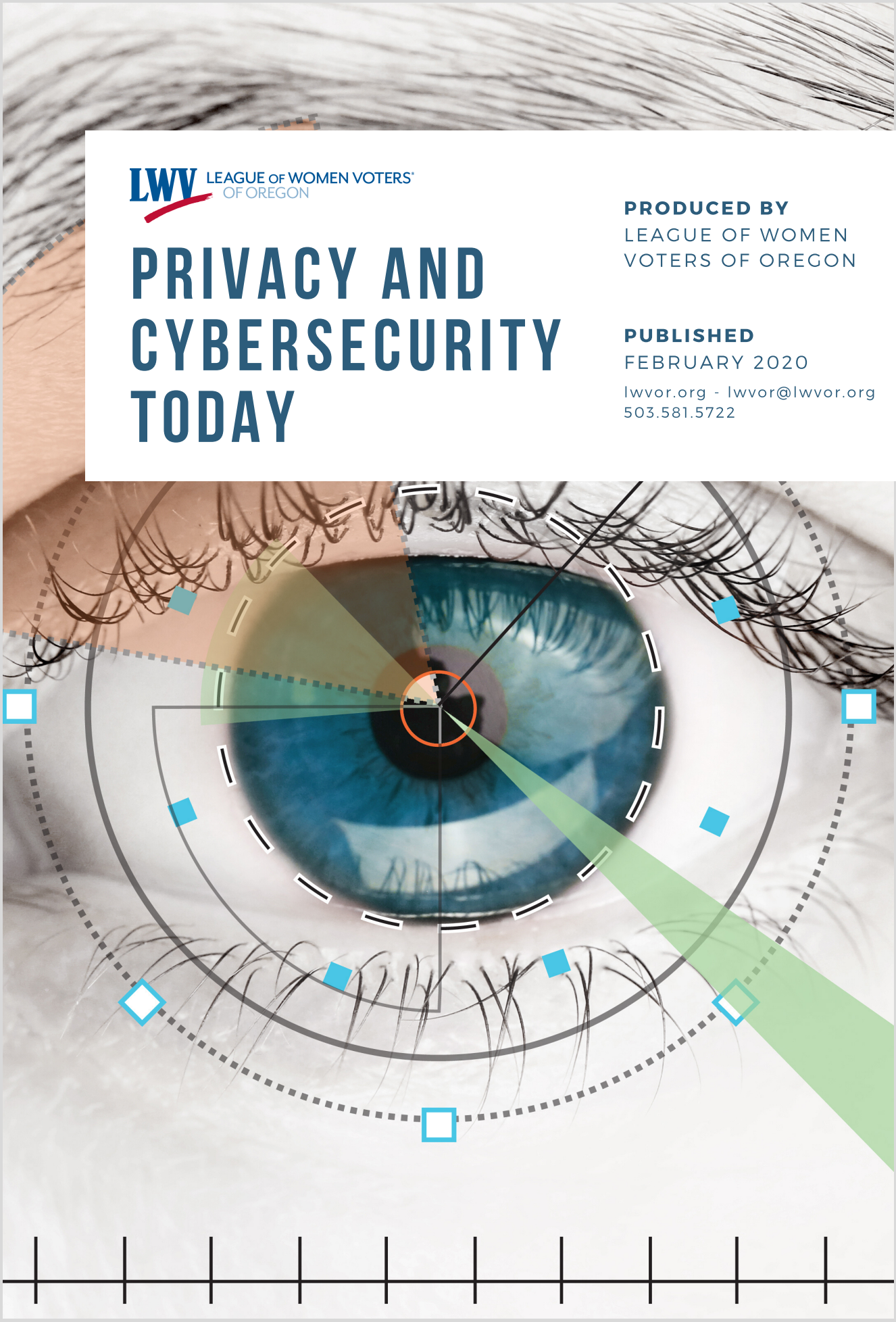


LWV LEAGUE OF WOMEN VOTERS® OF OREGON

PRIVACY AND CYBERSECURITY TODAY

PRODUCED BY
LEAGUE OF WOMEN VOTERS OF OREGON

PUBLISHED
FEBRUARY 2020

lwvor.org - lwvor@lwvor.org
503.581.5722

Privacy and Cybersecurity Today

TABLE OF CONTENTS

INTRODUCTION 4
I. PRIVACY 5
Changing Views of Privacy 5
Privacy and Personal Information Today 6
Informed Consent for Research and Patient Medical Records 6
II. TECHNOLOGY TODAY 8
Common Vulnerabilities - Data Breaches, Ransomware, and Hackers 8
Data Breaches 8
Ransomware 9
Hackers 9
Social Networking 9
Your Data Is Being Tracked 10
Big Data, Big Impact 10
Internet of Things (IoT) - Using Embedded Technology 11
E-Commerce 12
Surveillance and Privacy 15
Biometrics 17
Fake News and Deepfakes 19
Can We Believe What We See and Hear? 20
Technology That “Thinks” 20
III. ELECTIONS, POLITICAL ACTIVITY, AND THE CENSUS 22
Protecting Elections in the Cyber Era 22
Disinformation and Foreign Interference 22
Election Cybersecurity 23
Political Privacy 24
Nonpartisanship Policies 24
The 2020 US Census 25
IV. POLICY ACTORS: Governmental, Non-governmental, & Industry 26
European Union (EU): General Data Protection Regulation (GDPR) 26

NATO Cooperative Cyber Defence (sic) Centre of Excellence 27
NGOs Global 27
Center for Democracy and Technology (CDT) 28
Data & Society (D&S) 28
Digital Advertising Alliance (DAA) 28
Interactive Advertising Bureau (IAB) 28
World Privacy Forum 29
US Federal Privacy and Cybersecurity Governance 29
Review of Federal Privacy Legislation and Regulatory Agencies 29
The Department of Homeland Security (DHS) 31
Cybersecurity and Infrastructure Security Agency (CISA, in DHS) 31
Federal Communications Commission (FCC) 32
Federal Trade Commission (FTC) 33
Shaping State Legislation 33
National Conference on Uniform State Laws (Uniform Law Commission) 33
National Conference of State Legislatures (NCSL) 33
California Legislation 34
Oregon Legislation 34
League Studies and Policies 36
V. KEY FINDINGS – Policy Issues 37
Privacy Policy Is Not Uniform 37
Individuals and Personal Data Protection 38
E-Commerce Data Protections 38
REFERENCES 40
APPENDIX A: Glossary 47
Definition Sources 47
Definitions 47
APPENDIX B: Privacy Policies 51
APPENDIX C: Legislation 52
Federal Law 52
Gramm-Leach-Bliley Act 52
Fair Credit Reporting Act 52
Oregon Legislation 52

Banking Security Breach Rules 52
Election Bills that Passed, Oregon 2019 - A Win for Transparency and Privacy! 52
Election Bills that Failed to Pass - Oregon 2019 53
Privacy/Transparency Bills Passed - Oregon 2019! 54
Oregon Public Records Law 54
Privacy/Transparency Bills that Failed to Pass - Oregon 2019 54
Immigration Status 55
Public Record/ Privacy Bills 55
APPENDIX D: Personal Privacy Practices 56
[Have I Been Pwned] HIBP? 56
Social Media - R U There? (geolocation tracking) 56
Me/Not Me: Impersonations 56
What Does A Computer Problem Look Like? 57
Password Management 57
Use Diverse Passwords 58
Malware, Spyware, and Viruses, Oh My! 58
Google Download Option 58
Facebook Download Option 58
Acknowledgements: 59
Study Committee 59
Technical review and commentary 59
Editors, LWVOR 59

INTRODUCTION

The Oregon State Legislature, like other states, is actively addressing privacy and cybersecurity concerns such as identity theft and consumer privacy. The League of Women Voters of Oregon conducted this study of Privacy and Cybersecurity in 2019 to support League development of a policy position statement. Results of this study will inform League recommendations for voter education, civic engagement and policy advocacy regarding privacy and cybersecurity.

Policymakers debate existing legislation—a fragmented regulatory framework which fails to provide comprehensive cybersecurity—in an effort to balance personal information privacy with accountability, transparency (information disclosure), and responsible oversight (Craig, Shackelford, & Hiller, 2015). Individuals have limited recourse to protect their personal privacy (Bamberger & Mulligan, 2013). Stakeholders must thoroughly consider regulatory actions to avoid unintended consequences (Messer, 2019) and try to future-proof laws in anticipation of the inevitable technological changes ahead (Kerry, 2018).

US cybersecurity privacy concerns today include the following:

- Effective cybersecurity must balance benefits of data use with privacy and protection needs. E-commerce and privacy advocates seek to address policy and legal gaps which fail to integrate privacy with cybersecurity.
- Compelling benefits of new technologies transform every corner of modern society. Everyone expects instant connectivity, smart technologies, and 24/7 access to the world every day. Cyber threats escalate the demand for tighter security.
- US law gives private firms wide discretion over consumer information privacy, permitting business self-regulation and choice of user data protection methods. The resulting notice and consent privacy safeguards are inconsistent and provide uneven personal information protection.
- E-commerce of personal data is highly profitable. Increasingly powerful data handling and data mining result in sophisticated user profiles, data packaging and selling, and micro-targeted marketing.

This League of Women Voters of Oregon report highlights numerous technological advances and related cyber concerns that affect citizens' information privacy and describes some key organizations shaping cybersecurity policy.[1]

- Part I recounts changing views of privacy over time.
- Part II describes recent technological advances that will greatly benefit society yet pose privacy risks.
- Part III discusses election security, privacy in political activity and census privacy.

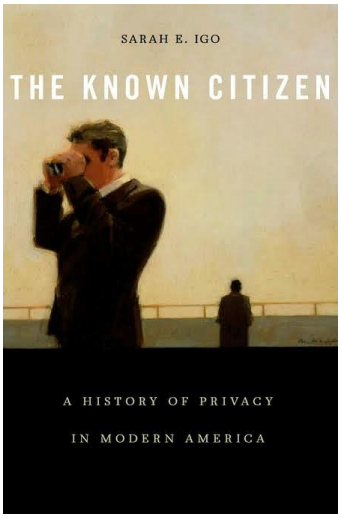
[1] This report was prepared by members of the League of Women Voters of Oregon who are not technology experts, and we regret any errors. While consumers flock to the obvious benefits of new technologies, many users do not understand their inner workings. Knowing that users appreciate technology's benefits, this report focuses on its potential privacy drawbacks.

- Part IV describes key privacy and cybersecurity actors, including their roles and activities.
- Part V Key Findings discuss policy issues in the privacy and cybersecurity debate.
- Appendices provide additional resources.[2]

I. PRIVACY

Changing Views of Privacy

As the cyber era challenges data privacy and information transparency, it is helpful to examine how societal views of privacy have been challenged and changed throughout history. One 1960s researcher noted: "...the claim to privacy will always be embattled" since "its collision with the community's need to know is classic and continuous." (Igo, 2018)



The Known Citizen, Sarah Igo. Harvard University Press, 2018.

Four key privacy torts developed in the 1900s:

1. Intrusion upon seclusion
2. Public disclosure of embarrassing facts
3. False light (similar to defamation)
4. Appropriation of name or likeness

Some historical claims to privacy:

- Protection from intrusion, e.g. parental rights, railroad work injury physical exams
- Ownership of papers and data, including mail privacy
- The right to be "let alone", from reproductive rights intervention, to "sacred relations between a man and his wife", or from the press
- A *private* personal sphere: freedom of thought and from forced pledging of allegiance
- Political privacy and right to privacy of association
- Privacy of the home and curtilage (i.e., property between a house and a fence), as in the case of illegally procured evidence
- Copyright privacy - See Google legal help

Igo (2018) describes American colonists' privacy concerns. Sometimes privacy claims were seen as suspect or selfish, not a positive attribute or civil right. Societal cohesion was valued over individualism, since the colony's survival could depend on monitoring the community members' behavior. In the 1910s, wartime citizen surveillance was encouraged, enlisting the American Protective League, to monitor German citizens in the US. A counterpart, the American Civil Liberties Union (ACLU) formed in 1920. By the 1930s, most Americans eagerly enrolled for Social Security numbers, sacrificing some privacy for the economic security of federal retirement benefits. Today, sharing Social Security numbers risks data breaches and identity theft.

American common law initially protected upper-class privacy; free white property-holding men were entitled to home and asset protection, focusing on property, sanctity of the home, and mail. A man's

[2] Hyperlinks to sources and resources were created in January, 2020, and may subsequently be broken after publication of this report.

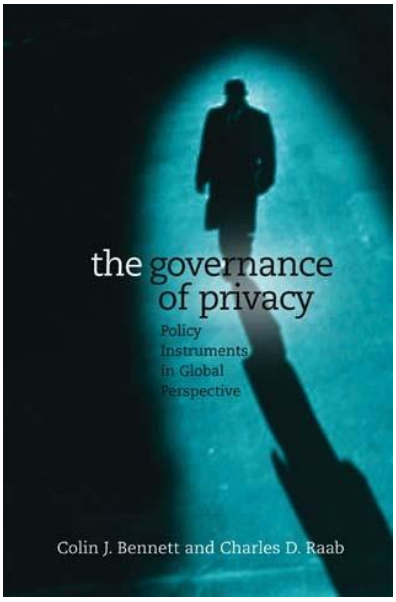
reputation was linked to the modesty and reserve of his wife and daughters, so property protection extended to families, since exposure could harm the good names of those men. This family *aggregate privacy* failed to provide *individual* privacy rights for women and other family members.

In 1881 a Senator opposing women's suffrage for individual rights saw it as "breaking through a man's household, through his fireside… to open to the intrusion of politics and politicians that sacred circle of family." An 1888 Supreme Court decision tied "the sanctity of a man's home and the privacies of life" to "his indefeasible right of personal security, personal liberty and private property" (Boyd v United States, 1886). Over time, privacy claims shifted from a physical conception of personal autonomy and freedom to the individual's rights and possessions.

Privacy and Personal Information Today

Privacy has meant different things at different times and can mean different things in different contexts. The wish for privacy may apply to solitude, physical space, decision-making, or one's control over access, information or decisions. In this report, the term *privacy* refers to data or *information privacy* as it applies to data security and cybersecurity, not broader views of personal or physical privacy. Since the mid-twentieth century, US privacy policy debates have typically focused on limiting or controlling access to an individual and/or their information.

Informed Consent for Research and Patient Medical Records



The Governance of Privacy, Bennett and Raab, MIT Press, 2006.

Researchers and healthcare workers collect and hold many kinds of personal information. They are expected to handle confidential data responsibly and securely. Often they need to demonstrate trustworthy stewardship of potentially sensitive information so that individuals will share it, or to maintain a long-term relationship (e.g., healthcare providers). While current research and health information privacy practices are generally robust, history reveals some egregious violations and slow responses to address them.

The movement to formalize *informed consent* standards and practices for research arose after World War II. The Nuremberg Code of international ethics is widely viewed as the basis for today's research and medical ethics standards, including the practice of informed consent. It was written in response to wartime atrocities (Schuster, 1997).

New 1980s protocols set institutional standards and ethics codes for individual researchers working with human subjects. Federal regulations now require institutional review board (IRB) approval for research study designs (including informed consent and confidentiality protocols).

Prior to the development of informed consent, the goal of advancing medical knowledge sometimes took priority over individual patient protections. Informed consent was not used in the 1950s for Henrietta Lacks, whose tumor cells were biopsied, harvested and used for research and profit, as chronicled in "The Immortal Life of Henrietta Lacks" (Skloot, 2010). The Nuremberg standards finally were adopted in the 1960s, in the wake of the unethical Tuskegee syphilis research and deceptive social science research practices.

During the 1960s social and medical scientists struggled with reconciling research and rising privacy protection demands. One noted, "It's very difficult to conclude that society does not want some of the

knowledge which it is possible for us to produce if the cost involves giving up of values of personal dignity and privacy, the majority of the people in society do not want to pay that price." Some experimented with methods to protect privacy by extracting data from people without "ever identifying individual actors or in any way manipulating them." (Igo, 2018)

The health professions' long history of evolving ethical standards for patient privacy has shifted toward privacy protection since the 1960s. National confidentiality standards for certain patient records were created via the 1996 insurance law, the Healthcare Insurance Portability and Accountability Act, known as HIPAA (HIPAA Journal, n.d.). This law established sector-specific patient privacy protections for healthcare providers and insurers.

When Apps Get Your Medical Data, Your Privacy May Go With It. Singer, N. New York Times, Sept. 3, 2019

Unlike other types of client records, a patient's health data record contains detailed, sensitive confidential information about a patient's history, medical conditions, genetics, mental health, substance abuse, and financial information. A breach of patient confidentiality or medical data could affect a patient's employability or insurability.

The adoption of new health data technologies may test HIPAA's ability to adequately safeguard patient record privacy and confidentiality. Tech giants Google (now a subsidiary of Alphabet), Microsoft, Amazon, and Apple have all recently partnered with healthcare organizations to provide a range of health data exchange and insurance claims services, including predictive analytics and artificial intelligence techniques (Coleman, 2019; Singer, 2019). Industry observers identify several privacy and security concerns regarding how artificial intelligence and precision medicine analytics are applied to health data. Powerful predictive analytics can bypass HIPAA health data protections to identify individual patients; potential data use and sharing may go beyond existing patient consent agreements; predictive algorithms using social media data are prone to significant bias (Mathur, 2019).

