The Battle for Online Privacy

GDPR and Privacy 1+ year later

ELECTRIC CITIZEN

About Me

Dan Moriarty

- CEO & Creative Director at Electric Citizen
- Web design for 20+ years
- Drupal for 10+ years
- Twitter: @minneapolisdan
- Drupal: minneapolisdan

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 experts
- ElectricCitizen.com

ELECTRIC
CITIZEN

What We'll Cover

The Battle for Online Privacy

- Why privacy still matters
- GDPR: what does it mean and what has changed since it became law
- PX: defining the privacy experience
- CCPA: privacy for the USA
- Drupal-specific topics around privacy laws

ELECTRIC CITIZEN

What led to new laws?

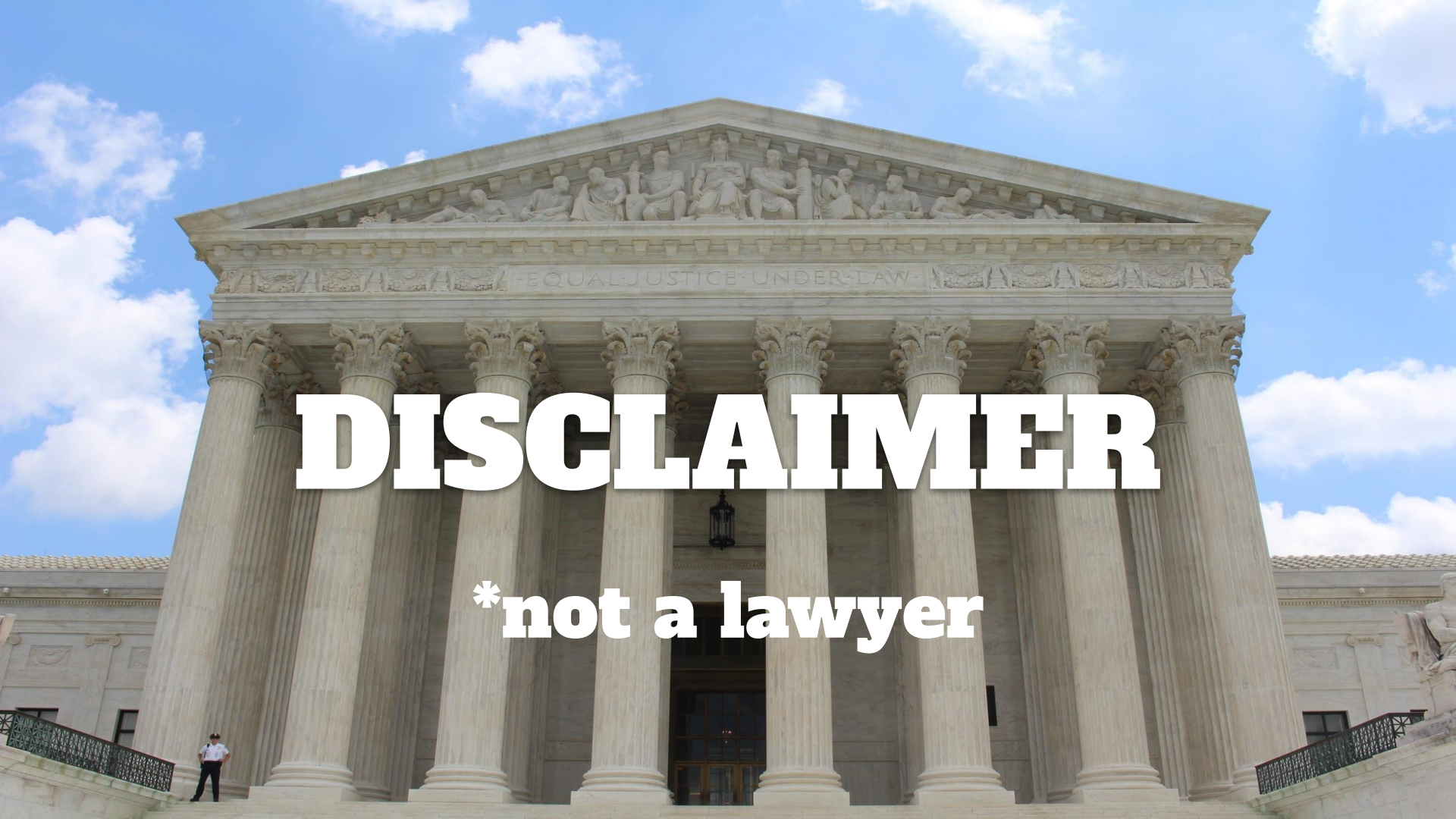
- Replacing outdated privacy laws
- Data breaches at Yahoo, Facebook, Equifax
- Impossible to read (or non-existent) privacy policies
- Unprecedented data collection
- Companies like Cambridge Analytica, FaceApp

EQUIFAX

YAHOO!

