# The Web's Sixth Sense:

## A Study of Scripts Accessing Smartphone Sensors

**Anupam Das**

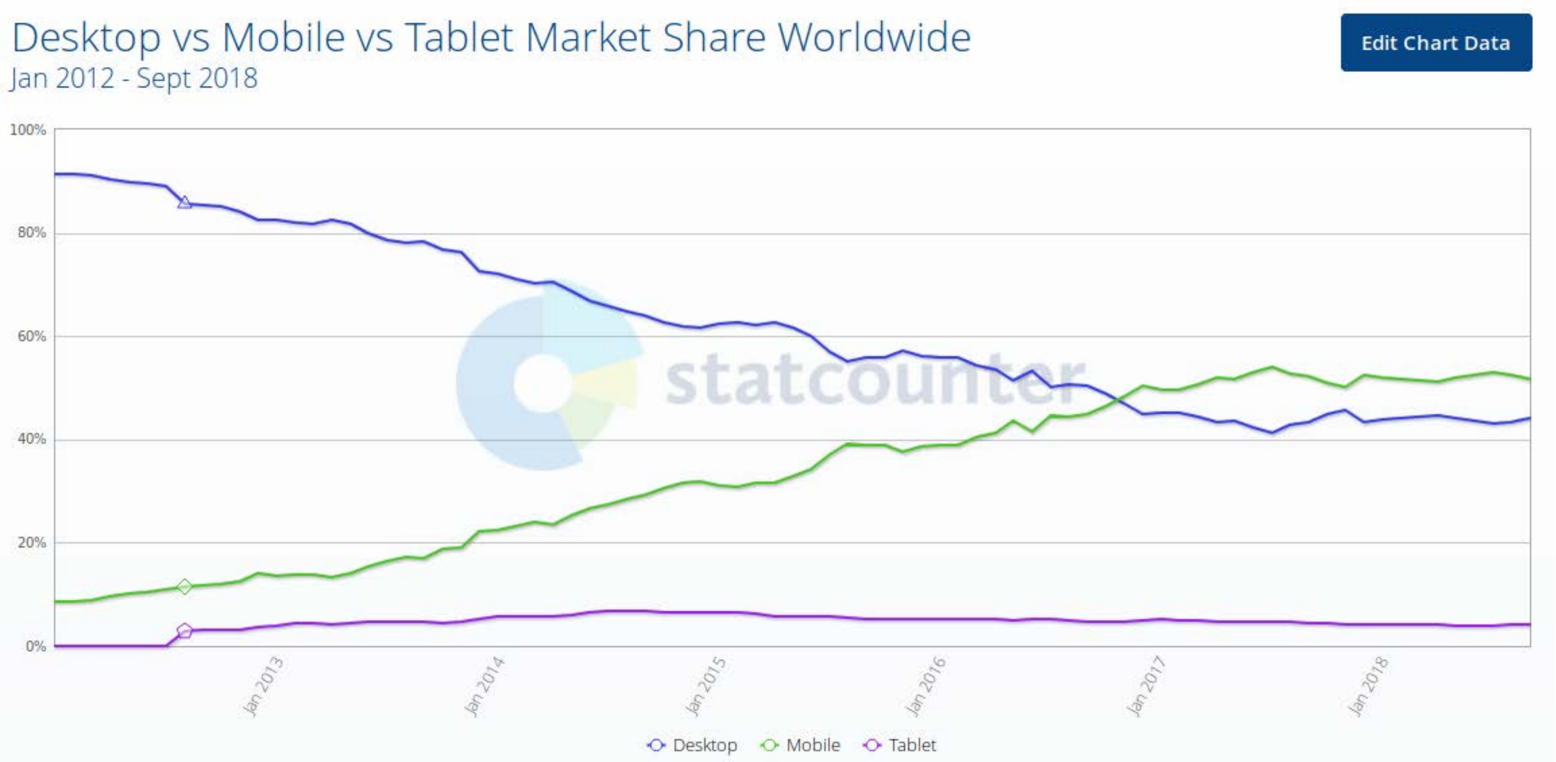
**North Carolina State University**

*Joint work with* Günes Acar, *Nikita Borisov and Amogh Pradeep*

https://sensor-js.xyz

PRIVACYCON

# Web Browsing is Increasingly Mobile

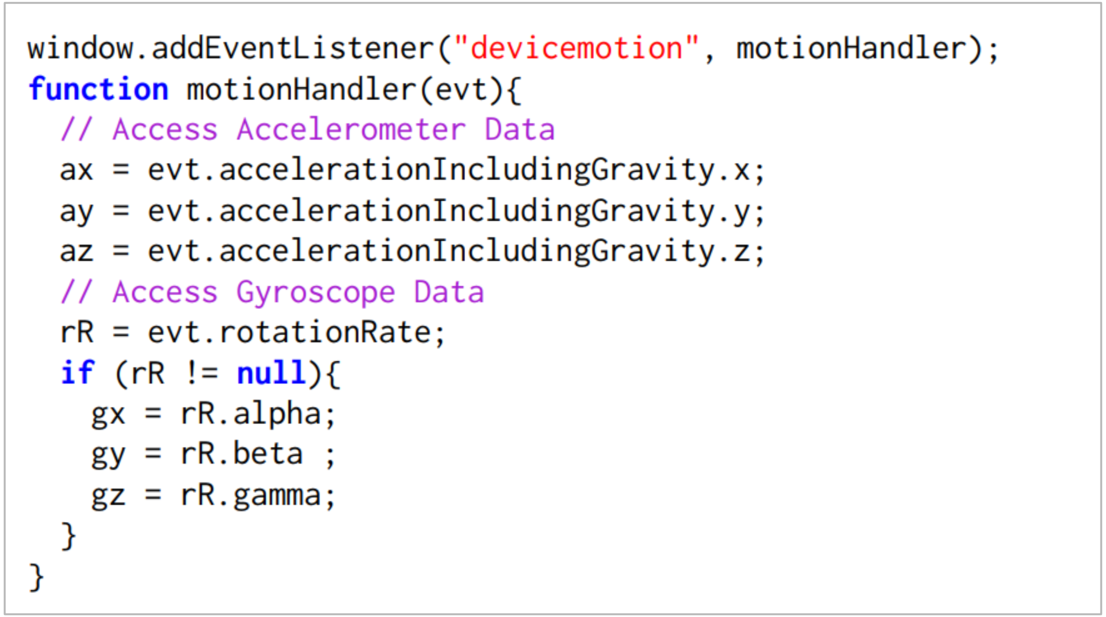


Desktop vs Mobile vs Tablet Market Share Worldwide

Jan 2012 - Sept 2018

# New Mobile Web APIs

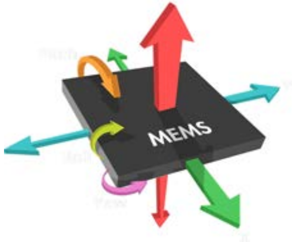
- Touch Events
- Vibration
- WebXR (VR/AR support)
