

Battle for Online Privacy

Dan Moriarty, @minneapolisdan

About Me

Dan Moriarty



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

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 experts
- www.ElectricCitizen.com



What We'll Cover

Battle for Online Privacy

- Privacy in danger
- Privacy and the law
- Best practices
- Technical considerations



disclaimer:
***not a lawyer**

Why are you here?

Battle for Online Privacy

- Privacy advocate
- Keeping up with new laws and regulations
- Understand best practices

What battle?

Privacy is losing





Data Breaches

- Companies hoarding too much personal info
- Poor security and determined hackers



BEST PRODUCTS ▾ REVIEWS ▾ NEWS ▾ VIDEO ▾ HOW TO ▾ SMART HOME ▾ CARS ▾ DEALS ▾ DOWNLOAD

How the Equifax hack happened, and what still needs to be done

A year after the revelation of the massive breach, there's unfinished business.



Alfred Ng  September 7, 2018 4:54 AM PDT



EQUIFAX

- o 143 million – half the US!
- o Social security numbers, birthdates, credit card numbers – all stolen

Cyber-Safe

Every single Yahoo account was hacked - 3 billion in all

by Selena Larson @selenalarson

🕒 October 4, 2017: 6:36 AM ET

👍 Recommend 202



Sitting down? An epic and historic data breach at Yahoo in August 2013 affected every single customer account that existed at the time, Yahoo parent company Verizon [said](#) on Tuesday.

That's [three billion accounts](#) -- including email, Tumblr, Fantasy and Flickr -- or three times as many as the company initially [reported](#) in 2016.

Names, email addresses and passwords, but not financial information, were breached, Yahoo said last year.

YAHOO!

- 3 billion accounts
- Names, DOB, passwords, answers to security questions, all hacked

☰ The New York Times 

PLAY THE CROSSWORD

Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens

By Kevin Granville

March 19, 2018     

[Leer en español](#)



Cambridge Analytica, a political data firm hired by President Trump's 2016 election campaign, gained access to information on 50 million Facebook users as a way to identify the personalities of American voters and influence their behavior.
Elise Amendola/Associated Press

[Our report](#) that a political firm hired by the Trump campaign acquired access to private data on millions of Facebook users has



Cambridge Analytica

- 87 million affected
- Personal info harvested without permission
- Used by campaigns for targeted political ads



Data Breaches: How to Respond?

- Freeze credit
- Identity protection
- Quit using the service?

2011年07月02





Id: 1/2
Gender: male
Age group: Young adult
Ethnicity: Caucasian
Angry: 0,5 %
Happy: 87 %
Time: 1623 s
Detection: 25621 pts
Pos (x/y/z): 1322 / 856 / 21

Id: 2/2
Gender: female
Age group: Young adult
Ethnicity: Caucasian
Angry: 0 %
Happy: 96 %
Time: 2672 s
Detection: 15621 pts
Pos (x/y/z): 1322 / 856 / 21

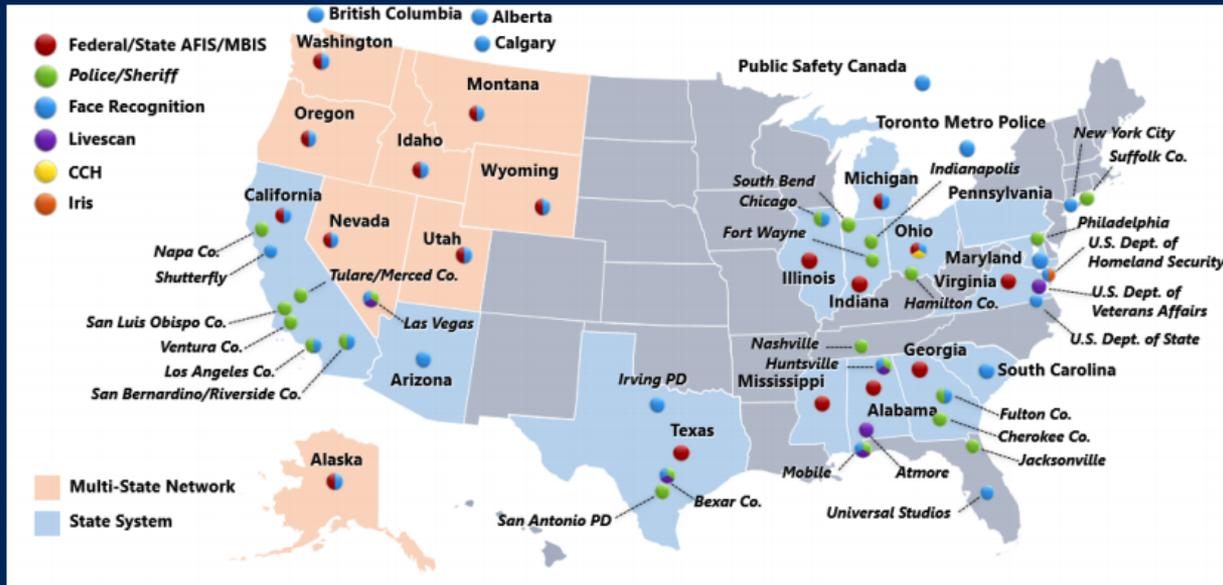
Facial Recognition

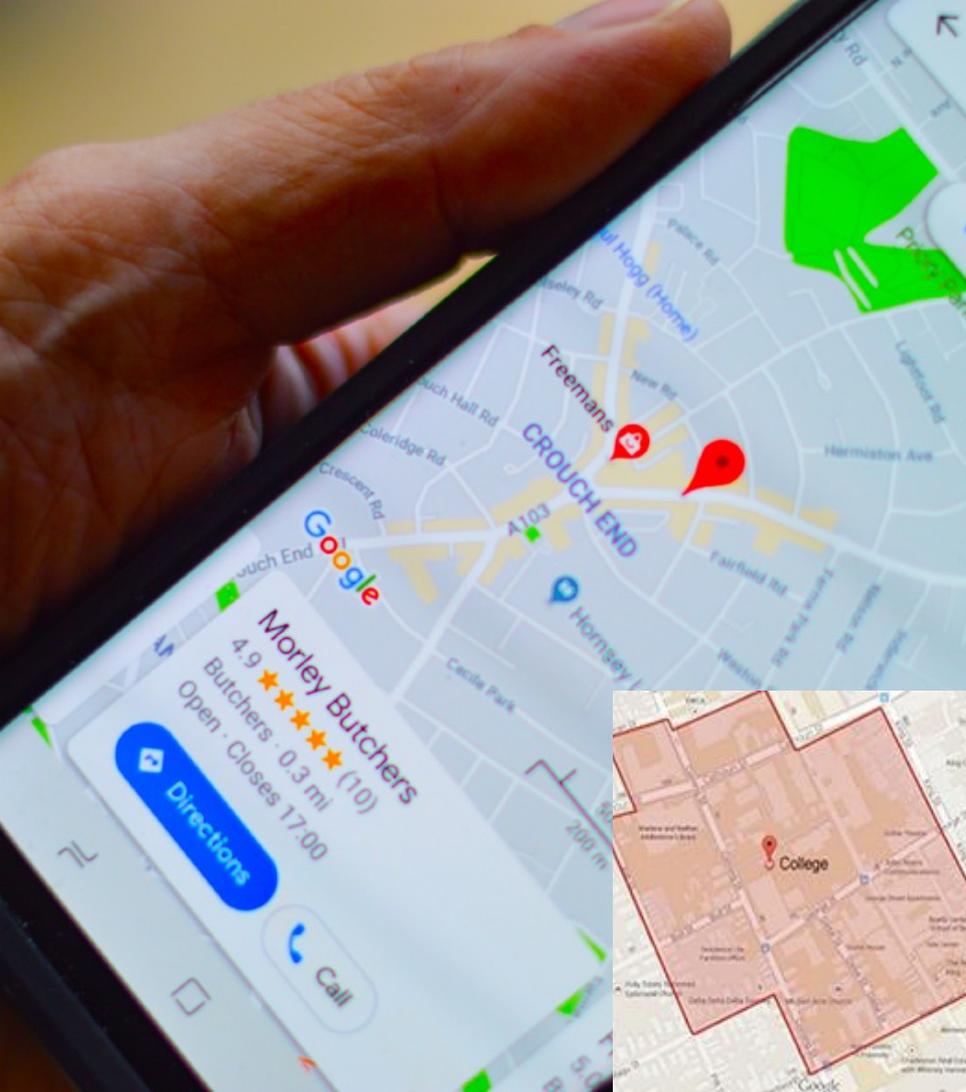
- Repressive governments
- Law enforcement
- For profit companies
- Clearview AI
- NEC



