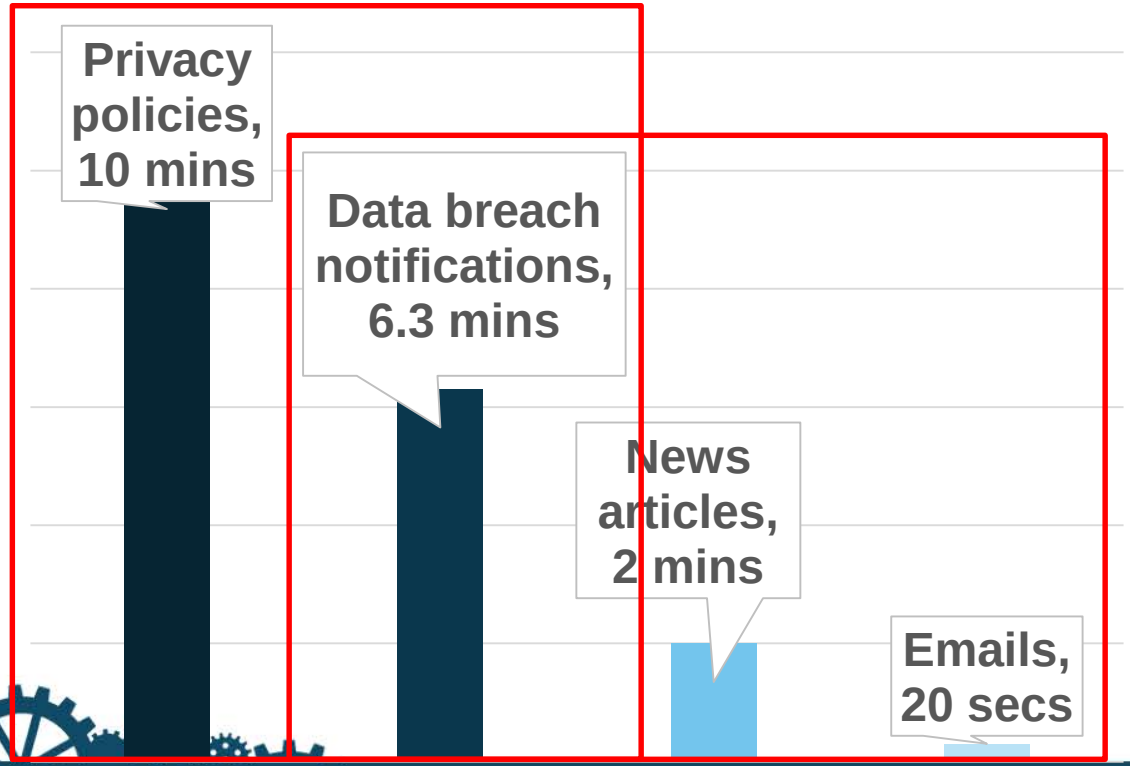
Code name	NVivo codes
Delivery method	Delivery method - mailed letter
	Delivery method - email
	Delivery method - website announcement
	Delivery method - other
Use of structural headings	Use of structural headings - yes (in separate lines)
	Use of structural headings - yes (in the same line as main text)
	Use of structural headings - yes (as tables)
	Use of structural headings - other

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Data breach notifications are hard to read



Six minutes estimated reading time on average



PRIVACYCON

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Techniques to downplay potential risks

70% used **hedge terms** when describing the likelihood of the recipient being affected.