- **Sensors**
  - **Orientation**
  - **Motion**
  - **Ambient Light**
  - **Proximity**

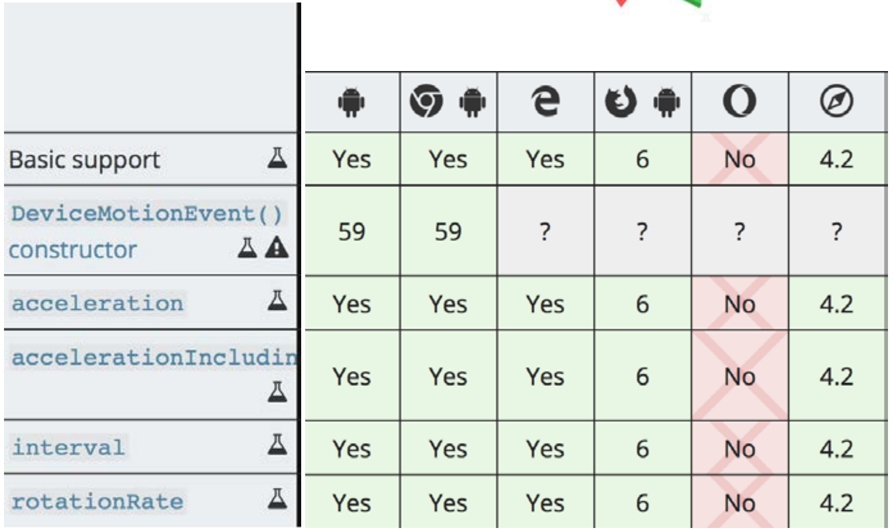


```
window.addEventListener("devicemotion", motionHandler);
function motionHandler(evt){
  // Access Accelerometer Data
  ax = evt.accelerationIncludingGravity.x;
  ay = evt.accelerationIncludingGravity.y;
  az = evt.accelerationIncludingGravity.z;
  // Access Gyroscope Data
  rR = evt.rotationRate;
  if (rR != null){
    gx = rR.alpha;
    gy = rR.beta ;
    gz = rR.gamma;
  }
}
```

