2020 Vision For Web Privacy

Eric Chan-Tin
Assistant Professor
Department of Computer Science
Loyola University Chicago

SNTA'20 Keynote

LOYOLA
UNIVERSITY CHICAGO
1870
AD · MAJOREM · DEI · GLORIAM

Preparing people to lead extraordinary lives

What does Privacy mean to you?

What does Privacy mean to you?

- Personal
  - What you buy
  - What you do
  - Where you work/live
  - Name, social security number, phone number, DoB
  - Who you talk to

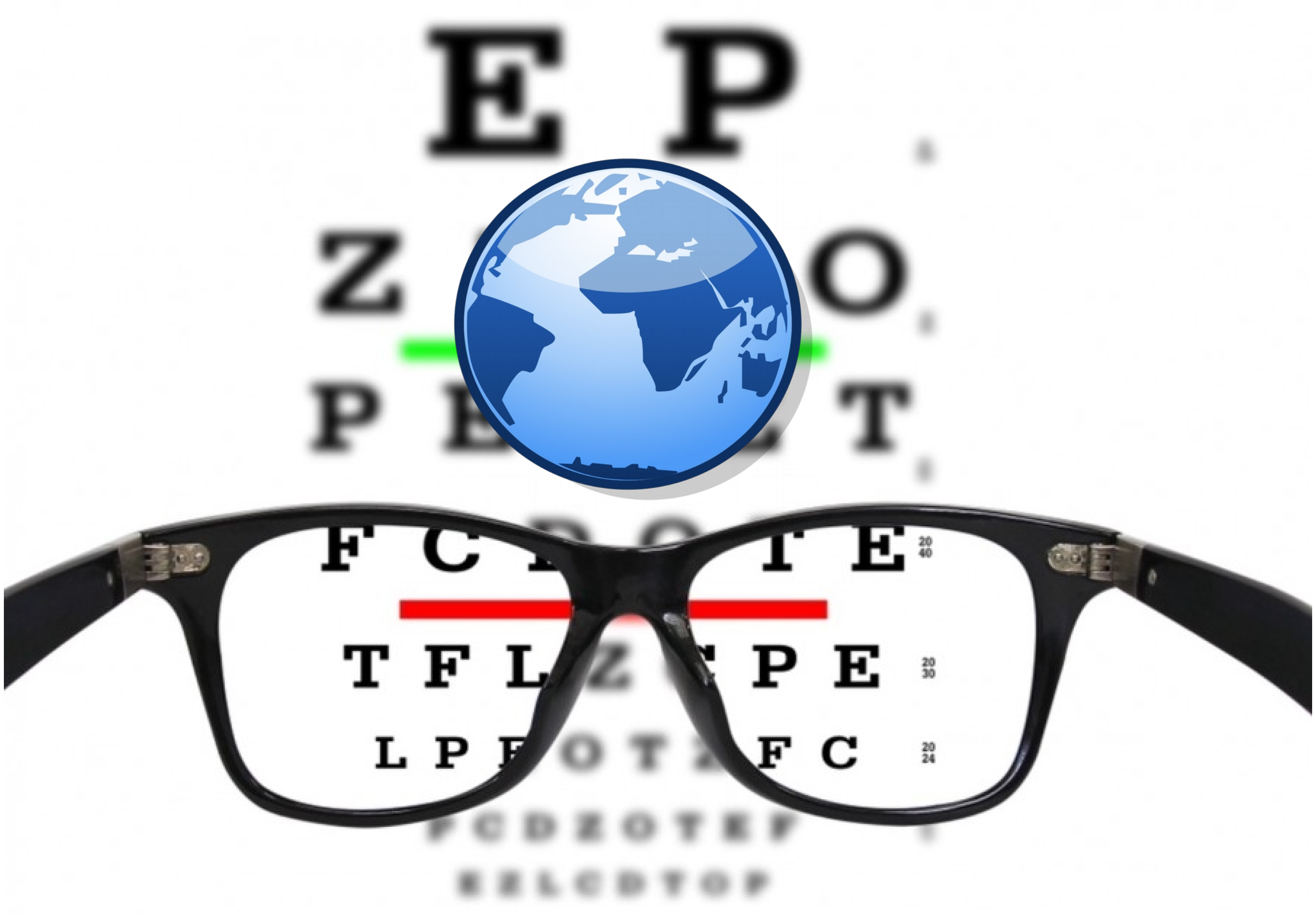
What does Privacy mean to you?

- Personal
  - What you buy
  - What you do
  - Where you work/live
  - Name, social security number, phone number, DoB
  - Who you talk to

- Web
  - What you buy
  - What you do
  - Where you are
  - Computer and browser information
  - Who you communicate with

Privacy in Hindsight

- Webcam/Babycam hack stories
- Target predicting girl was pregnant (2012)
- OPM, Equifax, Target, Marriott, etc.
- Advertisement


E P
Z O
P T
F C T E
T F L P E
L P F C
20
40
20
30
20
24

Personally Identifiable Information (PII)

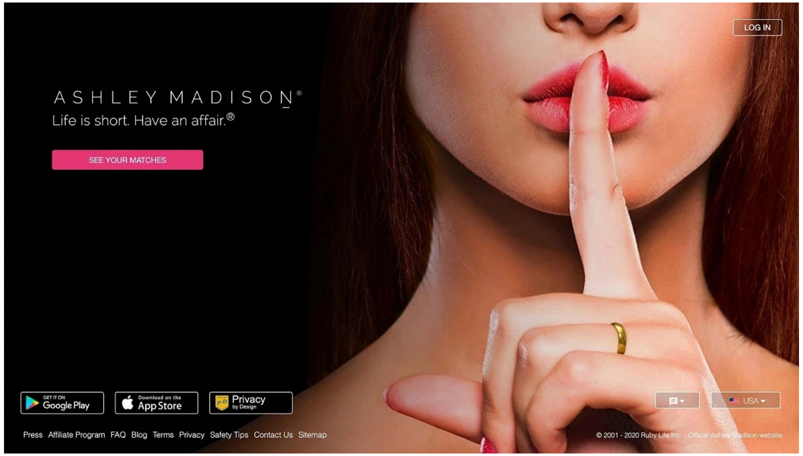
- Name
- Address
- Zip code
- Gender
- Race
- Date of birth
- Web cookie

What is Privacy?