NEC State & Local Police agencies

NEC Biometrics Identification System
in over 1/3 of US State Polices and Law Enforcement Agencies





Geofencing

- Uses phone data and “invisible fence”
- Tracks where you go, what you attend
- Location-based marketing



In Your Home

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







Hello!



Goodbye



Go To Story Time



Go To Games



Go To Photo Album

Go To Settings 

Tutorial Video

My friend Cayla Party Time!

Speech powered by NUANCE

If it's a 'smart' device, it's tracking you



Building Your Public Profile

- School
- Religion
- Work
- Politics
- Music
- Shopping
- Health
- Family

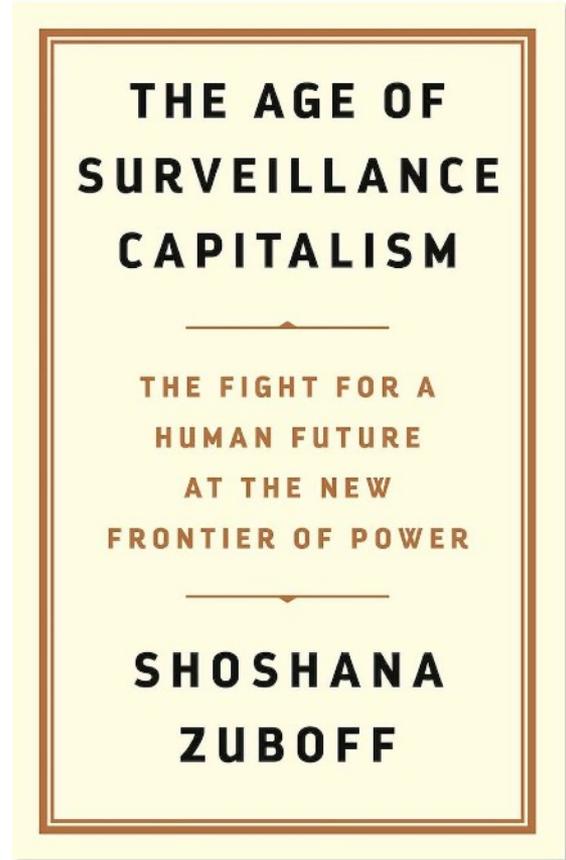


Feeding the Data Brokers

- Well-known data brokers like Experian, White Pages, West Publishing
- Hundreds of unknowns
- People search, credit reporting, marketing, advertising, risk mitigation
- Little regulation, billions of dollars at stake

Surveillance Capitalism

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



Surveillance Capitalism



Google

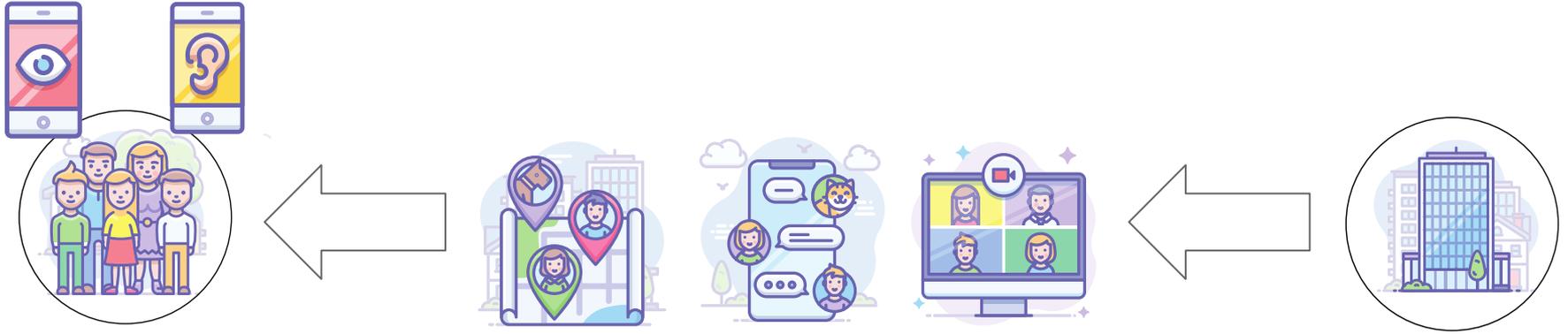


Surveillance Capitalism 101



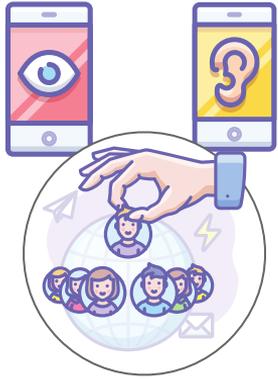
Free, low-cost apps and services
(search, docs, entertainment, chat, etc.)

Surveillance Capitalism 101

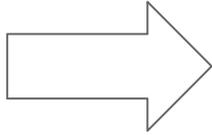


Tracking data

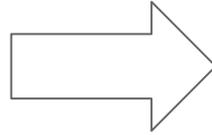
Surveillance Capitalism 101



Extracting your private data



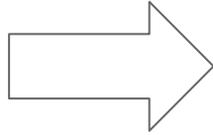
Sending your personal data back to same companies



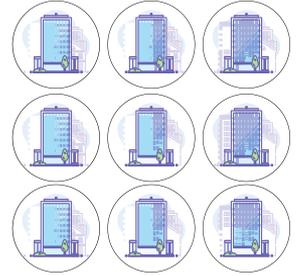
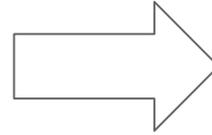
Surveillance Capitalism 101



Extracting your
private data



Selling your
private data



Buying your
private data



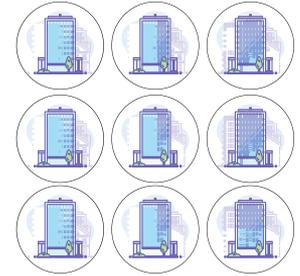
Surveillance Capitalism 101



Extracting your private data



Behavior as Raw Material



Targeting with your private data



We're under attack!

