### Cybersecurity and Privacy: Past, Present, and Future

### Lance J. Hoffman

Professor Emeritus of Computer Science The George Washington University Washington, DC

March 21, 2023

# Overview

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

- Caveats: An incomplete history (but IANAL -- I Am Not A Lawyer, I am a Computer Science professor)
- These are my views, not those of the U. S. government or any other person or automated system.
- These slides are available from the organizers.

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

### Surveillance of Individuals in Movies



- U.S. laws and regulations on cybersecurity and privacy
- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

### **Privacy and Speech**



# Regulation regimes differ Loose – US Moderate -- EU Strict – China

- U.S. laws and regulations on cybersecurity and privacy
- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

### An Incomplete History of U. S. Laws on Cybersecurity and Privacy

Currently, a patchwork – no omnibus law, no standard regulations Mainly **Sectoral** laws, but states starting to pass their own

Date passed	Title and brief description
1791	4 <sup>th</sup> Amendment to the Constitution: Before the government can search your home or seize your property, it needs a good reason.
1974	Privacy Act of 1974 limits collection and transfer of personal data by government agencies
1974	Family Educational Rights and Privacy Act restricts access to educational records
1984	Computer Fraud and Abuse Act addresses computer fraud or abuse using interstate or foreign commerce
1986	Electronic Communications Privacy Act deals with interception and access to electronic communications such as e-mail and voice mail
1987	Computer Security Act of 1987 required establishment of minimum acceptable practices for Federal computer systems
1996	Health Insurance Portability and Accountability Act regulates medical system privacy
1998	Children's Online Privacy Protection Act regulates online interactions with children under 13
1999	Gramm-Leach-Bliley Act regulates financial information privacy
2001	USA Patriot Act expanded surveillance capabilities of government in response to 9/11/2001 attacks, supplanted by USA Freedom Act in 2015
2003	California Online Privacy Protection Act requires website operators to post a privacy statement
2018	California Consumer Privacy Act protects consumers' personal data

### General Data Protection Regulation (GDPR)



All subject companies and organizations including governments must comply with these principles when they collect and process personal data of the European citizens.

- Lawfulness, fairness, and transparency.
- Purpose limitation. Specify purpose.
- Data minimization. Collect no more than needed.
- Accuracy. Up-to-date and accurate.
- Limited storage. Delete when no longer needed.
- Integrity and confidentiality. Keep secure.
- Accountability. Demonstrate compliance.

Fines: Up to 20M euros (\$21.7M [4/2020]) or 4% of revenue from preceding year, whichever is higher.

### GDPR (or any regulation) can lead to more user-friendly systems

GDPR applies in European Economic Area, Iceland is an European Economic Area ('EEA') member, and thus GDPR applies, even though it is not an EU Member State

We believe your o	data is your property and suppo	ort your right to privacy	and transparency.	
Select a	Data Access Level and Duration to cho	bose how we use and share	your data.	
31 0 31 0 31 0 31 0 31 0 31 0 31 0				
REJECTIONS OF REFERENCES TO REJECT	ALL ACCEPT SOME	ACCEPT ALL	6 months V	
Highest level of personalisation. Data accessed to main	ke ads and media more relevant. Data	shared with 3rd parties may	be use to track you on this site a	nd other sites you visit.
		Share this		
Customize Not known yet/General view of all meeting points	Save my prefer	rences		Do Not Sell
We believe your d	lata is your property and suppo	rt your right to privacy	and transparency.	
e stiel stie	Data Access Level and Duration to cho	oose how we use and share	your data.	
1 • 3 • 5 • 5 • 5 • 5 • 5 • 5				
REJECT	ALL ACCEPT SOME	ACCEPT ALL	6 months V	
Customize	Save my prefer	rences		Do Not Sell
We believe your o	lata is your property and suppo	ort your right to privacy	v and transparency.	omenduseum credine milienti or keilandasum (* 13) * 3) *
e al e al e al e al e al se a se Select a	Data Access Level and Duration to che	oose how we use and share	your data.	
			Golden	
REJECT	ALL ACCEPT SOME	ACCEPTALL	6 months V	
Highest level of privacy. Data accessed for ne	ecessary basic operations only. Data st	nared with 3rd parties to ens	ure the site is secure and works	on vour device
31 4 31 4 31 4 31 4 31 4 31 4 31 4 31 4	,	Share this	map via:	
Customize	Save my prefer	rences		Do Not Sell

### No federal law in USA

racinitate customer requests, we value your privacy and will not discriminate against california residents in response to your exercise of privacy rights.