- Not necessarily just your name
- Can infer type of person you are based on what you do

FCB

✝



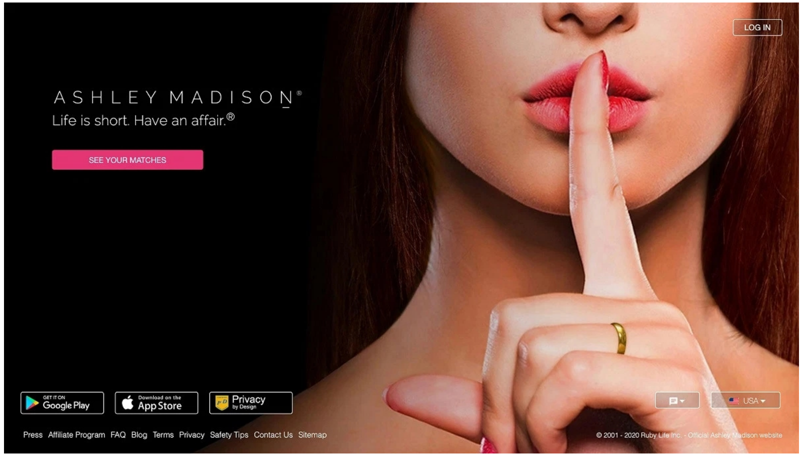
LOG IN
ASHLEY MADISON®
Life is short. Have an affair.®
SEE YOUR MATCHES
GET IT ON Google Play
Download on the App Store
Privacy by Design
USA
Press Affiliate Program FAQ Blog Terms Privacy Safety Tips Contact Us Sitemap

© 2001 - 2020 Ruby Life Inc. - Official Ashley Madison website

Grindr

What is Privacy?

- Not necessarily just your name
- Can infer type of person you are based on what you do
- Can link what you do
  - E.g. works at a university and likes sports

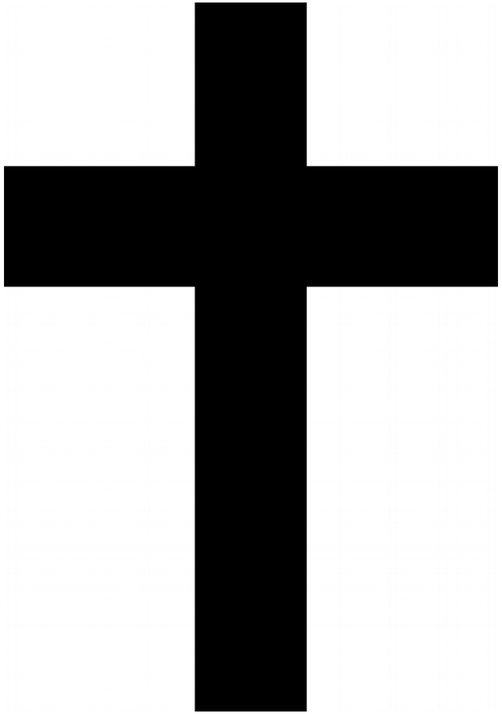


ASHLEY MADISON®

Life is short. Have an affair.®

LOG IN
SEE YOUR MATCHES
GET IT ON Google Play
Download on the App Store
Privacy by Design
USA
Press Affiliate Program FAQ Blog Terms Privacy Safety Tips Contact Us Sitemap

© 2001 - 2020 Ruby Life Inc. - Official Ashley Madison website



Web Privacy

ADVERTISEMENT

Pictures from ACLU.org and thejournal.com

Why?

- Over $100 billion in 2018 [CNBC]
- Censorship
- Collect data for use in the future

So what? Is that a bad thing?

- I got nothing to hide
- I trust the government
- It’s “just” advertisements

~~So what? Is that a bad thing?~~

- ~~I have got nothing to hide~~
- ~~I trust the government~~
- ~~It’s “just” advertisements~~

How to?

- IP address
- Web cookie

How to?

