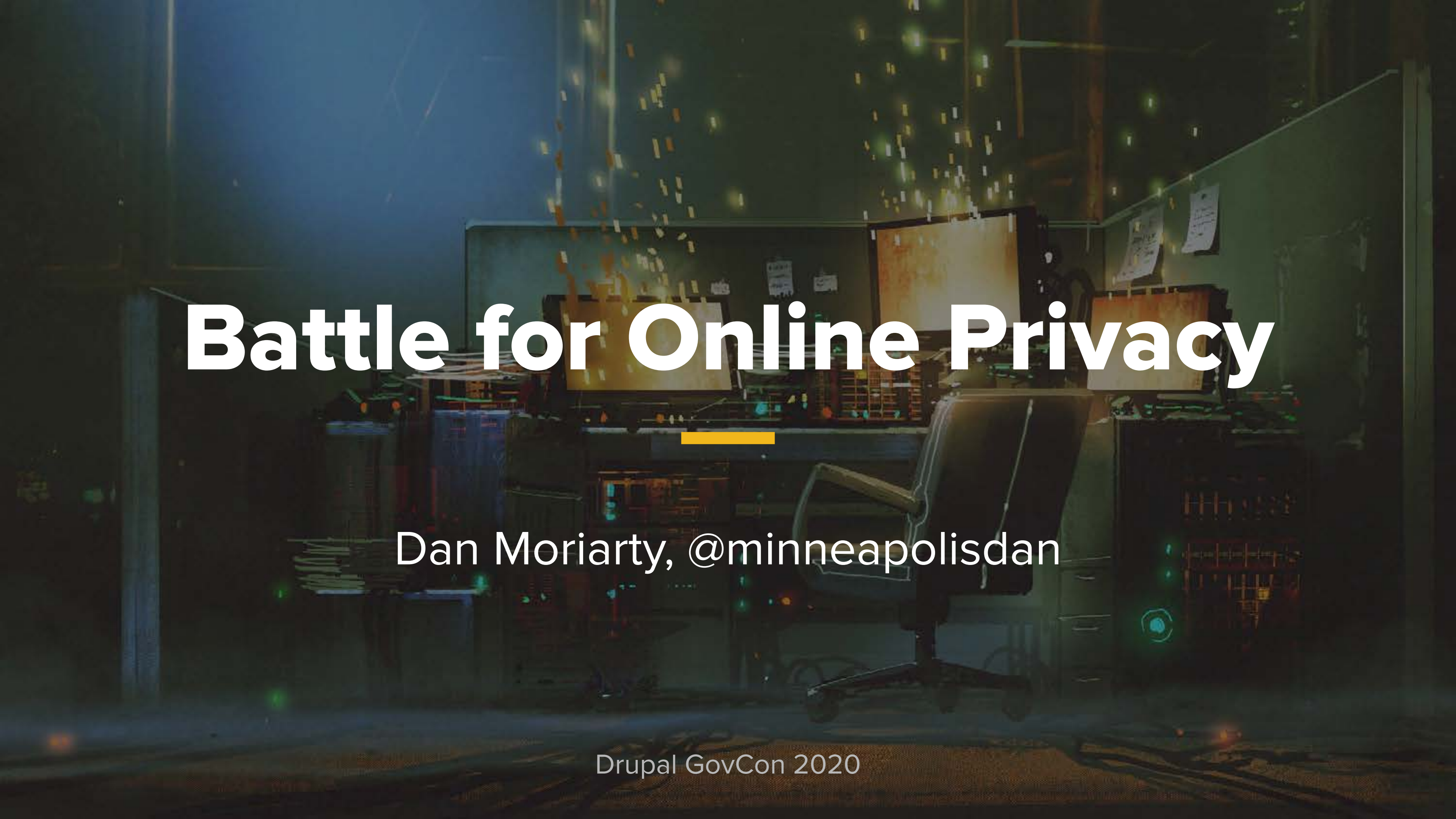


# Battle for Online Privacy

Dan Moriarty, @minneapolisdan

Drupal GovCon 2020

# About Me

Dan Moriarty

# About Me

Dan Moriarty

- Web design for 20+ years
- Drupal for 10+ years
- Twitter: @minneapolisdan
- Drupal: minneapolisdan
- Aka Citizen Dan

ELECTRIC CITIZEN

# About Electric Citizen

Web Agency

ELECTRIC
CITIZEN

- Based in Minneapolis since 2012
- Focus on civic sector (government, higher ed, nonprofits, arts, science)
- Open-source advocates
- Drupal Supporting Partner
- www.ElectricCitizen.com

### What battle?

# Privacy is losing

# Facial Recognition

- Repressive governments
- Law enforcement
- For profit companies
- Racially biased
- Clearview AI, NEC
- Coming to your browser?