While ethics and privacy are weighed deliberately in the collection and use of medical and behavioral research data, science and technology advancements continue to raise challenging questions about how to best protect and use personal data. HIPAA's privacy constraints hamper data-sharing between health providers and health researchers for purposes of medical research (Miner, 2019).

Shielding healthcare data may pose a significant cost to society. For example, greater access to genomic healthcare data could increase our knowledge of the human genome for improved understanding and screening of genetic disorders. Who decides the extent to which patients can be required to sacrifice their own health data privacy for the common good is the challenge.

From the early colonists to modern health data, history shows that understandings of privacy are continually evolving and renegotiated. A person's view of privacy is situational in that it is influenced by unique circumstances. Furthermore, changing technologies have often catalyzed society's changing views of privacy. Today, many worrisome privacy intrusions are virtual. New technologies that originate in cyberspace are welcomed into daily lives, often with unforeseen consequences.

II. TECHNOLOGY TODAY

Computerized information technologies continue to change our material and social worlds at a dizzying pace. Consumers enjoy technological conveniences. Businesses improve efficiency, productivity, and profit from E-commerce. Governments use technology to serve and protect citizens. Yet emerging technologies and hidden security and privacy risks can outstrip our ability to safeguard our data and ourselves. Networked computers are increasingly vulnerable to cyber-attacks; E-commerce leverages consumer data for profit. These risks are causing loss of individual's personal data and privacy. Robust cybersecurity protects against intrusions, attacks, damage, misuse or harm to all system components, including hardware, software, and the data stored in the system (Zlatanov, 2015).

Common Vulnerabilities - Data Breaches, Ransomware, and Hackers

Cybersecurity has become an urgent issue topping many policy agendas. Computer security services protect against a wide range of intrusions, from hackers and malware to phishing and denial-of-service. Data breaches, ransomware and hackers have been headline news.

Data Breaches

An Equifax hack settlement promises a $125 payout. Brice-Saddler, M. The Washington Post, 2019

Here's What You Need To Know About the Capitol One Breach. Yaffe-Bellamy, New York Times, 2019.

The Marriott and Capital One breaches had major economic consequences (Yaffe-Bellamy, 2019). Unauthorized system intrusion, data or security breaches, supply chain manipulations, and state-backed hacking campaigns all culturally redefine cyberspace as the new battleground. Equifax may now have greater corporate name recognition due to its security breach, which exposed nearly half the American population to the risk of identity theft (Brice-Saddler, 2019).

Ransomware

Ransomware is malicious software that can gradually or suddenly hijack part or all of a computer or network's content, files, and programs. A ransomware attack then holds the data hostage, usually announcing ransom terms, often asking for untraceable cyber currency payment. According to legislative committee testimony (JCLIMT, 2019), more than $200,000 is lost daily to ransomware (globally). The city of Portland was hit repeatedly between 2015 and 2017, costing $550,000 in lost work effort and $50,000 in recovery. The average time between exposure and actual intrusion is 243 days. Ransomware complexity, impact, and cost are volatile.

This graphic was included in Ransomware presentations for the November 2019 Interim hearing of the Oregon Joint Legislative Committee for Information Management and Technology.

Techniques are now more often designed to fool users rather than circumvent system security protocols. Users are enticed to "click here," luring them to a site designed to appeal to them—another example of current privacy challenges.

Hackers

Hackers, also known as *crackers* within the cyber community, are the cybersecurity warriors who execute system intrusions, reminiscent of safecrackers. They range from "black hat" offensive intruders to "white hat" ethical intruders, hired to examine system vulnerabilities in order to improve defense pre-emptively. "Gray hat" allegiance may be unclear.

Social Networking

Social networking has exploded in the last decade, and nearly a third of the world's population now uses social media (Ortiz-Ospina, 2019). Building on the US Department of Defense Advanced Research Projects Agency's (DARPA) development of the early internet, the European Organization for Nuclear Research, better known as CERN, launched the World Wide Web in 1989 (CERN, n.d.; Palermo, 2014). The web ultimately transformed computer connectivity around the world, with nearly 60% of the world's population using the internet today (Clement, 2019). Social media sites are used to share content and communicate with others, generate visual and audio media, share information and opinions, get the news, and gather information that influences users' political opinions and worldviews.

Social networking platforms and web browsers are arguably the largest information sources about users' personal preferences and online use. Google and Facebook may have the greatest reach in the US, but any internet service or tech-based firms (e.g. Apple, Amazon, Instagram, Microsoft, Twitter, Mozilla, etc.) has access to users' online activities. Under US policy, personal information collected by technology companies are controlled by the company (subject to their terms of service), rather than the user.

Your Data Is Being Tracked

Most smartphones users know their phone's location is tracked. But they do not realize the vast amounts of information tech-based firms gather from mobile and online devices based on logins, device types, browsing histories and IP addresses.

Here's a sample of the data Google tracks (Curran, 2018):

- Google tracks and stores location data every time phones switch on.
- A location timeline is recorded from the first day Google is installed on each phone.
- Google's search history is shared across devices.
- Google creates an advertisement profile based on search information, including location, gender, age, hobbies, career, interests, relationship status, and possibly weight.
- Google holds your entire YouTube history. Google offers a full user data download option. It could be a very large file, with everything already mentioned plus bookmarks, emails, contacts, photos taken with the phone, businesses you've bought from, calendar data, Google hangout sessions.

> Today, Google cautions:
>
> "Just because you appear in a video, image or audio recording does not mean you own the copyright to it. For example, if your friend took a picture of you, she would own the copyright to the image that she took. If your friend, or someone else, uploaded a video, image or recording of you without your permission, and you feel it violates your privacy or safety, you may wish to file a privacy complaint." (Google legal help, 2019)

Facebook also gathers extensive personal user information (Curran, 2018):

- Facebook aggregates and targets data for advertisers and opinion influence.
- Facebook stores and predicts user interests, based on "likes" and post threads.
- Facebook stores log-in times, locations, and devices.
- Facebook can access phone webcams and microphones.
- Facebook allows users to download a comprehensive file, including every message and file, all contacts, and audio messages ever sent or received.

In a recent court case, Facebook's lawyers stated: "There is no privacy interest, because by sharing with a hundred friends on a social media platform, which is an affirmative social act to publish, to disclose, to share ostensibly private information with a hundred people, you have just, under centuries of common law, under the judgment of Congress, under the SCA [Stored Communications Act], negated any reasonable expectation of privacy." (Warzel, 2019).

Social media and video sharing websites provide an opportunity for various forms of harassment and bullying, including derogatory comments, online rumors, sexual remarks (*sexting*) and distributing sexually graphic images of individuals without their consent (*revenge porn*). According to the Pew Research Center, "73% of adult internet users have seen someone be harassed in some way online and 40% have personally experienced it." (Dugan, 2019).

Big Data, Big Impact

Every internet user creates and accumulates a long trail of personal information, all available for data broker use. New technologies and techniques have enabled analysis of the constant stream of unstructured data that flows from all types of devices and all forms of data, such as text, media, images, and transactions. One of the hottest topics in the cyber world, big data means the volume, variety and high velocity of data transmission and transactions flowing through the internet and within business

operations (TechAmerica Foundation). *Big data* touches upon every sector: healthcare, law enforcement, security, financial services, transportation, energy, agriculture, and government (including elections).

Every website click, phone call, form fill, order placed and tracked, social network post, and surveillance beacon offers potential insights. For example, commercial businesses can manipulate, sort, combine and analyze almost all online actions to extract and market information on individuals, organizations, institutions, and industry.

Social network analysis (SNA) (Disney, 2014) is used commercially, for defense and numerous other applications. SNA is one example of how analysts mine unstructured big data sets to reveal underlying patterns. For example, connectivity and betweenness measures (algorithms that calculate how closely data are linked), are central to managing the stability and defense of the internet, for banking, electrical grids, global and local communications networks, air and road traffic, even elections. Cryptocurrency hinders our ability to "follow the money" and can complicate financial disclosure and campaign finance.

While big data has enormous potential to provide new insights, observers caution that there are also privacy and cyber security risks (EPIC, n.d.). Personally identifying information is commonly de-identified to assure anonymity, but big data methods are so powerful they may be able to identify individuals despite anonymization. Big data algorithms automate decisions based on personal profiles, which may discriminate against protected classes. The growth of massive data stores also increases the risk of security breaches and erroneous data.

Big data is truly a growth industry, rapidly adopted for innovative applications. Its vast scope reaches deep into the everyday lives of individuals and broadly across global economic and political systems. It leverages emerging technologies and analytic techniques in ways that current security and privacy practices have not anticipated. Embedded technologies, E-commerce and smart devices discussed below are just a few examples of Big Data's transformative possibilities and challenges.

Internet of Things (IoT) - Using Embedded Technology

"The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it"—Mark Weiser (quoted in Preston, 2014).

Computer scientist Mark Weiser anticipated *ubiquitous computing* as a third computing wave, seen as today's IoT (Weiser, 1993). Mainframes serving many users constituted the first computing wave and personal desktop computing, the second wave. The third wave computing eliminates computer terminals and provides direct human-to-device interaction and device-to-device networking.

Devices can sense and report real-time status without computers, hence the label *internet of things* (Bohn, Coroamă, Langheinrich, Mattern, & Rohs, 2005). Miniaturized microelectronic processors and sensors are embedded in everyday devices and can be remotely controlled to track, monitor, sense, and adapt to changing conditions. For example, a blind person's walking stick can be connected by Bluetooth to Google maps, provide voice assistance for directions, and signal nearby movement with ultrasonic sensors (Corbley, 2019).

These are a few of the consumer devices on the IoT:

- Smartphones, watches, and wearable health/fitness monitors;
- Intelligent assistants like Siri and Alexa, and GPS devices;
- Household appliances, including refrigerators, baby monitors, light bulbs, TVs, speakers, smart plugs, and switches;

- Household systems, including thermostats, irrigation, security systems, video doorbells, and locks;
- Connected vehicles, which sense speed, GPS data, passenger weight, phone use, even financial information, are continuously sending performance and maintenance data to makers (Hanvey, 2019). US Senator Jeff Merkley (D-Oregon) recently stated: "We need to know about any data their (i.e., carmakers) vehicles collect, where that data goes, and who owns it."

In addition to consumer devices, the IoT applies to industrial-scale manufacturing, energy, transportation, and defense networking. Robots and smart production lines control manufacturing, city control systems adjust for traffic, utilities' smart metering manages energy demand and monitors potential problems, and airlines use IoT to increase flight efficiency and track baggage.

Security and Privacy Concerns with the Internet of Things

Networked devices simplify personal lives and provide economic benefits and industrial efficiency. Not surprisingly, increased device use with continual online data exchange adds to cybersecurity risk. These devices operate without direct human oversight, giving attackers ready physical device access; IoT's wireless communication networks provide easy access to confidential information; IoT devices perform basic computing tasks that use little energy, so they cannot support elaborate security measures. The authors note that a cyberattack on just a part of the IoT network may damage or disable the entire system, possibly resulting in catastrophic physical and/or economic damage, and endangering lives (Abomhara & Køien, 2015).

The Internet of Things increasingly permeates consumers' lives with an array of convenient services, while its interconnectivity increases privacy breach risk. Government and private communications, global financial networks, power grids, traffic relay systems, and social media all may increase individual and collective intrusion breach risk. DefCon 2019—a professional hackers' cybersecurity conference—revealed US military aircraft vulnerabilities. Ethical hackers exposed problems that could shut down a jet's data systems (Pawlyk, 2019).

E-Commerce

Consumer data gathered by online retailers and web browsers are tracked, warehoused, and combined from multiple sources to provide one-to-one targeted marketing and customized service. This wealth of data is mined and analyzed with sophisticated techniques like machine learning and artificial intelligence, and data can also be shared and sold to third-party businesses. In the digital economy, businesses make huge profits using personal information for internet advertising that funds "free" websites and social media.

Ad Tech –or advertising technology firms—use a "system of software programs, data servers, marketing agencies, and data markets which facilitate the sale of user data and the display of advertising messages to users of the internet, including search engines and social-media sites and apps." (Watkins, 2018).

While recent General Data Protection Regulation (GDPR) rule changes give consumers more control over personal data, online advertising and technology firms continue to largely self-regulate. In the US, the firms themselves control the personal data they hold, and firms determine how they will handle and enforce consumer privacy protection.

Consumer Data Is The product

E-commerce brought new business models and ways to reach customers. Advertising profit is the fee for Google and Facebook, micro-targeting user *likes*, buying, and browsing habits. Harvested consumer data

is the product, without giving users disclosure control. US industries largely self-regulate consumer data privacy in digital commerce under FTC oversight. Two challenging online commerce issues are *cross-device tracking* and *online behavioral advertising*.

Cross-device tracking allows companies to follow consumer activities across smartphones, computers, and other connected devices (Ramirez, 2017). In 2015, the FCC placed cross-device tracking under behavioral advertising self-regulation.

Online Behavioral Advertising (OBA) is "the practice of tracking an individual's online activities to deliver advertising tailored to the individual's interests." (FTC, 2009). Advertisers gather or acquire, then analyze consumer online behavior, for specifically targeted ads. This data tracking, mining and third-party sharing is largely unregulated.

Users may not realize that websites track and sell their searches, URL visits and content viewed to third-party firms. Innovations allow gathering, storage, analysis and sharing of tremendous amounts of user data, often willingly provided, though permission may be inadvertent or seem unavoidable. Typically, the only way to access "apps" or social media, is to accept privacy policies. All require consent – but few users read the 2000 to 3000-word use policies or understand the legal jargon permitting economic profit. Google, Facebook, data brokers, and geolocation trackers use consumer data and cross-device trackers for behavioral advertising. Consumers continue to encounter privacy problems as various platforms track online activity.

Some observers are concerned that E-commerce practices are unfair to consumers, giving businesses a free hand to intrude on privacy with too little personal data protection. Fuchs (2011) called the appropriation of user data for profit *economic surveillance*, while Zuboff (2019) dubbed it *surveillance capitalism*. Industry counters that efficiency and services are being provided.

The World Privacy Forum submitted its proposed Consumer Privacy and Data Security Standards Act of 2019 for deliberation with the Federal Trade Commission (FTC) and the Senate Banking Committee (Winn & Dixon, 2019). This proposal for voluntary consensus standards addresses industry self-regulation flaws outlined in their report "Many Failures: A Brief History of Privacy Self-Regulation in the United States" (Gellman & Dixon, 2011).

Credit Cards

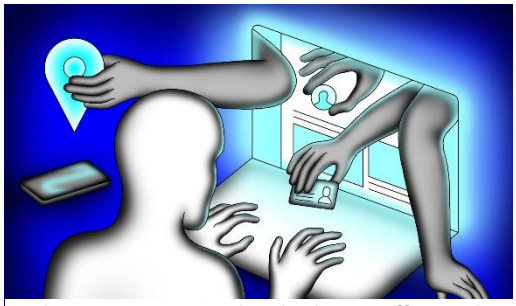
The Spy in Your Wallet: Credit Cards Have A Privacy Problem. Fowler, The Washington Post, 2019.

Fowler (2019) calls credit cards "the spies in your wallet." In an unusual privacy experiment tracing how his credit card data was used, he purchased one banana with his Apple Card MasterCard and another with his Chase Amazon Prime Rewards Visa. The 1999 Gramm-Leach-Bliley Act federal law requires that credit card issuers protect consumer data privacy. Yet Fowler learned that six business types (the store, the card network, point of sale systems, retail and other banks, mobile wallets and other financial apps) could share and mine his 29-cent banana purchases. Noting that this tracking and exposure is "multiplied untold times by other companies" (Fowler, 2019) contends it is time to add privacy, alongside rewards and rates, as a factor for evaluating credit cards.

Fowler's takeaway: "The card data business is booming for advertisers, for aiding investors and helping retailers and banks to encourage more spending. There are many ways to exploit a card swipe, not always requiring a "sold" or "shared" transaction. Data can be aggregated, anonymized, hashed or

"pseudonymized" (given a new name), or used to target users without ever technically changing hands" (Fowler, 2019).

What's the harm? "We're legally protected from fraudulent charges and unfair lending practices. But spending patterns can reveal lots– possibly enough for blackmail. Anytime data passes to new hands, there's another chance it could get stolen" (Fowler, 2019).



Intel executive: Rein in data brokers. Hoffman, The New York Times, 2019.

Data Brokers

According to Hoffman (2019), personally identifiable information (PII) is discoverable and available online from data brokers, the collectors (miners) and legal vendors of addresses, phone numbers, and other personal data (Hoffman, 2019). Data comes from "public records – court documents, marriage licenses, driver's licenses, and other sources" – to create marketable personal profiles. Hoffman reports that for less than $25 a month, Peoplefinders, a popular information-finding site, sells data on any private citizens in their database. Consumer protection, including privacy, is now being addressed by the Oregon Attorney General's Task Force.

Geo-location data - The market value

About half of US mobile devices used today have active location tracking that relate to 1200 Android apps and 200 Apple apps. Consumers value the many services available on apps, e.g., traffic and navigation data, local weather forecasts, fitness activity tracking, parking spaces locations.