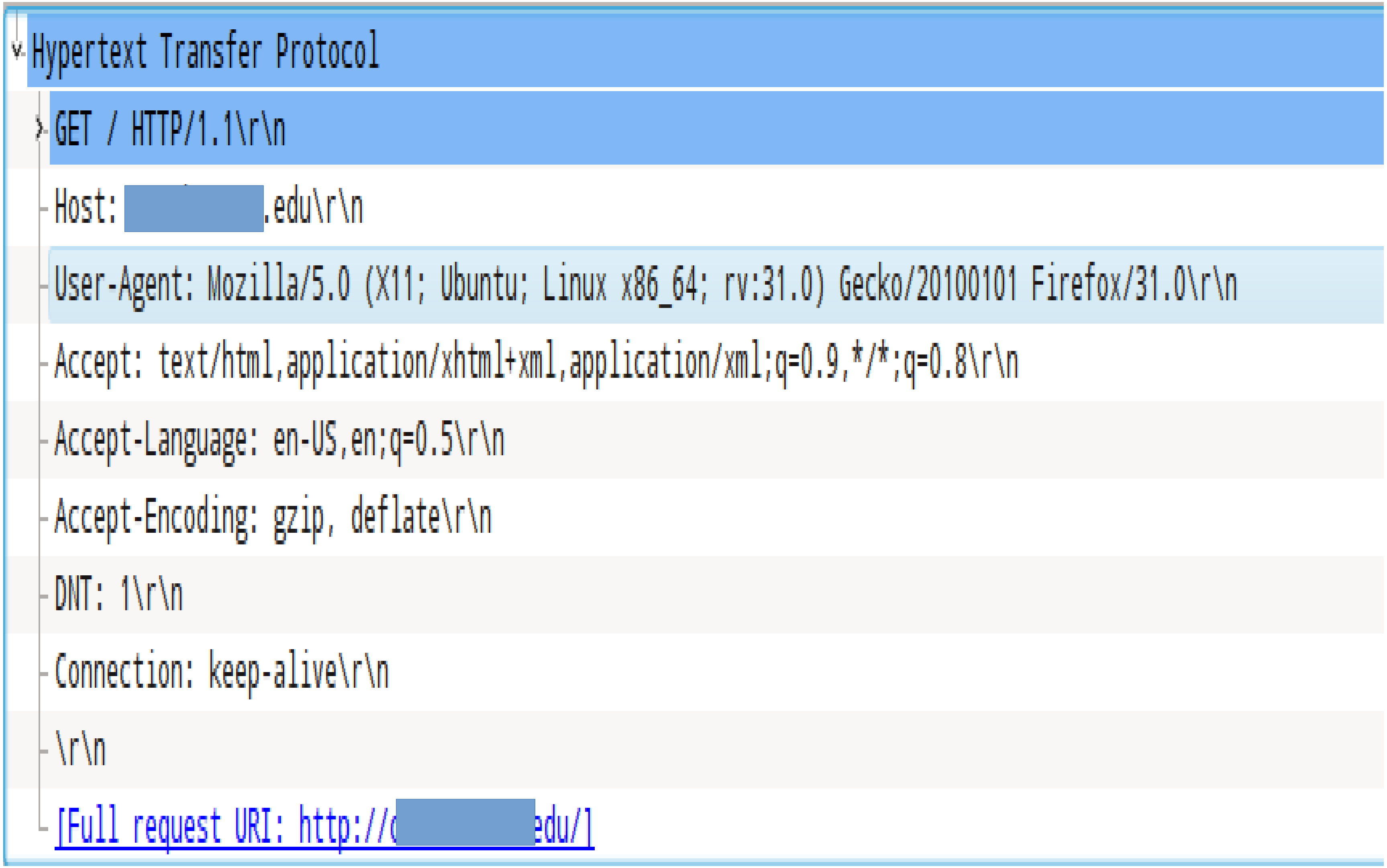
- IP address
- Web cookie

- DHCP or change location
- Delete cookies

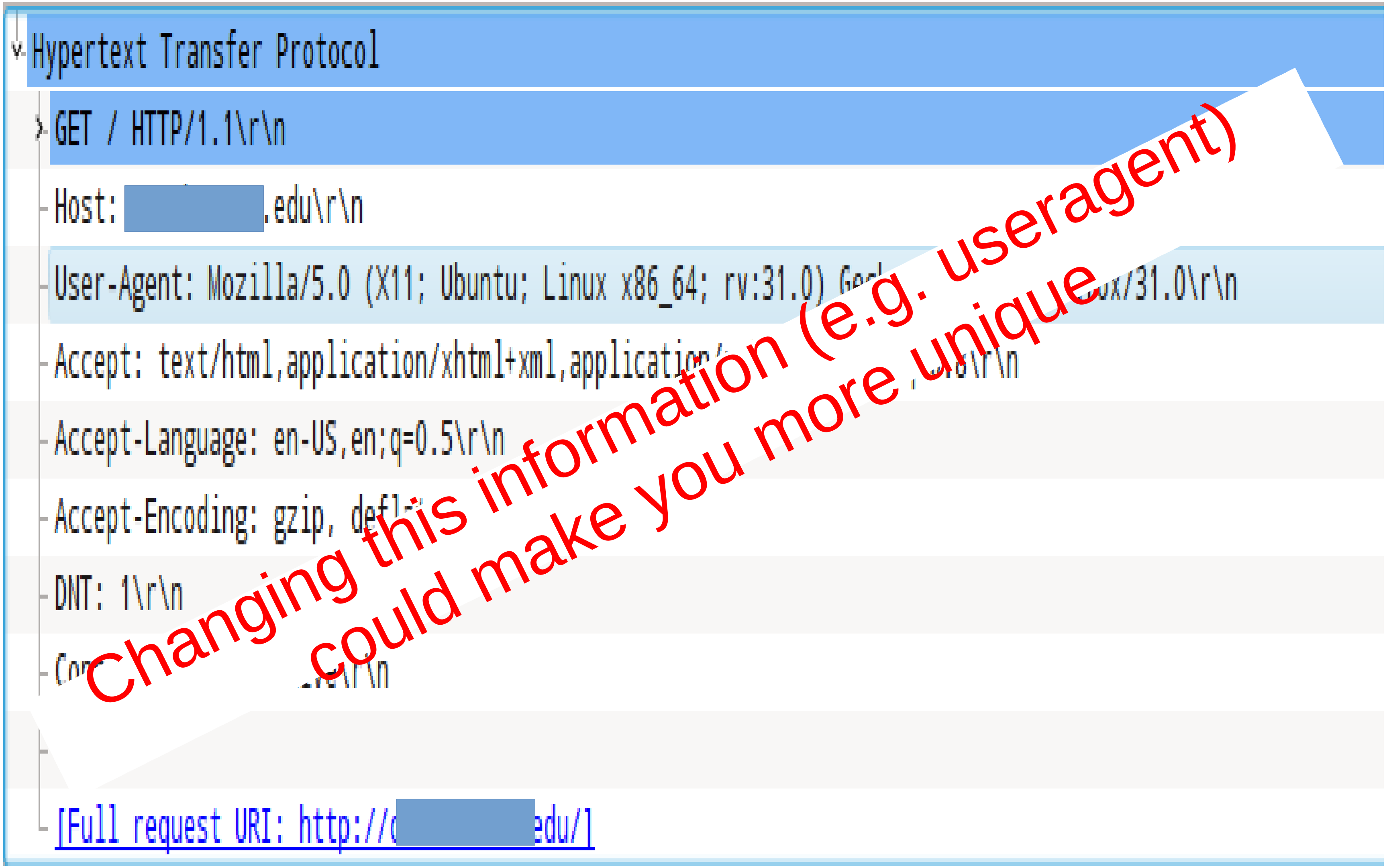
How to?

- IP address
- Web cookie
- Evercookie
  - Restores cookie using flash storage, local storage, session storage, etc.