# Sensor APIs

- Orientation
  - Orientation about the X, Y, Z axis (°)
- Motion
  - Accelerometer (m/s$^2$)
  - Accelerometer w/o gravity (m/s$^2$)
  - Gyroscope (°/s)
- Ambient light
  - Light sensor (lux)
- Proximity
  - Proximity sensor (cm)



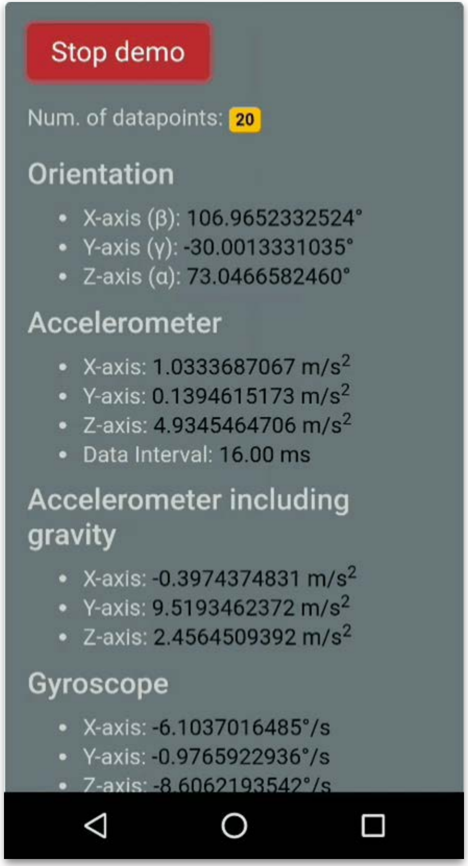


| | | | | | | |
|---|---|---|---|---|---|---|
| Basic support ⚗ | Yes | Yes | Yes | 6 | No | 4.2 |
| DeviceMotionEvent() constructor ⚗ ⚠ | 59 | 59 | ? | ? | ? | ? |
| acceleration ⚗ | Yes | Yes | Yes | 6 | No | 4.2 |
| accelerationIncludin ⚗ | Yes | Yes | Yes | 6 | No | 4.2 |
| interval ⚗ | Yes | Yes | Yes | 6 | No | 4.2 |
| rotationRate ⚗ | Yes | Yes | Yes | 6 | No | 4.2 |

# No Permissions for Sensor APIs

- Available to any web page ***without* permission** check

- Try it! https://**sensor-js.xyz/demo**



Stop demo

Num. of datapoints: 20

Orientation

- X-axis (β): 106.9652332524°
- Y-axis (γ): -30.0013331035°
- Z-axis (α): 73.0466582460°

Accelerometer

- X-axis: 1.0333687067 m/s$^2$
- Y-axis: 0.1394615173 m/s$^2$
- Z-axis: 4.9345464706 m/s$^2$
- Data Interval: 16.00 ms

Accelerometer including gravity

- X-axis: -0.3974374831 m/s$^2$
- Y-axis: 9.5193462372 m/s$^2$
- Z-axis: 2.4564509392 m/s$^2$

Gyroscope

- X-axis: -6.1037016485°/s
- Y-axis: -0.9765922936°/s
- Z-axis: -8.6062193542°/s

# API Exposure Risks

- **Keylogging**
  - PIN recovery[1], keystroke recovery from nearby keyboard[2]
- **Surreptitious recording**[3]
  - Accelerometer and Gyroscope are low-fi microphones!
- **Surreptitious geolocation**
  - Motion changes (e.g., subway)[4]
  - Ambient light changes
- **Fingerprinting**
  - Stateless tracking[5]
- **Biometrics**
  - e.g., gait

[1] Mehrnezhad et al. "*Touchsignatures: identification of user touch actions and PINs based on mobile sensor data via JavaScript*." JISA, 2016.