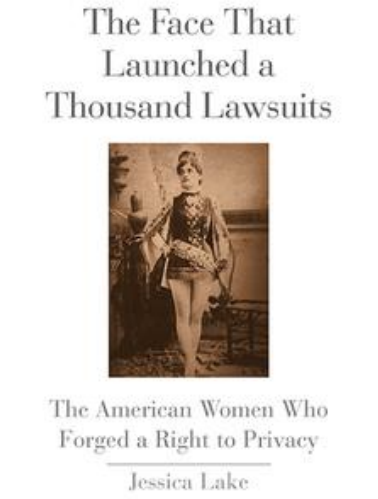
US advertising revenues are forecast to reach $148.5 billion in 2019, which includes $24.4 billion for location-targeted ads to mobile devices (Matthiesson & Fratrik, 2019), an increase of $3.4 billion from the previous year (Valentino-DeVries, Singer, Keller, & Krolik, 2018). Targeted customer ads and geolocation data have high market value. Facebook and Google track both customer online activity and their response to targeted ads. Data is supposed to be protected, but an individual's identity and lots of linkable private information can be revealed.

US Senator Ron Wyden (D-Oregon) has proposed bills to limit collection and sale of this data, largely unregulated in the United States: "Location data can reveal some of the most intimate details of a person's life—whether you've visited a psychiatrist, went to an A.A. meeting, and who you might date. "It's not right to have consumers kept in the dark about how their data is sold and shared and then leave them unable to do anything about it." (Valentino-DeVries, Singer, Keller, & Krolik, 2018).

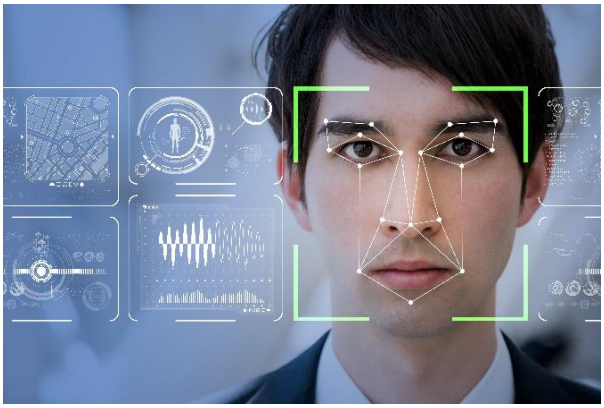
Surveillance and Privacy

Imaging: from Daguerreotypes to Facial Recognition

Nineteenth-century photo developments brought urgent legal attention to privacy. Daguerreotypes might take 20 minutes to expose film, but snapshots took a flash. Faster, portable photos led to newspaper "keyhole journalism," decried by one critic as "espionage as universal and active as any despot ever established." Igo (2018). Circa 1890, photographers owned images and subjects began to sue for privacy. Copyright law protected "disreputable and even immoral" advertisers, who profited from photos of individuals, known as the "crisis of the circulating portrait." An 1888 House of Representatives bill "to Protect Ladies," saw that much more often than men, women were surreptitious photo subjects. The bill did not refer to individual privacy but to the offense caused by the circulation of "vulgar and unauthorized" images of "the wife, daughter, mother or sister of any citizen of the United States." Because of this image traffic, the majority of privacy plaintiffs were women, though they were the minority of overall litigants (Lake, 2016).



Published by Yale Books. 2016.



Credit: Shutterstock

An 1890 Harvard Law Review article, "The Right to Privacy" by Samuel Warren and Louis Brandeis, spoke to a "potent trinity of press, photography, and publicity" (Igo, 2018) by calling for an individual's "right to be let alone." The most enduring legal legacy of "The Right to Privacy" article is creating a "right to *publicity* in one's name or likeness, including the privilege of profiting from one's distinctive persona." Ironically, Warren and Brandeis's seminal essay remains a cornerstone of privacy jurisprudence. (quoted, Igo, 2018).

Body Cameras

Recent high-profile legal cases with body-worn cameras (*bodycams*) focused national attention on police use of force. A California law that bans facial recognition for body cam footage will go into effect in 2020 (Liberatore, 2019).

This rapidly adopted and sometimes controversial technology intends to improve policing and increase transparency and accountability (Mateescu, Rosenblat and Boyd, 2015).

Preliminary evaluations show bodycams may improve police-subject relations and reduce both police use of force and citizen complaints. Pilot studies also identify inconsistent implementation and administrative data storage and management challenges. Though police departments consider bodycams valuable tools, further research on implicit bias and privacy is needed.

These cameras are fixed onto the front of police uniforms to record video during duty. Bodycam use may pose serious privacy concerns, such as when recording takes place inside private homes or when compromising recordings are inappropriately disseminated. The privacy of minors should be assured if police are responding to domestic calls from adults. Also, police officers themselves may feel they are subject to workplace surveillance (Mateescu et al., 2015).

The cameras, commonly available today for $50 to $200, are not the central program expense. Overarching costs include records management, cataloging, appropriate video or data recording storage, archive retention and disclosure policies. The City of Seattle received legal but unreasonably broad and extensive public record requests for police bodycam recordings. Those requests overwhelmed police and city officials (Funk, 2016). As with other public record issues, disclosure rights regarding privacy and transparency are often in conflict with official policy which is lagging or absent to address these concerns (Police Executive Research Forum, 2018).

Surveillance, extensive monitoring, and personal data collection are inherently about politics and power. Public observation is extensive, with widely varied purposes. Who sees you or data representing you? Why are they looking, and what do they get to do with it? Who should administer security standards? Privacy concerns arise in multiple contexts, with legislation opportunities abounding to protect individuals, infrastructure, businesses, and government operations, including elections, personal records, etc. Automated surveillance has expanded, although with a generational divide in attitude, as younger people take it for granted (LaForgia, 2015). Surveillance by Immigration and Customs Enforcement (ICE) agents, preceding the disappearance of southwestern Washington residents, is chronicled in “The Watchers” (Funk, M, 2019).

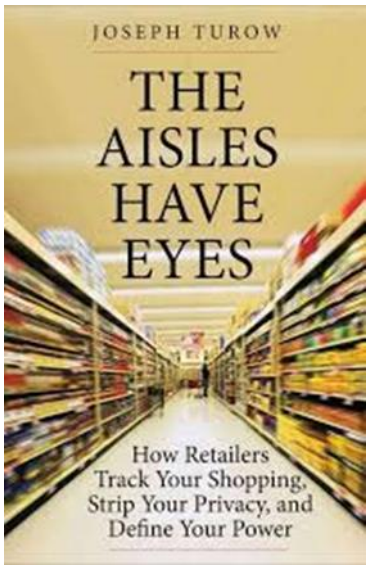
Automated License Plate Readers (ALPRs)

Geotagged license plate images, more than 80 million recorded monthly, are the product. Our taxes pay for 3,000+ police agency customers, but financial and insurance agencies also buy the data from Motorola Solutions and its competitors. ALPRs can replace tracking devices that require warrants. The NYPD over-stepped municipal bounds with a multi-year, $442,500 contract for national surveillance data. Misuse of the readers and their information is documented. With a database of more than 2.2 billion images in 2016, Supreme Court jurisprudence suggests that tracking at this volume is “akin to building a mosaic of information so complete and intrusive that it may violate the Constitutional rights of those subject to it.” (Friedersdorf, 2016). The ACLU, for example, reports on the NYPD scope and methods, which imposes “an unwarranted badge of suspicion and stigma on law-abiding Muslim New Yorkers” (ACLU, n.d.).

Traffic Cop’s Ticket Bonanza In A Poor Texas Town. Buzzfeed News, Campbell & Taggart, 2019.

Police in Port Arthur, Texas, track plates from cameras mounted on their cars to collect court fines and other fees, recently generating $1.5M in annual fine revenues for their small town. The populace is affected unevenly, since some simply pay up, but minorities and the poor may miss work or court dates for revoked licenses or registrations, then jail time for more significant economic losses. Police assert the goal is safer roads (Campbell, A, Taggart, K, 2016).

Pedestrian Surveillance



Mentioned on NPR, Fresh Air, The Aisles Have Eyes, 2019.

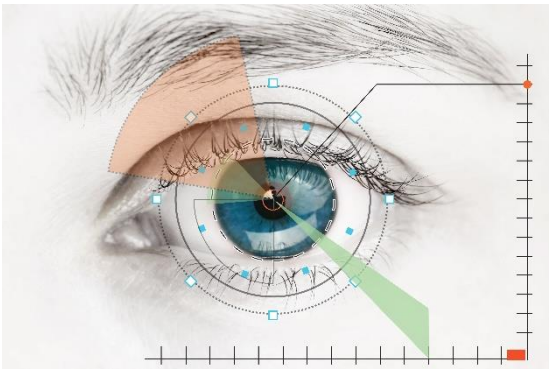
Most people aren't aware of Bluetooth beacons—*beacosystems*. Watching and tracking millions every day. These surveillance cameras are placed in airports, malls, subways, buses, taxis, sporting arenas, gyms, hotels, hospitals, music festivals, cinemas, and museums, and even in billboards. Imagine grocery stores. As you approach the dairy aisle, a phone notification offers a yogurt discount. How did your smartphone know? It was tracking you, using Bluetooth beacons (NPR, 2017).

Merchants get location data and pay marketers to apply data to send targeted ads. However, to trigger an action like sending a coupon, the app must be installed. Location marketers have also bundled beacon tracking codes into developer toolkits. App users may not be aware of these toolkits, which may be inserted into popular news and weather apps. While the location marketing firms argue that users can opt out of location services, that is not easily done (Kwet, 2019).

Doorbells

The doorbell-camera company Ring has partnered with more than 400 US police forces, granting video-sharing access to homeowners' camera footage, a role the company calls the nation's "new neighborhood watch." (Harwell, 2019) Police can request video within specified time and locations, from millions of Internet-connected cameras. Ongoing or live-video access is not granted and homeowners can decline email requests from Ring, thanking customers for "making your neighborhood a safer place." (Harwell, 2019)

Biometrics



Credit: Shutterstock

Emerging biometric technology offers new ways to observe human bodies. As noted above, photography evolved from the 20-minute Daguerreotype exposure to digital body cams (cameras). So too, biometrics has evolved from hunters observing prey footprints to applying artificial intelligence to identifying body features. In the late nineteenth century, "dactyloscopy" (fingerprinting science) overtook "Bertillonage", (using other precise body measurements) to identify possible anarchists, aliens, dissidents, union members, and potential criminals (Igo, 2018).

Fast forward to today, as new methods record more of the populace at large. Techniques are readily available to identify faces, fingerprints, signatures, voice analysis, palm vein, and even hand geometry. Other techniques are less commonly used and all are now processed and analyzed digitally: brain waves, gait, DNA, heartbeat, and retinal scans.

Author's photo, taken in September, San Francisco airport.

Biometric data have commercial applications. By subscribing to airport services, air travelers can check- in using iris scans or fingerprints. This is currently available in 100+ US airports, making physical ID unnecessary for customers. More common biometric uses include fitness monitors for cardiac performance, respiration, and walking; ambient light exposure and geolocation data; and fetal image measurements to determine gestational age (Kraudel, 2019).

Facial Recognition

Facial recognition can uniquely identify or verify someone by comparing and analyzing facial contour patterns. It is a privacy issue because data is often accessed without the subject's knowledge or permission, or because data access is not confined and has not been legally circumscribed.

Facial recognition is profoundly intrusive. While names are typically not attached, images can be recognized because each face is unique. For example, when Hong Kong protesters used face masks to protect their identity from facial recognition technology (Chappell, 2019), the government quickly banned face masks (Berlinger, 2019).

Along with Google and Facebook, many companies and agencies compile facial images databases – often without individuals' knowledge – and share this globally to spread facial recognition technology (Metz, 2019). Databases are compiled from social networks, photo websites, dating services and cameras in restaurants and other public places.

Facial Recognition Profiling Errors

Facial recognition is not infallible. Programs seem optimized for white males, markedly less reliable for darker skin images. Feminine faces are not interpreted as well as masculine faces, and darker feminine images also show much poorer results (Simonite, 2019).

Marketers are promoting recognition of fear for police observation (Simonite, 2019). Successful psychological profiling by facial recognition remains elusive since "how people communicate anger, disgust, fear, happiness, sadness, and surprise varies substantially across cultures, situations, and even across people within a single situation." Also, similar facial movements can express multiple emotions (Feldman et al., 2019).

October 3, 2019, Hong Kong May Ban Face Masks By Invoking Colonial-Era Emergency Powers -- NPR announces the ban on wearing face masks in Hong Kong.

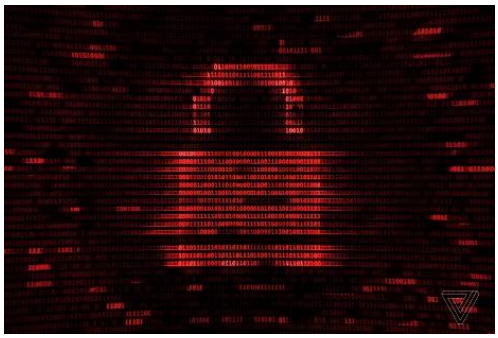
DNA Testing

DNA testing has been used for criminal investigations, solving difficult cases by helping to locate individuals under investigation, by clearing defendants, and even by proving some convicted prisoners innocent. The US Department of Homeland Security recently announced plans to test immigrants held in detention (Dickerson,2019), raising serious privacy issues. Results can link to family members and can distinguish people presenting as biological families, who prove not to be genetically related.

Facial recognition has consumer advantages. It can organize your photos. Google photos correctly suggests that these are the same person, actually eighty years apart. Personal photos.

Biometric Breaches

Many smartphones are protected with fingerprint scanning, facial recognition, or both. Early merchants promoted biometric sensors as an ultimate security technology, but the biggest biometrics security issue is inability to "reset the password." Artificial intelligence makes biometric identity theft much easier. Fingerprint copies have been successfully generated to unlock mobile devices. More concerning, researchers have demonstrated how deep artificial neural networks can be trained over time to recreate faces, or generally create facial images (Alexander, 2019). It is not complicated to reproduce face or fingerprint data using multiple methods. Fingerprint and facial scans can replace physical presence. Gaining system access can be as simple as using physical copies, clay fingerprint spoofs, or stealing stored biometric data. This was reported recently when unencrypted biometric data was exposed: "Huge security flaw exposes biometric data of more than a million users" (Porter, 2019); "Major breach found in biometrics system used by banks, UK police and defence firms" (Taylor, 2019). Although biometric hacking is not currently widespread, responsible users are advised to use two or multi-factor authentication (Bowman, 2019: NYU, 2019).



Huge security flaw exposes biometric data of more than a million users .The Verge. Illustration by Alex Castro / The Verge

Credit: Shutterstock

Fake News and Deepfakes

Fake news and media hoaxes have existed for a long time, but *deepfakes* are relatively new, the product of artificial intelligence and social networking. This section offers a brief overview of why some experts view manipulated media and deepfakes as serious threats to democracy. It then discusses the technology and psychology behind deepfakes, and why everyone is susceptible to deepfakes.

Danielle Citron, law professor and leading expert on manipulated media, and her colleague Robert Chesney, consider deepfakes "A Looming Challenge for Privacy, Democracy, and National Security" (Chesney & Citron, 2018). They argue that the combination of highly realistic false media in rapid circulation via the internet and viewed through our all-too-human cognitive distortions erodes both truth and trust.

Chesney and Citron (2018) explain that the societal impact of deepfakes will be widespread. They can be used to distort policy debates, manipulate elections, erode trust in institutions, exacerbate societal divisions, damage national security, and disrupt international relations (Chesney & Citron, 2018, p. 4).

> "Not only do we believe fakes, we are starting to doubt the truth."
>
> (Citron, 2019)

Research confirms that "False news online spreads faster than truth." (Vosoughi, Roy, & Aral, 2018). These authors paint a stark picture: "Falsehood diffused significantly farther, faster, deeper, and more broadly than the truth in all categories of information, and the effects were more pronounced for false political news than for false news about terrorism, natural disasters, science, urban legends, or financial information….Contrary to conventional wisdom, robots accelerated the spread of true and false news at the same rate, implying that false news spreads more than the truth because humans, not robots, are more likely to spread it." (Vosoughi et al., 2018).

Can We Believe What We See and Hear?

Jon Stewart's "Fake News" was entertainment in 2004 (Williams, 2018). Today, fake news is a partisan taunt, challenging press coverage veracity. Synthetic news, using realistic, simulated newscasters, is seen daily by millions in China who don't seem to mind non-human images. Everyone sees altered images, video, manipulated facial expressions and voices, often without realizing it. People aren't conditioned to be skeptical, to ask "Is this real?" when they see and hear media. A picture may no longer be worth a thousand words when new technologies generate our media content. (Plaisance, 2019).

Ethics and Synthetic Media, Psychology Today, Plaisance, 2019

Technology That "Thinks"

Deepfakes alter photos and videos to convincingly--and sometimes wildly--misrepresent reality. These and other state-of-the-art internet misinformation techniques are often based on artificial intelligence (AI), machine learning, and deep learning. With AI, computers are increasingly able to emulate human cognition (visual perception, speech recognition, language use, and decision-making). One AI form—machine learning—allows computers to independently process data and use it to improve their performance. Deep learning methods yield higher performance levels on similar tasks.

False news' staying power is rooted in the psychology of human thinking processes—how individuals perceive, process, and store data. Thinking is complicated and human brains process information quickly, easily, and all too often incorrectly. Thus, there are several ways false news can quickly take hold and be difficult to correct.

- False information is often designed to be startling. Emotion-laden language is intended to elicit a strong emotional response, which both sharpens message awareness and reinforces recall--even if the original information was false.

