

Privacy Challenges in the Age of Data Breach for State and Local Government

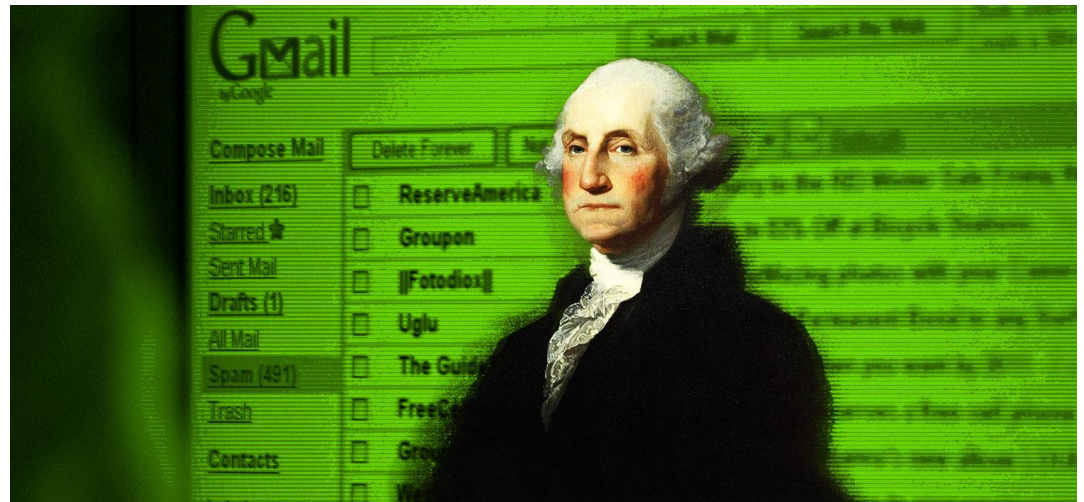
PNWER, Victoria, B.C.

Nov. 7, 2017

Alex Alben

Chief Privacy Officer

Washington State



Office of Privacy
& Data Protection

Washington State

Predicting the Future

- The security environment is evolving in one direction– things are getting worse, not better.
- State resources are not likely to keep up with the proliferation of data– both in volume and in new formats.
- More government functions and services will be data-driven.