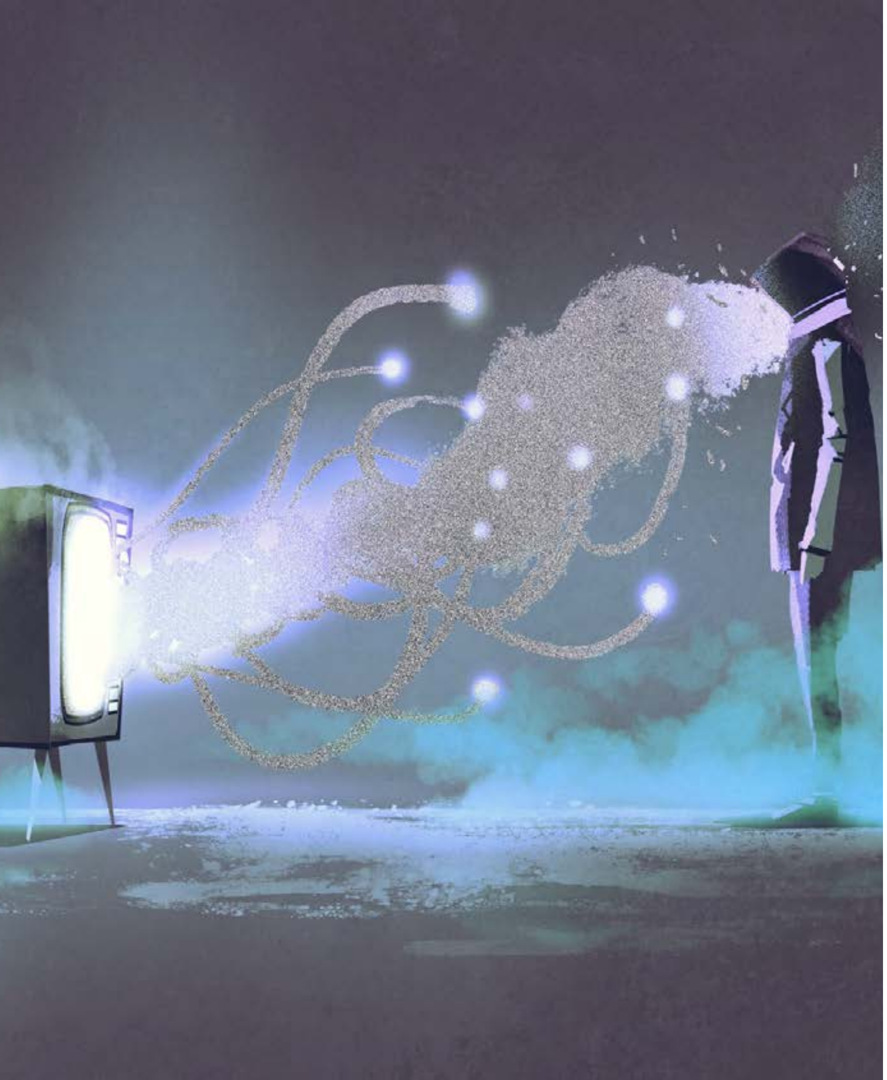
# Data Breaches

- Poor security
- Hoarding personal info
- Hackers from criminal to government spies

EQUIFAX

YAHOO!

Cambridge Analytica



# Data Companies

- Corporations like Google, Facebook, Apple, Oracle
- Data brokers such as Experian, White Pages, West Publishing
- Measuring credit reports, health risk, purchase history, legal, jobs
- Mass personalization
- Little regulation, billions of dollars at stake