How to respond



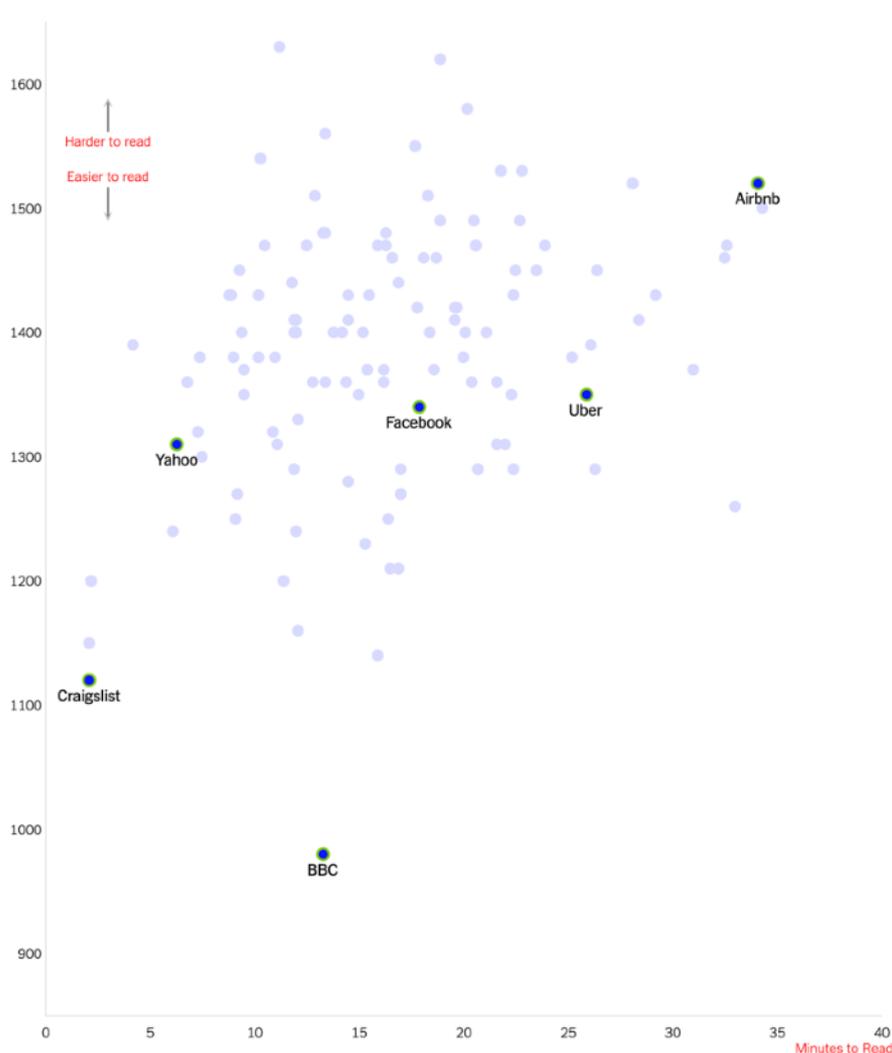
A water mill with a large wooden wheel and log buildings. The scene is set in a rural, wooded area with a stream flowing through it. The water mill is the central focus, with a large wooden wheel and a log building attached to it. The sky is a deep blue, and the overall atmosphere is serene and rustic. The text "Option 1: Off the Grid" is overlaid on a yellow banner across the middle of the image.

Option 1: Off the Grid



Is that a choice?

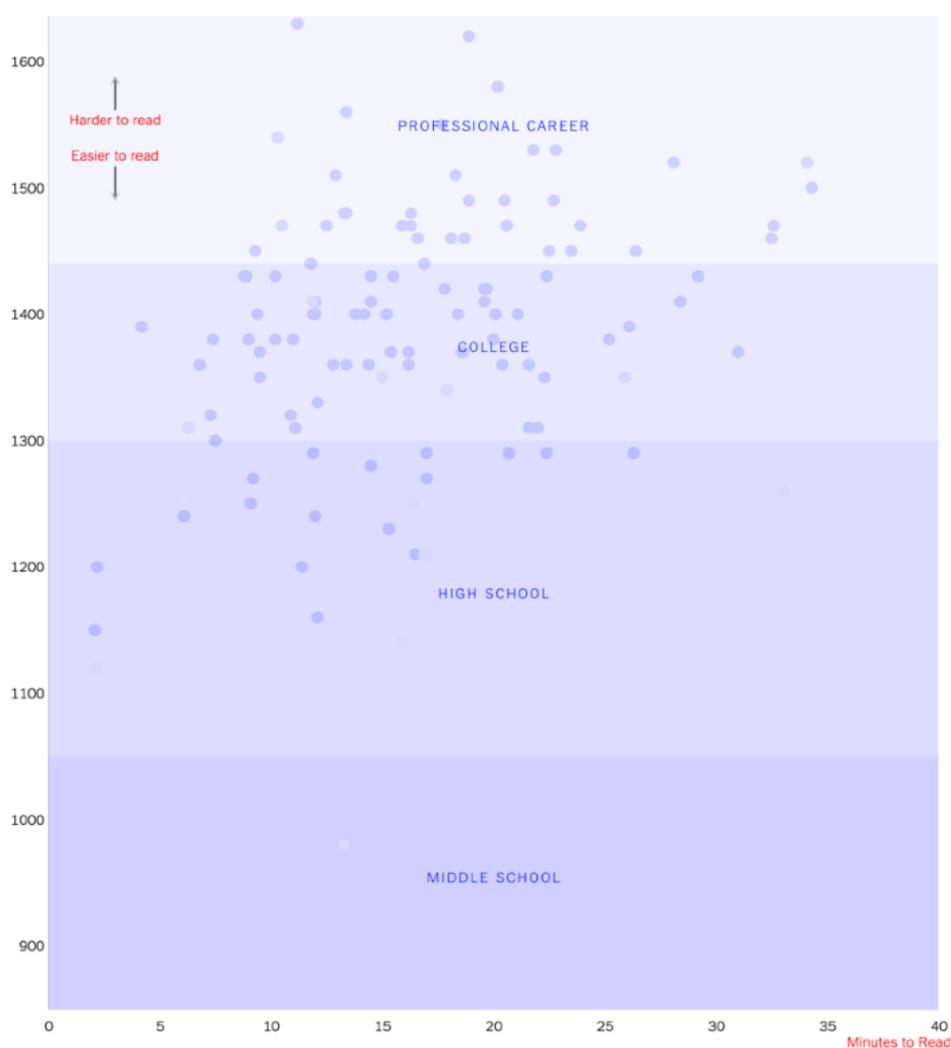
- Maps to find your way
- Conduct banking
- Find a job
- Pay for goods
- Find a partner
- College applications
- Customer service



Privacy Policies

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

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



Privacy Policies

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

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

A futuristic, industrial cityscape at night. The scene is filled with complex machinery, scaffolding, and structures illuminated by various lights, including a prominent bright yellow light source in the center. Two figures are visible in the foreground, standing on a platform and looking towards the city. The overall atmosphere is dark and atmospheric, with a mix of blue, green, and yellow tones.