- DHCP or change location
- Delete cookies



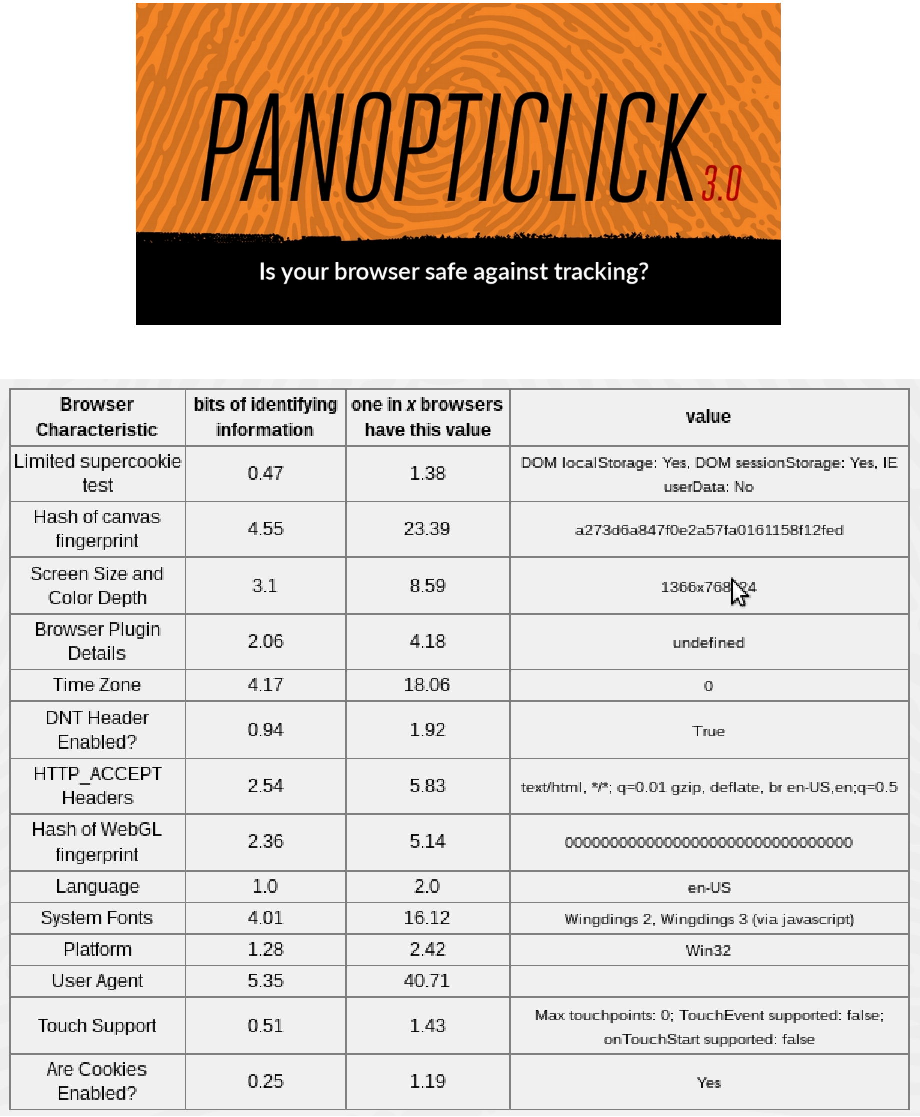
```
Hypertext Transfer Protocol
  GET / HTTP/1.1\r\n
  Host: [redacted].edu\r\n
  User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0\r\n
  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
  Accept-Language: en-US,en;q=0.5\r\n
  Accept-Encoding: gzip, deflate\r\n
  DNT: 1\r\n
  Connection: keep-alive\r\n
  \r\n
  [Full request URI: http://[redacted]edu/]
```



```
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: [redacted].edu\r\n
    User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:31.0) Gec   ox/31.0\r\n
    Accept: text/html,application/xhtml+xml,application/   ,   8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, defl
    DNT: 1\r\n
    Con   e\r\n

    [Full request URI: http://[redacted]edu/]
```

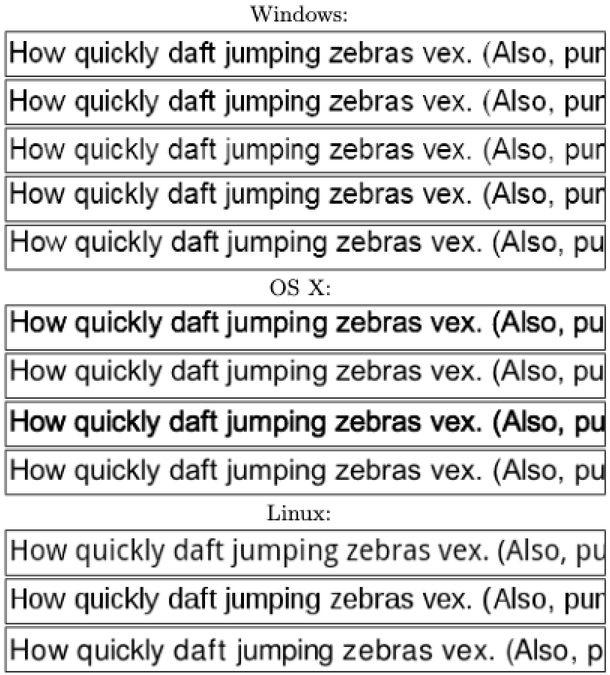
Changing this information (e.g. useragent) could make you more unique



PANOPTICLICK 3.0

Is your browser safe against tracking?

Browser Characteristic	bits of identifying information	one in *x* browsers have this value	value
Limited supercookie test	0.47	1.38	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	4.55	23.39	a273d6a847f0e2a57fa0161158f12fed
Screen Size and Color Depth	3.1	8.59	1366x768x24
Browser Plugin Details	2.06	4.18	undefined
Time Zone	4.17	18.06	0
DNT Header Enabled?	0.94	1.92	True
HTTP_ACCEPT Headers	2.54	5.83	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	2.36	5.14	00000000000000000000000000000000
Language	1.0	2.0	en-US
System Fonts	4.01	16.12	Wingdings 2, Wingdings 3 (via javascript)
Platform	1.28	2.42	Win32
User Agent	5.35	40.71	
Touch Support	0.51	1.43	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.25	1.19	Yes



Windows:

How quickly daft jumping zebras vex. (Also, pur

How quickly daft jumping zebras vex. (Also, pur

How quickly daft jumping zebras vex. (Also, pur

How quickly daft jumping zebras vex. (Also, pur

How quickly daft jumping zebras vex. (Also, pu

OS X:

How quickly daft jumping zebras vex. (Also, pu

How quickly daft jumping zebras vex. (Also, pu

How quickly daft jumping zebras vex. (Also, pu

How quickly daft jumping zebras vex. (Also, pu

Linux:

How quickly daft jumping zebras vex. (Also, pu

How quickly daft jumping zebras vex. (Also, pur

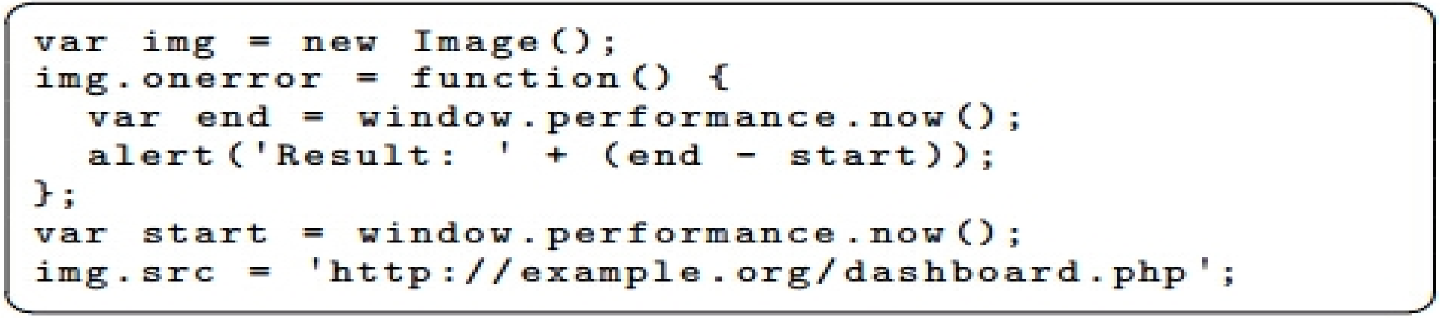
How quickly daft jumping zebras vex. (Also, p