#### Multi-State Privacy Statement for Virginia, Connecticut, Colorado

This Multi-State Privacy Statement is provided pursuant to applicable state laws and applies to Virginia, Connecticut, and Colorado residents, and supplements our overall Statement with additional disclosures and rights.

If you are a resident of Virginia, Connecticut, or Colorado you may take advantage of the following rights in accordance with applicable law:

- Confirmation/Access. You can request to confirm whether we process your personal information. Subject
  to certain exceptions, you can also request a copy of your personal information you provided to us.
- Deletion. You can request that we delete personal information we have about you.
- Correction. You can request that we correct inaccurate personal information we maintain about you.
- Opt Out of Sale. You can request to opt out of the sale of your personal information to a third party.
- Opt Out of Targeted Advertising. We may display advertisements to you where the ad was selected based on personal information obtained from (or in some instances inferred) from your activities over time and across unaffiliated websites or online applications to predict your preferences or interests. To the extent permitted by law, you can request that we stop using your personal information for such targeted advertising by clicking on the "Cookie consent" link that may be in the footer of our websites. Additionally, you can opt out of certain uses of cookies for advertising purposes by visiting www.aboutads.info/choices. For more information, please see Section 9 above. Your opt-out of cookie-based tracking for advertising purposes is specific to the device, website, and browser you are using; it is deleted whenever you clear your cookies or your browser's cache.

To take advantage of any of these rights, please contact us via our dedicated privacy portal by clicking here or in writing at Viator, Inc., 400 First Avenue, Needham, Massachusetts, 02494, USA. Note that Connecticut and Calerado residents may designed an authorized agent to request on their helpelf that we stop colling or

# China's Evolving Social Credit System

- Chinese government plans to assign each citizen a "social credit" score.
- Citizens will get perks and restrictions accordingly based on their score.
- The government would have access to data regarding specific behaviors, like traffic violations and spending habits.
- Your digital profile would influence your future (as it does today).
- To set the tone, the project's official slogan is:

"[to] allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step." VISUAL INVESTIGATIONS

#### Four Takeaways From a Times Investigation Into China's Expanding Surveillance State

Times reporters spent over a year combing through government bidding documents that reveal the country's technological road map to ensure the longevity of its authoritarian rule.

🛱 Give this article 🔊 🗍 🖵 147



A New York Times analysis of over 100,000 government bidding documents found that China's ambition to collect digital and biological data from its citizens is more expansive and invasive than previously known.

> By Isabelle Qian, Muyi Xiao, Paul Mozur and Alexander Cardia Published June 21, 2022 Updated July 26, 2022

5 MIN READ



### Is "Study the Great Nation" studying its users right back?

Chinese app on President Xi's ideology, "Study the Great Nation", is most downloaded app in China (on over 100 million users' phones)

Use of the app is required by CP and many workplaces, including employers of journalists

- Users must register real names and cellphone numbers which link to a national ID; thus a trail is created
- Chinese law requires all tech companies to share user data with the government
- The app has superuser privileges allow developers to install keystroke loggers
- access photos and videos
- transmit user's location
- activate audio recording
- trawl through user's contacts and Internet activity
- send back information

China denied the app contained such functions. Report funded by US Government under Radio Free Asia is available at <u>https://cure53.de/analysis-report\_sgn.pdf</u>.

Detailed description and analysis at https://en.wikipedia.org/wiki/Social\_Credit\_System



#### Governments around world have moved to ban or restrict TikTok amid security fears

New Zealand lawmakers recently agreed to ban TikTok on government-issued phones, joining a list of government officials that have moved to rein in or bar the platform.

By Jennifer Hassan, Ruby Mellen and Adam Taylor . 55 minutes ago

#### MORE COVERAGE

- Biden's TikTok plan echoes failed Trump bid that China called a 'smash and grab'
- Biden administration wants TikTok's Chinese owners to divest



TikTok: Teen sensation to political pariah By Hamza Shaban and Jonathan Baran

### Supply chain: Who is a trusted supplier? **Countries with complete or partial bans** on some software/hardware



Portugal

military personnel)

### Should Software (and Hardware) Come With An "Ingredient List"?

ntia.gov/page/software-bill-materials

An official website of the United States government Here's how you know > National Telecommunications and Information Administration								
Information Administration United States Department of Commerce						Search	Search	
About Us	~	Issues	Ý	Grants	News	~	Data Central	Publications