# Internet of Things

- Google Home
- Amazon Alexa
- Apple Siri
- Anything “smart”

nest
COOLING
75

ring

PHILIPS
hue
800
White
Starter kit
Automate your lights
for peace of mind

SONOS

OK
amazon
BLOCKBUSTER
MGO
NETFLIX
Roku

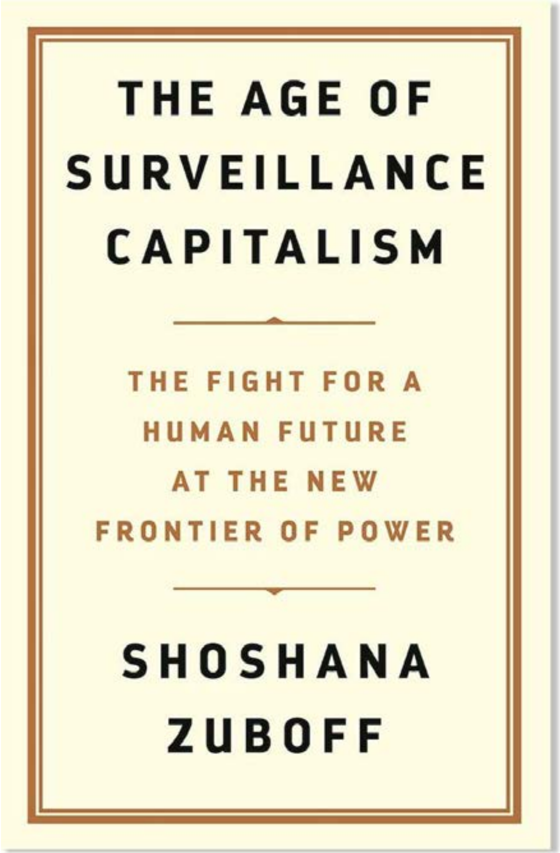
包牌上道

# The Internet

- Websites we build
- Data we manage
- Information we collect
- Products we sell
- Tracking scripts, tracking pixels, geofencing, etc.

# Surveillance Capitalism

- Buying and selling data of predictive behavior
- Human behavior as free raw material
- The new age of robber barons


THE AGE OF SURVEILLANCE CAPITALISM

THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER

SHOSHANA ZUBOFF

# Surveillance Capitalism

Fast rise to incredible power

Microsoft

Google

facebook®

amazon

# What choice?

- Maps to find your way
- Find a job
- Pay for goods
- Find a partner
- Banking
- Customer service

**“Privacy is dead” … we just step into this “discomfort each and every day”**

– Erik Qualman

# The People
# Strike Back

ELECTRIC CITIZEN

disclaimer:

*not a lawyer

# GDPR

- General Data Protection Regulation, May 2018
- Give users rights to their personal data
- Protecting user privacy
- ePrivacy Directive (EPD) defines use of Cookies

# GDPR Summary: Rights and Protections

01 Breach Notification

02 Access to Personal Data

03 Right to be Forgotten

04 Data Portability

05 Privacy by Design

# Who Does GDPR affect?

Any Size Organization

For Profit AND Nonprofit

Serving EU users

# What’s Happened Since May 2018

- $490+ Billion in fines!
  - Marriott, $99 million*
  - British Airways, $183 million*
  - Google, $50 million
- New/renewed focus on Privacy Experience (PX)
- New laws in the USA (CCPA)

## Privacy in the USA

# CCPA

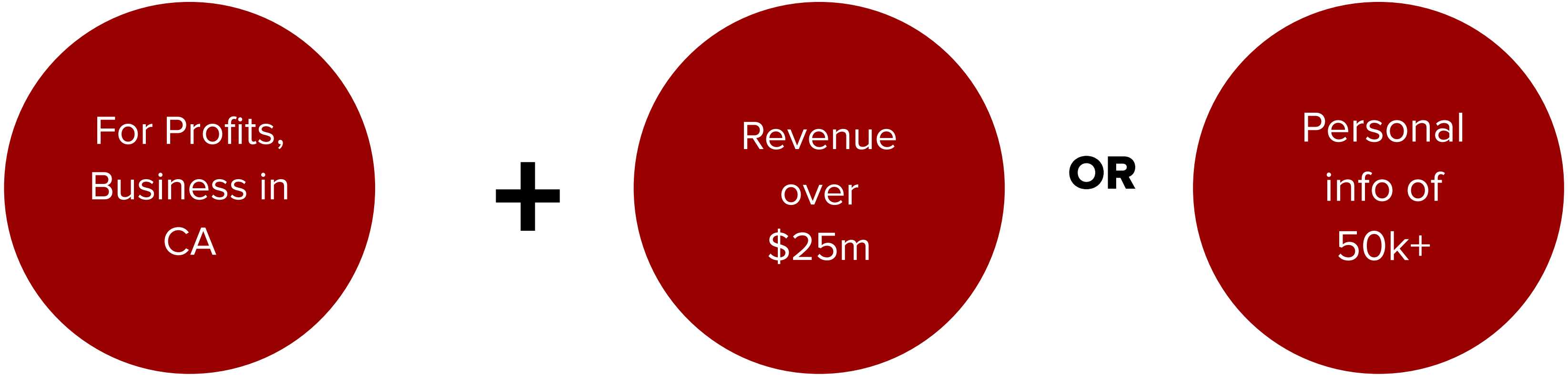
# Who’s Ready for the CCPA?