Figure 6: 13 ways to render 20px Arial

K. Mowery and H. Shacham. Pixel Perfect: Fingerprinting Canvas in HTML5. IEEE W2SP 2012.

Tracking using Latency

- Javascript code on attacker.com (maybe served as an ad to victim.com)



```
var img = new Image();
img.onerror = function() {
  var end = window.performance.now();
  alert('Result: ' + (end - start));
};
var start = window.performance.now();
img.src = 'http://example.org/dashboard.php';
```

- Timing attack to see if user visited example.org and is logged into example.org
  - In cache or not

T. Van Goethem, W. Joosen, and N. Nikiforakis. The Clock is Still Ticking: Timing Attacks in the Modern Web. ACM CCS 2015

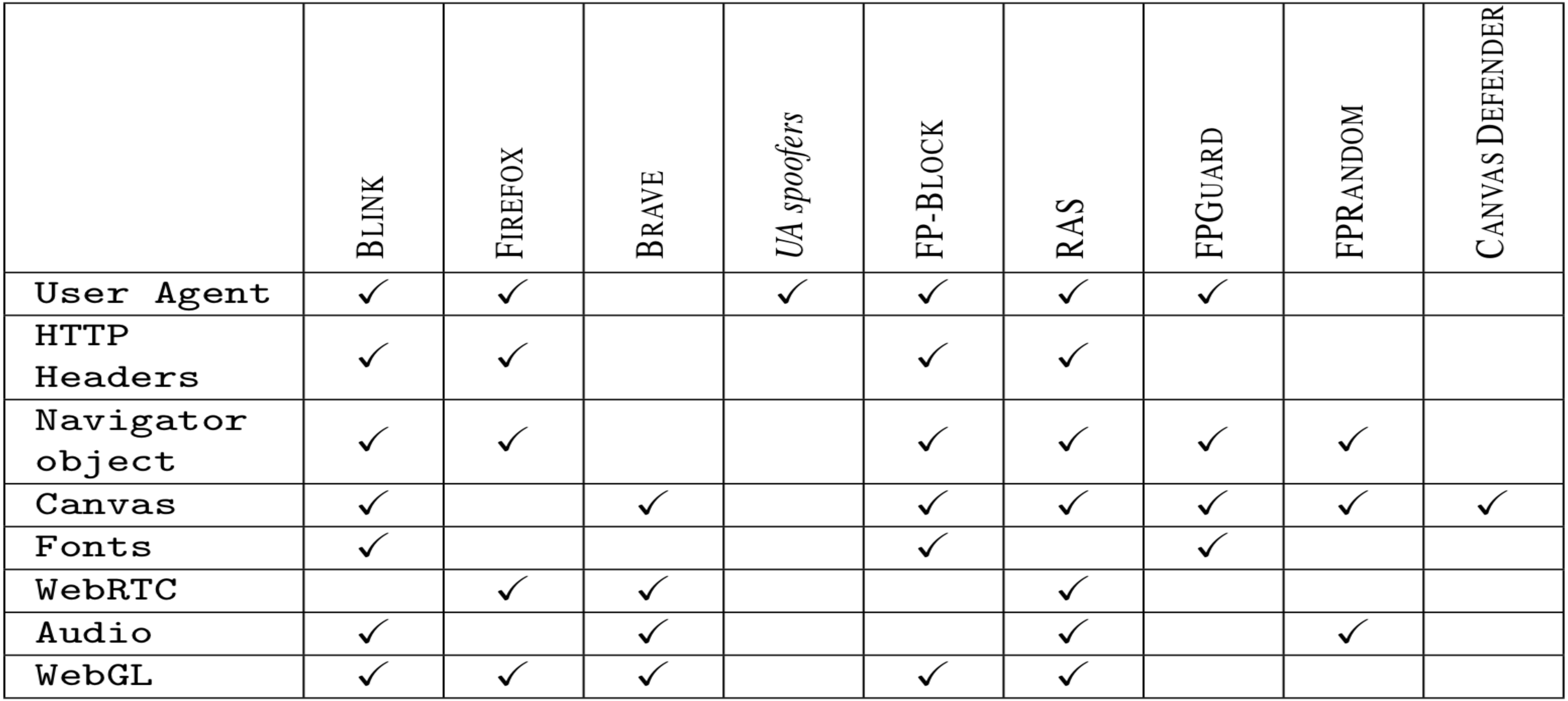
Others

- List of webbrowser extensions makes you unique (Xhound)
- Accessibility features
- Mobile tracking
- Cross-device tracking
- ...

What can you do?

- Do Not Track
- Install tracking-blocker tools
- Use a private browser

Table 1: Overview of fingerprinting countermeasures



	Blink	Firefox	Brave	*UA spoofers*	FP-Block	RAS	FPGuard	FPRandom	Canvas Defender
User Agent	✓	✓		✓	✓	✓	✓		
HTTP Headers	✓	✓			✓	✓			
Navigator object	✓	✓			✓	✓	✓	✓	
Canvas	✓		✓		✓	✓	✓	✓	✓
Fonts	✓				✓		✓		
WebRTC		✓	✓			✓			
Audio	✓		✓			✓		✓	
WebGL	✓	✓	✓		✓	✓			

A. Vastel, P. Laperdrix, W. Rudametkin, and R. Rouvoy. FP-scanner: the privacy implications of browser fingerprint inconsistencies. USENIX Security 2018.

“Legitimate” Uses

- Banks to detect fraudulent logins
- Games to detect cheaters

How Prevalent?