- Biases are systematic thinking errors that distort information processing. *Confirmation bias* is a common one: people unconsciously and selectively notice and retain information, reinforcing existing beliefs and expectations.
- Attempting to correct someone's false impression often backfires because of the tendency to resist information that contradicts existing beliefs and expectations.
- Frequently a source is misremembered, and false information is deemed trustworthy.
- Repeated exposure to false information can make it seem true. This illusion of truth can be repeatedly and effectively shared in campaigns and on social media.

Fake News is an Information Literacy Problem, not a Technology Problem, Forbes, 2019.

- The views of others have a strong influence on behaviors and opinions; this *social influence* is readily communicated on social media.

The social media culture has changed how people write and communicate and affects their confidence in perceiving reality. Analytics show higher reading rates for shorter texts because brevity invites readers to skim but doesn't encourage critical thinking. It becomes difficult to discern what is real news, biased information, and source authenticity.

The truth may get lost among credible falsehoods, social media algorithms that replay popular content irrespective of accuracy, and human thinking imperfections. Inaccurate *misinformation* circulates unchecked, while malicious actors (even foreign governments) capitalize on these loose norms to deliberately promote deceptive *disinformation*.

The preceding discussion of emerging technologies identifies a wide range of privacy and security risks. Unfortunately, there are no simple or inexpensive remedies for individuals, industries or governments. Global technology experts in business, industry and government constantly seek to anticipate, protect, detect, and mitigate operational errors, data breaches, service disruptions, intrusions and sabotage. Most experts agree that technology alone cannot assure cyber protection; users must be resistant to the deceptions of social media. For example, combating fake news asks society to improve information literacy and asks readers to think critically and verify and validate sources (Leetaru, 2019). In addition, Chesney and Citron (2018) recommend a combination of technology fixes, legal remedies, regulatory oversight, and technology firms that police their platforms to counteract manipulated media.

III. ELECTIONS, POLITICAL ACTIVITY, AND THE CENSUS

The federal government and the states have a long history of collecting and processing information to serve citizens and administer public responsibilities. A host of government services are now available online, improving the practice of public administration. Government information technology faces the same cybersecurity challenges as other businesses and industries. This report focuses on the intersection of privacy and cybersecurity in civic life—elections, political activity, and the US Census.

Protecting Elections in the Cyber Era

Numerous Federal agencies and technology experts are collaborating with state and local election administrators to protect political campaigns and the elections infrastructure from foreign meddling and cyber intrusions.

The US House Homeland Security Committee Hearing on Secure Elections (CSPAN, 2019) examined state-by-state election cybersecurity efforts to test and certify voting systems in response to known foreign election intrusions.

February 13, 2019. House Homeland Security Committee Hearing on Secure Elections (CSPAN, 2019)

Excerpted comments:

> The good news is every state is moving towards paper, if it isn't already on a paper-type ballot (hand-marked or whatever), including the five that are on electronic machines right now.
>
> Foreign election interference can take 3 forms: hacking into campaigns, sowing divisiveness in influence campaigns, some on social media, and technical cyberattacks on election infrastructure. Foreign intelligence services, domestic partisans, and online vandals don't care what our laws say.
>
> People are aware of 2018 election hacking attempts, and "spear-phishing."
>
> Citizens should continue our quest to have all elections audited, because then the confidence in elections remains high. And everyone needs to do everything they can to ensure confidence in the system, because if you don't vote, then your vote definitely won't count.

Disinformation and Foreign Interference

The Internet is a powerful campaign tool. Automated and micro-targeted robocalls and social media vie for voter attention and support. These inspire voter sentiments but also interfere with and damage trust, to the degree that some feel their votes don't matter. (Citron, 2019). On foreign intrusion of the 2016 US election Shane & Mazzetti, 2018 wrote:

"The Russian intervention was essentially a hijacking—of American companies like Facebook and Twitter; of American citizens' feelings about immigration and race; of American journalists eager for scoops, however modest; of the naïve, or perhaps not so naïve, ambitions of Mr. Trump's advisers. The Russian trolls, hackers and agents totaled barely 100, and their task was to steer millions of American voters. They knew it would take a village to sabotage an election."

Scholars (Bennett, 2013) have examined how technology influences voter behavior. Voter databases are maintained and can be sold to political parties to reach constituents. By compiling and managing data, local campaigns leverage this information. Political parties have adopted some E-commerce practices based on third-party voter data use, including micro-targeting social media and other ads, targeting specific voters and sharing personal data via commercial data brokers. Bennett, further notes: "To a considerable extent, these practices have been facilitated by the absence of information privacy laws that apply to political parties and election campaigns, and by the First Amendment to the Constitution that provides robust protections for freedom of speech and association" (2013).

OREGON ELECTIONS

County and municipal officials administer our elections and report results to the state Elections Division, overseen by the Secretary of State. Oregon is ahead of the election security curve in several respects:

HAND-MARKED PAPER BALLOTS are used and retained for recounts. This is important because the ballot recounts can readily show voters' pen marks, not obscured by substituting bar codes.

OFFLINE MACHINES, ballot tallying is not connected to the internet.

RISK-LIMITING AUDITS. The League supported Oregon SB 944 (2019) to adopt risk-limiting audits (RLAs). The bill passed and Oregon county elections' officials may now choose to use RLAs to randomly sample ballots to compare electronic and paper records. Risk-limiting audits:

- Are considered the gold-standard of efficiency, transparency and verifiability of vote counts to assure integrity of election tabulations.
- Check ballot count accuracy by applying statistical review procedures.
- Sample ballots with increasingly large samples until they statistically assure the ballot count with a predetermined level of certainty.
- Specify the minimum level of acceptable risk—providing strong statistical evidence that voting system outcomes correctly reflect the marks on the ballots. (Lindeman & Stark, 2012).

Beyond arguably legitimate political party influence efforts, various US and foreign internet actors seek to influence voters, with motivations ranging from honest to questionable to malicious. There is growing concern that intrusive practices, misinformation, and flagrant internet and social media deception sow dissention, mistrust, and cynicism among the electorate and undermine its faith in democratic processes and institutions.

Election Cybersecurity

Election cybersecurity concerns include vulnerable voting machines and systems, the inaction by the Federal Elections Commission, and foreign interference in the elections process and its effect on voter perceptions. A 2019 CISA report refers to the "Weaponization of Information":

"No single entity has officially been provided with a mandate to [counter foreign influence]. To date, the United States has no national strategy to counter foreign influence." (Soufan, 2019). See the "War on Pineapple: Understanding Foreign Interference in 5 Steps" infographic, (CISA (2019).

In an effort to protect voter registration databases from Russian hackers who accessed them in 2016, the US government is providing support to help states increase cybersecurity for the 2020 election. "

'We assess these systems as high risk' said a senior US official, because they are one of the few pieces of election technology regularly connected to the Internet." (Bing, 2019).

Intelligence officials are concerned that foreign hackers will try to manipulate, disrupt, or destroy data in 2020. Christopher Krebs, Director of The Cybersecurity Infrastructure Security Agency, (CISA), a division of the Department of Homeland Security (DHS), fears ransomware targeting, which recently crippled networks in Texas, Baltimore and Atlanta:

"Recent history has shown that state and county governments and those who support them are targets for ransomware attacks. That is why we are working alongside election officials and their private sector partners to help protect their databases and respond to possible ransomware attacks." (Bing, 2019).

As in other study aspects, election security is topical. In 2018, an 11-year-old showed how a functioning election machine could be "hacked" in under 10 minutes." (Blaze, 2019).

In August 2019, federal officials met with Oregon and other states' elections officials to discuss how to improve password strength, identify "phishing" attempts, and defend against power and communication disruption, social media misinformation and elections websites hacking (OR Secretary of State Press Release, 2019).

Voter Fraud

Partisan opponents of both major parties have claimed voter fraud. The Brennan Center for Justice publication, "The Truth About Voter Fraud" (Levitt, 2007), demonstrates that voter fraud at the polls is "exceedingly rare."

Political Privacy

What does a lack of political privacy mean today? Access to data, such as party member lists or campaign donor lists, certainly affects political privacy. In our current highly partisan climate, where every issue position may be accused of being partisan, what course should individuals take? Everyone needs to balance the tension among protecting our democracy, an individual's prerogative to participate in political activity without recrimination, and political influence transparency. The latter includes protecting our elections from foreign intervention.

The US Supreme Court makes exceptions to campaign contribution disclosure law requirements for cases of harassment. That is currently being discussed, with some experts recommending that donation disclosure thresholds be raised (Rogers, 2019).

Lack of political privacy has meant crippling discrimination, as seen in the McCarthy House Un-American Activities Committee hearings in the 1950s. By contrast today, an NAACP policy protects member identity, and its website preamble alerts users to data collection from page visitors. Campaign finance reform and disclosure, Citizens' United, and so forth, are transparency concerns. This report includes a reference to current Oregon legislative efforts.

Nonpartisanship Policies

What should nonpartisanship policies say and how can they protect organizations, such as the League, when members are encouraged to be "politically active?" To maintain campaign contribution transparency, even small political contributions are discoverable today and can reveal an individual's partisan stances. The League is actively working for campaign finance reform that includes opposition to a proposed IRS rule which threatens to invite more foreign money into US elections.

Electronic Voting Tested in Oregon

Because voting access may be threatened by international mail system conflicts, two Oregon counties tested an electronic option for overseas voters in the November 2019 election. In September 2019, an international mail crisis was averted when the US compromised with the Universal Postal Union, a UN Agency which coordinates postal policies among 192 countries.

Jackson County Clerk Christine Walker expressed confidence and said it will help ensure that overseas ballots will be counted. "We need to make sure that our military and overseas voters have (sic) the not only ability to vote, but they can easily access their ballots in a safe manner," …."There was a potential crisis going on." (Selsky, 2019).

The 2020 US Census

The US Census has consistently raised both privacy and transparency concerns. As the range of census queries grew during early censuses, some questions were seen as "an outrageous invasion of the personal and private business of the citizen." (Igo, 2018). Today's census citizenship issue is linked to concern of ICE intervention (see the 72-Year Rule). (United States Census Bureau, 2019)

The 2020 census will be the first census fully available online. It will count the homeless and transients and use satellite images to analyze residential structure changes. The Supreme Court rejected allowing a 2020 census citizenship status question, because the rationale for adding it appeared to be "pretextual—in other words, a sham" (Totenberg, 2019). Some observers fear this controversy alone may reduce participation and suppress response rates (Maciag, 2019). Current population estimates predict Oregon could add a sixth Congressional District.

"The 72-Year Rule"
The US government will not release personally identifiable information (PII) about an individual to any other individual or agency until 72 years after it was collected for the decennial census. This "72-Year Rule" (92 Stat. 915; Public Law 95-416; October 5, 1978) restricts access to decennial census records to all but the individual named on the record or their legal heir.

Census takers have been held both suspect as intrusive and welcomed as a way for residents to gain legal rights and benefits. The census used to be a door-to-door visit to count residents, property owners, family members, slaves, and other household members and collecting other information. (Igo, 2018).

Census privacy was always a consideration, with records to be sealed for 72 years following each census. That number was chosen as the average lifespan to protect the privacy of those surveyed. For example, the 1940 data was released in 2012.

Early census records may become indecipherable as cursive script reading and writing becomes less commonly taught. Interestingly, this trend away from cursive may also make the matching of Oregon's DMV license signature for vote-by-mail ballot verification a thing of the past.

Using the "Hollerith card puncher" for the 1890 census enabled faster processing. Technology improved the 1900 census population tracking with card-punch cross-tabulation. Census questions used since 1790 are available from the US Census, (US Census Bureau, 2019).

By the late 1960s, Congressional bills proposed census question limits as well as the requirement to answer them. Confidentiality protection seemed inadequate. Republican congressman Jackson Betts of Ohio, argued that the Census Bureau's "probing of people's affairs is certainly unwanted and unnecessary." He tagged questions as invading citizens' privacy and serving no public purpose. His supporters suggested that "titillating questions," such as whether households shared a shower, were

out of bounds, constituting "invasion of privacy" and "harassment." Democrat congressman Cornelius Gallagher of New Jersey, a notable individual privacy champion, opposed efforts to curb the census, and testified to how much had changed in a decade. Conscious of "the lease of power such information will give to the government to invade the private lives of its citizens," Gallagher nevertheless worried that reining in official data-gathering would imperil the "government's need to know."(Igo, 2018).

IV. POLICY ACTORS: Governmental, Non-governmental, & Industry

Stakeholders now face a patchwork of state-by-state and federal privacy and cybersecurity protection laws. Cybersecurity policy is set and influenced by a variety of entities. This section describes a range of global governmental and nongovernmental collaborations, plus US federal and state agencies and advocacy organizations.

These policy experts face an upsurge of new privacy concerns. How to appropriately gather, use, and share Personally Identifiable Information (PII) is a top issue. The "right to be forgotten" is also being explored, because individuals are poorly informed on granting or rescinding data permissions or lack the access to correct or remove permissions.

Policy makers are expected to weigh individual data privacy protections against information transparency. The idea of censorship may sound alarming, yet internet censorship is being considered for hate speech, mass shooting videos, terrorist propaganda, child pornography and torture. For example, child pornography was considered a problem ten years ago when a million images were reported. Tech firms report that image traffic has doubled in the last year to 45 million images. (Keller & Dance, 2019). These are urgent and growing issues for policymakers.

Such policy decisions can have major consequences. In another example, a proposed European rule would require firms to remove terrorist-related images within an hour of posting. Violators would face a punitive fine of 4% of global revenue, prompting United Nations observers to warn that the rule "may lead to infringements to the right to access to information, freedom of opinion, expression, and association, and impact interlinked political and public interest processes." (Satariano, 2019).

How these privacy-transparency trade-offs will be resolved currently depends on where you live. Each nations individually addresses privacy, hate speech and disinformation policies. The European Court of Justice recently ruled that Facebook could be forced to remove images deemed "defamatory or otherwise illegal" (Satariano, 2019).

Existing legislation is fragmented and varies by enacting jurisdictions and their stated privacy or security objectives. Here is an overview of relevant European Union, US, and state entities and their laws.

European Union (EU): General Data Protection Regulation (GDPR)

The European Union (EU) General Data Protection Regulation (GDPR), considered the gold standard for privacy and personal data protection, is perceived as reining in Silicon Valley "tech giants" (EU GDPR, 2018). The EU aims to protect all EU citizens from privacy and data breaches with the GDPR (EU GDPR, 2018).

In April 2016, the EU Parliament approved the GDPR, updating previous privacy and data regulations, effective May 25, 2018, (EU Commission, 2019).

In September 2019, the European Court of Justice ruled that "the right to be forgotten", also known as "data erasure," is not an absolute right and restricted GDPR enforcement to the European Union. The ruling to "balance the right to privacy and protection of personal data, on the one hand, and the freedom of information of internet users, on the other, is likely to vary significantly around the world" (Satariano, 2019). The legal case, brought by France against Google, heightens questions of privacy, free expression, and censorship. Guidelines in 2014 aimed to require Google and other search engines to take down offending sites outside the EU, stating that "Under EU law, everyone has a right to data protection", (Scott, 2014).

Key EU Government Data Protection Regulation (2019) provisions include:

- **Increased Territorial Scope** – Applies to all companies processing personal data of subjects residing in the EU, regardless of the company's location.
- **Consent** – Companies are no longer able to use long impenetrable terms and conditions. Consent requests must be intelligible and easily accessible, in clear and plain language. Consent withdrawal must be as easy as granting.
- **Right to Access** – The right to confirmation as to whether (or not), where, and for what purpose personal data is being processed. Further, a copy of the personal data shall be provided, free of charge, in an electronic format.
- **Right to be Forgotten** – This entitles subjects to have their personal data erased and cease further dissemination of the data.
- **Privacy by Design** – Privacy by design calls for initial system design inclusion of data protection, rather than as an add-on.
- **Breach Notification** – Notifications are mandatory in all member states where a data breach is likely to result in a risk to individuals' rights and freedoms. Notification must occur within 72 hours of first becoming aware of the breach.

NATO Cooperative Cyber Defence (sic) Centre of Excellence

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCE) is a multinational and interdisciplinary cyber defence hub supporting member nations and NATO (2019). Experts, including researchers, analysts, and educators from the military, government, academia and industry provide cyber defence expertise from 25 nations: Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Italy, Latvia, Lithuania, the Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Spain, Sweden, Turkey, the United Kingdom and the United States.

CCDCE (2019) produced the Tallinn Manual 2.0, the most comprehensive guide for policy advisors and legal experts on how existing International Law applies to cyber operations. The Tallinn Manual process is continuing with legal, technical, strategic and operational assessment of cyber scenarios, aiming to publish a practical reference source for Cyber Commands."

NGOs Global

Many non-governmental organizations, (501(c)(3) and 501(c)(4)), academic, consumer or industry-based or a mixture, evaluate and recommend privacy and cybersecurity policy. The League of Women Voters of Oregon does not support or endorse any of the following examples, and all information comes from the organizations' websites.

Center for Democracy and Technology (CDT)

The Center for Democracy and Technology is a 501(c)(3) nonprofit organization that works to preserve the user-controlled nature of the internet and champion freedom of expression... and support(s) laws, corporate policies, and technology tools that protect the privacy of internet users, and advocate for stronger legal controls on government surveillance. They are headquartered in Washington, with an international presence in Brussels. CDT works inclusively across sectors and the political spectrum to find tangible solutions to today's most pressing internet policy challenges. Approximately 43% of their support is from corporations and 30% from foundations (CDT, 2019).