- California Consumer Privacy Act
- Became state law on Jan 1st, 2020

# CCPA: What it Does

- Know what personal data is collected
- Know if data is sold to others
- Opt out of sale of your personal data
- Request personal data be deleted
- Not discriminated against for exercising privacy rights

# CCPA: Who Must Comply?



For Profits, Business in CA

+

Revenue over $25m

**OR**

Personal info of 50k+

**OR** earn half your revenue selling personal information

# CCPA: Meeting the Requirements

## Security

Reasonable security procedures and practices

## Data

Users can opt-out

Request copy of data

Ask to be forgotten

## Policies

Update privacy policy, detail what is collected

Ask parental consent

Toll-free access to data

# CCPA: What’s Happened Since

- Updated privacy policies
- Billions spent on compliance
- Companies scrambling to make private data accessible to users
- Fines issued
- California Privacy Rights Act of 2020 (ballot)

# Other States

- Massachusetts Data Privacy Law
- New York Privacy Act
- Maryland Online Consumer Protection Act
- Hawaii Consumer Privacy Protection Act

# Federal Privacy Law?

(yes please)

# Other Countries

PIPEDA (Canada)

AAP (Australia)

LGPD (Brazil)

# But what can I do?

**The overwhelming majority of web practitioners have no training, education, or guidance in online privacy.**

– Heather Burns,
webdevlaw.uk

Best practice in PX:

# Privacy Experience

ELECTRIC CITIZEN

# Web Design Process

PLAN

DESIGN

BUILD

DEPLOY

**Discovery**

Technical Architecture, Content Strategy, Define Goals and Users

**UX/UI Design**

User Experience, Visual Design, Wireframes, Mockups

**Web Development**

Coding, Building, Testing, Deploying

**Launch**

Move site to live server, update domain records

# Web Design Process

PLAN

DESIGN

BUILD

DEPLOY

### Discovery

Technical Architecture, Content Strategy, Define Goals and Users

+ PX

What data do we need to collect, How can users opt in/opt out, how do protect PII, make data portable, how long to save data

### UX/UI Design

User Experience, Visual Design, Wireframes, Mockups

+ PX

Privacy tools visible

### Web Development

Coding, Building, Testing, Deploying

+ PX

How are developers handling data, add opt tools for cookies, webforms, analytics

### Launch

Move site to live server, update domain records

+ PX

Privacy policy, data breach response team

# PX: yet another (good) thing to know

- Plan for user privacy and security
- Consider privacy in your build
- Budget for privacy
- Focus on protecting PII

# What is PII?

**By Itself:**

- Name: full name, maiden name, mother’s maiden name, or alias
- Personal identification numbers: social security, passport number, driver’s license, credit card, etc.
- Personal address, telephone numbers
- Face, fingerprints, or handwriting
- Biometric data: retina scans, voice signatures, or facial geometry
- Internet Protocol (IP) or Media Access Control (MAC)