- Long tail
- Becoming more common in most popular websites
- Some sites use different tracking tools

Browser Fingerprinting

- Here to stay

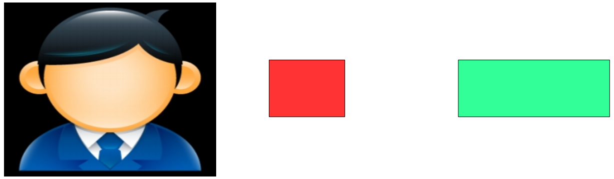
- You **SHOULD** be concerned about your privacy
- What if the tracking dataset gets leaked?

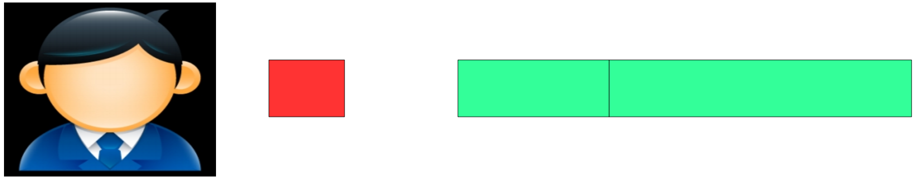
Network Traffic Analysis

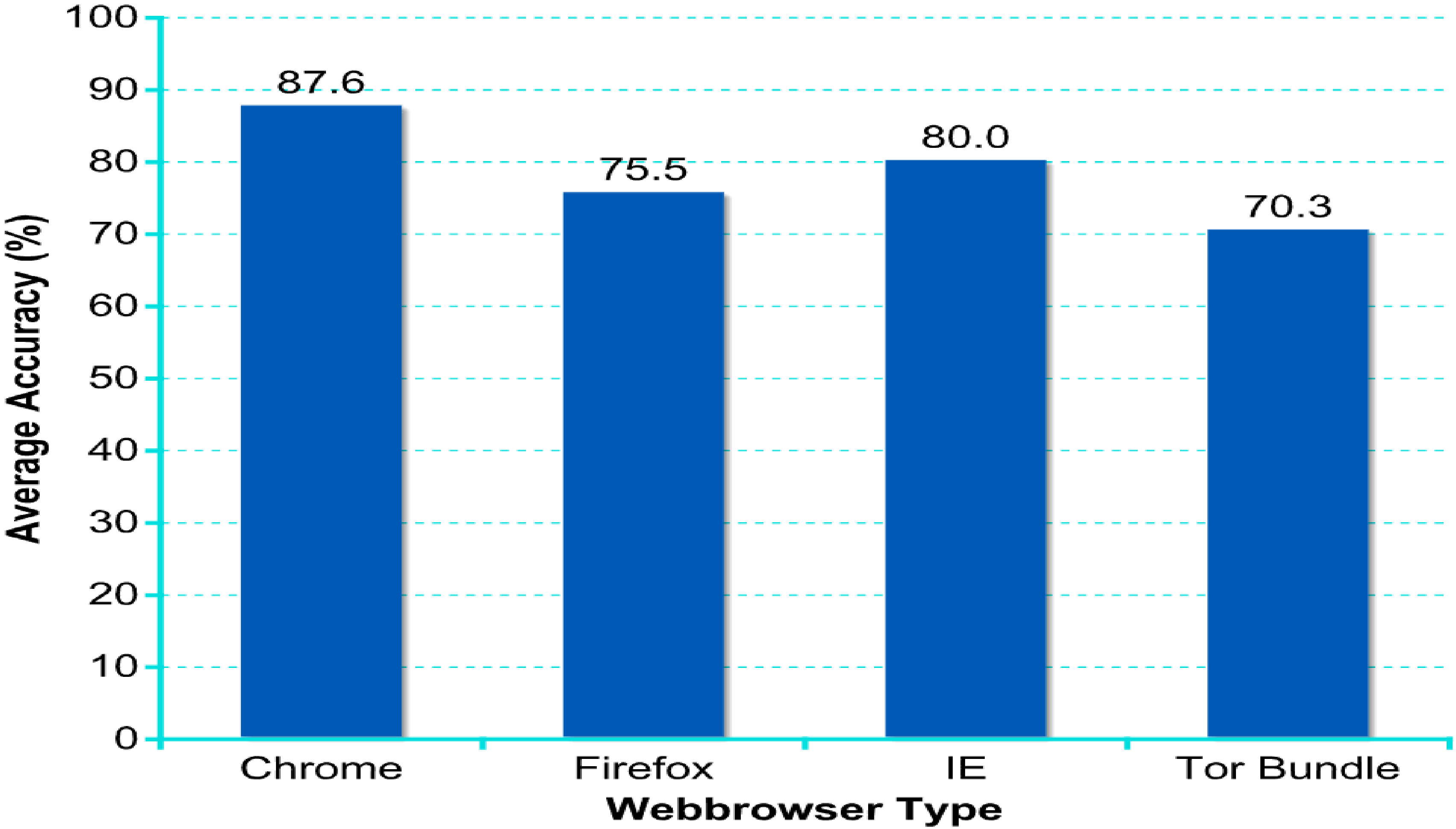
- Assume that all communications are encrypted
- Assume that the eavesdropper is not the server nor the client
- What do you see?