#### SOFTWARE BILL OF MATERIALS



**EXECUTIVE ORDER 14028, IMPROVING THE NATION'S CYBERSECURITY** 

Software Supply Chain – Security Guidance

Software Security in Supply Chains

Guidance, Purpose, Scope, and Audience

EO-Critical Software and Security Measures for EO-Critical Software

Software Cybersecurity for Producers and Users

Software Verification

Evolving Standards, Tools, and

Recommended Practices Software Bill of

Materials (SBOM)

Enhanced Vendor Risk Assessments

Open Source Software Controls

Vulnerability

Management Additional Existing

Industry Standards, Tools and Recommended Practices

### Software Security in Supply Chains: Software Bill of Materials (SBOM)

Section 10(j) of EO 14028 defines an SBOM as a "formal record containing the details and supply chain relationships of various components used in building software, []]" similar to food ingredient labels on packaging, SBOMs hold the potential to provide increased transparency, provenance, and speed at which vulnerabilities[2] can be identified and remediated by federal departments and agencies. SBOMs can also be indicative of a developer or suppliers' application of secure software development practices across the SDLC. Figure F-1 illustrates an example of how an SBOM may be assembled across the SDLC.



Figure 2 - Illustrative Example of Software Life Cycle and Bill of Materials Assembly Lir	ne
---	----

Nutriti	on	Fa	<b>ict</b>	S
?? servings per c	ontaine	r		
Serving size		??????	(??g)	
	D/	rcorving	Por	ontaina
Calories		<u>?</u> ?		<u> </u>
		% <b>DV</b> *		% <b>DV</b> *
Total Fat	?g	?%	?g	??%
Saturated fat	?g	?%	?q	??%
Trans Fat	?g		?q	
Cholesterol	?mg	?%	?mg	??%
Sodium	??mg	?%	??ma	??%
Total Carbohydrate	??g	?%	??q	??%
Dietary Fiber	?g	?%	?a	?%
Total Sugars	??q		??a	
Incl. Added Sugars	??g	??%	??a	??%
Protein	?g		?g	
Vitamin D	?mcg	?%	?mcg	?%
Calcium	??mg	?%	??mg	?%
Iron	??mg	?%	??mg	?%
Potassium	??mg	?%	??mg	?%

\* The % Daily Value (DV) Tells you How mush a nutrient in a serving of Food contributes to a daily diet . 2,000 calories a day is used for general nutrition advice.



### Surveillance / Vetting by Whom? Is a Private Sector System Much Different Than a Government-Based System?

- How different is a centralized government-run social credit system from existing private social credit systems?
- Credit reporting agencies
- Insurance companies
- Banks
- What happens when private systems link with national and local government systems?
- What happens when these link with facial recognition systems (of varying accuracy)?
- What is the remedy if government blacklists or censors you or you can't buy a plane ticket or get a driver's license or ???

# These fears were expressed before the Internet was born

Journal of Privacy and Confidentiality (2013) 5, Number 1, 1–37

#### Statistical Dèjá Vu: The National Data Center Proposal of 1965 and Its Descendants

Rebecca S. Kraus, Ph.D.

#### 1 Introduction: Computers, Researchers, and the Need for Data

In the early 1960s, social scientists recognized the need for greater access to microdata maintained by the federal government. Computer technology had improved the efficiency and affordability of research with large data sets, and the expansion of government social programs called for more data and research to inform public policy. As a result, in 1963 social scientists recommended that the federal government develop a national data center that would store and make available to researchers the data collected by various statistical agencies. Because of its massive data holdings and its pioneering work in the use of computers for the storage and analysis of data, the Census Bureau became involved in the national debate, though relexicantly.

The government's endorsement of the national data center proposal led to public outray and intense congressional scruting over the data on individuals maintained by federal agencies, potential misuse of such data, and threats to privacy posed by emerging technologies. One key lesson of the data center dehate is that social scientist and government agencies must consider the practical implications of their plans and clearly communicate those plans to the public. Although the research community and the government understood the potential benefits of a national data center, and agreed that the data would be used only for research, a significant portion of the public seemed not to share their embasisms for a national data center. Fasto 7 Big Brother<sup>2</sup> and secret government dossiers swirled around discussions of the national data center, and the issue became identified with other concerns about invasions of privacy ranging from psychological testing to illegal wire tapping, culminating in the passage of the Privacy Act of 1974.

While a national data center ultimately was not created, advances in technology and statistical methodology have led to greater data sharing and linkage capabilities. Intense political scrutiny of federal statistics has resurfaced occasionally, as have discussions concerning centralization of statistical functions. What can we learn from 1965 that can help us form sound statistical information policies in the 21<sup>st</sup> century?