Cyber crime and data breach

Data Breaches Happening at Record Pace

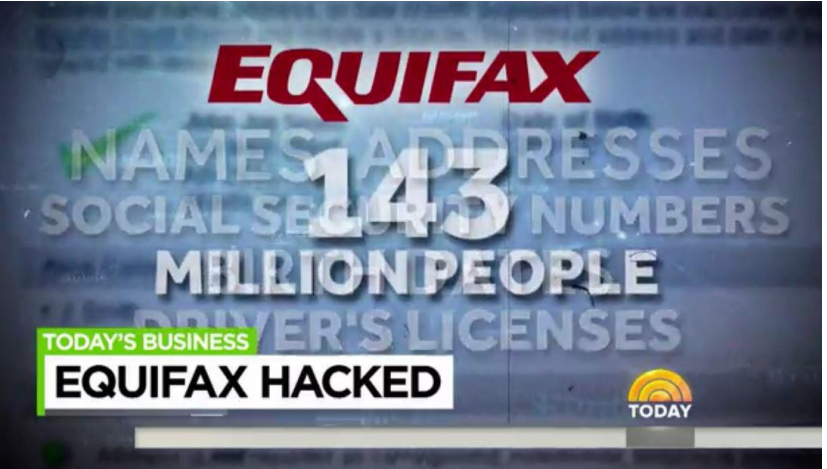
by HERB WEISBAUM

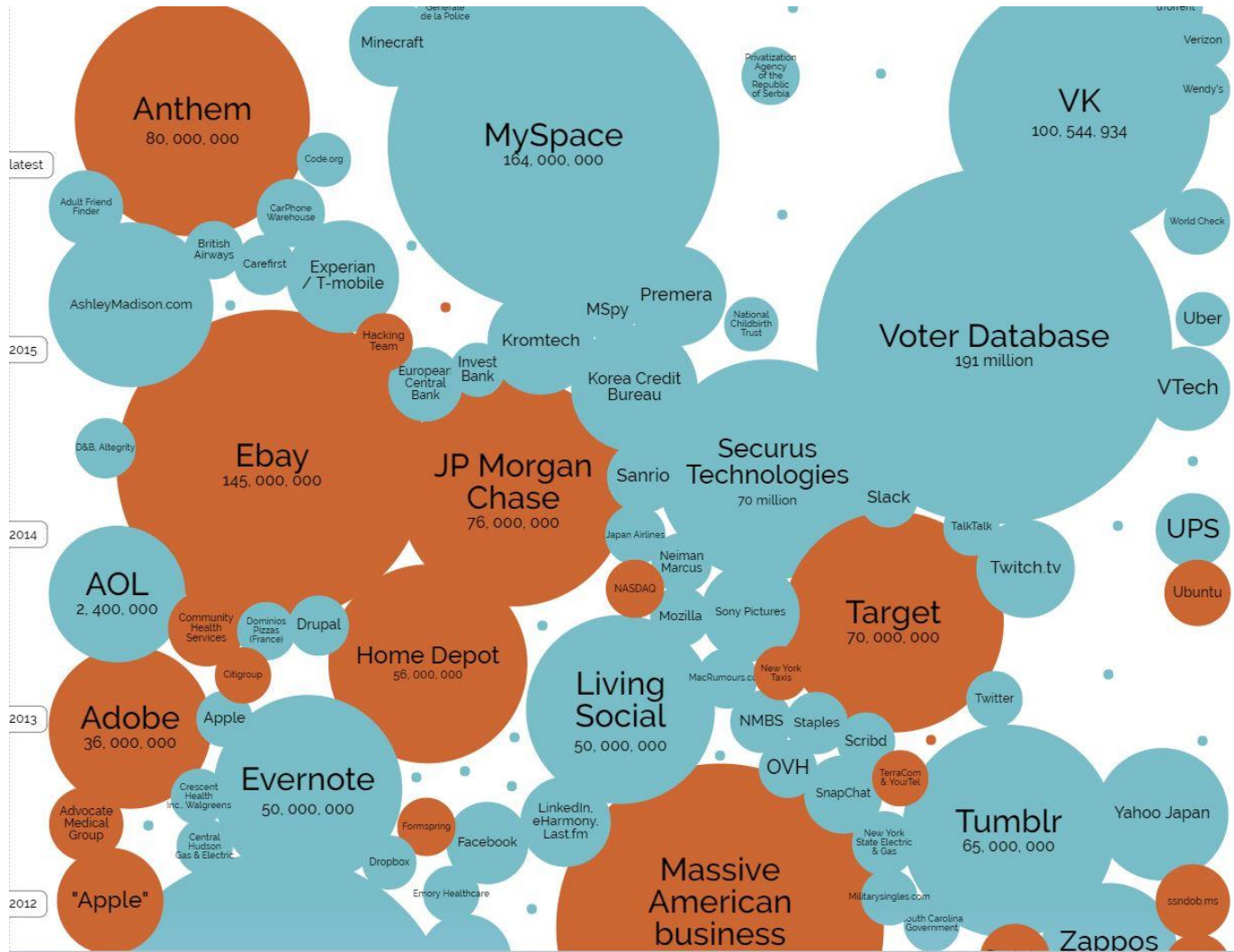
The number of data breaches in the U.S. jumped 29 percent in the first half of this year, hitting a record high of 791, according to a new report from the Identity Theft Resource Center and CyberScout, the data risk management company.

"Frankly, I was surprised at how significantly the number of breaches has grown," said Eva Velasquez, ITRC's president and CEO. "We knew this was a trend, we knew that the thieves would continue to find this lucrative, but the sheer volume of growth has been really surprising."