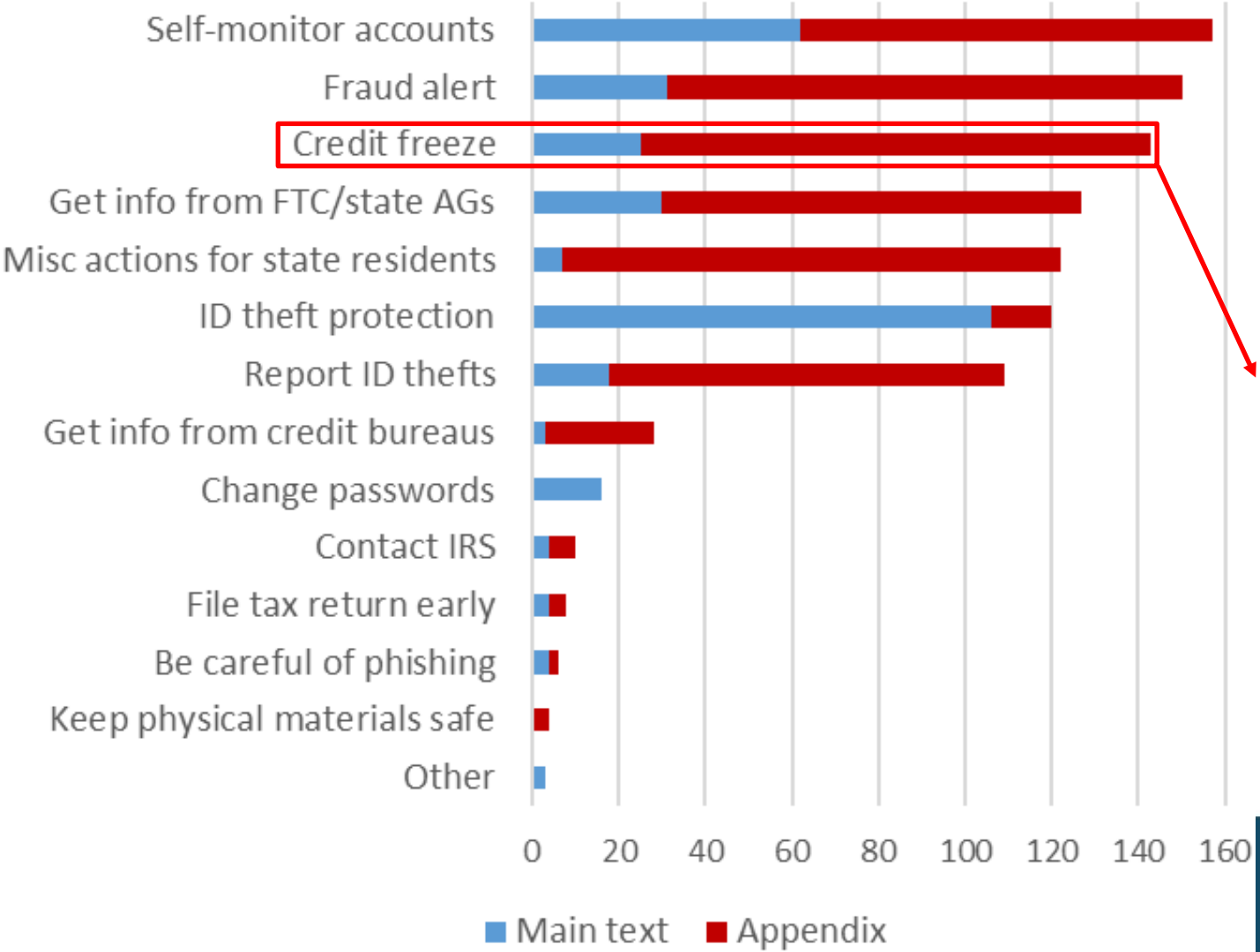
employees and contractors. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information. This notice explains the incident, measures we have taken, and some steps you can take in response.

40% used "no evidence" claim when describing the possibility of exposed data being misused.

of the school district's internal computer systems or networks, or that any student information or any other employee information was affected. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

PRIVACYCON

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.



8 as the median number of suggested actions.

73% mentioned credit freeze in the appendix.

Important actions buried in long paragraphs

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

Fraud alert

Credit freeze

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Little guidance for comparison and prioritization