Cambridge Analytica

ELECTRIC CITIZEN



DISCLAIMER

*not a lawyer

Before we begin...

Does Privacy Still Matter?

ELECTRIC CITIZEN

“Privacy is dead” … we just have to lean in to that reality – Erik Qualman

ELECTRIC CITIZEN

Is Privacy Dead?

- Everything is exposed and shared
- “I have nothing to hide” so what’s the problem
- I get free services in exchange for tracking my data
- Personalized ads based on my behavior, better than random ads
- Facial recognition, tracking software
- Genie is out of the bottle, can’t put it back in

ELECTRIC CITIZEN

Most people are willing to sacrifice privacy in return for convenience

– Jameson Lopp

ELECTRIC CITIZEN

Digital Stalkers

- Picture someone following you the entire day and recording:
  - What you eat
  - Where you drive
  - Who you meet with
  - How you work
  - What you read
  - What you think

ELECTRIC CITIZEN

Privacy Online vs “Real World”

- Stalking someone in person is against the law, and universally decried as wrong
- Buying and selling your personal information for profit online is not.
- Why? What’s the difference?

ELECTRIC CITIZEN

Why is Privacy Online Important?

- Privacy is a limit on power + control
- Privacy is about respect for others
- Privacy = freedom of expression
- Privacy protects vulnerable groups
- We don’t know what personal information may become an issue

ELECTRIC CITIZEN

Privacy is for everyone!

- You may not get hurt by privacy, but other could be
- Web developers, site owners, organizations all have a role to play!

ELECTRIC CITIZEN

Back in the

GDPR

ELECTRIC CITIZEN

Who remembers when the GDPR took affect?

- General Data Protection Regulation, effective since May 2018
- Give users rights to their personal data
- Protects anyone with a temporary or permanent residence in the EU

ELECTRIC CITIZEN

What effect did it have on you? Any?

- Wow! Big, game changing event for global privacy, **OR**
- Wut? Confusing, easy to ignore, technical, legal mumbo jumbo

ELECTRIC CITIZEN

Summary of Protections and Rights

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

ELECTRIC CITIZEN

GDPR: Who needs to comply?

- 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

ELECTRIC CITIZEN

GDPR: Who does NOT need to comply?

- Governments, law enforcement
- Data for personal use
- Organizations with no connection to EU residents

ELECTRIC CITIZEN

What's Happened Since

- **Fines** has been issued: $359 billion!
  - Marriott, $99 million
  - British Airways, $183 million
  - Google, $50 million
- New/renewed focus on **Privacy Experience (PX)**
- **Additional EU laws** being approved
- **New laws in the USA** (CCPA)

ELECTRIC CITIZEN

GDPR Lessons to Remember

- “GDPR is a journey, not a destination, and ongoing compliance is required”
- Can apply to any size business
- Organizations must be prepared to respond to breach in data
- Rethink how you handle personal data

ELECTRIC CITIZEN

Focus on PX:

Privacy Experience

ELECTRIC CITIZEN

Attn: Site Owners, Web Developers, Editors, QA, Trainers, etc.

We have access to a lot of personal data when building or maintaining a website.

How careful are we with it?

ELECTRIC CITIZEN

PX: yet another (important) thing to know

- Just like accessibility, responsive design, UX, site performance, etc.
- PX needs to become part of every web project
- Plan for user privacy and security
- Protect PII (Personally identifying information)

ELECTRIC CITIZEN

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)

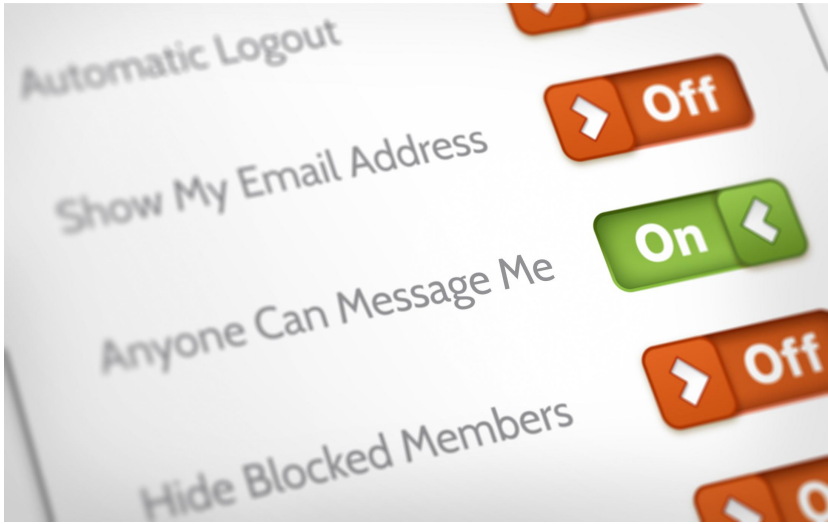
Info Combined with Previous Column:

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

ELECTRIC CITIZEN

PX: Follow transparent policies

- Opt-in to data collection, not opt-out
- Provide ample documentation
- Set expiration dates on data
- Easy for understand what data is collected, how it is used
- Users can view what data is saved
- Users can export personal data
- Easy for users to be forgotten



ELECTRIC CITIZEN

PX: Handling PII

- As Needed -- only collect personal data you need at this time
- Pseudonymization -- don’t attribute personal data to individuals in your records
- Data minimization -- don’t expose or use personal data except when needed
- Technical Planning - decide before launch how to handle

The GDPR is here. Are you ready? (You need to be!) -- Ochen Kaylan

https://youtu.be/CyIFNsSHPxQ

ELECTRIC CITIZEN

PX: Plan for disasters

- How will you respond to data breach
- Consult with lawyers
- Have someone in charge of privacy

ELECTRIC CITIZEN

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

ELECTRIC CITIZEN

Privacy in the USA

CCPA

ELECTRIC CITIZEN

Who’s Ready for the CCPA?

- California Consumer Privacy Act
- Effective Jan 1st, 2020!

ELECTRIC CITIZEN

CCPA: What Does it Do?

- **Establish privacy rights for residents of California, including rights to:**
- Know what personal data is collected
- Know if data is sold or disclosed to others
- Opt out of sale of your personal data
- Request your personal data be deleted
- Not be discriminated against for exercising privacy rights

ELECTRIC CITIZEN

CCPA: Who Must Comply?

- For-profit businesses that collect personal data and do business in CA
- AND:
  - Annual revenues over $25 million, **OR**
  - Possess personal info of 50,000 or more people/households/devices, **OR**,
  - Earn more than half your revenue selling consumer's personal information

ELECTRIC CITIZEN

CCPA: Who is Exempt?

- Non-profits
- Organizations who have no consumers residing in CA, or residents of CA

ELECTRIC CITIZEN

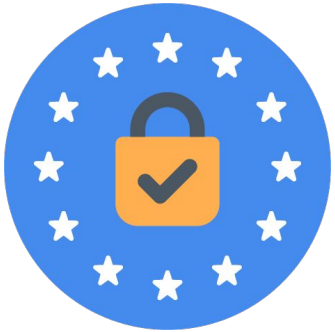
CCPA: Meeting the Requirements

- 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

ELECTRIC CITIZEN

CCPA vs GDPR

- EU vs California
- CCPA only covers info provided by consumers, not data purchased from third parties
- CCPA exemptions for nonprofits, extremely small businesses