[2] Marquardt et al. "*(sp) iPhone: decoding vibrations from nearby keyboards using mobile phone accelerometers*." CCS, 2011.

[3] Michalevsky et al. "*Gyrophone: Recognizing Speech from Gyroscope Signals*." USENIX Security, 2014.

[4] Watanabe et al. "*RouteDetector: Sensor-based Positioning System That Exploits Spatio-Temporal Regularity of Human Mobility*." WOOT. 2015.

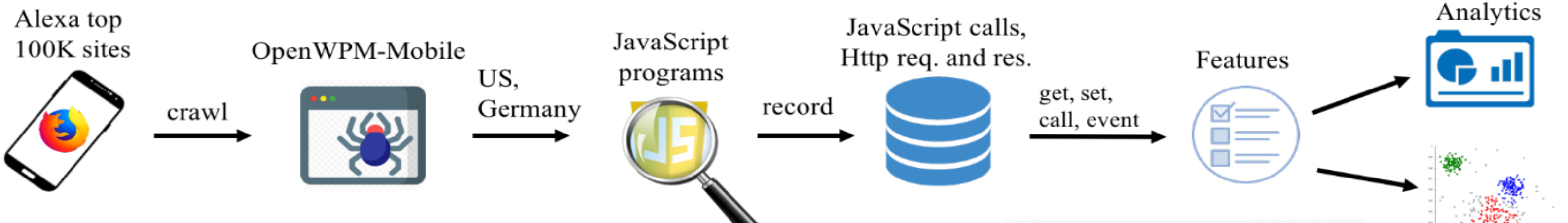
[5] Das et al. "*Tracking Mobile Web Users Through Motion Sensors: Attacks and Defenses*." NDSS. 2016.

# In This Talk

We look at -

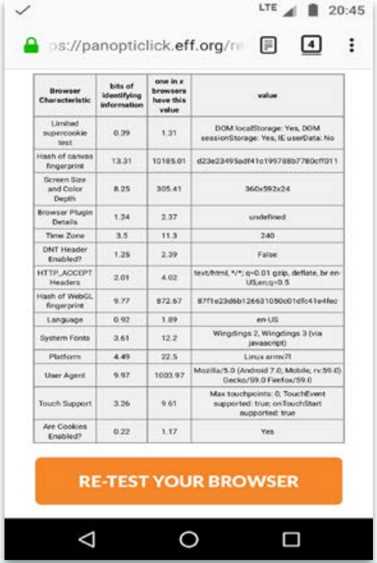
- which websites and scripts use sensors?
- ...for what purposes?
- what can be done to mitigate the risks?

# Data Collection and Analysis



## Crawler: OpenWPM-mobile

- Based on OpenWPM framework
- Develop a *Mobile* version
  - Emulate mobile environment: user agent, screen size, extensions, fonts, etc.
  - Capture `addEventListener` calls
  - Generate sensor APIs events and return realistic sensor data stream



| Browser Characteristic | bits of identifying information | one in x browsers have this value | value |
|---|---|---|---|
| Limited supercookie test | 0.39 | 1.31 | DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No |
| Hash of canvas fingerprint | 13.31 | 10185.01 | d23e23495adf41c199788b7780cff011 |
| Screen Size and Color Depth | 8.25 | 305.41 | 360x592x24 |
| Browser Plugin Details | 1.24 | 2.37 | undefined |
| Time Zone | 3.5 | 11.3 | 240 |
| DNT Header Enabled? | 1.25 | 2.39 | False |
| HTTP_ACCEPT Headers | 2.01 | 4.02 | text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5 |
| Hash of WebGL fingerprint | 9.77 | 872.67 | 87f1e23d6b126631050c01dfc41e4fec |
| Language | 0.92 | 1.89 | en-US |
| System Fonts | 3.61 | 12.2 | Wingdings 2, Wingdings 3 (via javascript) |
| Platform | 4.49 | 22.5 | Linux armv7l |
| User Agent | 9.97 | 1003.97 | Mozilla/5.0 (Android 7.0; Mobile; rv:59.0) Gecko/59.0 Firefox/59.0 |
| Touch Support | 3.26 | 9.61 | Max touchpoints: 0; TouchEvent supported: true; onTouchStart supported: true |
| Are Cookies Enabled? | 0.22 | 1.17 | Yes |