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

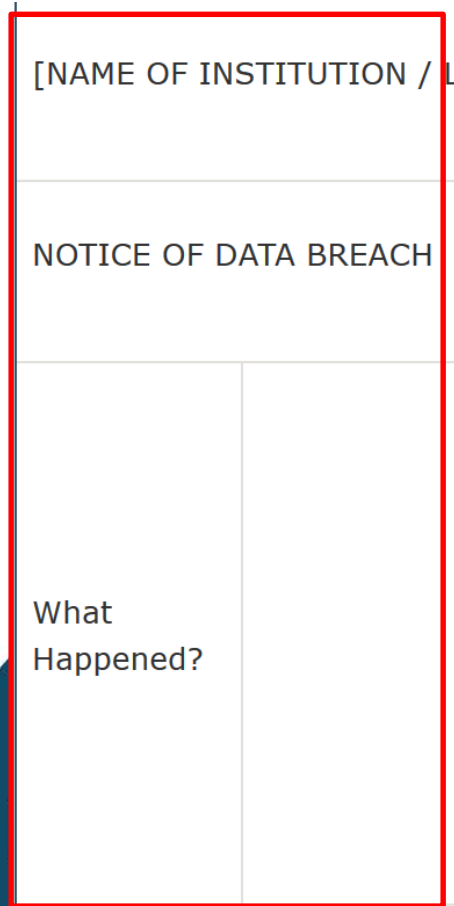
Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

Which one is more effective?

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Prevalence of the California headings



[NAME OF INSTITUTION / LOGO] _____ _____ Date: [insert date]

NOTICE OF DATA BREACH

What Happened?

94% of notifications that used headings followed the exact wording suggestions in California's breach notification law.[5]

[5] https://www.oag.ca.gov/privacy/databreach/reporting

Long list of state attorney general contact info

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or http://www.oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or http://www.riag.ri.gov/. You may also file a police report by contacting local or state law enforcement agencies.

Does a Maryland resident really need to see this?

Consumers **DO NOT** react to data breaches for **various reasons**, such as behavioral biases, source of advice, and jargon in notification.

In order to make data breach notifications **effective** at **motivating** consumers to take actions, we need to **fix these uncovered issues**.

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Recommendations for data breach regulations

Incorporate **readability testing** based on standardized metrics.

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

What does **“plain language”** mean in California’s law? [5]

(1) The security breach notification shall be written in plain language, shall present the information described in paragraph (2) under the fol Information Was Involved,” “What We Are Doing,” “What You Can Do,’ information may be provided as a supplement to the notice.

Specific **metric-based** requirement for **health insurance policies** [6]

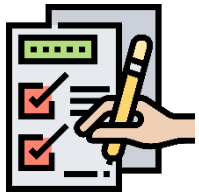
Effective August 31, 2010, the Rhode Island Office of the Health Insurance Commissioner (“OHIC”) will impose a readability requirement for all health insurance policies to be readable at the eighth grade level measured by the Flesch-Kincade formula. The readability requirement comes in response to Rhode Island’s low adult literacy rate, and is designed to protect consumers by making health insurance policies, which are often complicated, easy to understand.

[5] https://www.oag.ca.gov/privacy/databreach/reporting

[6] https://media.lockelord.com/files/upload/1_Regulation_5_final.pdf

Recommendations for data breach regulations

Incorporate **readability testing** based on standardized metrics.



Provide concrete guidelines of **how** information should be presented.

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

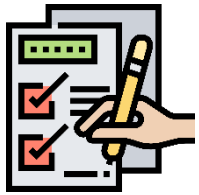
- Place credit freeze **on top of** fraud alert.
- Explain **why it's important** for the recipient to do so.
- Use **visuals** to highlight key info.

PRIVACYCON

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.

Recommendations for data breach regulations

Incorporate **readability testing** based on standardized metrics.