To
30
15
5/
\$2
\$3
■





With very few consumer remedies

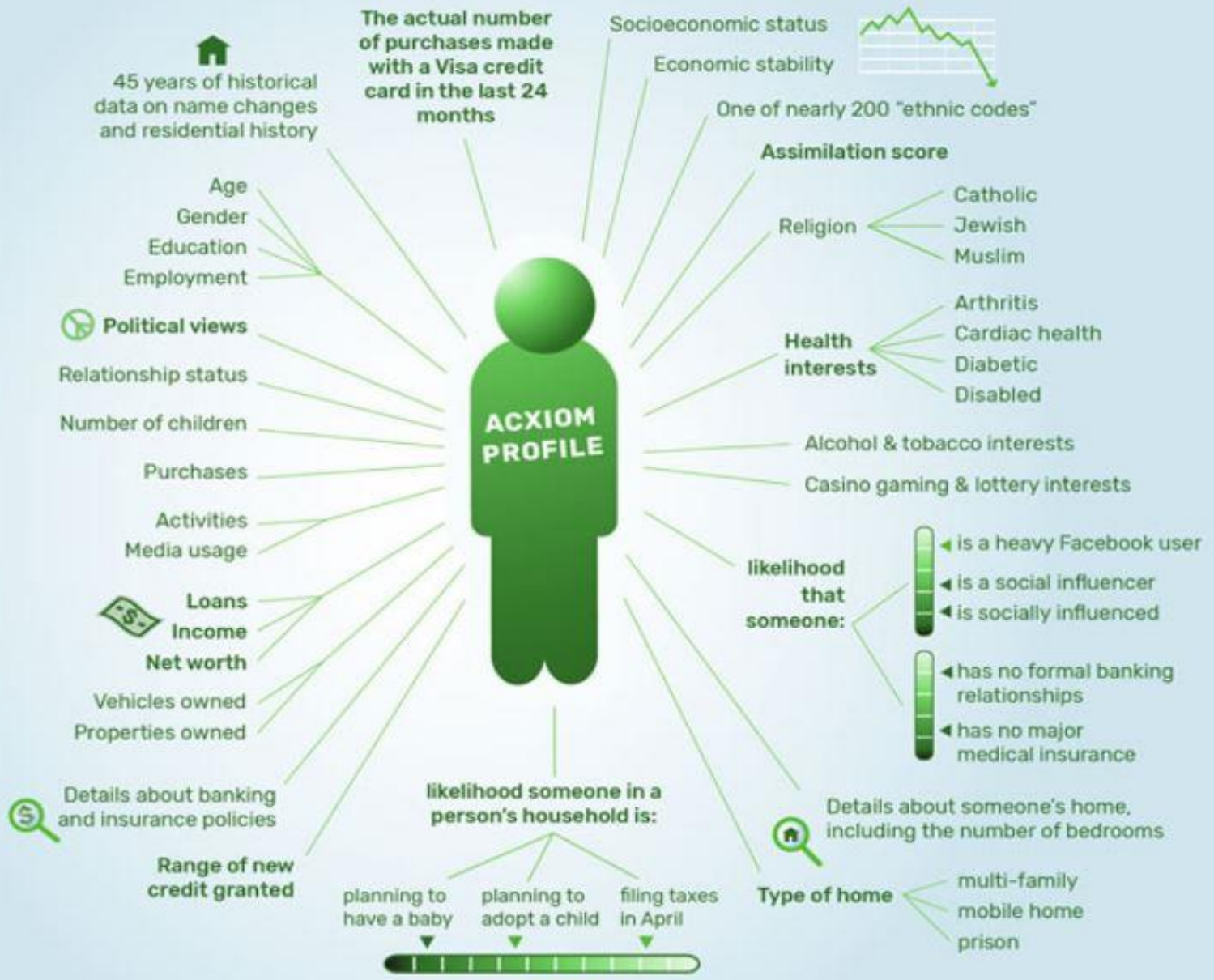
- Notice of Breach
- Credit Monitoring
- Credit Freeze
- Wait for a class action suit

How did we get here?

- Our analog data became digital: 1990-2017
- The Internet loves data.
- Data profiling and data brokers.
- No consistent security standards, either within borders or outside borders.
- It pays to be a hacker . . .