# Sensor Access

| Sensor | # sites | # script domains |
|---|---|---|
| Motion | 2653 | 384 |
| Orientation | 2036 | 420 |
| Proximity | 186 | 50 |
| Light | 181 | 35 |
| **Total** | **3695** | **603** |

***including...***

- *cnn.com*
- *taobao.com*
- *tmall.com*
- *cnet.com*
- *alibaba.com*
- *foxnews.com*
- *zillow.com*
- *wellsfargo.com*
- *reuters.com*
- *bloomberg.com*
- *groupon.com*
- *hotels.com*

# Who is using sensors?

| Sensor | Top 3 domains | # sites | Top rank |
|---|---|---|---|
| **Motion** | serving-sys.com | 815 | 67 |
| | adsco.re | 648 | 570 |
| | doubleverify.com | 517 | 187 |
| **Orientation** | adsco.re | 648 | 570 |
| | alicdn.com | 417 | 9 |
| | yieldmo.com | 83 | 100 |

# Exfiltration detection

- Trigger sensor events with easy-to-recognize values:

```
 42.1234 (fixed) + 0.00005468 (random)
            = 42.12345468
```

- Look for raw and base64 encoded values in the request URLs and payload

| Domain | Sen-sors | Enco-ding | # sites | Top site |
|---|---|---|---|---|
| b2c.com | AOPL | b64 | 53 | 498 |
| perimeterx.com | A | b64 | 45 | 247 |
| wayfair.com | A | b64 | 7 | 1136 |
| moatads.com | O | raw | 5 | 3616 |

∗ ‘A’: accelerometer, ‘G’: gyroscope, ‘O’: orientation, ‘P’: proximity, ‘L’: light

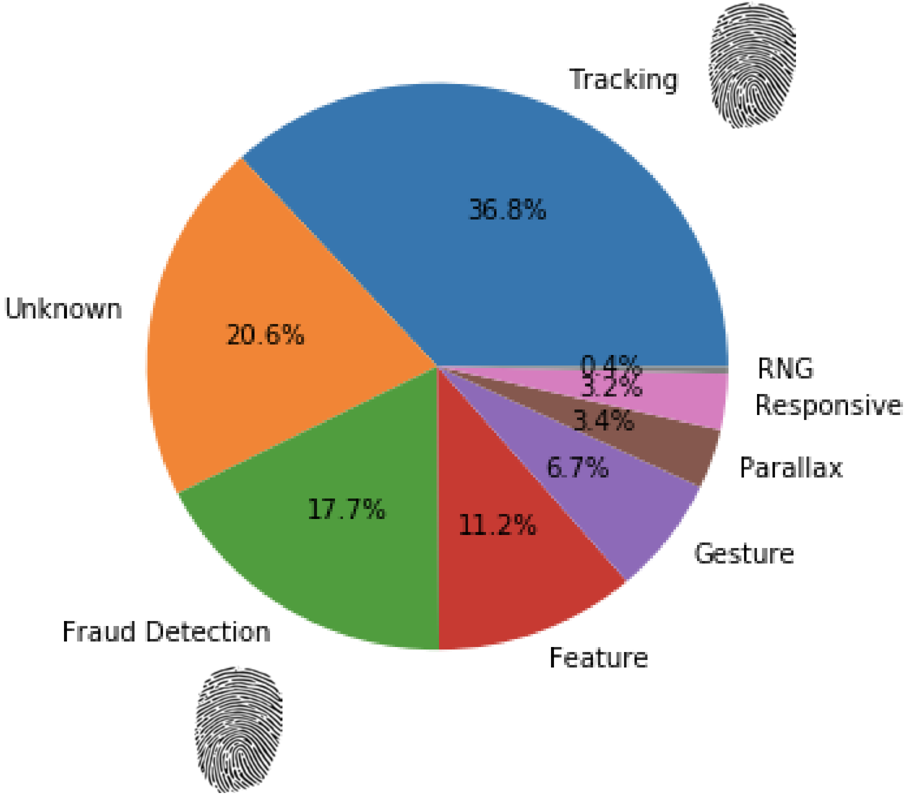
# Clustering to understand use cases

- Low-level features: JS API
    - `get_window.navigator.userAgent`
    - `set_window.document.cookie`
    - `call_HTMLCanvasElement.toDataURL`
    - `addEventListener_deviceMotion, ...`
- High-level features: fingerprinting
    - Canvas, Battery, AudioContext, `...`
- ~400 features per script