**Info Combined with Previous Column:**

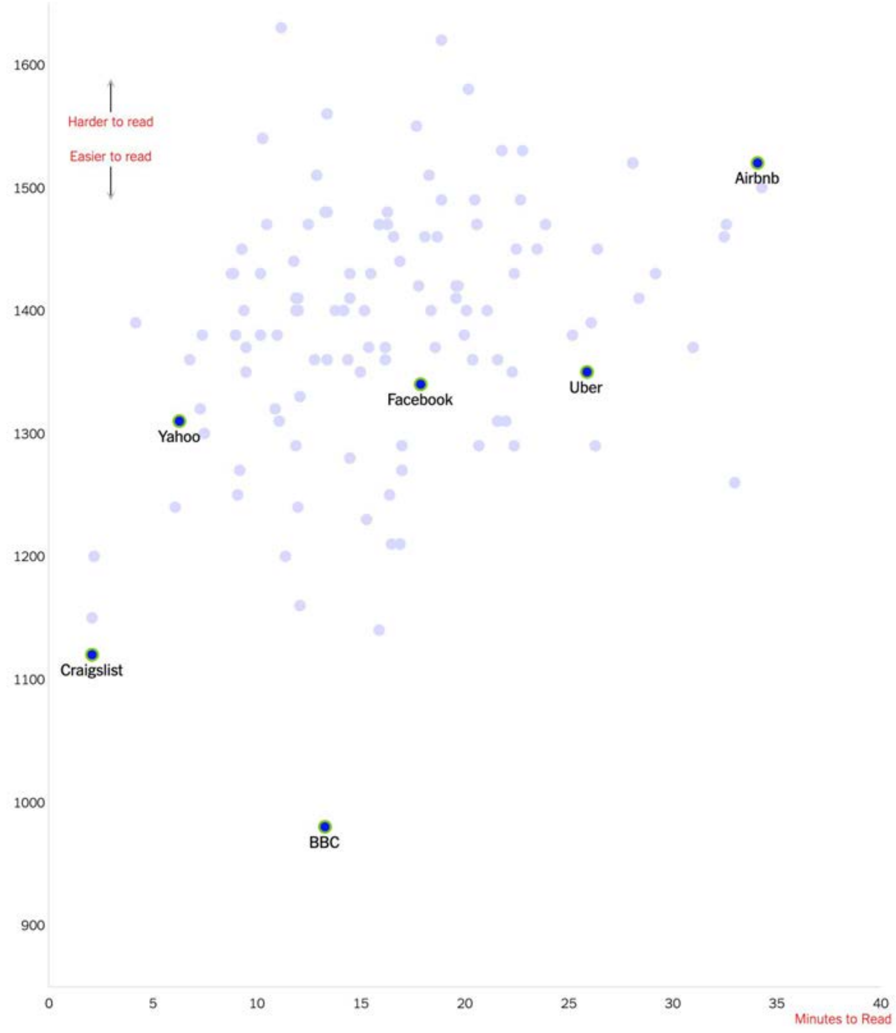
- Date of birth, place of birth
- Business number, address, email
- Race, religion
- Geographical indicators
- Employment information
- Medical information
- Education information
- Financial information

# Set Clear Policies

- Opt-in to data collection (not out)
- Ample documentation
- Limit what you’re collecting
- Set expiration dates on data
- Easy for understand
- Users can export personal data
- Easy to be forgotten

# Have a Strong Privacy Policy

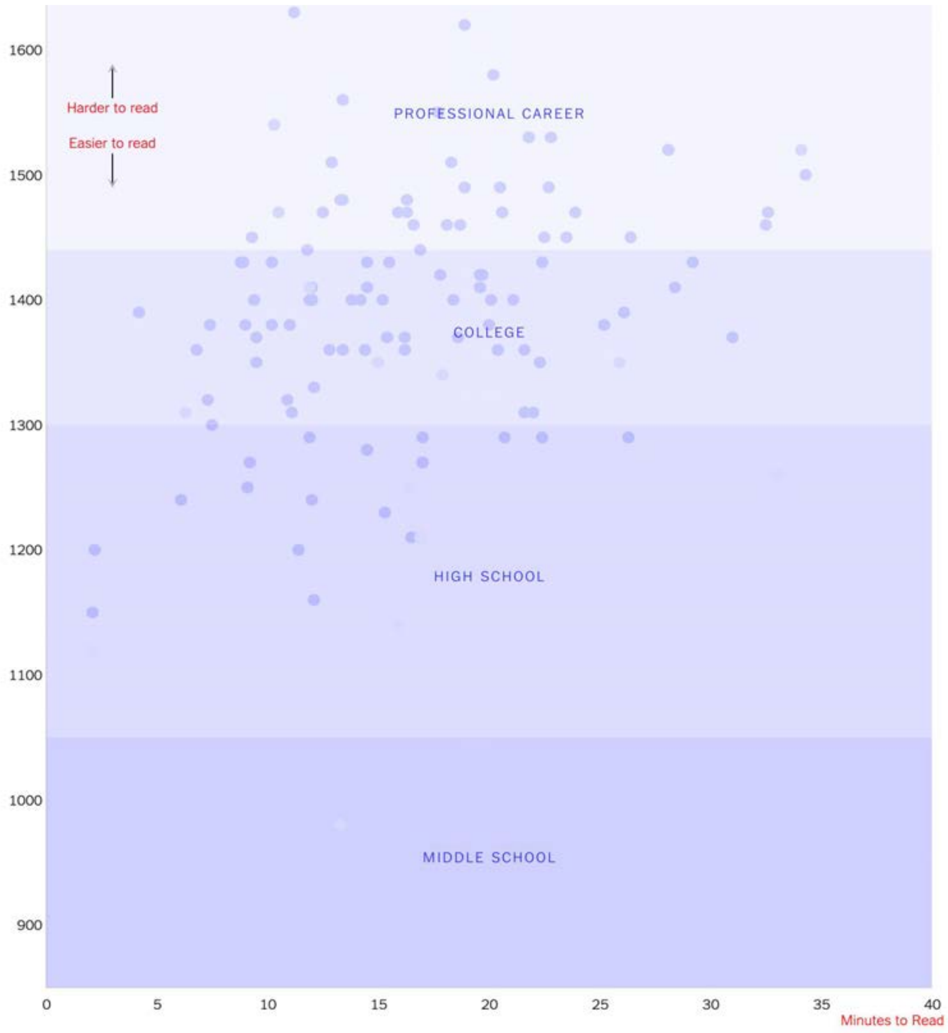
- Don’t wait to end of project!
- Easy to understand
- List all data tracked
- Plan for disasters
- Try a policy creator