Scope of data profiling:

Large Online Platforms			
Facebook	has profiles on	<u>1.9 billion</u>	Facebook users
		<u>1.2 billion</u>	Whatsapp users
		<u>600 million</u>	Instagram users
Google	has profiles on	<u>2 billion</u>	Android users
		<u>1+ billion</u>	Gmail users
		<u>1+ billion</u>	YouTube users
Apple	has profiles on	<u>1 billion</u>	iOS users
Credit Reporting Agencies			
Experian	has credit data on	<u>918 million</u>	people
		<u>700 million</u>	people
		<u>2.3 billion</u>	people
Equifax	has data on	<u>820 million</u>	people
		<u>1 billion</u>	devices
TransUnion	has data on	<u>1 billion</u>	people
Consumer Data Brokers			
Acxiom	has data on	<u>700 million</u>	people
		<u>1 billion</u>	cookies and mobile devices
	it manages	<u>3.7 billion</u>	consumer profiles for clients
Oracle	has data on	<u>1 billion</u>	mobile users
		<u>1.9 billion</u>	website visitors
	provides access to	<u>5 billion</u>	“unique” consumer IDs



Acxiom provides of up 3,000 attributes and scores on 700 million people in the US, Europe, and other regions.

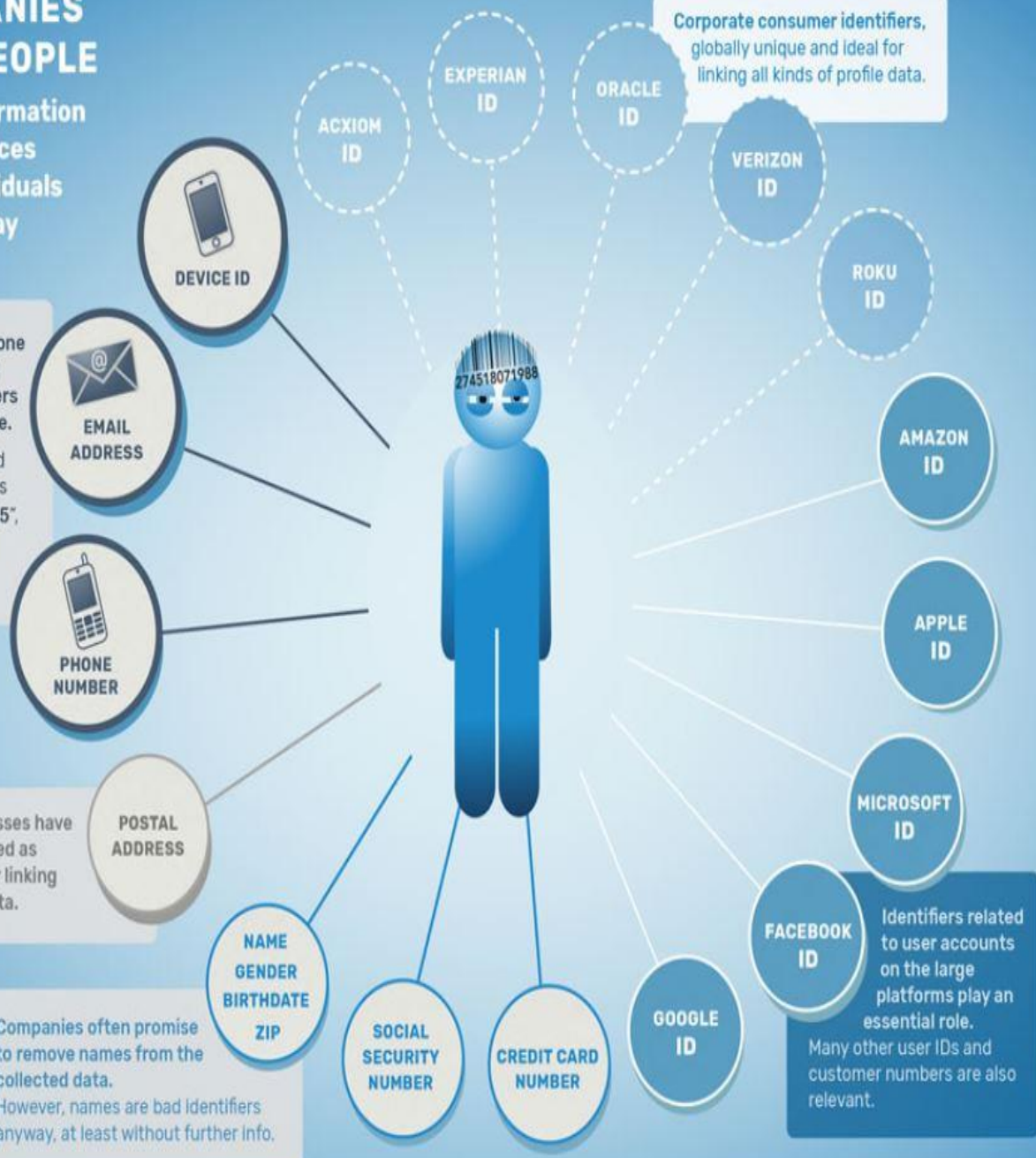
HOW COMPANIES IDENTIFY PEOPLE

to link profile information from various sources and monitor individuals throughout the day

Email addresses and phone numbers are among the most important identifiers used to recognize people. They are often converted into pseudonyms such as "e907c95ef289bxw2345", which can still serve as personal ID numbers.

Postal addresses have long been used as key nodes for linking consumer data.

Companies often promise to remove names from the collected data. However, names are bad identifiers anyway, at least without further info.



Many other kinds of temporary identifiers are used to track people across websites, platforms and devices:

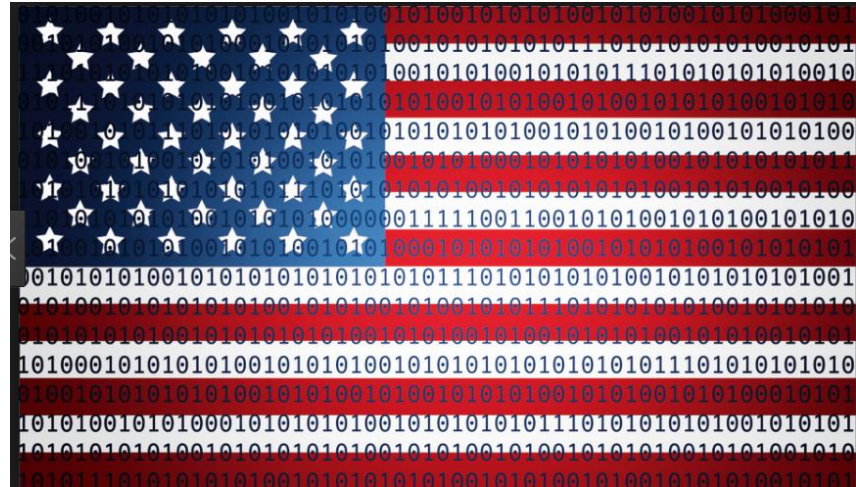
- Cookie IDs
- Device Fingerprints
- IP Addresses
- Browser Fingerprints

People can also be (re)identified through calculating digital fingerprints from behavioral data:

- Websites visited
- Apps in use
- Videos viewed
- Purchase History
- Contacts added
- Places visited