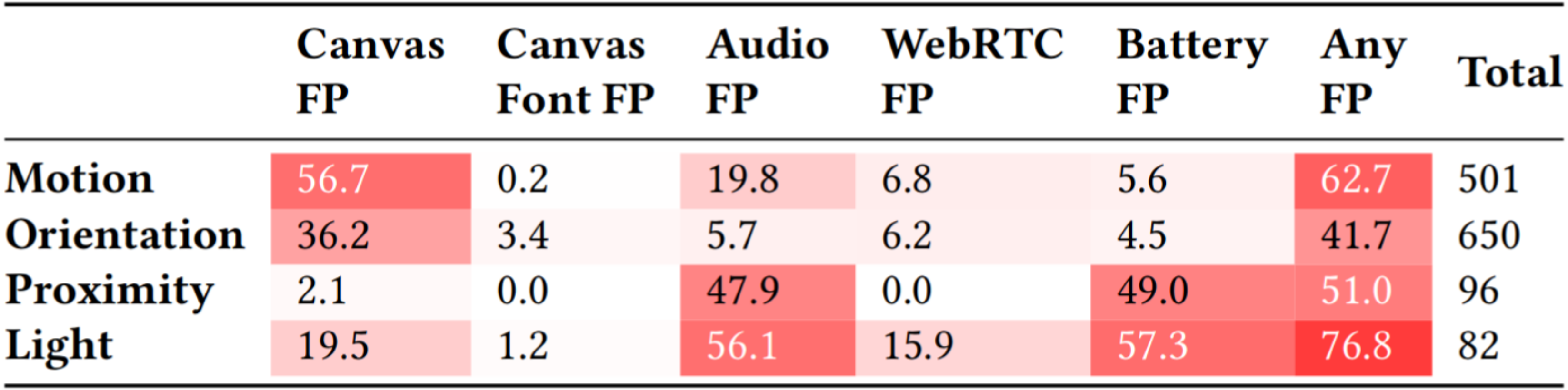
- Use DBScan for clustering
- Refinement techniques to reduce “noisy” cluster
- Use Moss to look at source code similarity
- Manual analysis of 3–5 scripts in each cluster

# Use Cases

- Tracking
  - Fingerprinting, audience recognition, session replay
- Fraud detection
  - Bot detection
- Feature detection
- Gesture control
- Parallax tilt scrolling
- Responsive design
- RNG



# Fingerprinting



| | Canvas FP | Canvas Font FP | Audio FP | WebRTC FP | Battery FP | Any FP | Total |
|---|---|---|---|---|---|---|---|
| **Motion** | 56.7 | 0.2 | 19.8 | 6.8 | 5.6 | 62.7 | 501 |
| **Orientation** | 36.2 | 3.4 | 5.7 | 6.2 | 4.5 | 41.7 | 650 |
| **Proximity** | 2.1 | 0.0 | 47.9 | 0.0 | 49.0 | 51.0 | 96 |
| **Light** | 19.5 | 1.2 | 56.1 | 15.9 | 57.3 | 76.8 | 82 |