\*U.S. Census Bureau, Washington D.C., mailto:rebecca.s.kraus@census.go

© 2013 by the authors

http://repository.cmu.edu/jpc

# Much of the world already has comprehensive data protection laws

National Comprehensive Data Protection/Privacy Laws and Bills 2023



Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2023 (January 28, 2023). Available at SSRN: <u>https://ssrn.com/abstract=1951416</u> or <u>http://dx.doi.org/10.2139/ssrn.1951416</u>







Plan B is to train them.



Prof. Lance J. Hoffman lancehoffmancyber.com

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

# **Cybersecurity Training**

Securing your devices		
Task	Personal Accounts	Work Accounts
Laptop: I have applied all <i>operating system</i> updates to my <u>Mac, PC</u> , or <u>Chromebook</u>		
Laptop: I have applied all application updates to my Mac or PC		
Laptop: My laptop drive is encrypted (Macs, PCs)		
Laptop: The passphrase on my laptop is at least 12 characters long		
Laptop: I have installed the <u>HTTPS Everywhere</u> extension		
Phone/tablet: I have applied all operating system updates to my <u>iPhone/iPad</u> or to my <u>Android phone</u>		
Phone/tablet: I have updated all application updates (iPhone, Android)		
Phone: I have set a passcode for my mobile provider ( <u>AT&amp;T</u> , <u>T-Mobile, Verizon</u> )		
Phone/tablet: I set an unlock code that is at least 6 characters long		

#### Securing your accounts

Task	Personal Accounts	Work Accounts
I use a password manager to store <u>all</u> my passwords		
The master password for my password manager is longer than 16 characters, and is unique		
I have enabled 2FA (see below) for my password manager		

#### Two-factor authentication (2FA)

I have enabled 2FA on all of the following accounts. Note that you may have more than one account on these services. Protect them all.

Task	Personal Accounts	Work accounts		
Gmail				
AppleID				
Outlook.com				
Yahoo				
AOL				
Twitter				
Facebook				
Instagram				
LinkedIn				
Dropbox				

#### For people who use Gmail for personal mail:

Task	Personal Accounts
I have enrolled my personal account in the <u>Advanced</u> <u>Protection Program</u>	
I have reviewed my account security at https://mvaccount.google.com/security-checkup	

from DNC's chief security officer, Bob Lord: "Focus on the basics."

# Cybersecurity Training – How to Spot Phishing

Phishing								
<ul> <li>Phishing attacks         <ul> <li>Use email or malicious websites to infect your machine with malware by duping users into clicking on fake links, supplying PII, or opening malicious attachments</li> </ul> </li> <li>Spear Phishing         <ul> <li>Targeted phishing – often using publicly available personal information to make a message appear that is coming from a trusted sender</li> </ul> </li> </ul>								
A	Email addresses (FROM, CC, TO)							
	B Generic salutation							
From: Package Delivery <david37428@gmail.com> Subject: Package Not Delivered Date: December 15, 2013 16:48 GMT -5:00 1 Attachment, 154 Kb</david37428@gmail.com>	C Grammar or spelling mistakes D Urgency, asking for personal information							
Unfortunately we unable to deliver you package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.	E Mouse over link to see where click takes you							
Order# 44187	F Unexpected attachments							
Shipping Tracking Information	Message too good to be true (No, you did not win							
Tracking #: 129Y424V039787851X Tracking Information: http://www.fedex.com/tracking/179Y424V039787851X Ship Date: 12/10/2013	<ul> <li>lottery)</li> <li>Email not expected from this source</li> <li>Did your friend really send this? (Call them to find out )</li> </ul>							
Thank you, Package Delivery Specialist	51 Survey							
From SANS Securing the Human								

# **Cybersecurity Education: Elementary and High School**



K12cybersecurityconference.org

# **Cybersecurity Education: College**

### CyberCorps Scholarships for Service Program for U. S. Citizens 98 Participating Universities 6 Community Colleges in Pilot Program



Produces educated security workforce for federal, state, local, and tribal governments (including publicly funded universities)

- Tuition and fees 100%
- Textbook Allowance
- Monthly Stipend for Living Expenses
- Professional Development Allowance
- Students attend an annual meeting and job fair that facilitates summer internships at government agencies and jobs upon graduation

# **CyberCorps Scholarships for Service Program for U. S. Citizens**

98 Participating Universities 6 Community Colleges in Pilot Program

Specific programs vary by institution

# **Cybersecurity Education:** College

### George Washington University

Cybersecurity in Computer Science majors: 3 core Computer Science. 5 cybersecurity in CS, 2 more cybersecurity CS or non-CS courses

Non-Computer Science majors (e.g., Engineering, Policy, Business, Management, International Affairs): 4+ cybersecurity courses + major



Students at **Cybersecurity** Executive Order Briefing at Commerce Dept.