Government collection of data

- Federal, State & Local



Local Surveillance

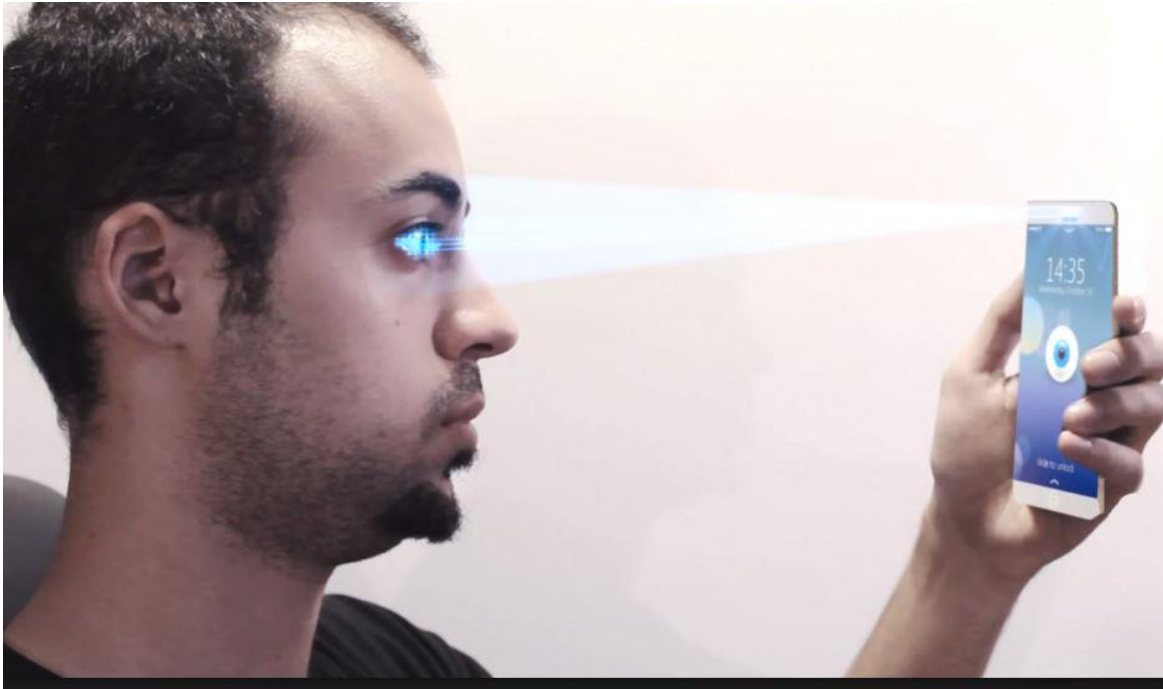
- Drones
- Body Cameras
- Traffic cameras
- Plate readers
- Smart Cities



“Alexa, go to the next slide!”



Biometric Identifiers



- Unique to the Individual--unlike other “personal” data.
- Cannot be changed
- Already in widespread use.

Washington is already using biometric identifiers



We're using facial recognition to protect your identity

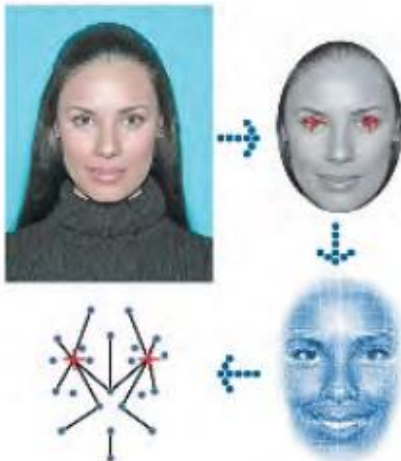
The Department of Licensing (DOL) uses facial recognition as part of our ongoing efforts to prevent individuals from obtaining multiple licenses or ID cards or attempting to obtain a license or ID in the name of another Washington resident. DOL is committed to doing everything it can to combat identity theft and protect the identities of Washington residents.

How does the facial recognition system work?

Using your regular driver license or ID card photo, the system creates a digital template using a precise map of facial features that aren't easy to alter, such as eye sockets, cheekbones and sides of the mouth.

Before a new license is issued, the system compares the template it creates to all the templates currently in our database and determines if someone is applying for a license using a name other than their own. When mismatches are detected, the system flags them for review by specially-trained DOL staff.

DOL's facial recognition system is designed to be an accurate, non-obtrusive fraud detection tool. When staff investigators confirm an individual may have more than one identity in our system,



- ▶ Enhanced drivers license
- ▶ Fingerprints
- ▶ Background checks
- ▶ Iris photography
- ▶ Two new state laws passed in 2017 address biometrics.

Questions for every data collector:

- Who keeps our data?
- Can it be shared?
- Can it be sold?
- How long is it retained?
- Is it really “anonymized?”
- Can a person update or delete their data once it is sent?
- How secure is it?

Washington State Structure

- State Constitution
- Public Records Act
- Data Breach Law
- One of a five states to have a Chief Privacy Officer