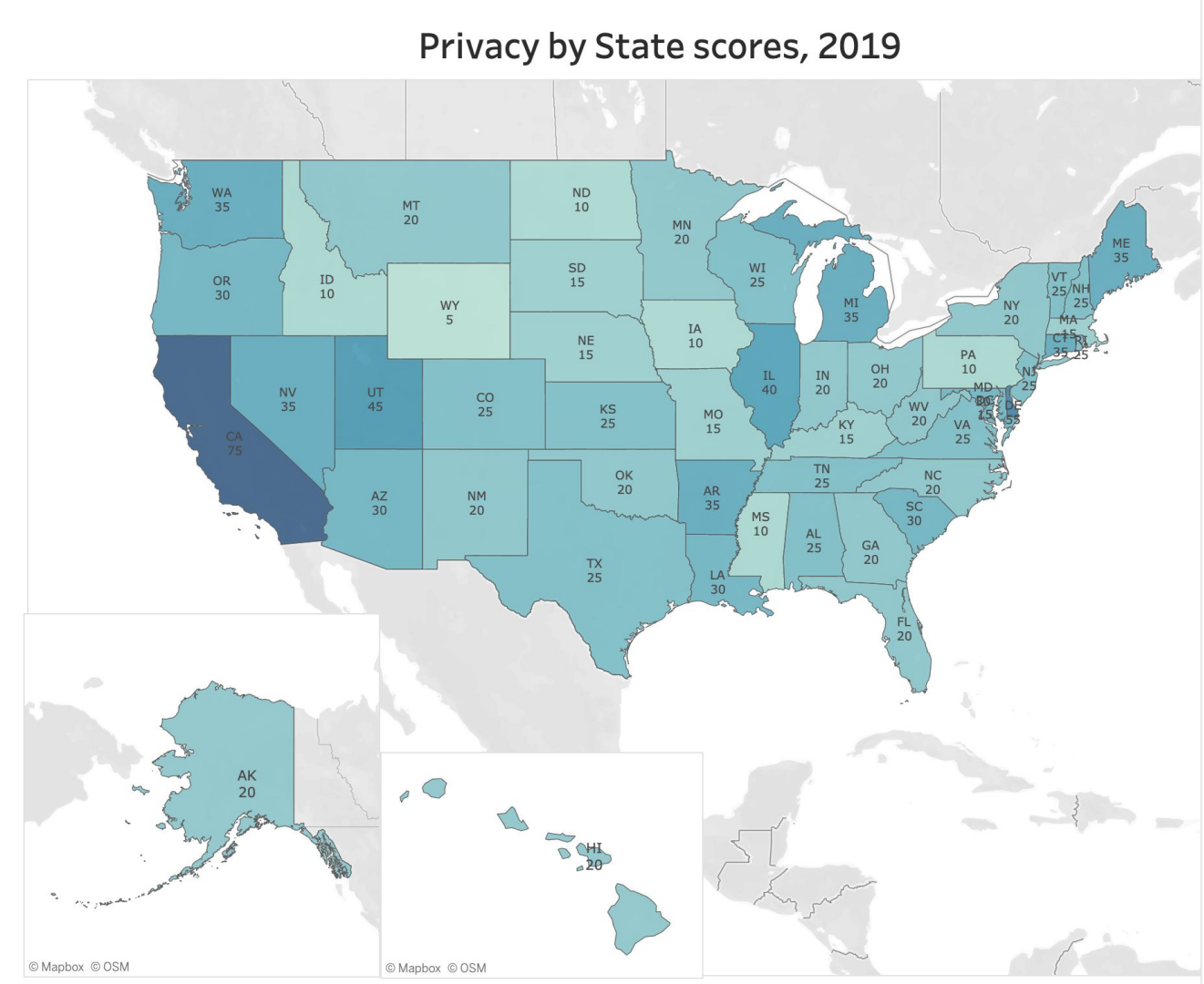


ELECTRIC CITIZEN

Other States Next Up?

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

ELECTRIC CITIZEN



Best: California (75)

Worst: Wyoming (5)

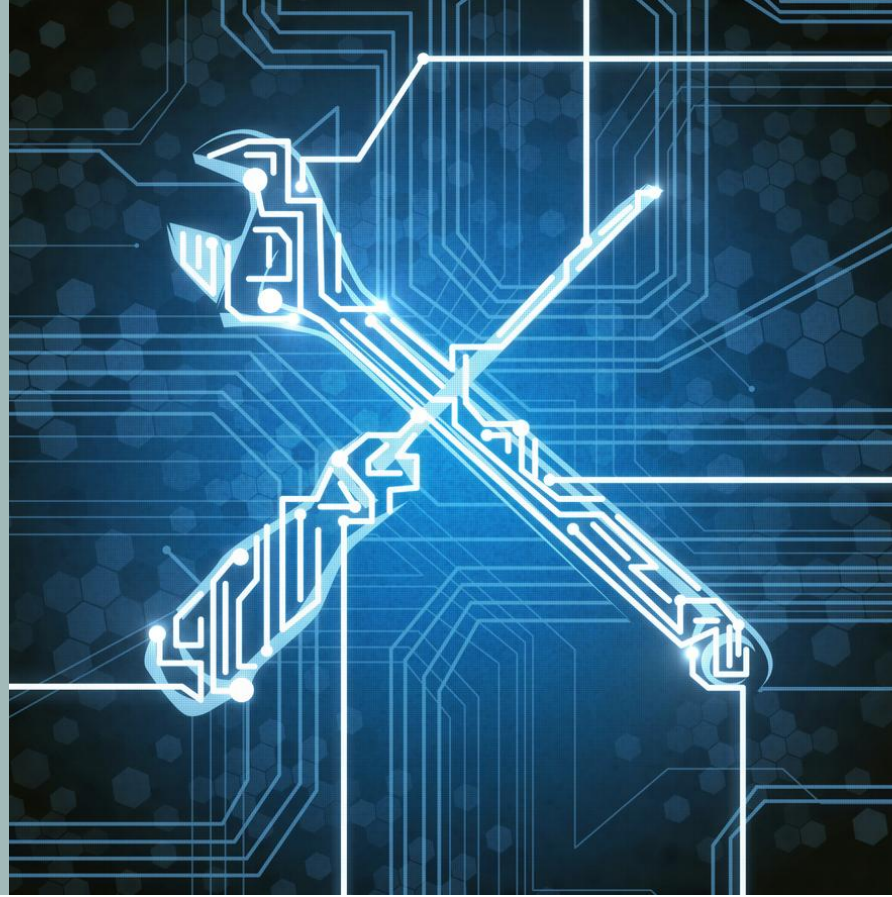
Iowa tied for the second-lowest score :(