Deputy Undersecretary Schneck with GW students after her public lecture



**CyberCorps** Student questions chair of Privacy & Civil Liberties Oversight Board

Prof. Lance J. Hoffman lancehoffmancyber.com





Dr. Vint Cerf VP, Google



Dr. Phyllis Schneck Former chief cybersecurity official



Congressman James Langevin



Gen. Michael Hayden Former director NSA, CIA



Kevin Mandia CEO, FireEye



Brian Krebs, author, Krebsonsecurity.com

ALL STUDENTS TAKE REQUIRED IN-PERSON CYBERSECURITY SEMINAR

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

### Institutions Are Often Challenged by New Technology YESTERYEAR

- Traditional development of written material done by elite educated scribes.
- General population was not educated.
- The availability of written material accessible to the public was limited.

INNOVATION: The printing press made it possible to produce multiple copies of a text quickly and cheaply

RESULT: spread of knowledge and the dissemination of ideas.

### THREAT TO INSTITUTIONS, in particular ruling class and the church

The institutions saw the potential for printed material to challenge their authority and spread dissent.

### **RESULTANT REGULATION:**

Catholic Church, established the Index Librorum Prohibitorum, a list of prohibited books that was maintained until the mid-20th century.

In England, the Licensing Act of 1662 required that all printers obtain a license from the government before they could legally print any material.



### Institutions Are Often Challenged by New Technology TODAY



#### **BUSINESS**

First-to-market gives competitive advantage

Users initially want "GOOD, FAST, CHEAP"

OTHER ITEMS like security and privacy, ethics, product (algorithm) quality, etc., are often relegated to "later"

This leads to



#### GOVERNMENT

 Internet provides coercive power to individuals and groups, often anonymous, that are independent of the state

#### ACADEME

- Uses Disciplinary Approaches on Multidisciplinary Problems (no dilettantes)
- Result = micro-solutions that may not work together on the actual complex system (broad vision lacking)
- Example: Where do you teach cybersecurity? It has components of computer science, forensics, economics, political science, etc. How to construct an interdisciplinary team?

### Iranian protest using Israeli app reported in Italian newspaper





ICE ISRAEL NEWS HEALTH & WELLNESS WORLD NEWS MIDDLE EAST

### Iranians use Israeli app Waze in recent round of protests – report

Italian daily 'La Repubblica' reported that the protesters managed to communicate where to drive and leave their cars to maximize the disruption using Waze.

By ROSSELLA TERCATIN Published: NOVEMBER 19, 2019 14:32





### Incentives to Build In Cybersecurity: Are They Perverse? [cost of all defects and problems are externalized to customers with zero liability]

### The Economist

The Pearl river delta: a special report Hospitals of the future Jacob Zuma must go

Parking, wrong on so many levels

# Why computers will never be safe



M

### Tilting the Playing Field: How Misaligned Incentives Work Against Cybersecurity

Cybercriminals have long had the advantage, continually finding new ways to steal data, break services, and disrupt the legitimate flow of information—not because they are better but because of a mismatch between the incentives of attackers and defenders. To better understand this misalignment of incentives, we surveyed 800 cybersecurity professionals from five major industry sectors. The <u>report</u> identified three key incentive misalignments: between corporate structures and the free flow of criminal enterprises, between strategy and implementation, and between senior executives and those in implementation roles.

#### Three levels of misaligned incentives put defenders at a disadvantage

Attackers versus defenders	Attackers' incentives are shaped by a fluid, decentralized market, making them agile and quick to adapt, while defenders are constrained by bureaucracy and top-down decision making.
Strategy versus implementation	While more than 90% of organizations have a cybersecurity strategy, less than half have fully implemented their strategies.
Executives versus implementers	Senior executives designing cyber strategies measure success differently to those who put strategies into practice, limiting their effectiveness.

https://www.csis.org/programs/technology-policyprogram/cybersecurity/other-projectscybersecurity/misaligned-incentives

http://www.economist.com/news/leaders/21720279incentives-software-firms-take-security-seriously-are-tooweak-how-manage

These are industry incentives. What about government incentives?