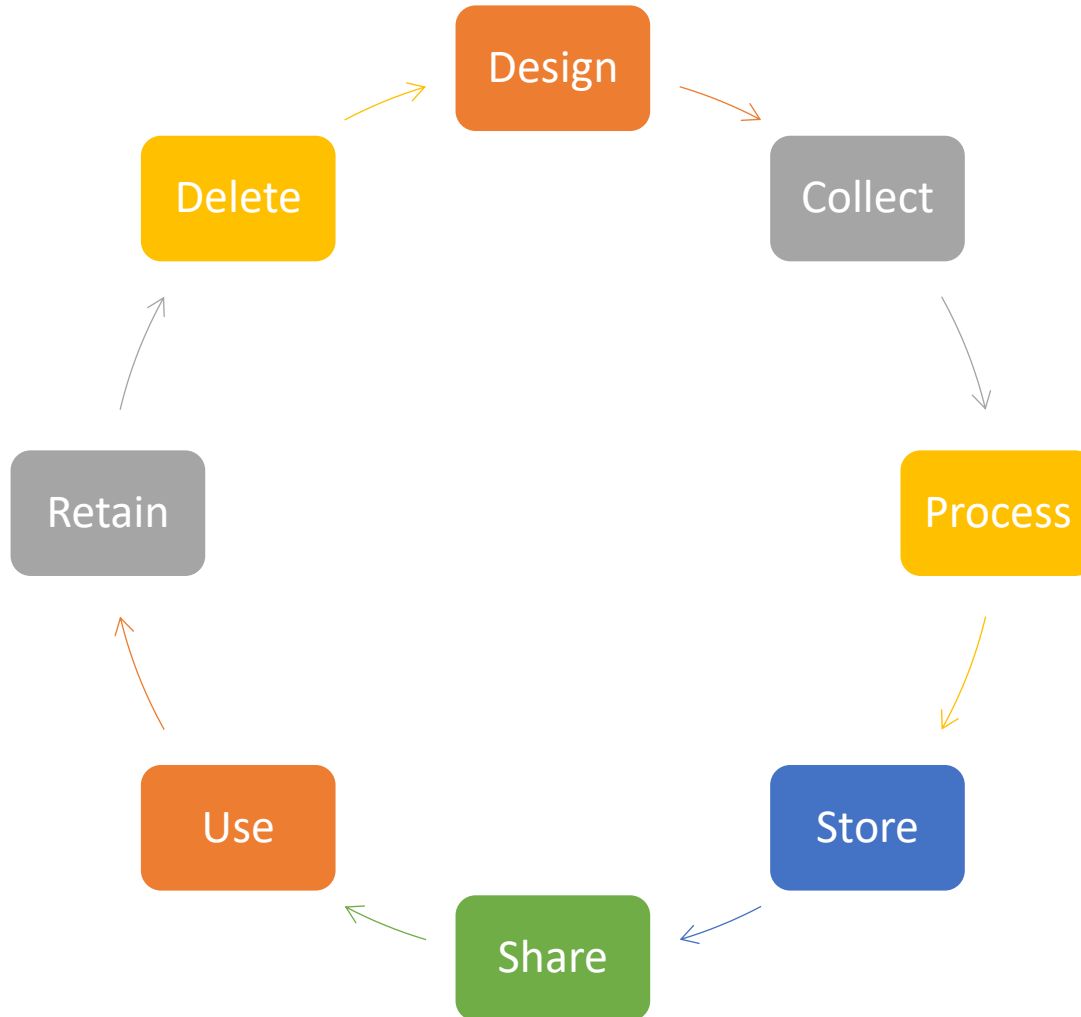
What do we do well:

- Cooperation between CISO, CPO and Governor's Office.
- Cooperation with forward-looking legislators.
- Formation of cross-agency Privacy Working Group.
- Consumer outreach and privacy.wa.gov
- Good relationship with academic world.
- Response to data breach.
- Trying to get ahead of the policy curve on mobile devices and the Internet of Things.

What do we don't do well:

- Monitoring inter-agency data sharing.
- Limiting collection of data to an “as needed” basis.
- Understanding the Life Cycle of Date.
- Privacy Assessments.
- Enforcing policies throughout state government and related entities, e.g. data back-up policies.
- Monitoring contractors.
- Reforming the Public Records Act to protect privacy and critical infrastructure.

Data Life Cycle





What tools are at our disposal?

- ① Privacy by design
- ② Data minimization
- ③ Anonymize personal data for analytics
- ④ Greater cooperation between agencies, including law enforcement
- ⑤ Work sessions for legislators
- ⑥ Privacy training across state government

Comments and questions?

Alex Alben

alex.alben@ocio.wa.gov



**Office of Privacy
& Data Protection**

Washington State