Option 2: Get Over It

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

– Erik Qualman



Live with it

- Focus on generating your best social profile
- Trust the market will look out for your best interests



Option 3: Fight Back



Join the Fight

- Follow privacy laws, support new legislation
- Learn best practices
- Choose the right tools to protect your data
- Choose **responsible** open source

The People
Strike Back





GDPR

- General Data Protection Regulation, May 2018
- Established guaranteed rights with personal data, how it is collected and managed



Rights and Protections

- Breach notifications
- Access to personal data
- Right to be forgotten
- Data portability
- Privacy by design
- Require data protection officers and processors



Who Does it Affect?

- Offering goods and services outside of personal use
- Collecting personal data
- Organizations who could envisage serving EU users
- Could be for-profit and nonprofit
- Any size organization



EPD

- ePrivacy Directive (EPD) defines use of Cookies, along with GDPR

The image shows a blue background with a circle of yellow stars, similar to the European Union flag. In the center, the text 'GDPR' is written in large, white, bold letters. Below it, the text 'GENERAL DATA PROTECTION REGULATION' is written in smaller, yellow, bold letters, following the curve of the stars.

GDPR

GENERAL DATA PROTECTION REGULATION

What's Happened Since Law

- Over \$360 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)

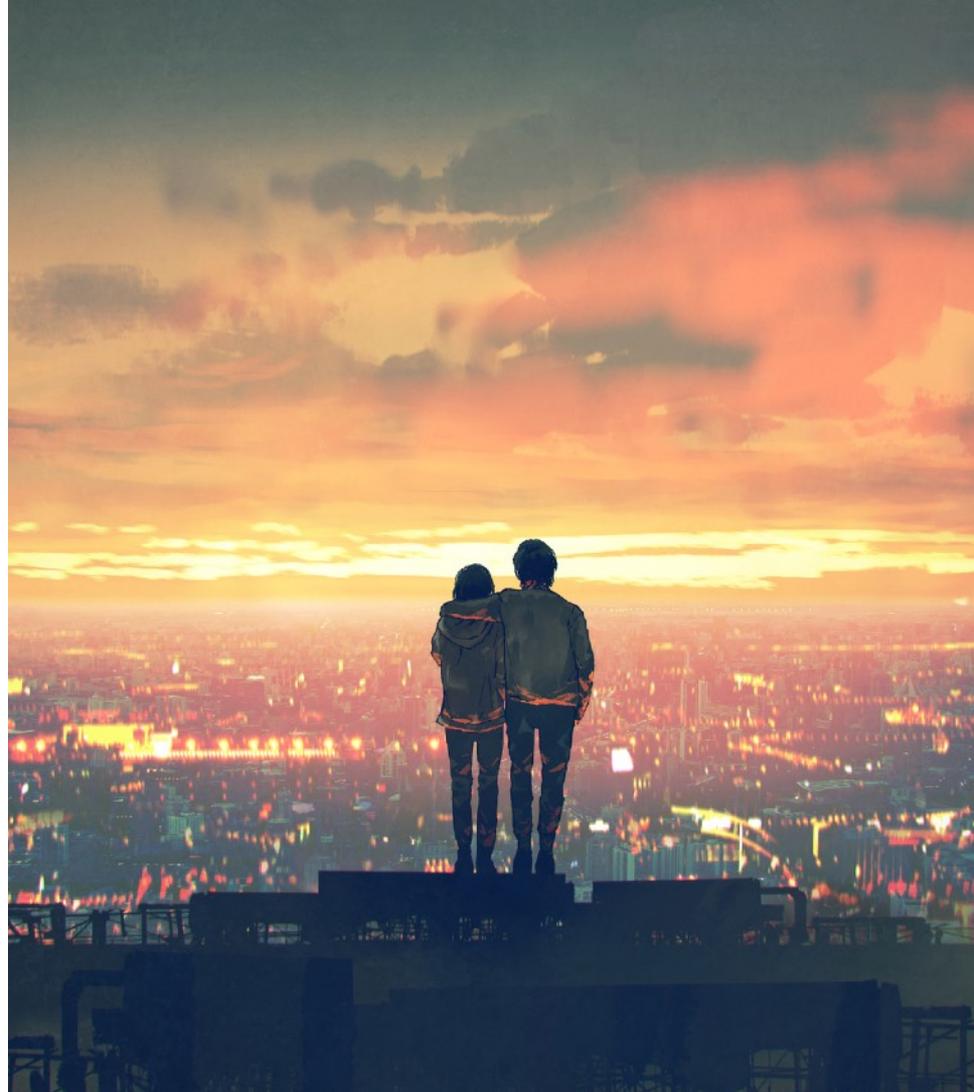
Privacy in the USA

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 who collect personal data and do business in CA, and
- Annual revenues over \$25m, **OR**
- Possess personal info of 50,000+ people/households/ devices
- **OR** earn half your revenue selling personal information



CCPA: Meeting the Requirements

- Implement and maintain reasonable security procedures and practices
- Ask for parental consent for kids under 13; affirmative consent for 13-16 year olds
- Clearly visible opt-out link of sales of personal info
- Toll-free number for data access
- Update privacy policy



CCPA: What's Happened Since

- Updated privacy policies
- Billions spent on compliance
- Companies scrambling to make private data accessible to users
- Fines issued



Exporting Data



```
    }, {
      "productTitle": "Service Charge",
      "price": "5770000",
      "quantity": "1"
    }, {
      "productTitle": "Dispatch Service Charge",
      "price": "13470000",
      "quantity": "1"
    }, {
      "productTitle": "Aloo Tikki",
      "price": "4950000",
      "quantity": "1"
    }, {
      "productTitle": "Chicken Chili",
      "price": "12950000",
      "quantity": "1"
    }, {
      "productTitle": "Vegetarian Dinner for Two",
      "price": "35990000",
      "quantity": "1"
    }, {
      "productTitle": "Tandoori Dinner for Two",
      "price": "38990000",
      "quantity": "1"
    }, {
      "productTitle": "Chana Masala",
      "price": "11950000",
      "quantity": "1"
    }, {
      "productTitle": "Mixed Salad",
      "price": "3950000",
      "quantity": "1"
    }, {
      "productTitle": "Cheese Pakora",
      "price": "5950000",
      "quantity": "1"
    }, {
      "productTitle": "Dish",
      "price": "13470000",
      "quantity": "1"
    }
  ]
}
```



General

Security and Login

Your Facebook Information

Privacy

Timeline and Tagging

Stories

Location

Blocking

Language and Region

Face Recognition

Notifications

Mobile

Public Posts

Apps and Websites

Instant Games

Business Integrations

Ads

Payments

Support Inbox

Videos

Your Facebook Information

You can view or download your information and delete your account at any time.