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

## Examples of Regulation by Governments

- India turned off the Internet in its capital to prevent protests against an anti-Muslim law
- Iran blacked out Internet to thwart "car protests" using Waze to block streets to protest gas prices
- **China** created "Great Firewall" (widespread content filtering for online networks)





skare (f) (w) (m)

# **Key Internet Controls 2022**

Freedom House documented how governments censor and control the digital sphere. Each colored cell represents at least one occurrence of the cited control during Freedom on the Net's coverage period of June 2021 to May 2022.

Key										
V <sup>*</sup> S CONTROL SHOWN		20	2020	2019						
Search										
Country	Social media platform blocked	Websites blocked	internet shutdown	Pro- government commentators	New censorship law	New surveillance law	Internet user arrested or imprisoned	Internet user physically assaulted	Technical attacks	Status
Angola							~			Partly Free
Argentina									~	Free
Armenia				~	~		v		~	Free
Australia					~	~			~	Free
Azerbaijan		~	~	~	~		~	~	~	Not Free
Bahralo		2		2			2		2	Not Free

# U. S. Cybersecurity and Governance Strategies (still no nationwide overall laws)



5 pillars of current U. S. cybersecurity strategy

- Defend critical infrastructure
- Disrupt and dismantle threat actors
- Shape market forces to drive security and resilience
- Invest in a resilient future
- Forge international partnerships to pursue shared goals

## U. S. Cybersecurity and Governance Enforcement of Sectoral Laws

### FTC Enforcement Action to Bar GoodRx from Sharing Consumers' Sensitive Health Info for Advertising

Under proposed order, GoodRx will pay a \$1.5 million civil penalty for failing to report its unauthorized disclosure of consumer health data to Facebook, Google, and other companies

February 1, 2023



WHAT IT DID

- •Shared Personal Health Information with Facebook, Google, Criteo, and Other
- •Used Personal Health Information to Target its Users with Ads
- •Failed to Limit Third-Party Use of Personal Health Information
- •Misrepresented its HIPAA Compliance
- •Failed to Implement Policies to Protect Personal Health Information

WHAT IT MUST NOW DO •Pay \$1.6 civil penalty •Prohibit the sharing of health data for ads •Require company to seek deletion of data •Limit Retention of Data •Implement Mandated Privacy Program

# **Algorithmic Expectations**



5 principles and associated practices for automated systems

- Safe and effective systems
- Algorithmic discrimination protections
- Data privacy
- Notice and Explanation
- Human Alternatives, Consideration, and Fallback

# The Sovereign State of Facebook

(Axios, Nov. 1, 2019)



Facebook's operations as a quasi-state span realms such as:

- 1. **Speech**: Facebook's mission of connecting people, combined with its global reach and billions of users, means that it is constantly making decisions about <u>who can say what</u>.
- 2. Money: Facebook launched its own global cryptocurrency. It failed due to pressures from regulators.
- **3. Safety**: Facebook's is constantly dealing with stakeholders wielding constantly shifting amounts of political power. Facebook tries to perform this dance everywhere.

### California Consumer Privacy Act (2018)

- Right to know
- Right to delete
- Right to correct
- Right to opt-out of sale or sharing
- Right to limit use and disclosure of sensitive personal data

updated by California including Privacy Rights Act (2023)

- Limited storage
- Geolocation data policy disclosure
- Consumers may prohibit sharing
- California Privacy Protection Agency created to enforce and promulgate regulations.





12% of the US population lives in California

If it were a sovereign nation, it would have the world's 5<sup>th</sup> largest economy, behind Germany and ahead of India.

# Whose rules? Nations, ICANN, ITU, Others? Al-GENERATED Results Not Verified

• **CHAT-GPT3 ANSWER TO:** give me a summary in two pages of how ICANN sees internet governance, how the ITU sees it, and how nation states see it.

• Internet governance refers to the principles, policies, and rules that shape the way the Internet functions. It includes issues such as domain name system management, IP address allocation, cybersecurity, online privacy, and content regulation. Different organizations and entities have different perspectives on how internet governance should be approached, leading to varying opinions and debates.

• The Internet Corporation for Assigned Names and Numbers (ICANN) is a non-profit organization responsible for managing the Domain Name System (DNS), which translates domain names into IP addresses that allow computers to connect with each other. ICANN sees internet governance as a multistakeholder model that involves the participation of various actors, including governments, private sector organizations, civil society, and technical experts. ICANN advocates for a bottom-up approach that empowers all stakeholders to participate in policy development and decision-making. ICANN's goal is to ensure the stability and security of the internet while also promoting innovation and competition.