Data & Society (D&S)

Data & Society (D&S) addresses many of the complex privacy issues discussed here. The same innovative technologies and sociotechnical practices that are reconfiguring society – enabling novel modes of interaction, new opportunities for knowledge, and disruptive business paradigms – can also be used to invade privacy, provide new tools for discrimination, and harm individuals and communities. D&S is "committed to identifying thorny issues at the intersection of technology and society, providing and encouraging research that can ground informed, evidence-based public debates, and building a network of researchers and practitioners who can anticipate issues and offer insight and direction." They are an independent, 501(c)(3) research institute, founded by Microsoft and other sources. (Golebiewski, M & Boyd, D. 2019)

Digital Advertising Alliance (DAA)

The DAA is an independent, non-profit organization led by advertising and marketing trade associations. DAA "establishes and enforces responsible privacy practices across the industry for relevant digital advertising, providing consumers with enhanced transparency and control through multifaceted principles that apply to multi-site and cross-app data gathered in desktop, mobile web, or mobile app environments.

DAA participating companies are leaders in every US area, an interest-based advertising ecosystem that uses consumer information responsibly for marketing purposes in accordance with DAA Principles. Those participating companies include brand advertisers, agencies, publishers, ad networks, and ad tech companies. Enforcement of the DAA Principles extends beyond participating companies to cover every company using consumer data for interest-based advertising and other covered purposes under the Principles." (Digital Advertising Alliance, 2019).

Interactive Advertising Bureau (IAB)

"The Interactive Advertising Bureau (IAB) empowers the media and marketing industries to thrive in the digital economy. Its membership is comprised of more than 650 leading media companies, brands, and technology firms that are responsible for selling, delivering, and optimizing digital ad marketing campaigns. The trade group fields critical research on interactive advertising, while also educating brands, agencies, and the wider business community on the importance of digital marketing. IAB, with the IAB Tech Lab, develops technical standards and solutions. IAB is committed to professional development and elevating the knowledge, skills, expertise, and diversity of the workforce across the industry. The trade association advocates through the Washington, D.C. public policy office for its members and promotes the interactive advertising industry to legislators and policymakers. Founded in 1996, IAB is headquartered in New York City." (Interactive Advertising Bureau, 2109).

World Privacy Forum

The World Privacy Forum is a nonprofit, non-partisan 501(C)(3) public interest research group conducting in-depth research, analysis, and consumer education in the area of data privacy, and focuses on pressing and emerging issues. It is one of only a few privacy-focused NGOs conducting independent, original, longitudinal research.

Forum research has provided insight into predictive analytics, medical identity theft, data brokers, and digital retail data flows, among others. Focus areas include technology and data analytics broadly, focusing on health care data and privacy, large data sets, machine learning, biometrics, workplace privacy issues, and the financial sector.

The Forum was founded in 2003, working nationally and internationally to encourage collaborative non-profit efforts. The World Privacy Forum is funded by the Rose Foundation Consumer Privacy Rights Fund, the California Consumer Protection Foundation, by Cy Pres privacy settlements, general support funding from corporations, and by individual donations (World Privacy Forum, 2019).

US Federal Privacy and Cybersecurity Governance

Data protection was valued long before today's E-commerce and cybercrime. Government agencies and independent reformers both intruded upon individual privacy (Igo, 2018). The US Census and other federal agencies that aggregate data have periodically sparked privacy intrusion concerns (e,g, "*Quarantine! Eastern European Jewish Immigrants and the New York City Epidemics of 1892", Markel).* Public health officials tracked disease outbreaks to avert pandemics and protect public health. They tried to provide prompt treatment to determine exposure scope and, when necessary, isolate or quarantine contagious individuals. This presaged our current vaccine privacy rights battle, with control and use of information the crux. Several different privacy issues are at stake, relating to bodily privacy, health surveillance, data, and to some degree, "family privacy", e.g., who decides for the child: the parents or the state. The jurisdiction should be clarified as local, state, or federal.

Review of Federal Privacy Legislation and Regulatory Agencies

1950: The Federal Records Act, as amended, established a framework for Federal Agency records management programs. The National Archives and Records Administration assists Federal agencies in maintaining adequate and proper policy documentation and transactions. It is the primary agency for records management oversight. This is done by appraising records, regulating and approving the disposition of Federal records, operating Federal Records Centers and preserving permanent records. (US Archives, 2015).

The **Code of Federal Regulations** (CFR) contains administrative rules guiding agency operations. Many of our privacy protections are dictated by rule-making rather than statute. For example, the DHS Privacy statement is: "We will protect your information consistent with the principles of the Privacy Act of 1974, the E-Government Act of 2002, and the Federal Records Act."

The **Federal Register** (FR) publication system issues daily administrative rule-making notices, agency actions, and other government activities.

1974: The Privacy Act of 1974, (5 U.S.C. § 552a) establishes a code of fair information practices governing collection, maintenance, use, and dissemination of information about individuals, maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which data is retrieved by the name of the individual or by some identifier assigned to the individual

The Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register. The Department of Justice (DOJ) provides a list for systems of records with Federal Register citations, (DOJ, 2019). The Privacy Act prohibits the disclosure of a record about an individual from a system of records without the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The Act also provides individuals with a means by which to seek access to and amendment of their records, and sets forth various agency record-keeping requirements.

2002: The E-Government Act (DOJ, 2002). The availability of information, from personal to public, is easier today due to computers, digitized networks, internet access, and the creation of new information products. This Act recognized that these advances also have important ramifications for the protection of personal information in government records and systems. The Act covers "privacy impact assessments." (See the glossary.)

2011 & 2014: The Presidential and Federal Records Act Amendments, H.R. 1233, modernizes records management by focusing more directly on electronic records and complements National Archives and the Office of Management and Budget efforts to implement the 2011 Presidential Memorandum on Managing Government Records.

Major updates to the Presidential and Federal Records Acts gave the federal government the ability to:

- Expand the definition of federal records to include electronic records, the first federal record definition change since 1950.
- Confirm that federal electronic (form) record transference to the National Archives.
- Grant the US Archivist final determination for what constitutes a federal record.
- Authorize early transfers of permanent electronic federal and Presidential records to the National Archives, while legal custody remains with the agency or the President.
- Clarify Federal government officials' responsibilities when using non-government email systems.
- Empower the National Archives to safeguard original and classified records from unauthorized removal.
- Codify procedures by which former and incumbent presidents review presidential records for constitutional privileges. Formerly, this process was controlled by an Executive Order subject to change by different administrations.

The United States' regulatory approach to privacy protection is centered on personal data protection rather than individual data privacy, without encroaching on commerce, particularly digital commerce. The Congressional Research Service (2019) provides a comprehensive overview of key data privacy laws in the US and examines legal issues related to data protection. In the US governance framework, the limitations of constitutional protections are supplemented by federal and state statutes protecting individuals' personal information and sector-specific (e.g., health care, data breaches, student records) self-regulation where private businesses determine how they will manage user data (Fuchs, 2011).

2015: The Congressional Cybersecurity Act of 2015, tucked into a massive omnibus appropriations bill as Division N, enabled companies to voluntarily disclose cybersecurity threats and attempted hacks with other firms and the federal government (Kosseff, 2015). The Cybersecurity Act takes 136 of the bill's 2,009 pages, establishing detailed rules for private network operators to defend their networks, monitor possible threats, and collaborate with the federal government. The new law also bolsters the Department of Homeland Security's (DHS) cybersecurity efforts. The legislation's focus, "cybersecurity" appears in the bill nearly 200 times.

There is just one problem, however. The Cybersecurity Act does not define "cybersecurity."

The Department of Homeland Security (DHS)

The DHS Cybersecurity and Infrastructure Security Agency (CISA) has a list of 55 things the government most needs to protect from digital attacks. It includes "everything from electricity to elections to community health." DHS believes a cyberattack on any of these government or private sector services or functions could have a "debilitating effect" on national security, the US economy or public health (Marks, 2019).

Cybersecurity and Infrastructure Security Agency (CISA, in DHS)

The following is a quote from CISA's website:

"The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build a more secure and resilient infrastructure for the future.

The threats we face—digital and physical, man-made, technological, and natural—are more complex, and the threat actors more diverse than at any point in our history. CISA is at the heart of mobilizing a collective defense as we lead the Nation's efforts to understand and manage risk to our critical infrastructure.

Our partners in this mission span the public and private sectors. Programs and services we provide are driven by our comprehensive understanding of the risk environment and the corresponding needs identified by our stakeholders. We seek to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities." DHS CISA (2019).

CISA Organizational Resources

- **National Cyber Security Division (NCSD)**
  The National Cyber Security Division is a division of the Office of Cyber Security & Communications, within the DHS Directorate for National Protection and Programs. They collaborate with the private sector, government, military, and intelligence stakeholders to assess IT risks and mitigate vulnerabilities and threats affecting civilian, government, and private sector critical cyber infrastructures. NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. NCSD carries out the majority of DHS' responsibilities under the Comprehensive National Cybersecurity Initiative (2008). NCSD works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets.
- **Office of Cybersecurity & Communications (CS&C)**
  CS&C is responsible for enhancing the security, resiliency, and reliability of the nation's cyber and communications infrastructure. CS&C actively engages the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm these strategic assets. Learn more about CS&C.
- **Federal Network Security (FNS)**
  FNS collaborates across the Federal Government to enhance the nation's cybersecurity posture by identifying common requirements, collaborating with components of the federal enterprise, implementing policy and technical solutions, and monitoring the effectiveness of solutions. Learn more about FNS. (CISA organizational Resources, 2019)

Comprehensive Cyber Protection

- CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24-7 cyber situational awareness, analysis, incident response and cyber defense to federal, state, local, tribal and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response, and assessment to safeguard networks that support the essential federal civilian departments and agencies.

Infrastructure Resilience

- CISA coordinates security and resilience efforts with trusted private and public sector partners and delivers training, technical assistance, and assessments to federal stakeholders, infrastructure owners, and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for US critical infrastructure through the National Risk Management Center. DHS CISA (2019)

Emergency Communications

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools, and guidance to help partners develop emergency communications.
- Working with stakeholders, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue communications during natural disasters, acts of terrorism, and other man-made disasters.

National Risk Management Center (NRMC)

- The NRMC is a planning, analysis, and collaboration center working to identify and address the most significant risks to our nation’s infrastructure.
- The NRMC works in close coordination with the private sector and other key stakeholders in the critical infrastructure community to: identify; analyze; prioritize; and manage the most strategic national critical function risks.

Federal Communications Commission (FCC)

The FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia and US territories. An independent US government agency overseen by Congress, the commission is the United States' primary authority for communications law, regulation, and technological innovation. In its work facing economic opportunities and challenges associated with rapidly evolving advances in global communications, the agency capitalizes on its competencies (Federal Communications Commission, 2019):

- Promote broadband service and facility competition, innovation and investment
- Support the nation's economy by ensuring an appropriate competitive framework for unfolding the communications revolution
- Encourage the highest and best use of spectrum domestically and internationally
- Revise media regulations so new technologies flourish locally, with diversity
- Lead in strengthening the nation's communications infrastructure defense

The White House has a National Cyber Strategy:

> "America's prosperity and security depend on how we respond to the opportunities and challenges in cyberspace. Critical infrastructure, national defense, and the daily lives of Americans rely on computer-driven and interconnected technologies. As all facets of American life have become more dependent on a secure cyberspace, new vulnerabilities have been revealed and new threats continue to emerge." (White House, 2018)

Federal Trade Commission (FTC)

The Federal Trade Commission (FTC) is an independent US law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace… the Commission [is empowered] to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models…The FTC has brought enforcement actions addressing a wide range of privacy issues, including spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile…[and against] companies that have engaged in unfair or deceptive practices involving inadequate protection of consumers' personal data. (Federal Trade Commission, 2018).

Shaping State Legislation

Should federal or state-by-state cybersecurity laws protect personal, corporate, and government information while also ensuring adequate transparency for appropriate oversight? For example, elections are run locally but have national impact, how can election processes be protected from outside interference?

National Conference on Uniform State Laws (Uniform Law Commission)

The Uniform Law Commission (ULC) is working on cybersecurity and privacy. The Collection and Use of Personally Identifiable Data Committee has been formed for drafting:

- **2018** Uniform Civil Remedies for Unauthorized Disclosure of Intimate Images Act, though only a couple of states have acted on either of these, so far.
- **2016** Uniform Employee and Student Online Privacy Protection Act.
- **2015** Uniform Fiduciary Access to Digital Assets Act of 2015 has been enacted in most states.

Many uniform law projects affect technology and privacy issues, though they are not necessarily the projects' main focus. For example, Oregon has a study committee to determine whether legislation is needed governing event data recorders in cars. Typical projects take about 2 years, so expect to see a uniform act on this subject in 2021 (Sterling, 2019).

National Conference of State Legislatures (NCSL)

The National Conference of State Legislatures (NCSL) works to coordinate privacy and cybersecurity legislation discussions among states. From their Cybersecurity Legislation 2018,

> "States are addressing cybersecurity through various initiatives, such as providing more funding for improved security measures, requiring government agencies or businesses to implement specific types of security practices, increasing penalties for computer crimes, addressing threats to critical infrastructure and more." (NCSL, 2018).

In 2018, at least 35 states, the District of Columbia, and Puerto Rico introduced/considered more than 265 cybersecurity bills or resolutions. At least 22 states had enacted 52 bills as of 2018. NCSL recommends checking state legislative websites for current status, summaries and bill text versions. Key legislative activities included:

- Improve government security practices
- Provide cybersecurity program and initiative funding
- Restrict public disclosure of sensitive government cybersecurity information
- Promote workforce, training, and economic development

California Legislation

Compare: California Consumer Privacy Act

California's recent privacy act became law on June 28, 2018, and will go into effect in January 2020. It followed the EU GDPR and is considered the toughest privacy legislation enacted in any US state, giving more power to consumers with regards to their private data. It was written quickly, specifically citing misuse of personal data by Cambridge Analytica. Many companies that already comply with the GDPR may currently meet many of the California Consumer Privacy Act requirements. As with the GDPR, the Act provides several protections to consumers, including:

- **General Disclosure** – Commercial collection of any type of personal information should be disclosed in a clear privacy policy available on that company's website.
- **Specific Requests** – Should consumers wish to know what data is being collected; the company is required to provide the data. The request may include: categories of personal information collected; specific data collected about the individual; data collection methods used; a business's purpose for collecting it; and third parties to which it may be shared.
- **Deletion** – If consumers wish, personal information (with exceptions) will be deleted by the company.
- **Same Service** – Regardless of consumers' requests and preferences about how their personal information is handled, businesses are required to provide equal service and pricing even when consumers exercise their privacy rights under the Act.

(Sources: De Groot, 2019, Stephens, 2019, CA Legislative Information, 2018).

Oregon Legislation

With innovations and rapid technological advances, cybersecurity and privacy issues will be with us for years to come. Oregon agencies and audits have urged for improvements and new policies. Legislators in the Joint Committee for Legislative Information Management and Technology will address cybersecurity on every meeting agenda into the foreseeable future. The July 2019 audit, "Cybersecurity Controls Assessment," listed serious vulnerabilities, understaffing and other needs. Staff noted in committee that relevant requests had not been filled.

Public records laws have seen the most reform in 30 years (listed below). The Attorney General is convening a Consumer Privacy Task Force, aiming to develop legislative concepts for the 2021 session.

The Oregon Legislature has recently considered numerous bills relevant to this study, with the aim of improving cybersecurity, transparency, and privacy protection. Public records requests in Oregon must be reviewed before delivery, in order to check extensive disclosure exemption lists. Requests can be denied for varied, valid, protective reasons, including protecting cases pending in court. Transparency is

the focus of the Oregon "Sunshine Committee," formed as part of recent efforts to reform Oregon's public records law. It includes state and local officials, press representatives, a search engine executive, and a public interest nonprofit director. Campaign finance reform legislation is anticipated, in an effort to increase funding transparency. The following is a partial list of recent bills.

Identity Theft Bills

Critical 2018 cybersecurity bills responded to security breach disclosure delays in mid-September 2017. The Equifax and Experian personal data breaches affected over 143 million Americans. See the Oregon Attorney General's Scam Alert. Per Attorney General (AG) Rosenblum's testimony, these were deemed "massive and remarkable"(video here) for the breach scope and "unusually sensitive" nature of the data, including drivers' license and SSNs, financial accounts, debit and credit card numbers, access codes, etc., "virtually everything an aspiring hacker needs to build a convincing profile."

League member, Rep Nancy Nathanson, an identity theft victim, testified to her personal vulnerability, urging passage of these bills. See the February 2017 hearing clip. The two complex breach protection bills, HB 4114 and HB 4147 did not pass in 2018.

This League testimony for SB 1551 (2018) was not filed because the League lacked a position to defend personal information from theft.

> The League of Women Voters of Oregon supports the protection of personal and economic information privacy for individuals and private businesses. This information must be protected in a uniform manner across all financial institutions statewide. When there is a breach of security at a financial institution, this bill clearly and thoroughly sets out the notification procedures, timing and associated costs for protecting consumer identity and account information, including the freezing and unfreezing accounts and consumer reports. It also ensures the implementation of safeguards for prevention and disposal of consumer data. These rules are designed to help minimize the negative effects of identity theft for the consumer.