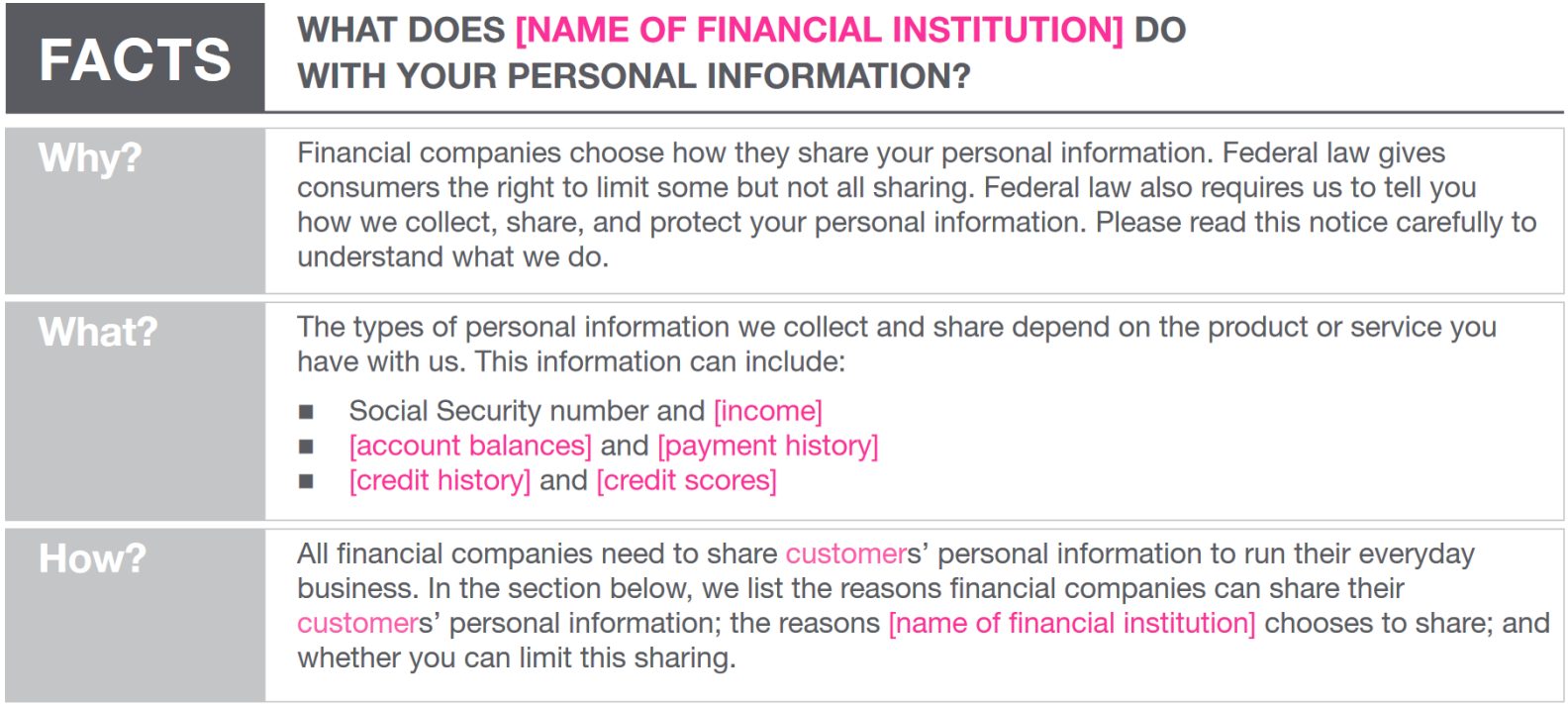


Provide concrete guidelines of **how** information should be presented.

Leverage the **influence** of **templates** to advocate positive changes.

PRIVACYCON

You 'Might' Be Affected: An Empirical Analysis of Readability and Usability Issues in Data Breach Notifications.
Zou et al., 2019. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (p. 194). ACM.



FACTS | **WHAT DOES [NAME OF FINANCIAL INSTITUTION] DO WITH YOUR PERSONAL INFORMATION?**

Why?

Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.

What?

The types of personal information we collect and share depend on the product or service you have with us. This information can include:

- Social Security number and [income]
- [account balances] and [payment history]
- [credit history] and [credit scores]

How?

All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons [name of financial institution] chooses to share; and whether you can limit this sharing.

The model privacy form for GLBA [7]

[7] http://www.ftc.gov/privacy/privacyinitiatives/PrivacyModelForm.pdf

Consumers are **NOT reacting** to data breaches.

Data breach notifications are **NOT protecting** consumers.

Let's have **stronger and more concrete** regulatory guidelines to affect changes.

Yixin Zou

SCHOOL OF INFORMATION
UNIVERSITY OF MICHIGAN

yixinz@umich.edu

@yixinzou1124

PRIVACYCON

The research presented was partially funded by the Mozilla Corporation.