Metadata

- Number of messages
- Size of each message
- Direction of the message

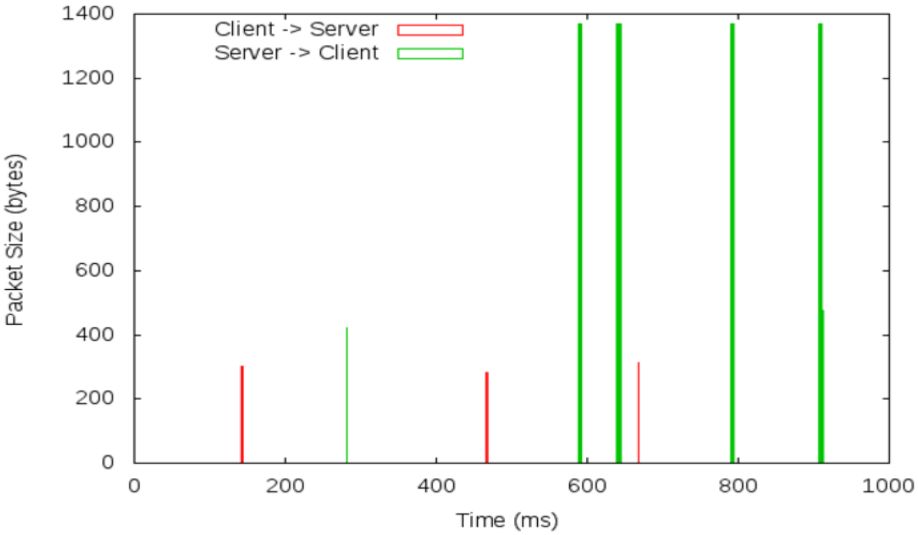


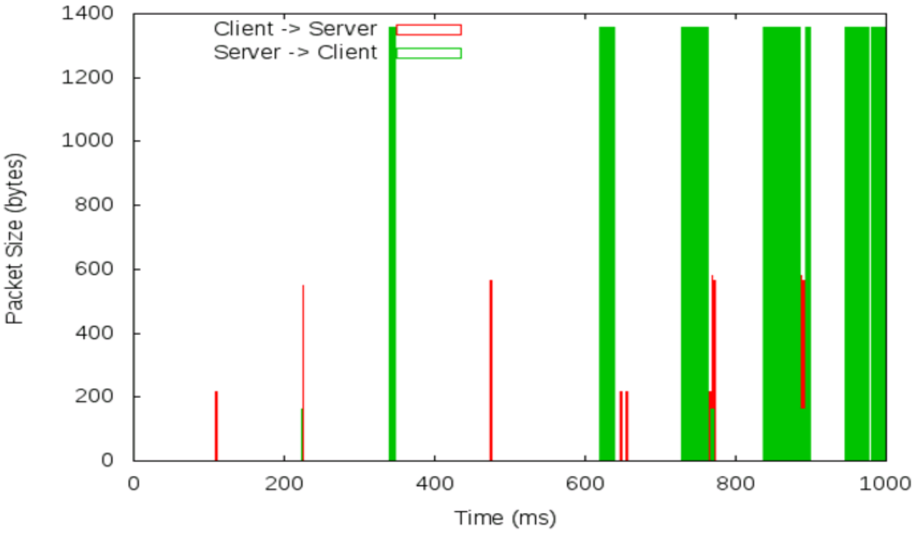


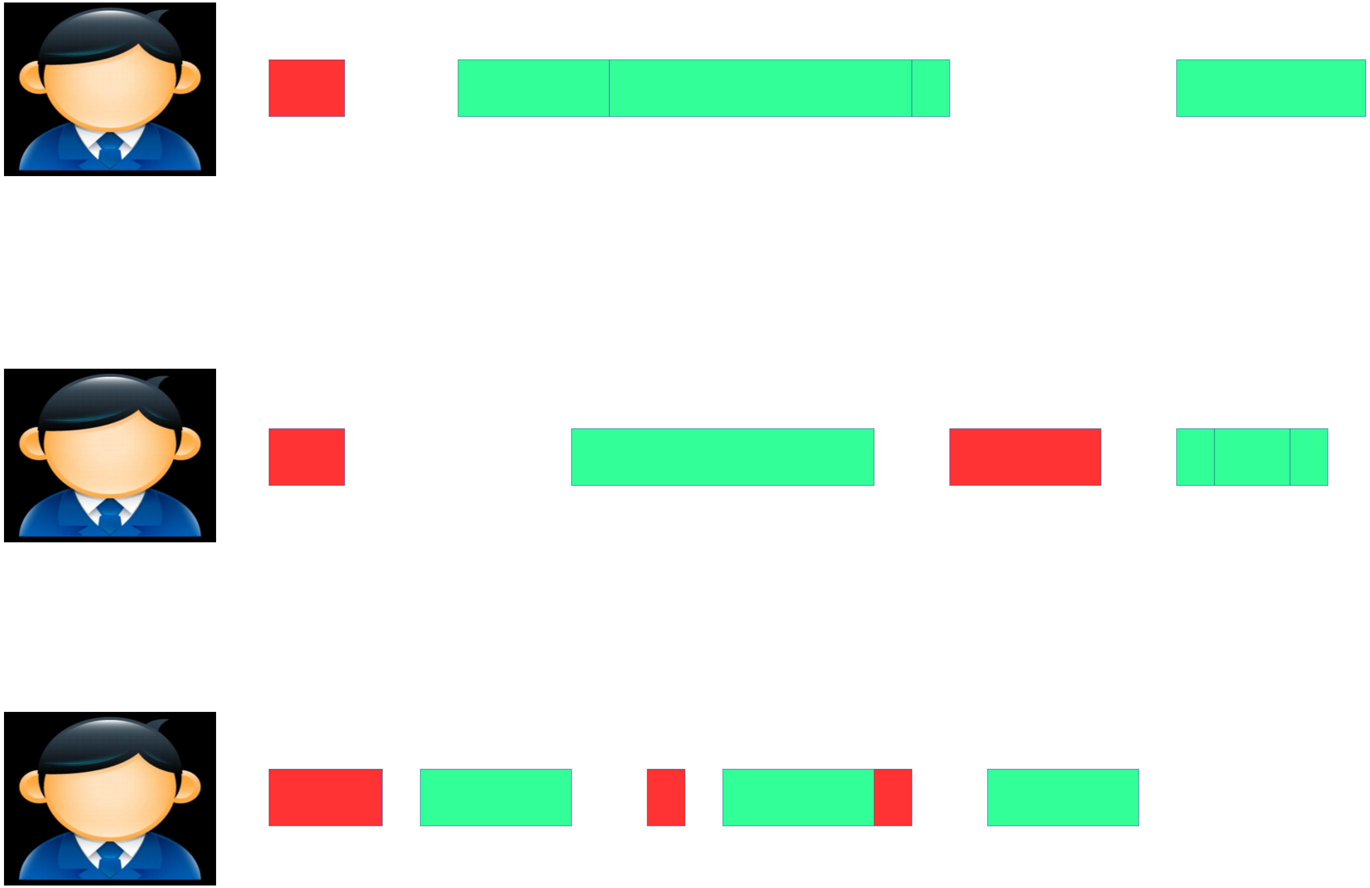


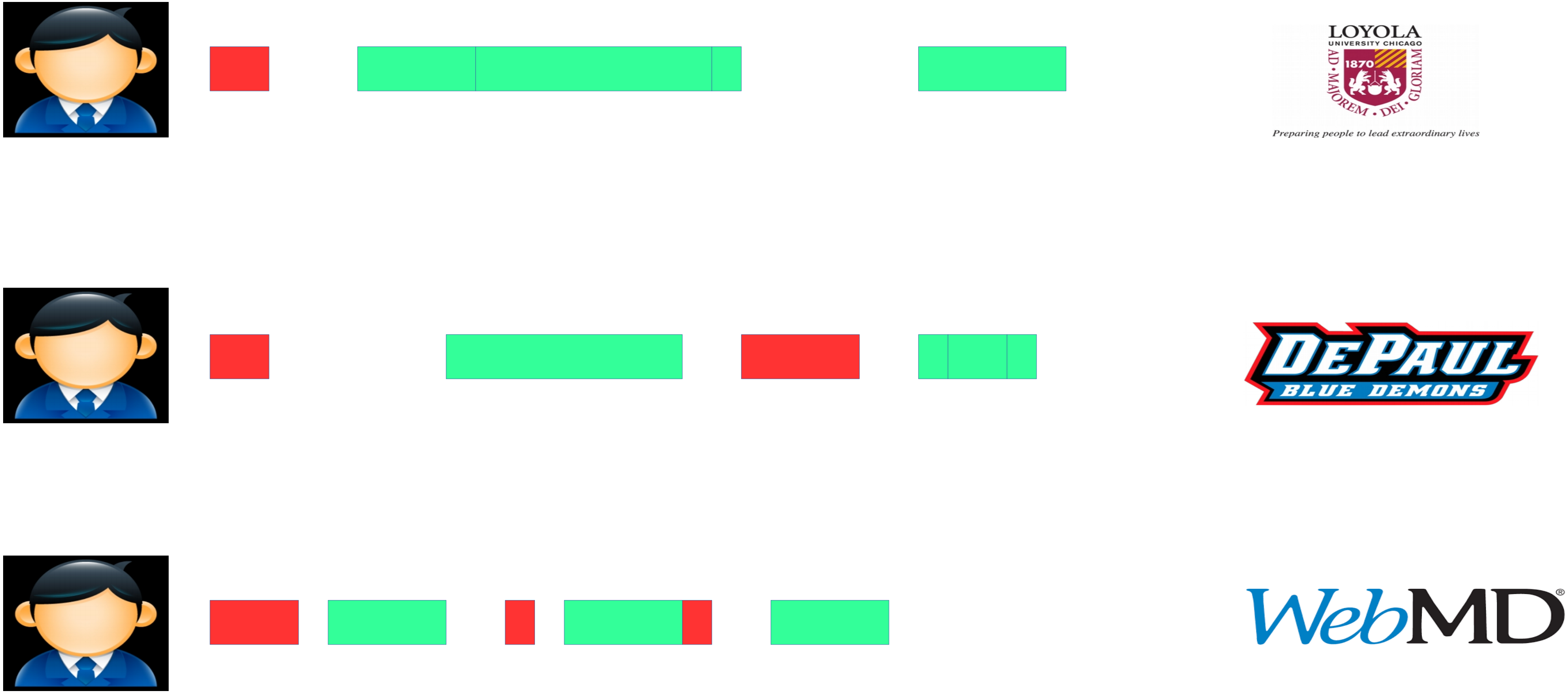
J. Yu and E. Chan-Tin. Identifying Webbrowsers in Encrypted Communications. ACM WPES 2014.

Website Fingerprinting








LOYOLA
UNIVERSITY CHICAGO
1870
AD MAJOREM DEI GLORIAM
Preparing people to lead extraordinary lives
DEPAUL
BLUE DEMONS
WebMD®

Closed World

- 90+% accuracy
- Predicting the correct website out of possible 1,000 websites

Open World

- 90+% accuracy
- High TPR, low FPR
- ~100 “monitored, sensitive” websites
  - E.g. facebook, wikipedia, attacker.com, etc
- ~1 million unmonitored websites
- Predicting whether network traffic is part of the monitored list or not
  - Binary classification

Future Privacy Impacts

- Track any citizen
- Predict who you are
  - Eliminate password authentication