Vaccine Bills

Vaccination fits into the historic legal definition for public health privacy. There were 11 bills hotly contested in the Oregon 2019 Legislature addressing vaccine issues. About half involved various records transactions and none of those passed. The controversy occurred during a measles outbreak, at epidemic levels in nearby Washington state.

HB 3063 would have removed parents' ability to decline required immunizations for their children for religious or other non-medical reasons. The bill passed in the House and was referred to the Senate Health Care Committee. It was traded, with a gun safety reform package, SB 978 A, to negotiate support for the biggest public school funding bill in decades, HB 3427 Enrolled. The League supported all three bills, regretting the gun bill loss in the wake of the Florida Parkland School mass shooting.

Jordan Cove Energy Project and opposition surveillance

The two-part Jordan Cove Project, a proposed liquid natural gas processing plant, pipeline, and related dredging of Coos Bay to accommodate large tankers, has been extremely controversial and contested for years. Surveillance of opposition protesters was reported in the press: Coos Sheriff Acknowledges Monitoring of Fossil Fuel Project Opponents (Burns, 2019). Coordination was confirmed between local municipal and Oregon State Police, and also the US Forest Service, BLM (Bureau of Land Management), and the FBI (Federal Bureau of Investigation). The relevant Oregon Revised Statute pertains only to Oregon law enforcement, (ORS, 2013).

Oregon law is specific about the handling of information pertaining to individuals. No law enforcement agency, as defined in ORS 181.010 (Definitions for ORS 181.010 to 181.560 and 181.715 to 181.730), may collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct. [1981 c.905 §8].

In August 2019, LWVOR wrote to Oregon's Governor Brown and Attorney General Rosenblum calling for a public apology to those affected and an immediate stop to purported surveillance activities. A letter was forwarded to Congressman DeFazio, who in response reiterated the urgent need to repeal the Patriot Act.

League Studies and Policies

The League of Women Voters (LWV) studies issues and takes positions based on its studies, then advocates for legislative policies based on those positions. In the past, cybersecurity issues from various standpoints have been indirectly addressed.

First, LWVOR has considered the public safety aspect of cybersecurity. Here is an excerpt from LWVOR testimony in support of SB 90 Enrolled (2017) calling for Information Technology Security oversight by a State Chief Information Officer:

> Cybersecurity is an emerging, serious concern the League has not studied per se. LWVOR does have positions addressing public safety. Oregon state agency vulnerability has resulted in large data breaches, exposing other agencies' data and resembling an epidemic. This bill calls for protective immunity with cybersecurity rapid incident response and investigation. It supports the development of appropriate federal, multi-state or private sector programs, and efforts to support or complement the center's cybersecurity mission, including provision for accepting donations, with no overall state fiscal impact. The League of Women Voters of Oregon believes:
>
> - Responsible government should share in solving economic and social problems that affect the general welfare, including public safety and the protection of personal privacy.
> - Technical uncertainties must be publicly recognized and planned for.
> - Pertaining to safety, among all levels of government – federal, state, local, and the private sector – effective coordination is imperative in planning and carrying out programs, with responsibility and authority clearly designated.

League positions speak to protecting property rights as resources. As LWV attests in the League studies section, data is a valuable resource that merits the same protections as other property. Many people may not think of data as a resource. In "The world's most valuable resource is no longer oil, but data," The Economist (2017) argues for a new approach to regulating internet giants in today's data economy. Many sources suggest that data breaches are a significant and growing problem.
Indirect League positions to consider include personal property, the US Constitution on individual liberties, and privacy of records. Consider identity theft as stealing property. The state has the right to ensure that a person not be deprived of property without due process of law. Therefore, the League could take a position in favor of protecting papers, information (data) and property.

Lastly, the League has positions supporting the US Constitution:

Article [IV] (Amendment 4 - Search and Seizure)

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Article XIV of the Constitution of the United States of America (Amendment 14 - Rights Guaranteed: Privileges and Immunities of Citizenship, Due Process, and Equal Protection)

> 1: All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

V. KEY FINDINGS – Policy Issues

Privacy Policy Is Not Uniform

In the digital age, it is increasingly challenging to protect the personal identity and privacy of individuals, and to provide the open, secure flow of information in cyberspace for the benefit of individuals and society. Efforts to address privacy and cybersecurity policy concerns today are complicated by the increase in big data, E-commerce, and artificial intelligence. A 2014 Pew Research Center study found that 91% of consumers think they have "lost control over how their personal information is collected and use by companies." (Madden, 2014).

The US Constitution does not recognize an explicit right to privacy, nor does the US have a single, comprehensive Federal privacy law. Current policy debates focus on *personal information privacy* to protect an individual's identity, while *cybersecurity* policies protect information access. Personal data protections are based upon a mix of differing Federal and state statutes and rules, common law precedents and business practices. This patchwork of laws and regulations creates a fragmented set of statutes with different privacy protections for individuals and different compliance requirements for public and private sector institutions.

There are many reasons for policy fragmentation in the US. Federal laws primarily apply to how the Federal government handles personal information. Federal laws applying to private sector organizations narrowly target specific sectors and certain types of sensitive personal information. Sector-level regulation typically takes the form of industry self-regulation and enforcement of voluntary on-line privacy protections. Businesses operating partially or completely in unregulated sectors may offer few if any privacy protections. Regulation tends to focus on specific violations and past abuses, and thus be unable to address future concerns.

The rapid pace of technology innovation is prompting a rethinking of how to approach personal data protection. Some experts recommend adopting use-based policies to prevent harmful use of sensitive data. Use-based policies focus on data use rather controlling data access or transmissions, apply to the original data and any subsequently derived data. Both current understandings of personal information and redress for data violations continue to evolve.

Individuals and Personal Data Protection

Current laws focus on personal data privacy, particularly personally identifiable information (PII), which is unique to an individual (e.g., account numbers, social security numbers). The surge in big data means a wide array of non-unique information can be used to reidentify supposedly anonymous individual data. Regulating an individual's PII is fast becoming obsolete. Some experts recommend that privacy protection be applied to all identified and *identifiable* persons. Furthermore, personal data use is based on who holds and controls the data. This means data about individuals collected by business or government is controlled by the collecting entity, not the person represented by that data and affected by how the data are used.

Individuals are largely responsible for protecting their own data, while computing service providers are responsible for cybersecurity compliance and protecting data access. Current laws are designed to assure data holders have a safe and secure system of controls for handling personal data. The primary tools to achieve this are user *choice* and *notice and consent* protocols, both intended to give the user greater control over their data. While these agreements may still be effective in some situations, experts argue they are pointless and cumbersome for users, ill-suited to the current realities of big data applications, and cannot address unanticipated future data uses. (Cate, Cullen, & Mayer-Schoenberger, 2014). Instead of consumer choice and notice and consent, many experts recommend shifting responsibility for data from individual users to the data holders. Data holders should become responsible stewards of data, protecting user's interests and accepting increased liability for harms to data users (see below).

Under US law, individuals whose data privacy is violated have limited legal remedies to hold firms accountable for improper data use. Privacy harms for data breaches are narrowly defined as causing physical, financial, or reputational loss. Some experts recommend recognizing privacy and security harms from improper use and inadequate protection of data. They also recommend a broader definition of harm that includes future risks such as identity theft and fraud, and other intangible harms.

E-Commerce Data Protections

E-Commerce is a business model driven by consumer data where private sector firms use data tracking and big data analytics to profit from personalized advertising. Individual data is a commodity and consumer profiling is highly profitable, yet third party users are often unregulated. In the US, the Federal Trade Commission (FTC) oversees consumer information privacy, enforces data protection regulations, and protects consumers against unfair or deceptive business practices. Using voluntary self-regulation, firms that gather, analyze, and distribute consumer information define how they will handle responsibility for individual's information. The FTC encourages on-line businesses to adopt fair, transparent privacy practices, and may act to assure firms comply with their own stated practices. It relies on consent agreements to remedy business fair practice violations because it does not have authority to impose fines.

With sector-specific, voluntary regulation it is not clear how firms protect specific personal information, and much personal information may be unprotected. Some businesses are subject to multiple overlapping requirements and others have few requirements. Information transferred to a third party may not be regulated, so data protections are lost as data changes hands. Businesses that operate in multiple sectors or that expand into new business sectors may not be regulated, creating gaps in privacy

protection. The weaker enforcement mechanisms found in self-regulation limit consumers' recourse for violations.

Stakeholders and experts have identified many privacy and cybersecurity policy issues, and there is a growing consensus for the need to find solutions. As with many policy questions today, the next step is to find the political will to make needed privacy and cybersecurity reforms.

REFERENCES

Abomhara, M. & Køien, G. M. (2015) Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. Journal of Cyber Security and Mobility, 4(1): 65.

Acquisti, A, Taylor, C, and Wagman, L. (2016) The Economics of Privacy. American Economic Association.

Alexander, D. (2019) AI Advancements Are Making It Easier to Hack Biometric Systems, Interesting Engineering

American Civil Liberties Union (ACLU) (2019), Cybersecurity.

American Civil Liberties Union (ACLU). (n.d.) Factsheet: The NYPD Muslim Surveillance Program.

Bamberger, K. (2013) Privacy in Europe: Initial Data on Governance Choices and Corporate Practices.

Bellemare, A. (2019) The real 'fake news': how to spot misinformation and disinformation online. CBC News.

Bennett, C.J., and Raab, C. (2006) The Governance of Privacy. MIT Press.

Bennett, C. J. (2002) Information Policy and Information Privacy: International Arenas of Governance. Journal of Law, Technology, and Policy.

Bennett, C J. (2013) The politics of privacy and the privacy of politics: Parties, elections and voter surveillance in Western democracies. First Monday, 18, 8.

Berlinger, J, and Regan, R. (2019) Hong Kong uses colonial-era emergency law to ban wearing masks at protests, sparking night of violence. CNN.com.

BIA Advisory Services. (2019) US Local Advertising Forecast. BIA Advisory Services.

Bing, C. (2019) Exclusive: US officials fear ransomware attack against 2020 election. Reuters.

Blaze, M. (2019) DEF CON 26 Voting Village Report on Cyber Vulnerabilities in U. S. Election Equipment, Databases, and Infrastructure. DeF CON.

Bogart, L. (1962) The Researcher's Dilemma, Current Controversies in Marketing Research. ed. Leo Bogart (Chicago: Markham, 1969).[MS1]

Bohn J., Coroamă V., Langheinrich M., Mattern F., Rohs M. (2005) Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing. Weber W., Rabaey J.M., Aarts E. (eds) Ambient Intelligence. Springer, Berlin, Heidelberg.

Bowman, B. (2019 04) Biometric Hacking. Security Boulevard.

Brice-Saddler, M. (2019, July 26) An Equifax hack settlement promises a $125 payout. The truth is more complicated. The Washington Post.

Brim, O. (1967) Reaction to the Papers, Journal of Educational Measurement 4: 1 (Spring 1967). The Known Citizen.

Burns, J. (2019) Coos Sheriff Acknowledges Monitoring Of Fossil Fuel Project Opponents.

California Legislative Information. (2018) "TITLE 1.81.5. California Consumer Privacy Act of 2018 [1798.100 - 1798.199] (Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3.)".

California Legislative Information, (2019) AB-1215 Law enforcement: facial recognition and other biometric surveillance.

Campbell, A., Taggart, K. (2016) A Traffic Cop's Ticket Bonanza In A Poor Texas Town. BuzzFeed News.

Cate, F.H., Cullen, P., & Mayer-Schoenberger, V. (2014). Data Protection Principles for the 21st Century. Oxford, England: Oxford Internet Institute (OII), University of Oxford.

Center for Democracy and Technology (CDT) (2019)

Chappell, B. (2019) Hong Kong My Ban Face Masks By Invoking Colonial-Era Emergency Powers. National Public Radio.

Chesney, R. & Citron, D. K. (2018). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security; Draft.

Citron, D. (2019) Deepfakes Undermine Truth and Threaten Democracy [Ted Talk video].

Citron, D. (2019). Prepared Written Testimony and Statement for the Record. Hearing, House Permanent Select Committee on Intelligence.

Clarno, B. (2019) Oregon Election Security Exercise. Oregon Secretary of State press release.

Clement, J. (2019, Nov 20). Worldwide digital population as of October 2019. Statistica.

Corbley, M. (2019) Blind Man Develops Smart Cane That Uses Google Maps and Sensors to Identify One's Surroundings. GoodNews Network.

Coleman, J. (2019) Google has collected health data on millions of Americans through new partnership: report.

Craig, A, Shackelford, S, Hiller, J. (2015) Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis, American Business Law Journal.

CTIA. (2019) Cellular Telecommunications Industry Association [Trade Association]

Curran, D. (2018) Are you ready? Here is all the data Facebook and Google have on you.

Cybersecurity and Infrastructure Security Agency (CISA). (2019) About CISA. CISA, Department of Homeland Security. Retrieved from: https://www.cisa.gov/about-cisa

Cybersecurity and Infrastructure Security Agency (CISA). (2019) The War on Pineapple: Understanding Foreign Interference in 5 Steps. CISA, Department of Homeland Security.

Cybersecurity and Communications (CS&C). (2019). CS & C Overview pages. CS&C, CISA, Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency (CISA). (2019) CISA National Critical Functions Set. CISA, Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency (CISA). (2019) CISA Organizational Resources. CISA, Department of Homeland Security.

Cybersecurity and Infrastructure Security Agency (CISA). (2019) CISA Risk Management. CISA, Department of Homeland Security.

Data & Society, (2019) Data & Society advances public understanding of the social implications of data-centric technologies and automation.

De Groot, J. (2019) What is the California Privacy Act? Data Insider [blog], Digital Guardian.

Dell Customer Support. (2019) What are the different types of Viruses, Spyware and Malware that can infect my computer? Dell Customer Support.

Department of Homeland Security (DHS) NICCS. Glossary of Common Cybersecurity Terminology. DHS National Initiative for Cybersecurity Careers and Studies.

Dickerson, C. (2019) US Government Plans to Collect DNA From Detained Immigrants. The New York Times.

Digital Advertising Alliance (DAA). (2019)

Disney, A. (2014) KeyLines FAQs: Social Network Analysis. Cambridge Intelligence.

Do Not Call Registry. (2019) National Do Not Call Registry. Federal Trade Commission (FTC).

Dugan, M. (2017). Online Harrassment. Pew Research Center.

EPIC (n.d.) Big Data and the Future of Privacy, Electronic Privacy Information Center.

EU GDPR.org. (2018) GDPR Key Changes. GDPR.EU.org.

European Commission, European Union. (2019) Government Data Protection Regulation (GDPR). European Commission, European Union.

Fagone, J. (2017) The Woman Who Smashed Codes: A True Story of Love, Spies, and the Unlikely Heroine Who Outwitted America's Enemies. New York: HarperCollins.

Federal Communications Commission (FCC). (2019)

Federal Trade Commission (2018). Privacy and Data Security Update: 2018.

Federal Trade Commission (FTC). (1999) Gramm-Leach-Bliley Act.

Federal Trade Commission (FTC). (2009) Self-Regulatory Principles For Online Behavioral Advertising. FTC Staff Report.

Feldman, B. (2019, Oct 31). MacArthur Genius Danielle Citron on Deepfakes and the Representative Katie Hill Scandal. New York Magazine.

Feldman, L et al. (2019) Emotional Expressions Reconsidered: Challenges to Inferring Emotions From Human Facial Movements. APS Assn for Psychological Science.

Flaherty, D. (1991) On the Utility of Constitutional Rights to Privacy and Data Protection. Case Western Reserve Law Review, 41:3.

Fowler, G. (2019) The spy in your wallet. Washington Post.

Friedersdorf, C. (2016) An Unprecedented Threat to Privacy. The Atlantic.

Fuchs, C. (2012) The Political Economy of Privacy on Facebook. Television and New Media, Sage Journals.

Fuchs, C. (2011) Teaching and Learning Guide for: New Media, Web 2.0 and Surveillance. Department of Informatics and Media, Uppsala University, Sweden.

Funk, M (2019) How ICE Picks Its Targets in the Surveillance Age. New York Times Magazine.

Funk, M. (2016) Should We See Everything a Cop Sees? New York Times Magazine

Gellman, R, and Dixon, P. (2011) Many Failures: A Brief History of Privacy Self-Regulation. World Privacy Forum.

Golebiewski, M & Boyd, D. (2019) Data Voids: Where Missing Data Can Easily Be Exploited. Data & Society

Goodin, D. (2012) Why passwords have never been weaker- and crackers have never been stronger. Ars TECHNICA.

Google Support. (2019) What is the difference between copyright and privacy? Google Copyright Help Center.

Hanvey, B. (2019) Your car knows when you gain weight. The New York Times.

Harwell, D. (2019) Doorbell-camera firm ring has partnered with 400 police forces, extending surveillance reach. Washington Post.

Haslam, K. (2019) Can Macs Get Viruses & Do Macs Need Antivirus Software? Macworld.

Hill, K. (2019) Katie Hill: It's Not Over After All. New York Times.

Hoffman, D. (2019) Intel executive: Rein in data brokers. The New York Times.

Igo, S. (2018) The Known Citizen. Harvard University Press.

Interactive Advertising Bureau (IAB). (2109)

Kaye, K. (2013) Mastercard, AMEX Quietly Feed Data to Advertisers. AdAge.

Keller, H, Dance, G. (2019) The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong? The New York Times.