US News & World Report

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

Web-specifics:

Technically Speaking



ELECTRIC CITIZEN

Cookies

The web's little spies

- Both GDPR and CCPA require you disclose use of cookies
- Cookies required to make site function do NOT require consent (e.g. shopping cart)
- Any other use DOES require consent (e.g. analytics)

ELECTRIC CITIZEN

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

ELECTRIC CITIZEN

Drupal-specific

Modules and initiatives

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

ELECTRIC CITIZEN

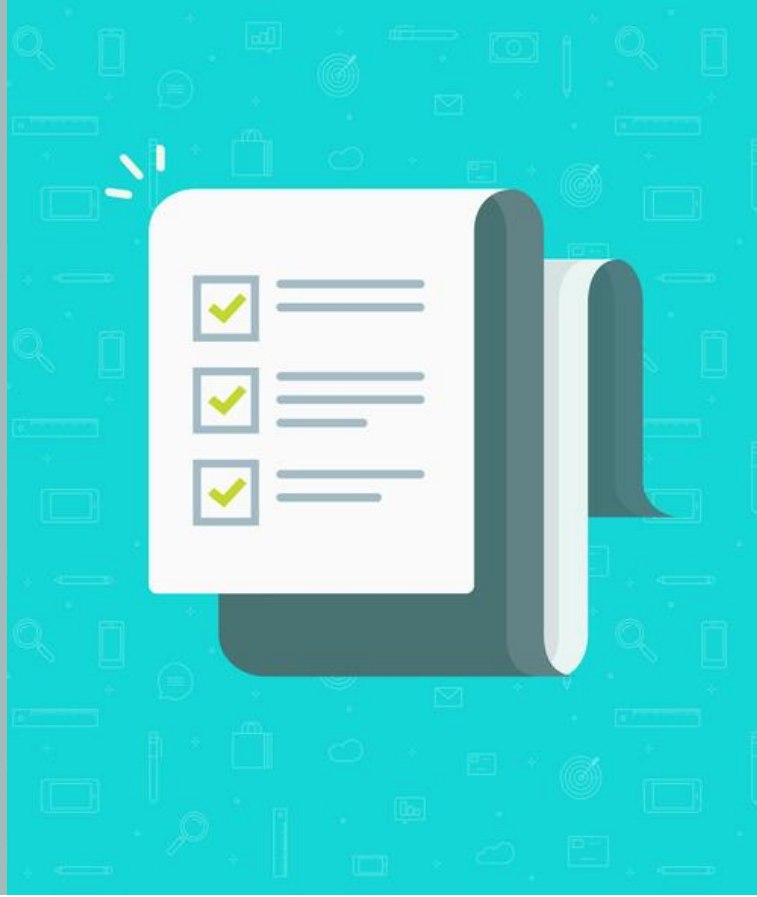
Other privacy practices

Tips for websites

- Use HTTPS, prevent ISPs or others spying on your activity
- Don’t embed YouTube player on page or it will track activity regardless of use
- Avoid APIs and third-party libraries without privacy by design
- Don’t collect more data than is needed
- Have a privacy policy in place!

ELECTRIC CITIZEN

Final Takeaways



ELECTRIC CITIZEN

Does Privacy Still Matter?

- Citizens and their legislators are saying it does
- New laws are saying it does
- Privacy experience is something that can apply everywhere
- It’s not dead yet!

ELECTRIC CITIZEN

Thank you!

Questions

ELECTRIC CITIZEN

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
- California Consumer Privacy Act (CCPA): What Does It Mean For You?

ELECTRIC CITIZEN