• In contrast, the International Telecommunication Union (ITU) is a specialized agency of the United Nations that focuses on information and communication technologies. The ITU sees internet governance as a matter of global public policy that should be guided by international regulations and treaties. The ITU advocates for a top-down approach that gives nation-states a more prominent role in decision-making. It aims to promote universal access to the internet, protect users' rights and interests, and prevent the digital divide.

• Nation-states have diverse perspectives on internet governance, reflecting their varying political, economic, and cultural priorities. Some countries advocate for greater state control over the internet, citing concerns about cybersecurity, online extremism, and hate speech. Others support a more liberal and open approach, promoting the free flow of information and protecting users' privacy and freedom of expression. The ongoing debate around internet governance reflects the tensions between these different perspectives, and finding a balance between them is essential for ensuring the internet's continued development and growth.

• In summary, ICANN advocates for a multistakeholder approach that empowers all stakeholders to participate in internet governance, while the ITU supports a more centralized approach guided by international regulations and treaties. Nation-states have diverse perspectives on internet governance, reflecting their varying political, economic, and cultural priorities.

### When Are Algorithms Likely to Go Astray And What Can Be Done To Prevent That? (Not a New Question)

(It's better to anticipate problems and design solutions into systems, rather than attempt to bolt on "fixes" afterwards.)

- "In an age of instant access to information, and our ability to propagate information globally with the click of a mouse, we are experiencing a global, digital Wild West.
- Everyone equipped can fire their .45 caliber digital weapons at any target with very little consequence.
- The metaphorical equivalent of digital Stage Coaches can be hijacked at will and digital gangs roam with impunity.
- The question before us is how to pacify this relatively lawless environment while preserving the utility of its openness to creative innovation and technological revolution. ..."

### **Algorithm Regulation**

- China: In 2021, Cyberspace Administration of China announced it will create governance rules for algorithms in the next three years.
- E.U.: policymakers are considering regulating AI use in
  - self-driving cars
  - hiring decisions
  - bank lending
  - school enrollment selections
  - law enforcement
  - courts
  - scoring of exams
- U. S.: Cybersecurity strategy, AI blueprint, but still no nationwide laws
  - U. S. cities and organizations: Due to some evidence of inaccuracy or discrimination, some declined to use facial recognition systems but other organizations use them (banks, apps, passport control, etc.)

# Will the U.S. finally act on Internet governance? The drumbeat is getting louder to "Do something."

Opinions Editorials Columns Guest opinions Cartoons Submit a guest opinion

THE POST'S VIEW

### **Opinion** | Who's responsible when ChatGPT goes off the rails? Congress should say.



By the Editorial Board



"Scholars believe that Section 230 was responsible for the web's mighty growth in its formative years. Otherwise, endless lawsuits would have prevented any fledgling service from turning into a network as indispensable as a Google or a Facebook. That's why many call Section 230 the "<u>26 words that created the</u> <u>internet</u>." The trouble is that many now think, in retrospect, that a lack of consequences encouraged the internet not only to grow but also to grow out of control. With AI, the country has a chance to act on the lesson it has learned."

"Yet the United States also can't afford to repeat its greatest mistake on internet governance, which was not to govern much at all."

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

Nation-States Use Various Types of Power – Military, Economic, Diplomatic, etc. And there is a growing literature on cybersecurity as a tool of power.





# Warfare has transitioned from industrial age to information age

1949 North Atlantic Treaty (NATO) Treaty

"collective defence" in the event of an "armed attack"

"If the U.S., Russian, and Chinese governments are not working on black hat programs that, in the event of war, will knock out the computational infrastructure of the other two, they aren't doing their jobs. Such programs are weapons of mass destruction, and, if used, the death toll could be colossal. A first world country with no computational infrastructure is a country with no economy, no food, no power and ultimately not a country at all."

– Dr. Len Adleman, 2002 ACM Turing laureate

### Many U.S. jurisdictions hit by ransomware attacks

Examples: Atlanta, Baltimore, Cleveland, ...



BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE

#### HARM CITY -

# Baltimore ransomware nightmare could last weeks more, with big consequences

Houses can't be sold, bills can't be paid while city networks are shuttered.

SEAN GALLAGHER - 5/20/2019, 12:47 PM



numbers.

## State sponsored attacks (publicly known)



"Since 2005, 34 countries are suspected of sponsoring cyber operations. China, Russia, Iran, and North Korea sponsored 77% of all suspected operations."