Kerry, C. (2018) Why protecting privacy is a losing game today- and how to change the game. The Brookings Institution.

Kosseff, J. (2015) Defining Cybersecurity Law. Iowa Law Review Vol. 103, Issue 3.

Kraudel, R. (2019) What are biometric parameters and why do they matter? Velencel Biometric Sensors.

Kwet, M. (2019) In Stores, Secret Surveillance Tracks Your Every Move. The New York Times.

LaForgia, R. (2015) Cyberwarfare, Surveillance, and Security. University of Adelaide.

League of Women Voters of Oregon (2017) Election Methods Study Update.

Levitt, J. (2007) The Truth About Voter Fraud. Brennan Center for Justice.

Liberatore, S. (2019) California bans cops from using facial recognition technology in bodycams amid fears of 'dystopian technology'. Daily Mail.

Lindeman, M. & Stark, P.B. (2012). A Gentle Introduction to Risk-limiting Audits. IEEE Security And Privacy, Special Issue On Electronic Voting.

Maciag, M. (2019) Despite Census Citizenship Ruling, Officials Say 'Damage Has Been Done'. GOVERNING The States and Localities; Public Safety & Justice.

Madden, M. (November 12, 2014). Public Perceptions of Privacy and Security in the Post-Snowden Era. Pew Research Center

Markel, H. (1999). East European Jewish Immigrants and the New York City Epidemics of 1892. John Hopkins University Press.

Mateescu, A, Rosenblat, A, & Boyd. (2015) Police Body-Worn Cameras. New York: Data & Society Research Institute.

Matthiessen, C, and Fratrik, M. (2019) US Local Advertising Forecast. BIA Advisory Services.

Messer, H. and Dance, G. (2019) Why We Should Stop Fetishizing Privacy. The New York Times.

Metz, C. (2019) Facial recognition Tech is growing stronger, thanks to your face. The New York Times.

Miner, L. (2019) For a longer, healthier life, share your data. The New York Times.

Morawski, J. (2015) Epistemological Dizziness in the Psychology Laboratory: Lively Subjects, Anxious Experimenters, and Experimental Relations, 1950-1970.

National Conference of State Legislatures. (2019)

National Public Radio. (2019) 'Aisles Have Eyes' Warns That Brick-And-Mortar Stores Are Watching You.

National Public Radio. (2019) How Hijacked Cellphone Numbers Can Be Security Risks,

NATO Cooperative Cyber Defence Centre of Excellence. (2019) NATO CCD COE. Tallinn, Estonia.

Newman, L. (2019) The Biggest Cybersecurity Crises of 2019 So Far. Wired.com.

NIST. Computer Security Resource Center Glossary. National Institute of Standards and Technology

NYU Tandon School of Engineering. (2018) Machine Learning Masters the Fingerprint to Fool Biometric Systems. NYU Tandon School of Engineering.

Office of Cyber Security & Communication (CS&C). (2019) CS & C Overview pages. CISA, CS&S, Department of Homeland Security. Office of Cybersecurity and Communications.

Oregon Attorney General Consumer Protection.)2019) Report Scams and Frauds. Oregon Dept of Justice.

Oregon Attorney General Consumer Protection, (2019) SCAM Alert Network.

Oregon Cybersecurity Advisory Council. (2017) Oregon Cybersecurity Advisory Council. Cyber Oregon.

Oregon Revised Statute. (2013) ORS 181.575 regarding collecting individual's information..

Oregon Secretary of State. (2019) Oregon Election Security Exercise. Press Release.

Ortiz-Ospina, E. (2019, September 18). The rise of social media. Our World in Data.

Pawlyk, O. (2019, August 16). Hackers Find Serious Vulnerabilities in an F-15 Fighter Jet System. Military.com.

Pettit, M. (2013) The Science of Deception Psychology and Commerce In America. The University of Chicago Press.

Plaisance, P. (2019) Ethics and Synthetic Media: Machine-learning digital 'people' pose moral questions of harm and authenticity. Psychology Today.

Police Executive Research Forum. (2018) Cost and Benefit of Body-Worn Camera Deployments. Police Executive Research Forum.

Porter, J. (2019) Huge security flaw exposes biometric data of more than a million users. The Verge.

Preston, D. (2014) How the Internet of Everything Transforms Traditional Industries. Forbes.

Raab, C D. (2004) The Future of Privacy Protection: Cyber Trust & Crime Prevention Project.

Ramirez, E. (2017) Cross-Device Tracking A FTC Report. The Federal Trade Commission.

Rogers, K, Karni, A. (2019) Trump's opponents want to name his big donors. His supporters say it's harassment. The New York Times.

SANS Institute. Glossary of Security Terms. SANS (ESCAL Institute of Advanced Technologies).

Satariano, A. (2019) Right to Be Forgotten. The New York Times.

Satariano, A. (2019) Europe is Reining in Tech Giants. But Some Say it is Going Too Far. The New York Times.

Satariano, A. (2019) Facebook Can Be Forced to Delete Content Worldwide, E.U.'s Top Court Rules. The New York Times.

Schuster, E. (1997) Fifty Years Later: The Significance of the Nuremberg Code.

Scott, M. (2014) 'Right to Be Forgotten' Should Apply Worldwide, E.U Panel Says. The New York Times.

Seleky, A. (2019) Federal officials work with Oregon, other states to protect elections against hackers. Salem Statesman Journal.

Selsky, A. (2019) Overseas Oregonians can 'vote by mobile' in 2 counties

Shane, S. Mazzetti, M. (2019) The Plot to Subvert an Election: Unraveling the Russia Story So Far.

Simonite, T. (2019) Amazon Says It Can Detect Fear on Your Face. You Scared? Wired.

Simonite, T. (2019) The Best Algorithms Struggle to Recognize Black Faces Equally. Wired.com.

Singer, N. (2019) When Apps Get Your Medical Data, Your Privacy May Go With It. New York Times.

Software Engineering Institute CMU. (2017) Cyber Hygiene: A Baseline Set of Practices. Carnegie Mellon University.

Soufan, A, and Jackson, M. (2019) Interim Report of the Countering Foreign Influence Subcommittee. Homeland Security Advisory Council.

Stark, L. (2011) Behind Closed Doors: IRBS and the Making of Ethical Research.

Stephens, J. (2019) California Consumer Privacy Act. American Bar Association.

Sterling, N. (2019) Uniform Law Commission.

Supreme Court of the United States. (2019) Dept of Commerce et al. v. New York et al. Supreme Court Opinions.

Surane, J. (2018) Banks Are Eying $1.5 Trillion in Credit Card Secrets. Bloomberg Businessweek.

Symantec. (2019) 5 tips for social media security and privacy. Norton by Symantec.

Taylor, J. (2019) Major breach found in biometrics system used by banks, UK police and defence firms. The Guardian.

TechAmerica Foundation, 2019. Demystifying Big Data: A Practical Guide To Transforming The Business Of Government. TechAmerica Foundation, Big Data Commission.

The White House. (2018) National Cyber Strategy of the United States of America. The White House.

Totenberg, N, and Wang, H. (2019) Trump Threatens Census Delay After Supreme Court Leaves Citizenship Question Blocked. National Public Radio.

US Archives. (2014) National Archives Welcomes Presidential and Federal Records Act Amendments of 2014.

US Census Bureau. (2019) History. United States Census Bureau. US Census Bureau. (2019) Index of Questions, 2019.

US Congress. (2014) H.R.1233 - Presidential and Federal Records Act Amendments of 2014. Congress.gov.

US Dept of Justice. (2019) DoJ Systems of Records. US Dept of Justice.

US Dept of Justice. (2002) E-Government Act of 2002. US Dept of Justice.

US Dept of Justice. (2019) Privacy Act of 1974. US Dept of Justice.

US Federal Trade Commission. (1999) Gramm-Leach-Bliley Act. Federal Trade Commission (FTC).

Valentino-DeVries, J, Singer, N., Keller, M., & Krolik, A. (2018) Your apps know where you were last night and they're not keeping it secret. The New York Times.

Valentino-DeVries, J, Singer, N., Keller, M., & Krolik, A. (2018) How to Stop Apps From Tracking Your Location. The New York Times.

Vosoughi, S., Roy, D., Aral, S., (2018) The spread of true and false news online. Science, 359: 6380, 1146-1151. DOI: 10.1126/science.aap9559.

Want, R. (2018). An Introduction to Ubiquitous Computing. In J. Krumm, ed. Ubiquitous Computing Fundamentals. NY: Chapman and Hall/CRC.

Warzel, C. (2019) Facebook Under Oath: You Have No Expectation of Privacy. The New York Times Privacy Project.

Watkins, E. A. (2018). Guide to Advertising Technology. Columbia University: Tow Center for Digital Journalism.

Weiser, M. (1993) Ubiquitous Computing. IEEE Computer Society, October 1993, pp. 71-72, Vol 26.

West, DM. 2016. How 5G technology enables the health internet of things. Center for Technology Innovation at Brookings.

Westin, A F. (1967) Privacy and Freedom.

White House. (2008) Comprehensive National Cybersecurity Initiative.

Winn, J K, and Dixon, P. (2019) Consumer Privacy and Data Security Standards Act of 2019. World Privacy Forum.

World Privacy Forum. (2019)

Wyden, R. (2016) Issues: Secret Law. Senate.gov.

Yaffe-Bellany, D. (2019) Here's What You Need to Know About the Capital One Breach. The New York Times.

Zlatanov, N. (2015) Computer Security and Mobile Security Challenges. ResearchGate.

Zuboff, A, Jackson, M. (2019) Homeland Security Advisory Council Interim Report of the Countering Foreign Influence Subcommittee. Department of Homeland Security

Zuboff, S. (2019) The Age of Surveillance Capitalism: The Fight for a Human Future at the Frontier of Power. Public Affairs Books.

APPENDIX A: Glossary

Definition Sources

The study committee collected a broad spectrum of current information. Please understand that term interpretations are a moving target because privacy and cybersecurity Issues evolve and expand daily. All links verified January 22, 2020.

The following glossary definitions are directly quoted from various sources, including individuals and corporate authors identified by these acronyms:

· CNSS: Committee on National Security Systems Instruction, combining terms from the Dept. of Defense, Intelligence Community, and NIST, (CNSSI Glossary)

· NIST: Computer Security Resource Center (CSRC), Information Technology Laboratory (ITL), National Institute of Standards and Technology (NIST), (NIST Glossary)

· NICCS: National Initiative for Cybersecurity Careers and Studies (NICCS), Department of Homeland Security. Glossary of Common Cybersecurity Terminology, (NICCS Glossary)

· SANS: SANS Technology Institute, part of ESCAL Institute of Advanced Technologies; offers specialized training and education for information security professionals. (SANS Glossary)

Definitions

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (NIST Glossary)

> **Multi-Factor Authentication (MFA)**: An authentication system requiring more than one distinct factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators to provide different factors. Three authentication factors can be something you know, something you have, and something you are. (NIST Glossary)
>
> NOTE: 'Two-factor' authentication is commonly used to add one extra layer of security to consumer devices.

Big data: Large volumes of high velocity, complex and variable data that require advanced techniques and technologies to enable the capture, storage, distribution, management, and analysis of the information. (Big Data Commission, TechAmerica Foundation.)

Biometric: Measurable physical characteristics or personal behavioral traits used to identify or verify the claimed identity of an individual. Facial images, fingerprints, and handwriting samples are all examples of biometrics. (CNSSI Glossary)

Bot: A computer connected to the Internet that has been surreptitiously/secretly compromised with malicious logic to perform activities under command and control by a remote administrator. (NICCS Glossary)

Botnet: A collection of computers compromised by malicious code and controlled across a network. (NICCS Glossary)

Breach: The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. (NICCS Glossary)

Cloud computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST Glossary)

Cookie: A piece of state information supplied by a Web server to a browser, in a response for a requested resource, for the browser to store temporarily and return to the server on any subsequent visits or requests. (CNSSI Glossary)

Cyber Hygiene: a set of practices for managing the most common and pervasive cybersecurity risks faced by individuals and organizations. (Software Engineering Institute, Carnegie Mellon University, 2017)

Cybersecurity: Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (CNSSI Glossary)

Deep learning: a type of machine learning that trains a computer to perform human-like tasks, such as recognizing speech, identifying images or making predictions. Instead of organizing data to run through predefined equations, deep learning sets up basic parameters about the data and trains the computer to learn on its own by recognizing patterns using many layers of processing. (SAS Institute)

De-identification: general term for any process of removing the association between a set of identifying data and the data subject. (NIST Glossary)

Denial of Service (DoS): The prevention of authorized access to a system resource or the delaying of system operations and functions. (NIST Glossary)

Disinformation: The deliberate creation and/or sharing of false information in order to mislead (Bellamare, 2019).

Distributed Denial of Service (DDoS): A denial of service technique that uses numerous hosts to perform the attack. (NIST Glossary)

Domain: A sphere of knowledge, or a collection of facts about some program entities or a number of network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe sub-domains or host. In Windows NT and Windows 2000, a domain is a set of network resources (applications, printers, and so forth) for a group of users. The user need only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network. (SANS Glossary)

Domain name: A domain name locates an organization or other entity on the Internet. (SANS Glossary)

Exploit: A technique to breach the security of a network or information system in violation of security policy. (NICCS Glossary)

Facial recognition: see biometric above [A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iriscan samples are all examples of biometrics.] (NIST Glossary)

Firewall: A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. (NIST Glossary)

Hacker: Unauthorized user who attempts to or gains access to an information system. (NIST Glossary)

Internet of Things (IoT): The network of physical objects, machines, people, and other devices that enable connectivity and communications to exchange data for intelligent applications and services. (West, 2016. (Center for Technology Innovation at Brookings).

Intranet: A computer network, especially one based on Internet technology, that an organization uses for its own internal (and usually private) purposes and that is closed to outsiders. (NIST Glossary)

Internet Protocol (IP): The method or protocol by which data is sent from one computer to another on the Internet. (SANS Glossary)

Local-area network (LAN): A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network. (NIST Glossary)

Malware (malicious code): Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. These include ransomware, spyware, Trojan horses, viruses, worms, and other code-based entities that infect hosts. (NIST Glossary)

[See malware example definitions ransomware, spyware, Trojan horse, virus, and worm.]

Misinformation: the act of sharing information without realizing it's wrong. (Bellamare, 2019).

Network: Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices. (NIST Glossary)

Penetration testing: A test methodology intended to circumvent the security function of a system. Note: Penetration testing may leverage system documentation (e.g., system design, source code, manuals) and is conducted within specific constraints. Some penetration test methods use brute force techniques. Also known as “pen testing.” (NIST Glossary)

Personally identifiable information (PII): Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother’s maiden name, etc.). (NIST Glossary)

Protected Health Information (PHI): PHI stands for Protected Health Information. The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. (HHS.gov)

The HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes.

Phishing: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent email or website solicitation, with an imposter masquerading as a legitimate business or reputable person. “Spear-phishing” is a targeted attack for particular data. (CNSSI Glossary)

Privacy (Informational): The control or protection of personal information (Acquisti, Taylor, & Wagman, 2016).

Risk-limiting audit: a method to ensure that at the end of the canvass, the hardware, software, and procedures used to tally votes found the real winners. (Lindeman & Stark, 2012)

Ransomware: A type of malware that is a form of extortion. It works by encrypting a victim's hard drive denying them access to key files. The victim must then pay a ransom to decrypt the files and gain access to them again. (SANS Glossary)

Spyware: Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code. (NIST Glossary)

Trojan horse: A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program. (CNSSI Glossary)

Ubiquitous Computing: "…small, networked portable computer products in the form of smart phones, personal digital assistants (PDAs), and embedded computers built into many…devices." (Want, 2018, pg. 2)

Virus: A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk. See malicious code. (CNSSI Glossary)

Virtual Private Network (VPN): A data network that enables two or more parties to communicate securely across a public network by creating a private connection, or "tunnel," between them. (NIST Glossary)

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively. (NIST Glossary)

Wide area network (WAN): A physical or logical network providing data communications to a larger number of independent users than are usually served by a local area network (LAN). WANs usually spread over a larger geographic area. (NIST Glossary)

APPENDIX B: Privacy Policies

Governments, NGOs, and commercial firms establish policies to protect themselves, to address legal concerns from both aspects of privacy, protection from disclosure and transparency to access information.

Privacy policies focus on the internet and specific websites. Privacy statements were found on sites for government agencies, organizations (profit and non-profit), and commerce. This study does not include individuals or local organizations because many do not have privacy statements.

- American Civil Liberties Union (ACLU) https://www.aclu.org/issues/privacy-technology/internet-privacy/cybersecurity accessed 2019 07 17
- National Association for the Advancement of Colored People (NAACP) https://naacp.org/privacy-policy/ accessed 2019 07 17
- National Rifle Association (NRA) https://membership.nrahq.org/privacy.asp accessed 2019 07 17
- National Republican Campaign Committee (NRCC) https://www.nrcc.org/privacy-policy/ accessed 2019 07 17
- Nature Conservancy https://www.nature.org/en-us/about-us/who-we-are/accountability/privacy-policy/ accessed 2019 07 17
- League of Women Voters (LWV) https://www.lwv.org/privacy-policy accessed 2019 07 17
- Chase https://www.chase.com/digital/resources/privacy-security/privacy/online-privacy-policy.html accessed: 2019 07 17
- Amazon: https://www.amazon.com/gp/help/customer/display.html?nodeId=468496 accessed 2019 07 17
- Firefox https://www.mozilla.org/en-US/privacy/firefox/ accessed: 2019 06 04
- Johnson & Johnson (J&J) https://www.jnj.com/corporate/privacy-policy accessed 2019 09 26
- Mississippi https://www.ms.gov/Site/PrivacyPolicy accessed 2019 09 26

APPENDIX C: Legislation

Federal Law

Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, requires financial institutions – companies offering loans, financial or investment advice, or insurance – to explain their information-sharing practices to customers and to safeguard sensitive data, (**FTC, 1999**).

Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, was enacted to promote accuracy, fairness, and privacy of consumer information by consumer reporting agencies. (**FTC, 2011**)

Oregon Legislation

Banking Security Breach Rules

2018 **SB 1551 Enrolled**: *See the statute link for details, paraphrased here for brevity:* Requires consumer notification for security breaches, from those who manage or got notice of personal information security breaches, subject to breach size conditions.

Election Bills that Passed, Oregon 2019 - A Win for Transparency and Privacy!

Immigration status privacy during court proceedings

SB 2932 Enrolled criminal defendants immigration status, passed on partisan lines.

- **A hate/bias crime bill**
  SB 577 Enrolled This bill echoes numerous legal privacy rights mentioned earlier in this paper and defined in American Jurisprudence: the right to be "let alone", the right to a "private sphere", and the right to political privacy. It calls for a standardized method of recording relevant data, to serve the individual, arguably both protecting bias crime victims' privacy and increasing transparency to allow their civil rights protection.
- **National Popular Vote Interstate Compact**
  SB 870 Enrolled enacts the Interstate Compact in Oregon for electing the US President by National Popular Vote. League has supported this since 1973.
- **Undisclosed ballot measure funding**
  HB 3348 Enrolled requires a financial impact disclosures by the Financial Estimate Committee: "MEASURE SPENDS MONEY WITHOUT IDENTIFYING A FUNDING SOURCE," if no source is provided, for initiatives costing the public more than $100,000. The League supported.
- **Prohibit concurrent candidate listing as election official in voting materials**
  SB 670 Enrolled prohibits voting material references to overseeing elections officials when they run as candidates. The League supported the related **HB 3049**.
- **Risk-limiting election audits** **SB 944 Enrolled**, institutes risk-limiting election audits, with League support.
- **Referral to Regulating Campaign Transparency** bills would have amended the state constitution to allow regulation of political campaign moneys. **SJR 18** eventually passed, will be on the November 2020 ballot, and will enable the next two bills. **This was a major victory for reform advocates after decades of attempts.**

- **Transparency, HB 2716** will require disclosure of donor information in campaign ads. **HB 2983** will require disclosure of "dark money" by organizations intending to influence Oregon elections. The problem with these two bills is that they are just an outline of significant reform with high dollar thresholds, and do not include any "drill down" to the actual source of the campaign contributions.

Election Bills that Failed to Pass - Oregon 2019

- **State-Wide "They Represent You" incumbent Website**
  HB 2210 The Veterans and Emergency Preparedness Committee forwarded our bill pre-session, as a "resiliency preparedness" cybersecurity issue to the Joint Information Management and Technology Committee. State Archives is discussing BlueBook links. This incumbent information website, to list all Oregon elected officials, is searchable by address. The web site has been built by the state Geospatial Enterprise Office and populated with League-researched data. It needs cybersecurity maintenance and oversight. The bill did not get a hearing.
- **Centralized, Online List of all Oregon Candidates**
  HB 2234, our bill for an optional, centralized, statewide online candidate filing system. Note that the Elections Division claims the need to replace two mutually exclusive, outdated candidate filing programs: OCVR, Oregon Centralized Voting Records, is used for local candidates and **is not posted publicly**. ORESTAR, for state-level candidate filing and all candidate financial tracking, **is posted online**, an important asset for our voter transparency. The bill failed to get out of committee.
- **Listing of Campaign Contact Information**
  HB 2685, our bill advocated for publicly listed candidate contact information, barring campaign use of incumbent office emails and telephone numbers. The bill would have helped voter service access, but it was not heard.
- **Listing of Race, Ethnicity and Language in Voter Registration**
  HB 3202 would have allowed voters to share race, ethnicity, and/or preferred language when registering to vote. The League was prepared to testify only to preferred language. The bill was not heard.
- **Voter Registration Task Force**
  HB 3441 set up an automatic voter registration task force, relevant for election transparency. LWVOR urged adoption of "filer voter," a Department of Revenue expansion beyond the DMV voter registration. Despite League support, it did not get out of committee.
- **Small Donor Elections**
  HB 3004 would allow certain candidates to opt for public campaign fund matching, up to $250 six-to-one with limited public funds. It is similar to an adopted Portland city elections program. A similar bill, **SB 1014**, was briefly considered in the Senate, but neither bill passed. The League believes these are needed campaign finance reforms.
- **Set Campaign Contribution Limits**
  HB 2714 A See the Campaign Finance Reform bill success. Taken as a group, these address transparency in campaigning and set actual contribution limits. The bill passed in the House, not in the Senate.

Privacy/Transparency Bills Passed - Oregon 2019!

- **Drivers' Licenses for All**
  HB 2015 Enrolled Another interesting blend of privacy and transparency, this bill eliminates the requirement for proof of legal residence in applying for various DMV documents, a type of privacy. The subsequent transparency granted allows drivers the capability to access driving insurance, for example, for which licensing, documented proof of certified driving safety, is a requirement.
- **Fines for Late Public Records Request Responses**
  HB 2353 Enrolled is a $200 penalty bill for late or unanswered public records requests. This is a follow-up to 2018 legislation, because some agencies had not improved response times within 15 days, with reasonable allowances for exceptions. Small agencies and the League of Oregon Cities opposed the bill, citing more time needed for training agency personnel.
- **Intimate Image Privacy**
  HB 2393 Enrolled modifies the crime of harassment and spells out lawsuit damages that can be awarded when a nude or sexually explicit image is disseminated without consent.
- **Public Posting of Certain DA Policies**
  HB 3224 Enrolled, with League support. It requires District Attorneys to "develop and adopt policies relating to discovery, charging decisions and case disposition and to make policies available to the public on a website."
- **Sharing of Confidential Records for Forensic Investigation**
  SB 25 Enrolled allows for sharing of mental health records in a forensic investigation, passed with League support.

Oregon Public Records Law

Public records laws adopted in 2017 were the biggest update in over thirty years, following comprehensive review by a Task Force under the Attorney General. Accomplishments included:

- Instituting an Office of the Public Records Advocate,
- SB 90 Enrolled (2017) established a Cybersecurity Advisory Council, CyberOregon, whose mission is to build tangible solutions to protect the digital lives of all Oregonians. See ORS 276A.326, (Oregon Cybersecurity Council, 2017)

Privacy/Transparency Bills that Failed to Pass - Oregon 2019

- **Agency Accountability for Public Records Reporting**
  HB 2431: The League supported this public records reporting bill; however, the bill did not get out of committee.
- **Cybersecurity Business Tax Incentives**
  HB 3109: Study tax incentives for cybersecurity businesses. Passed from House Business and Labor on a 10:1 vote, referred to House Revenue, not heard.
- **Cybersecurity Collaboration**
  HB 3233: the Secretary of State would establish a program to improve election administration systems cybersecurity, by encouraging independent technical experts, cooperating with state election officials, local government election officials and election service providers, to identify and report election cybersecurity vulnerabilities. In committee, not heard.

- **Personal Health Record Privacy Task Force**
  SB 703: a task force to protect personal health records from commercial sale, did not pass out of committee despite League support.
- **Cybersecurity Program to Identify and Report Election Vulnerabilities**
  SB 818 (2019): the Secretary of State would establish a cybersecurity program to identify and report election cybersecurity vulnerabilities of election administration systems. Technical experts would coordinate with state, local and other election "service providers" to improve cybersecurity. It was referred to but not heard in committee.
- **Cybersecurity Policy Declaration with Need for Management**
  SCR 4: cybersecurity policy and need for proactive cybersecurity risk management. Passed unanimously in Senate Judiciary, passed 24/1/5 (excused) on the Senate floor, but not heard in House Rules on adjournment.

Immigration Status

- **HB 3464**: Citizenship and immigration status privacy. This bill passed with League support, (basically) prohibiting disclosure of citizenship status, unless required by federal or state law.

Public Record/ Privacy Bills

Oregon's 2017 Legislative Session saw the most public records law progress in 30 years. Discussion reflected a struggle between privacy, transparency, and accountability, with efficiency in government strained by an unmanaged roster of more than 550 exemption categories for public records requests.

- Public Records Advocate and Council, **SB 106 Enrolled**. The Council was formed and an office established to oversee the Council and to coordinate state and local agencies.
- **HB 2101** established the Oregon Sunshine Committee to review public records request exemptions, including review of newly enacted legislation.
- **SB 481 Enrolled**. Establishes policy for Public Records Access, reasonable response times and managing a catalog of exemptions.

APPENDIX D: Personal Privacy Practices

What does everyone need to know and how should they responsibly protect ourselves? Privacy policies should provide accessible procedures for users to limit or prevent information or image sharing and selling by the merchant, beyond pressing lawsuits. Start by examining how connected modern life is, with online exposure growing, from social media to the Internet of Things, with ubiquitous cameras.

[Have I Been Pwned] HIBP?

This is a commercial internet security website, known by the acronym, enabling consumers to check for data breaches on their personal information. It stands for "Have I been Pwned", colloquially pronounced have I been "poned", referring to password theft.

Social Media - R U There? (geolocation tracking)

Phone app location tracking can be altered in phone settings. Detailed advice is available, (Valentino-DeVries, Singer, Keller, & Krolik, 2018).

Me/Not Me: Impersonations

Cell Phone: "sim-swapping" Scammers have been impersonating cell account holders and getting permission from service providers (sometimes acting as accomplices) to transfer phone service to another account. Text messages, emails, password confirmation codes, retail and financial account information all become accessible. Senator Ron Wyden, D-Oregon says "The industry is not exactly exerting itself, in order to better protect the consumer from these sim-swap scams." A wireless trade association, CTIA, formerly known as Cellular Telecommunications and Internet Association provides CTIAs Updated Messaging Guidelines and Best Practices, 2019).

Phone Calls: People are flooded by phone calls and automated robocalls, during election seasons and otherwise. Consider enrolling in the "National Do Not Call Registry." Callers may legally continue to call if you agree to accept calls. Don't reply "yes," even with an unrelated query, for example, "can you hear me?"

The Oregon Attorney General (AG) advises not answering calls you don't recognize and reporting suspicious calls, with details provided on the Consumer Protection, Fraud and Scams page. Callers can now spoof actual caller ID connections. A recent scam appeared to originate from actual County Sheriff's offices, listing the correct telephone numbers, but (criminally) demanding that funds be delivered and that callers "not hang up!." Details and email alert subscriptions are available from the Oregon AG Scam Alert Network for ongoing scams.

Phishing Emails: Our League state board and others report getting repeated emails and phone text messages asking, "are you busy- can you help?" These appear to be legitimate, registering with recognized names and contact photos but with other email addresses. A quick helpful reply will be answered with requests everyone has come to recognize, asking for money, gift cards, etc. A variant is asking "Grandma" for help, with the explanation, "I'd ask mom, but you know how busy she always is." If in doubt, check your contact files. You can block ersatz identity spoofing accounts, marking them as spam or reporting them as malicious, if need be.

Social Media "Me/Not me" Fake friend requests, if accepted, can hijack contact lists to spread maliciously and spread misinformation while masquerading with adopted identities. You may get suspicious requests, wondering- weren't they already friends? Check for your actual friend in a fresh tab or window. Duplicate identities appear and spoofers may use actual photos copied from friends already in your lists. The spoof profiles are usually shallow, with only a few images, few if any friends, and a

short account history with few posts. Privacy settings for legitimate accounts may look like this, too, so consider verifying in another way if you are curious. These can be sophisticated, targeted to appeal to interests reflected in posts. One conservative approach is to only "friend" those you know personally, or verifiable "friends of friends."

See further advice for all of these from Symantec.

What Does A Computer Problem Look Like?

Technology is evolving quickly and it may be hard to tell what is causing problems- outdated hardware or software, even user shortcomings. Getting advice intermittently is advisable. Here is some basic advice, starting with a summary from a computer manufacturer, Dell Customer Support (2019).

Install an antivirus program; keep it up-to-date and run scans regularly.

- Install an anti-malware program to block software from installing without the user's knowledge,
- Only download and install online software from trusted sources.
- Scan email attachments before opening the. Even images can carry a viruses.
- Don't trust cracked or hacked software. It often contains malware, Trojan horses.

Here are some symptoms to help diagnose malware:

- **Browser Redirects, Popups,** Homepage Changes: Browsers may suddenly redirect to unknown websites, or a previously set homepage may change without warning or input.
- **Slow Computer Response:** Computer may "freeze" or run slowly with regular use. Desktop operating system loading delays are common.
- Task Manager shows processes using 100%: Processor seems to work overtime and/or slowly. To check, press and hold down the CTRL + ALT + DEL keys at the same time. Then click the Performance tab. See process use in CPU Usage.
- Virtual Memory Low Message: This message will keep appearing no matter what changes are made to resolve the issue.

Note that this advice comes from Dell, a PC manufacturer. MacWorld cautions that Linux and MAC computers are also vulnerable and should be protected (Haslam, 2019).

Password Management

People manage many categories of services online, each with protected access. Consider the variety of accounts individuals sign into, easily running to hundreds of accounts per person. There are so many that managing password protection is highly advisable, with numerous programs available. It goes without saying that passwords should be varied, changed regularly, and never written in easily discoverable places.

- Personal records, for example work performance and pay, school, health care portals, professional society and civic memberships
- Financial transactions, including banking, investing, bill-paying, purchasing
- Household apps: lighting levels, irrigation, dishwashers, security cameras, engaging and monitoring kitchen appliances
- Government services: libraries, the DMV, and others for licensing, social services, other agency information, like weather

- Personal communication networking between smart devices, linking laptop, phone, tablet, and watch, including phone calls and texts, emails networked social media and organization pages; blogs, membership/group pages
- Any websites that remember user preferences and history: media accounts, hobbies, file-sharing, travel and wifi access away from home
- Other online tools and resources: calendar and shopping list managers, some with enhanced performance for premium users with sign-in, managed accounts

Account passwords need to be difficult to guess, protected, for example with two-factor authentication, and changed regularly. Password management programs are available, to generate random, multi-character passwords, to protect, change, and retrieve them.

Use Diverse Passwords

A single computer can test 8.2 billion password combinations per second and "penetration testers" can use free software. System security officials assume that every website or service uses the very worst security practices imaginable. They assume that any password stored by someone else is effectively public. They advise never using the same password, or even remotely similar passwords, between any two services (Goodin, 2012).

Malware, Spyware, and Viruses, Oh My!

Applications and operating system updates are often patching security holes that would otherwise allow malware to infect computers. Monitor and install security updates.

Malware, or malicious software, can infect computers and spread over networks. Install protection programs and keep definitions current. Examples of malware include viruses, ransomware, spyware, Trojan horses, viruses, and worms, covered in the glossary. Adware is not considered malware unless it damages systems.

Google Download Option

Google offers a full user data download option. It could be a very large file, with everything already mentioned plus bookmarks, emails, contacts, photos taken with the phone, businesses you've bought from, calendar data, Google hangout sessions.

How to download your Google full info: https://takeout.google.com/?pli=1

Facebook Download Option

How to download your Facebook full info: https://www.facebook.com/help/212802592074644

Acknowledgements:

On behalf of the League of Women Voters of Oregon, the study committee would like to thank several anonymous reviewers and the technical advisors who graciously shared their expertise and advice, offering valuable comments on this work. Special thanks go to the authors who clarified our interpretations of their work and the many individuals and organizations who shared their visual images.

Study Committee
Rebecca Gladstone
Sheila McGinnis
Mary Sinclair, Chair

Technical review and commentary
Peter Alcorn, digital media and publishing consultant
Rick Bennett, LWVOR, retired AARP
McKenzie Funk, author, journalist
Sarah E. Igo, historian and author
Judith Knudson, LWV Williamsburg Area
Sean McSpaden, Oregon Legislative Fiscal Office
Stephanie Singer, Ph.D., Research Assistant Professor, Portland State University
Former Chair, Philadelphia County Board of Elections
Ellen Smith, LWV Palo Alto, retired editor
Steven Trout, Oregon Director of Elections, US Elections Commission

Editors, LWVOR
Marge Easley
Jane Gigler
Karan Kuntz
Marnie Lonsdale
Norman Turrill

Published by the League of Women Voters of Oregon, 2020
President: Rebecca Gladstone
Program Chair: Karan Kuntz
Office Coordinator: Sarah Andrews
Office Support Specialist: Amanda Crittenden

Printing: Eagle Mailing (Salem, OR)

Our thanks to our staff for production support.

Our thanks to the Carol and Velma Saling Foundation for their long-term support.

We dedicate this study to the League members who have preceded us in the 100 years of the League's history, and to members engaged in today's issues. Those brave members who came before us inspire our efforts to address current challenges and to reach out to those who will follow us.

Cover image credit: Shutterstock

League of Women Voters of Oregon
1330 12th St SE Suite 200, Salem, OR 97302
lwvor.org – lwvor@lwvor.org – 503-581-5722