Access Your Information View your information by category. [View](#)

Download Your Information Download a copy of your information to keep, or to transfer to another service. [View](#)

Activity Log View and manage your information and some settings. [View](#)

Off-Facebook Activity View or clear activity from businesses and organizations you visit off of Facebook. [View](#)

Managing Your Information Learn more about how you can manage your information. [View](#)

Deactivation and Deletion Temporarily deactivate or permanently delete your account. [View](#)

Off-Facebook Activity

Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them, such as visiting their apps or websites. [Learn More](#)



Wellsfargo.com, Amazon and other websites or apps have shared your activity with Facebook.

What is off-Facebook activity?

Off-Facebook activity includes information that businesses and organizations share with us about your interactions with them. Interactions are things like visiting their website or logging into their app with Facebook. Off-Facebook activity does not include customer lists that businesses use to show a unique group of customers relevant ads.

How did Facebook receive your activity?

When you visit a website or use an app, these businesses or organizations can share information about your activity with us by using our business tools. We use this activity to personalize your experience, such as showing you relevant ads. We also require that businesses and organizations provide notice to people before using our business tools.

Here's How Activity is Shared with Facebook



Jane buys a pair of shoes from an online clothing and shoe store.



The store shares Jane's activity with us using our business tools.



We receive Jane's off-Facebook activity and we save it with her Facebook account. The activity is saved as "visited the Clothes and Shoes website" and "made a purchase".



Jane sees an ad on Facebook for a 10% off coupon on her next shoe or clothing purchase from the online store.

What You Can Do



Manage Your Off-Facebook Activity

View activity shared with us by the businesses and organizations you visit off of Facebook.



Clear History

Disconnect off-Facebook activity history from your account.

More Options

Information About You



Ads and Businesses

Ad topics that are relevant to you, advertisers who have collected information directly from you, information you've submitted to advertisers and your interactions with businesses and organizations you visit off of Facebook.

Ads Interests

Advertisers Who Uploaded a Contact List With Your Information

Your Off-Facebook Activity



Search History

A history of your searches on Facebook

Your Search History



Location

Information related to your location

Location History



About You

Information associated with your Facebook account

Friend Peer Group

Your Address Books



Security and Login Information

A history of your logins, logouts, periods of time that you've been active on Facebook and the devices you use to access Facebook.

Where You're Logged In

Account Activity

Logins and Logouts

Administrative Records

Used IP Addresses

Datr Cookie Info

Authorized Logins

Login Protection Data

Other States

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

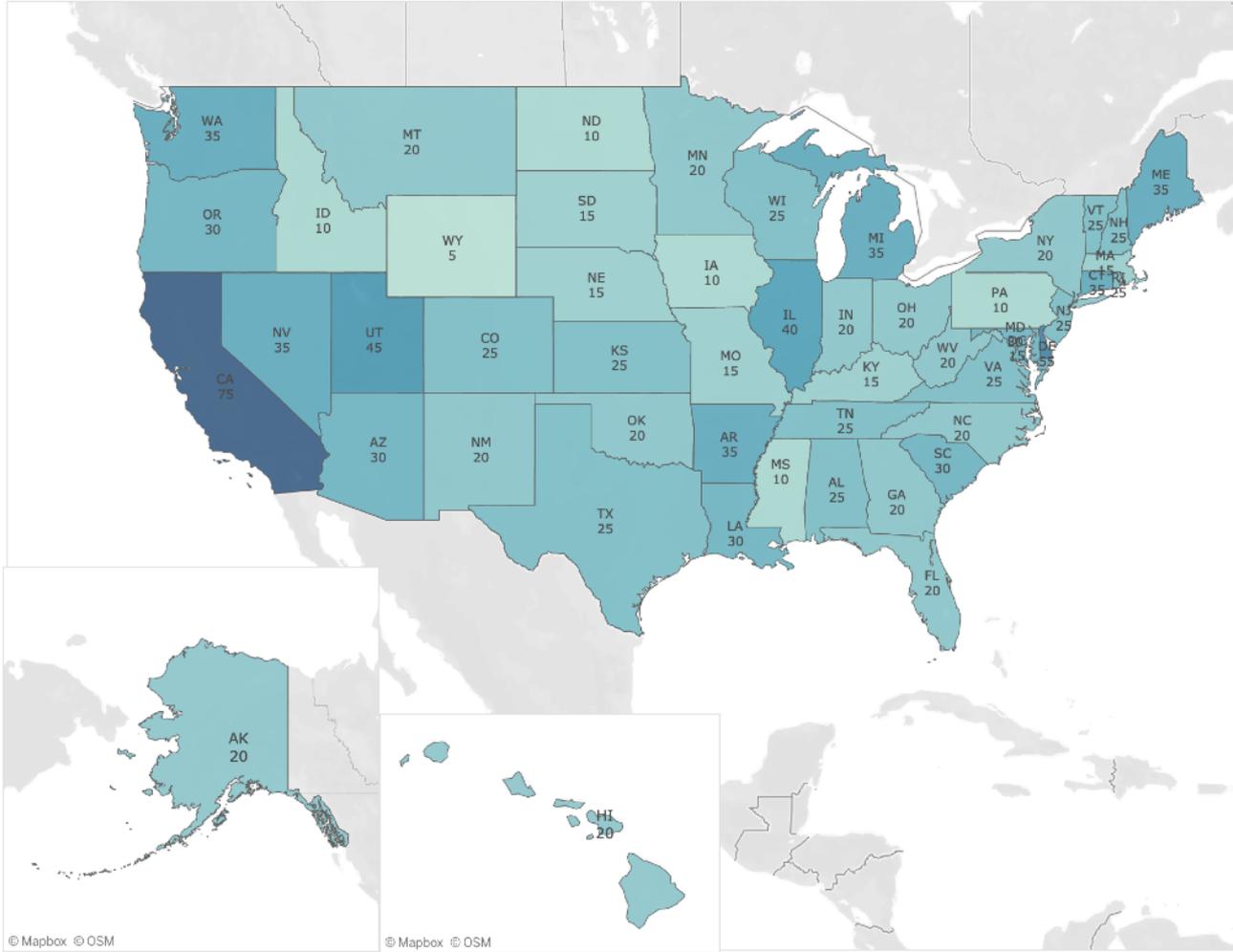


Other Countries

- PIPEDA (Canada)
- AAP (Australia)
- GDPL (Brazil)



Privacy by State scores, 2019



Best: California (75)

Worst: Wyoming (5)

US News & World Report

<https://www.usnews.com/news/best-states/articles/2019-10-23/states-with-the-strongest-online-privacy-laws>

Best practice in PX:
Privacy
Experience



PX: yet another (good) thing to know

- Plan for user privacy and security
- Budget for privacy
- Sharpen your site building routine
- 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