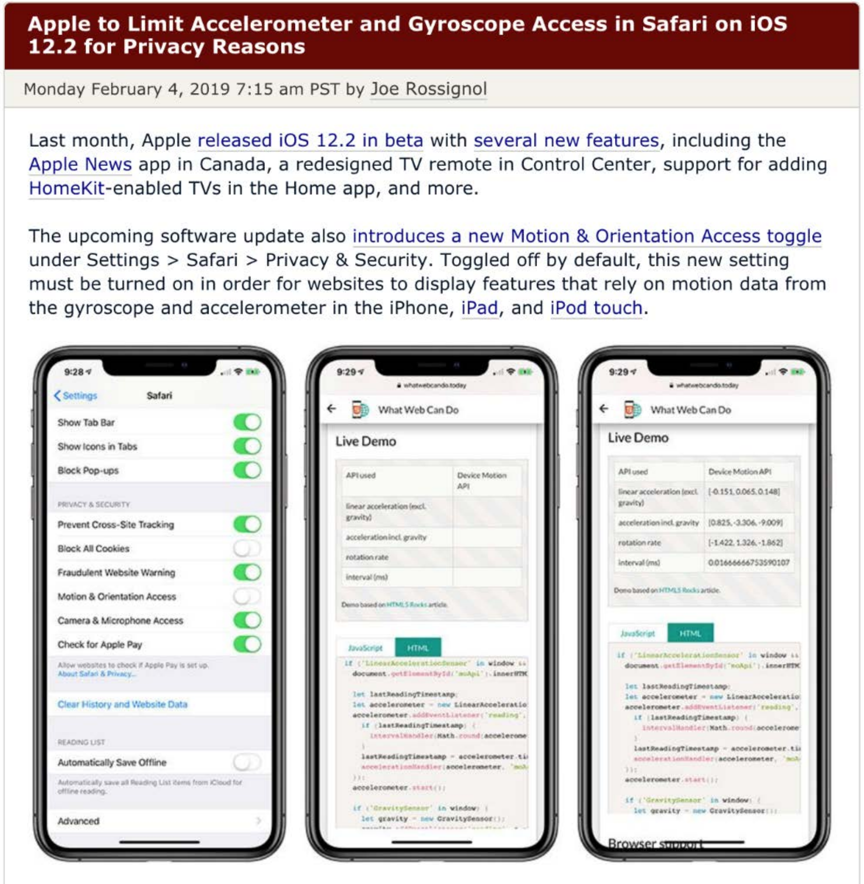
Percentage of sensor-using scripts that also perform fingerprinting

# What can be done?

- Ad blockers, tracking protection mode?
  - blocklists miss the long tail (blocking rate: 1.8%-8.6%)
  - some sites serve scripts as first-party to avoid blocklists
- Feature Policy API
  - enables publishers to control what APIs are accessible
- Block sensor access from insecure and cross-origin iframes (W3C)
  - browsers don’t always follow recommendations

# What can be done? (cont’d)

- Default to low resolution readings: ask user for high-precision readings if needed
- Visual indication when sensors are accessed
- Private browsing/incognito mode: lower resolution or disable by default
- (Future work...)



## Apple to Limit Accelerometer and Gyroscope Access in Safari on iOS 12.2 for Privacy Reasons

Monday February 4, 2019 7:15 am PST by Joe Rossignol

Last month, Apple released iOS 12.2 in beta with several new features, including the Apple News app in Canada, a redesigned TV remote in Control Center, support for adding HomeKit-enabled TVs in the Home app, and more.

The upcoming software update also introduces a new Motion & Orientation Access toggle under Settings > Safari > Privacy & Security. Toggled off by default, this new setting must be turned on in order for websites to display features that rely on motion data from the gyroscope and accelerometer in the iPhone, iPad, and iPod touch.

9:28

< Settings — Safari

| | |
|---|---|
| Show Tab Bar | ● |
| Show Icons in Tabs | ● |
| Block Pop-ups | ● |
| PRIVACY & SECURITY | |
| Prevent Cross-Site Tracking | ● |
| Block All Cookies | ○ |
| Fraudulent Website Warning | ● |
| Motion & Orientation Access | ○ |
| Camera & Microphone Access | ● |
| Check for Apple Pay | ● |

Allow websites to check if Apple Pay is set up.
About Safari & Privacy...

Clear History and Website Data

READING LIST

| | |
|---|---|
| Automatically Save Offline | ○ |

Automatically save all Reading List items from iCloud for offline reading.

Advanced >

9:29

whatwebcando.today

← What Web Can Do

Live Demo

| API used | Device Motion API |
|---|---|
| linear acceleration (excl. gravity) | |
| acceleration incl. gravity | |
| rotation rate | |
| interval (ms) | |

Demo based on HTML5 Rocks article.