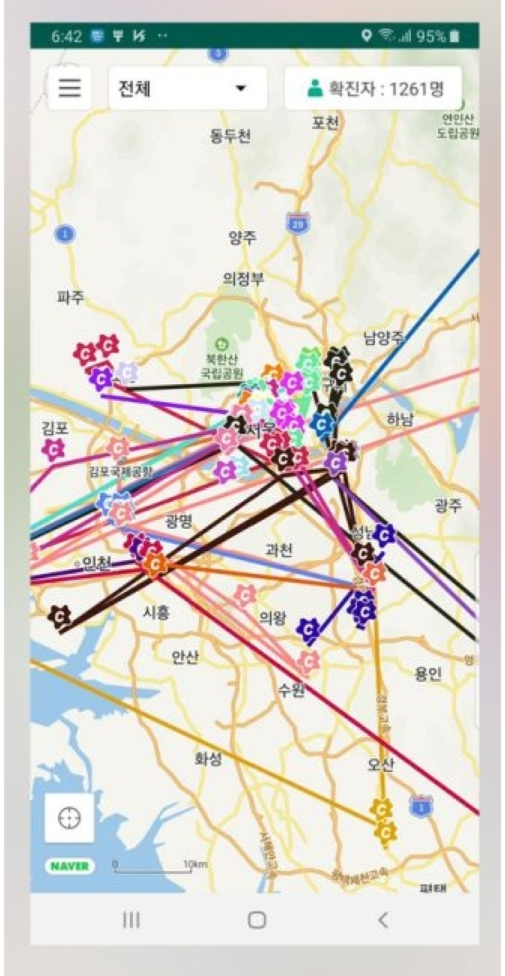
New Privacy laws

- GDPR (May 2018)
- California Consumer Privacy Act (Jan. 2020)

Societal/Human Impacts

- Find and track bad actors
- Fraud prevention

- Domestic partner surveillance
- Political/Religious/ Ethnic/Personal surveillance



전체

확진자 : 1261명

Picture from CNN.com

Arms Race

- Prevention vs Detection
- Tradeoff between privacy and “security”/“safety”

Are you sure you have nothing to hide?

Are you sure you have nothing to hide?

- Make your choice of tech
- Regulations
- Be careful what you “wish for”

Collaborators

- Yanmin Gong
- Jinoh Kim
- Shelia Kennison
- Jiangmin Yu
- Tao Chen
- Weiqi Cui
- Anthony Sierra
- Christian Fields
- Julianna Chen
- Spencer Johnston
- John Mikos
- Daisy Reyes

Acknowledgments

- This material is based upon work supported by the NSF under Grant No. IIS-1659645 and DGE-1919004
- Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation

Thank You!

chantin@cs.luc.edu
Post on the Slack channel