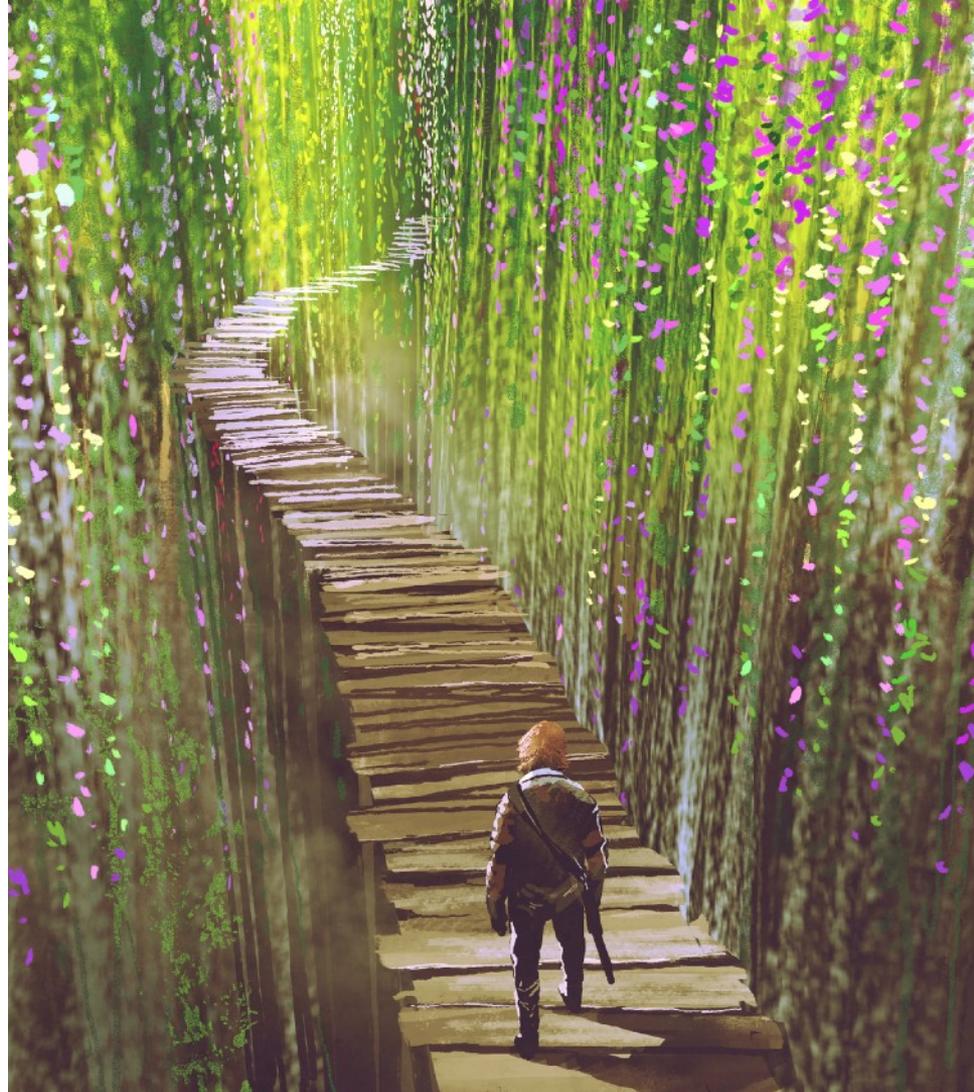
Set clear policies

- Opt-in to data collection (not out)
- Ample documentation
- Expiration dates on data
- Easy for understand what data is collected, how it is used
- Users can export personal data
- Easy to be forgotten



Plan for privacy

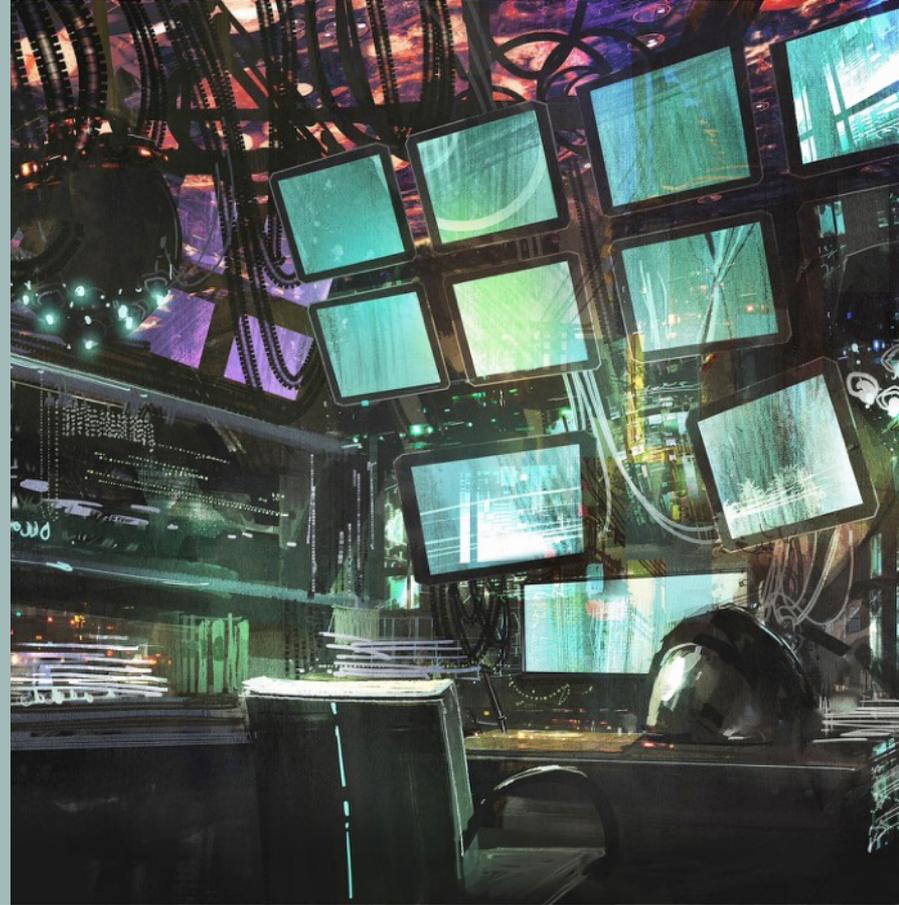
- Don't wait to end of project!
- Easy to understand
- List all data tracked
- Plan for disasters
- Try a policy creator

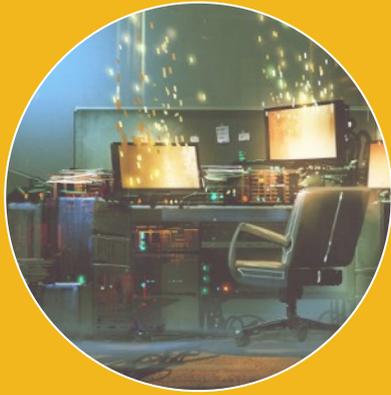


Accessibility isn't required everywhere yet either, but we do it because (a) it's the right thing to do and (b) it will be soon

Privacy Issues:

Technically Speaking





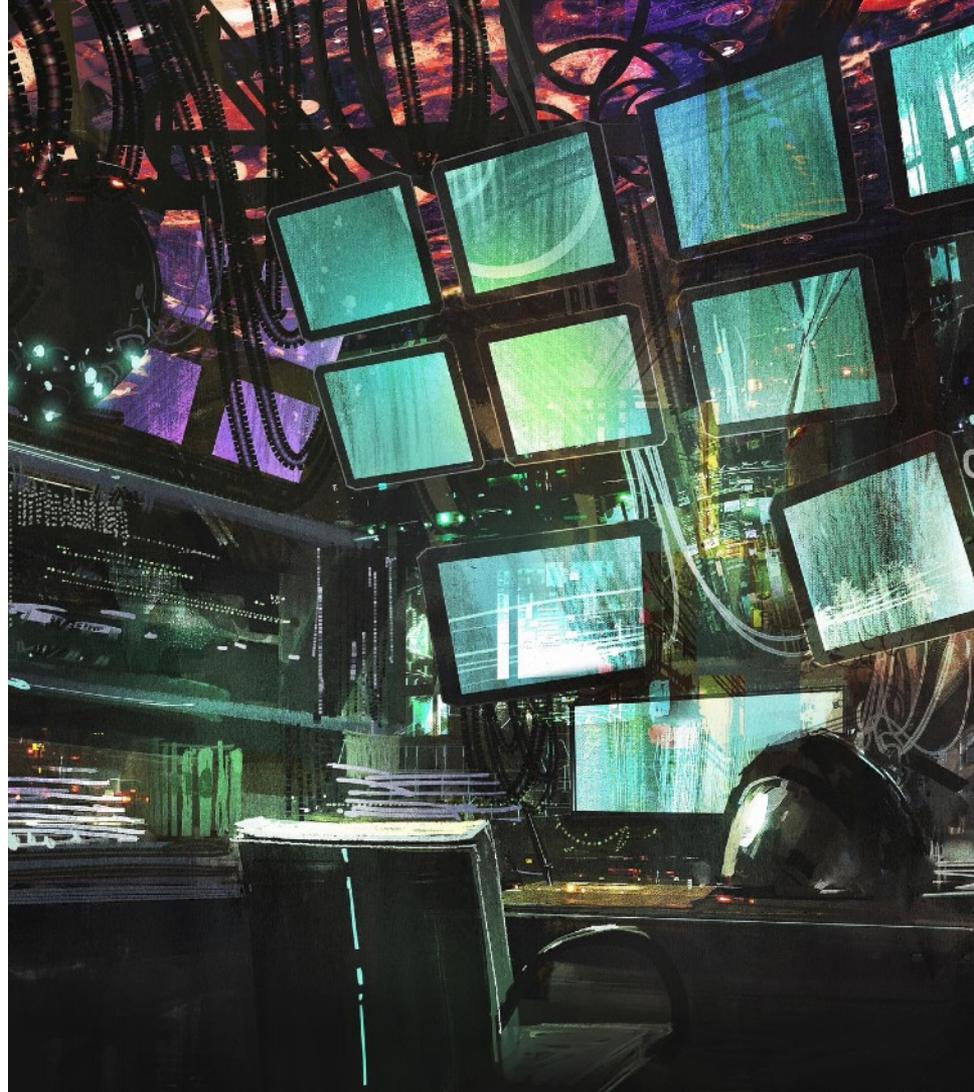
Developers

Change in process

- Plan how you manage PII and any data you collect
- Be conscious on how you protecting 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?





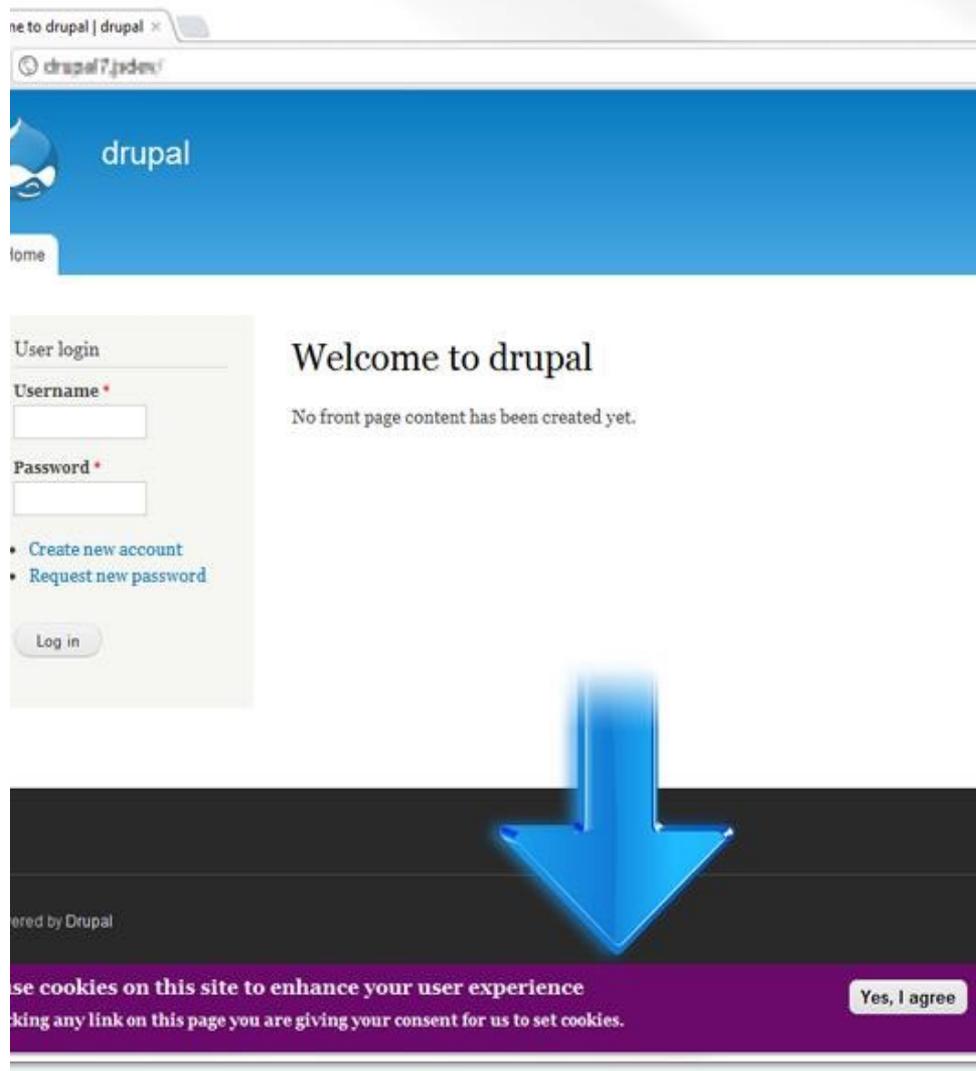
Cookies

The web's little spies

- First party and third party
- Tracking pixels/scripts
- 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
- wordpress.org/plugins/gdpr-cookie-compliance



The image shows a screenshot of the Drupal 7 homepage. At the top, there is a blue header with the Drupal logo and the word "drupal". Below the header, there is a "User login" form with fields for "Username" and "Password", and a "Log in" button. To the right of the form, there is a "Welcome to drupal" message and a note that "No front page content has been created yet." Below the login form, there are links for "Create new account" and "Request new password". At the bottom of the page, there is a dark purple footer with a white text box containing the message: "We use cookies on this site to enhance your user experience. Making any link on this page you are giving your consent for us to set cookies." and a "Yes, I agree" button. A large blue arrow points downwards from the top of the page towards the footer.