# Privacy Policies

- A false choice
- Hundreds of hours per year to read
- Too difficult for most

https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html



# Privacy Policies

- A false choice
- Hundreds of hours per year to read
- Too difficult for most

https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

**Accessibility isn't required everywhere yet either,** but we do it because (a) it's the right thing to do and (b) it will be soon

## Privacy Issues:

# Technically Speaking

ELECTRIC CITIZEN

# Developers

Change in process

- Plan for managing data and PII
- Plan how to protect users
- Measure privacy impact

# Managing Data

- Developers working locally
    - What data are you handling?
    - Do you need specific records?
    - How often do you purge data?
- Data on servers
    - Is it encrypted? Should it be?
    - Who has access
- Content and marketing
    - What data are you collecting?
    - How are protecting privacy?

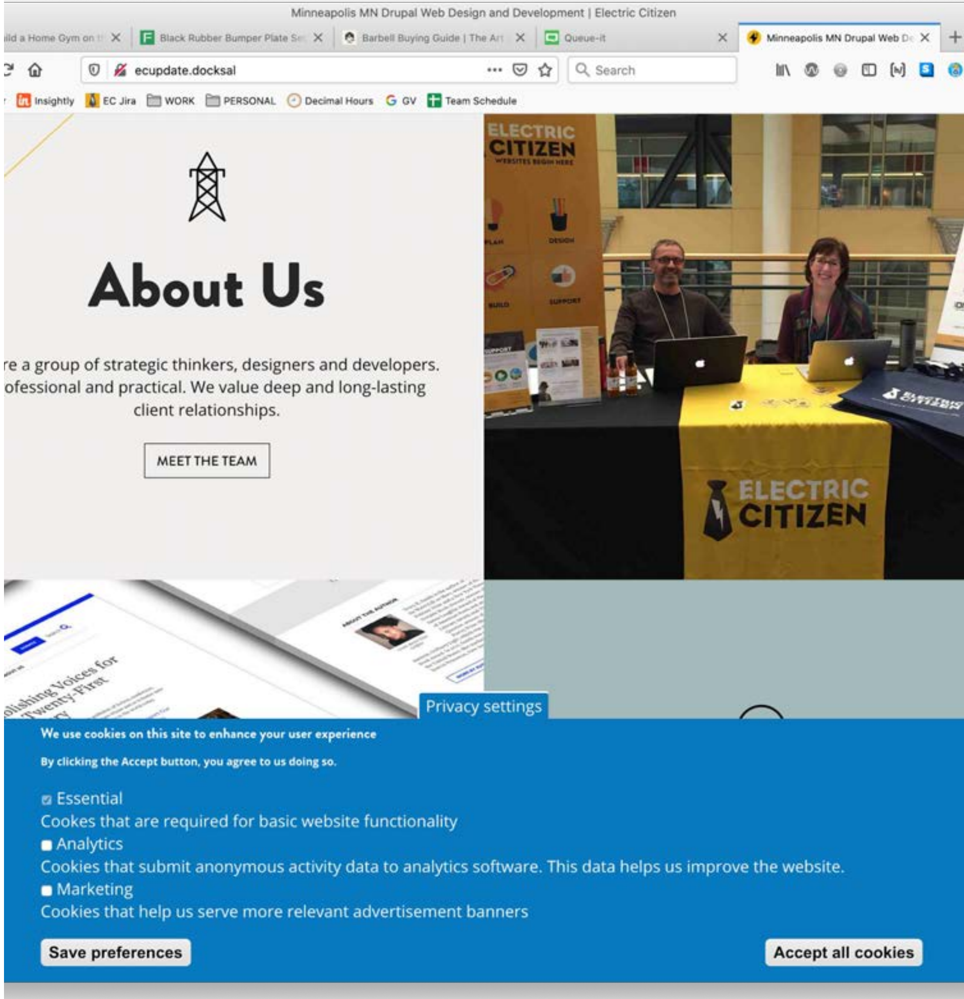
# Cookies

The web’s little spies

- First party and third party cookies, tracking pixels/scripts, web beacons
- Marketing and statistics cookies require consent
- Cookies required to make site function do not