JavaScript | HTML

```
if ('LinearAccelerationSensor' in window &&
  document.getElementById('moApi').innerHTM

  let lastReadingTimestamp;
  let accelerometer = new LinearAcceleratio
  accelerometer.addEventListener('reading',
    if (lastReadingTimestamp) {
      intervalHandler(Math.round(accelerome
    }
    lastReadingTimestamp = accelerometer.ti
    accelerationHandler(accelerometer, 'moA
  });
  accelerometer.start();

  if ('GravitySensor' in window) {
    let gravity = new GravitySensor();
```

9:29

whatwebcando.today

← What Web Can Do

Live Demo

| API used | Device Motion API |
|---|---|
| linear acceleration (excl. gravity) | [-0.151, 0.065, 0.148] |
| acceleration incl. gravity | [0.825, -3.306, -9.009] |
| rotation rate | [-1.422, 1.326, -1.862] |
| interval (ms) | 0.016666667535901O7 |

Demo based on HTML5 Rocks article.

JavaScript | HTML

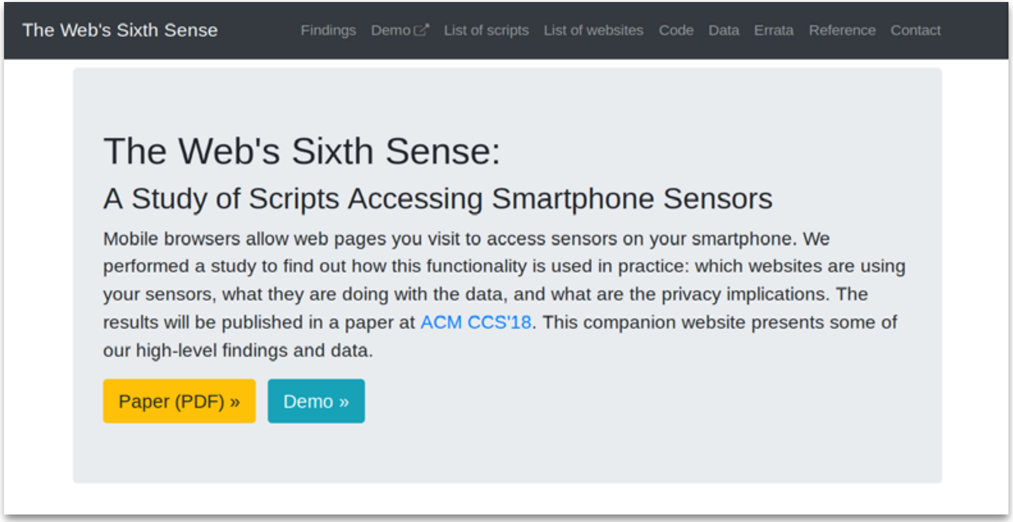
```
if ('LinearAccelerationSensor' in window &&
  document.getElementById('moApi').innerHTM

  let lastReadingTimestamp;
  let accelerometer = new LinearAcceleratio
  accelerometer.addEventListener('reading',
    if (lastReadingTimestamp) {
      intervalHandler(Math.round(accelerome
    }
    lastReadingTimestamp = accelerometer.ti
    accelerationHandler(accelerometer, 'moA
  });
  accelerometer.start();

  if ('GravitySensor' in window) {
    let gravity = new GravitySensor();
```

Browser support

- Apple has turned off access to accelerometer and gyroscope **by default** in Safari since iOS 12.2
- As of May 9, 2018 Firefox (version 60) disabled proximity and light sensor APIs

https://www.macrumors.com/2019/02/04/ios-12-2-safari-motion-orientation-access-toggle/

# Thanks for listening!



## The Web's Sixth Sense:

### A Study of Scripts Accessing Smartphone Sensors

Mobile browsers allow web pages you visit to access sensors on your smartphone. We performed a study to find out how this functionality is used in practice: which websites are using your sensors, what they are doing with the data, and what are the privacy implications. The results will be published in a paper at ACM CCS'18. This companion website presents some of our high-level findings and data.

Collaborators

- Günes Acar, Princeton Univ.
- Nikita Borisov, UIUC
- Amogh Pradeep, NEU

Paper, code, and data: **sensor-js.xyz**