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?

Accept

More information

The screenshot shows the Mailchimp website with a cookie consent modal open. The modal is titled "How Mailchimp Uses Cookies" and contains the following text:

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.

The modal also features a table of contents with the following categories:

- How Mailchimp Uses Cookies
- Essential Website Cookies
- Performance and Functionality Cookies
- Advertising (Targeting) Cookies
- Analytics and Customization Cookies

At the bottom of the modal, there is a "Confirm My Choices" button and a "Powered by OneTrust" logo.

The background of the website shows the Mailchimp logo and the text "Bring your vision to life" and "smarter with Mailchimp."

At the bottom of the page, there is a footer with the following text:

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

There are also buttons for "CUSTOMIZE SETTINGS" and "ACCEPT ALL COOKIES".



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
- Don't collect IP addresses
- [Matomo](#) is open-source analytics you host yourself



Online Forms

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

- What data are you collecting?
For how long?
- How is it protected?
- Can users see what data you've collected?



Third Party

Libraries, packages and scripts,
oh my!



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

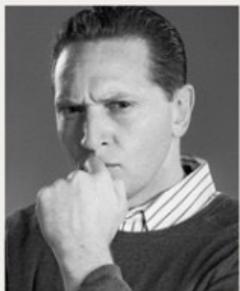




Be Privacy Smart

Encryption is your #1 weapon

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



Gavin Belson,
Founder

Gavin Belson has always been drawn to the most ethical practices of business. He worked tirelessly to change the world as CEO of Hooli, but realized it was time to use his talent and charisma in a life of public service. Since leaving Hooli behind, Belson has jettisoned the corruption of the tech industry to spread a more virtuous way of life.

Belson is no stranger to inventing new words and worlds, and his groundbreaking portmanteau "tethics" is only the tip of a very successful iceberg. He is a prolific author, recently penning a debut novel titled *Cold Ice Cream and Hot Kisses*. Belson is also an avid runner, agile biker, and adept swimmer, and recently won the HooliCares Triathlon, which was an event for charity.

The
Belson
Institute
of
TETHICS

TETHICS: A CODE OF CONDUCT



TETHICS is the promise to make best efforts to do everything in our power to enhance the quality of life for all ages, while maintaining our uncompromising principles while we grow. TETHICS is about fully investing in each other to inspire the human spirit. TETHICS is striving to meet and follow the principles below, in a worthy quest to make the world a better place.

- Integrity: We do the right thing. We are committed to the highest ethical standards.
- Excellence: We expect the best from ourselves and each other.
- Responsibility: We contribute to the growth, joy and enrichment of all the lives we touch.
- Courage: We dare to spark solutions that create a better, healthier world.
- Strength: Maintaining our uncompromising principles while we grow.
- Generosity: Contribute positively to our communities and our environment.
- Purpose: Build a society in which all people live with dignity and purpose, & fulfill their goals & dreams.
- Action: Champion positive social change & deliver value through advocacy, information, & service.

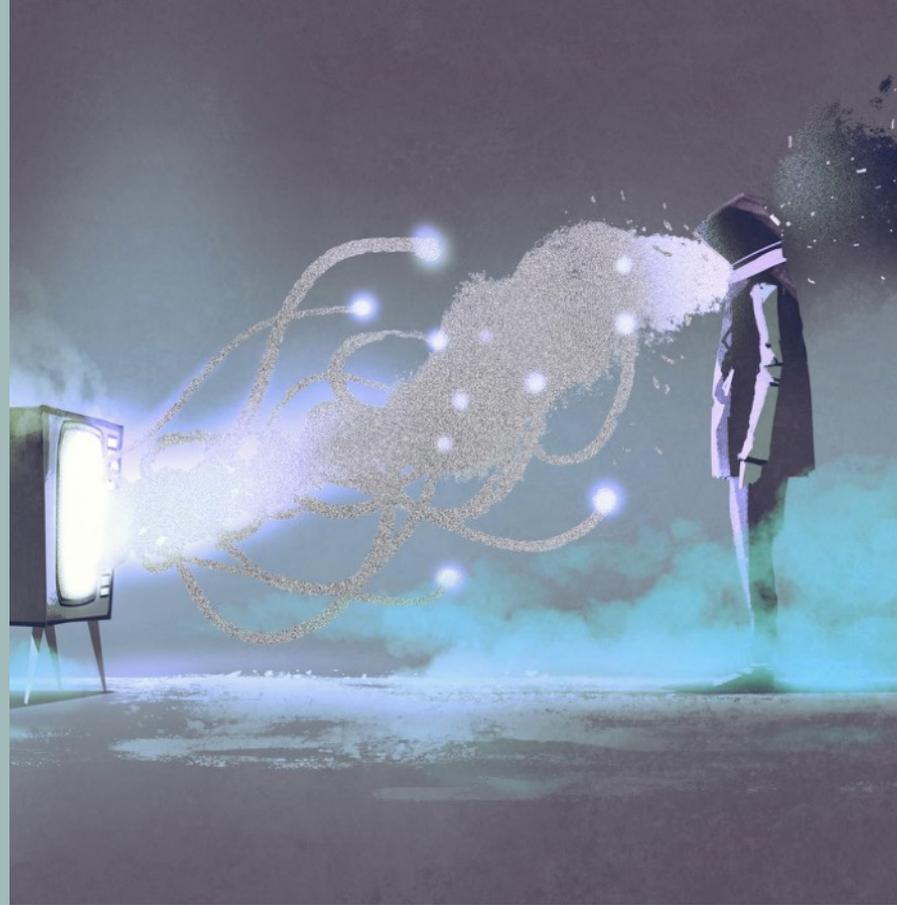


Drupal-specific

Modules and more

- GDPR compliance team
- Encrypt module
- Cryptolog
- IP anonymize
- Blizz Vanisher
- Drush sql-sanitize
- Faker
- Guardr (security distribution)

Final Takeaways



Does Privacy Still Matter?

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



Thank you!

Questions



PLEASE PROVIDE YOUR FEEDBACK!

mid.camp/6285

The top rated sessions will be captioned, courtesy of
Clarity Partners

Additional Resources

- [Think your website is GDPR compliant? Think again](#)
- [The GDPR is here. Are you ready? \(You need to be!\)](#)
- [How GDPR will change the way you develop](#)
- [Major GDPR fines](#)
- [California Consumer Privacy Act \(CCPA\): What Does It Mean For You?](#)
- [CCPA off to rocky start](#)
- [Major privacy breaches](#)
- [Behind the one-way mirror: technology of corporate surveillance](#)