# Cookie Compliance

- drupal.org/project/eu_cookie_compliance
- 3rd party integrations:
    - project/cookiebot
    - project/cookieconsent
    - project/divascookies



About Us

re a group of strategic thinkers, designers and developers. ofessional and practical. We value deep and long-lasting client relationships.

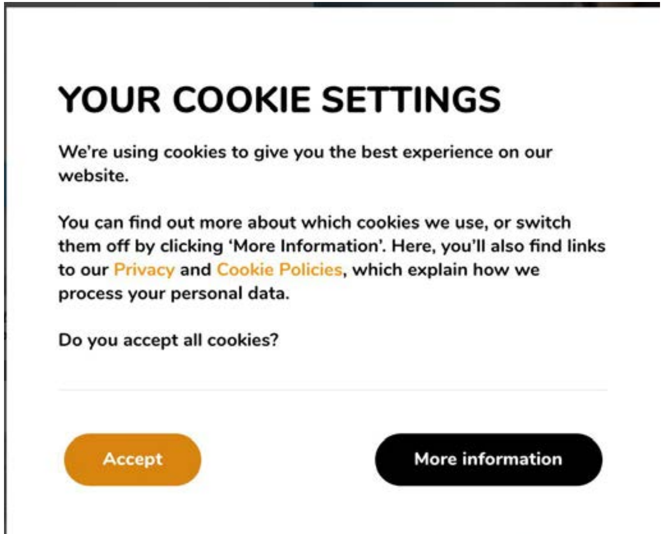
We use cookies on this site to enhance your user experience

By clicking the Accept button, you agree to us doing so.

☑ Essential
Cookes that are required for basic website functionality
□ Analytics
Cookies that submit anonymous activity data to analytics software. This data helps us improve the website.
□ Marketing
Cookies that help us serve more relevant advertisement banners

# GDPR Cookie Compliance

- Options to opt-in by default
- Let users control options
- Different types of cookies

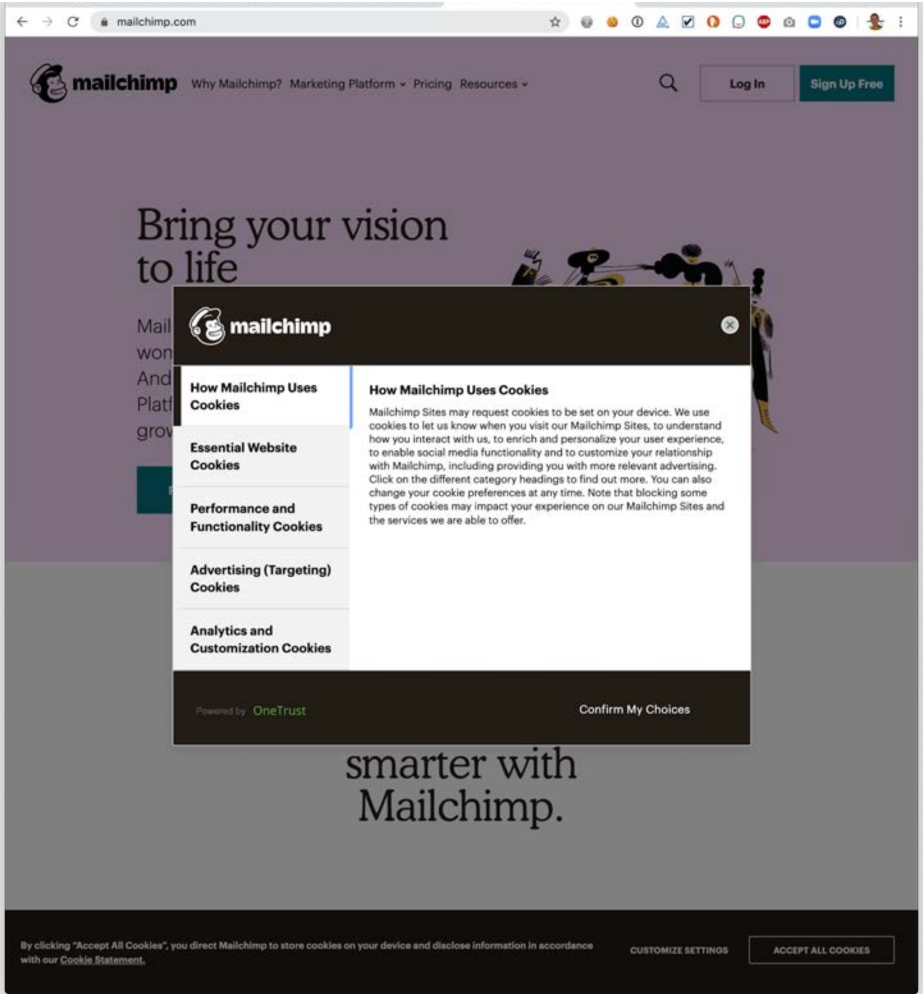


YOUR COOKIE SETTINGS

We're using cookies to give you the best experience on our website.

You can find out more about which cookies we use, or switch them off by clicking 'More Information'. Here, you'll also find links to our Privacy and Cookie Policies, which explain how we process your personal data.

Do you accept all cookies?



How Mailchimp Uses Cookies

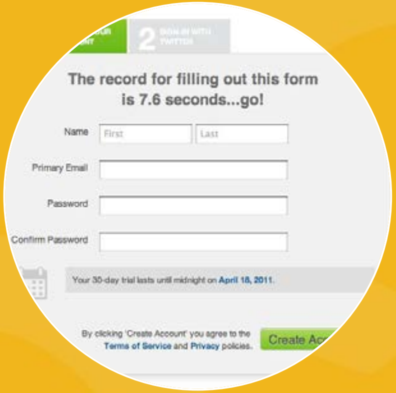
Mailchimp Sites may request cookies to be set on your device. We use cookies to let us know when you visit our Mailchimp Sites, to understand how you interact with us, to enrich and personalize your user experience, to enable social media functionality and to customize your relationship with Mailchimp, including providing you with more relevant advertising. Click on the different category headings to find out more. You can also change your cookie preferences at any time. Note that blocking some types of cookies may impact your experience on our Mailchimp Sites and the services we are able to offer.

By clicking "Accept All Cookies", you direct Mailchimp to store cookies on your device and disclose information in accordance with our Cookie Statement.

# Site Analytics

More data that you’ll ever need?

- Google Analytics is most widely used. Do they collect PII?
- Disclose use in privacy policy
- Offer users way to opt-out
- Matomo is open-source analytics you host yourself



The record for filling out this form is 7.6 seconds...go!

Your 30-day trial lasts until midnight on April 18, 2011.

By clicking 'Create Account' you agree to the Terms of Service and Privacy policies.

# Online Forms

How do you use **and** protect the data you are collecting?

- What data are you collecting? For how long?
- Explain why each field you include is needed
- Limit what you collect

# Third Party

Libraries, packages and scripts,
oh my!

- NPM and Composer
- JavaScript libraries
- Social sharing widgets
- Tracking scripts
- Embedded media

ELECTRIC CITIZEN

# Be Privacy Smart

Encryption is your #1 weapon

- Rely on (and support laws regarding) **encryption of data**
- EARN IT legislation
- Consider DuckDuckGo, Firefox, ProtonMail
- Support advocacy orgs like EFF, ACLU
- Support open-source, open web, ethical design

# Drupal-Specific

Modules and more

- GDPR compliance team
- EU Cookie Compliance
- Encrypt module
- Cryptolog
- Blizz Vanisher
- IP anonymize
- Drush sql-sanitize
- Faker
- Security Kit
- Guardr (security distribution)
- Core Privacy Initiative

# Final Takeaways

# Does Privacy Still Matter?

- Avoid getting comfortably numb!
- Understand new laws and learn best practices for privacy
- All of us have a role to play, especially those making the web

# Thank you!

**Dan Moriarty, @minneapolisdan**
CEO, Creative Director at Electric Citizen

# Additional Resources

### Privacy Laws

- The GDPR is here. Are you ready?
- GDPR will change the way you develop
- California Consumer Privacy Act (CCPA): What Does It Mean For You?
- Major GDPR fines
- CCPA off to rocky start

### Privacy Concerns

- Major privacy breaches

### Privacy Experience

- Privacy and Webforms
- Third-party scripts and privacy
- How tracking pixels work
- Privacy policies