2022: 147 operations



"Belarusian threat actor UNC1151 targeted the private email addresses of Ukranian soldiers in a phishing attack. UNC1151 hacked the email accounts of military personnel and then leveraged the compromised address books to send further malicious emails, many of which were sent to Polish military personnel."

### Individual keyboard warriors, volunteer and mercenary



BY SHAUN WATERMAN ON 3/14/23 AT 5:00 AM EDT

# It's easy to shop for exploits!



- Aftermarket in cyberweapons makes milware-like capabilities available to terrorists or criminals or other non-state actors.
- Exploits (attacks) sold to take advantage of users whose systems are not up-to-date

(Smart) Weapons can be neutralized and turned on their users

### BROOKINGS



- Any 21st century war will include cyber operations.
- Weapons and support systems will be successfully attacked.
- <u>Rifles</u> and <u>pistols</u> won't work properly.
- Drones will be <u>hijacked midair</u>.
- Boats won't sail, or will be misdirected.
- Hospitals won't function.
- Equipment and supplies will <u>arrive late</u> or not at all.

### **Influence Operations**

IEEE Spectrum Detection Stays One Step Ahead of Deepfakes—for Now

Q Type to search

BY MATTHEW HUTSON | 06 MAR 2023 | 6 MIN READ | 🗍



4 MIN READ

WASHINGTON - A hacking group with ties to the Russian government appears to be preparing new cyberattacks on Ukraine's infrastructure and government offices, Microsoft said in a report on Wednesday, suggesting that Russia's long-anticipated spring offensive could include action in cyberspace, as well as on

The report also said that Russia appears to be stepping up influence operations outside Ukraine, in a push to weaken European and American support for continuing military aid, intelligence sharing and other assistance to the Ukrainian government. The effort would come as a faction in the Republican Party — and some in the Democratic Party — argues that supporting Ukraine is not a core interest for the United States.

# Regulation is Coming to entire world

- There is no effective developer liability for harms yet
- (Very) old days: Code of Hammurabi (1800 BCE) generally recognized as the world's first building code (essentially a criminal statute that included capital punishment for shoddy workmanship that resulted in death)
- Legal and Computing Literature is Converging
  - P. Ohm and B. Reid, Regulating Software When Everything Has Software
    - 84 GEO. WASH. L. REV. 1672 (2016), available at https://scholar.law.colorado.edu/faculty-articles/19
  - Carl Landwehr, We Need a Building Code for Building Code
    - <u>Communications of the ACM Volume 58 Issue 2</u> February 2015 pp 24–26 <u>https://doi.org/10.1145/2700341</u>

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion

### Security and Privacy Concerns for These Current or Projected MEDICAL Systems using **Things** and **Big Data (and now AI)**

Smarter	What	
Heart rate monitor	[Garmin, \$24.82]	
Step counter	[FITBIT, \$59.99]	
Blood Pressure Monitor	[IHEALTH, \$48.00]]	
Glasses	Monitor eyesight; advise age correction	
Pacemaker and stent	Broadcast data to cardiologist plus ECG	
Toilets	Test excrements both liquid and solid	
Chairs	Plot posture; broadcast spine data	
Earphones	Measure hearing; analyze emotions of people we are listening to	
Cancer Pill	Google X developing digestible pill that contains nanotechnology that works alongside wearable device to spot early signs of cancer and other diseases	
Big Data and AI	Limbic ("We give therapists superpowers.")	
Genetic Data	Use of Big Data with Generative AI to plot predictive suggestions and treatment plans	

# **Big "Things"** Cars -- Platforms on Wheels



# Tesla 'full self-driving' triggered an eight-car crash, a driver tells police



By <u>Matt McFarland</u>, CNN Published 5:41 PM EST, Wed December 21, 2022

> Safety Technologies in Cars 1885 First U. S. patent for seat belts 1988 U. S. required seat belts

### Generative AI is a legal minefield

Axios Login by Ina Fried, Feb. 24, 2023

Four broad areas of legal uncertainty around AI:

- Should AI developers pay for rights to training data?
  - US Authors'Guild has just released legal language for Publishing and Distribution Agreements Prohibiting AI Training Uses
- Can generative AI output be copyrighted?
  - Works entirely generated by a machine, in general, can't be copyrighted.
     It's less clear how the legal system will view human/AI collaborations.

#### Can Al slander or libel someone?

- Al systems aren't people, and as such, may not be capable of committing libel or slander. But the creators of those systems could potentially be held liable if they were reckless or negligent in the creation of the systems, according to some legal experts.
- The problem is trickier still because Al may show different results to different people.

### • Who's responsible if AI systems offer private or dangerously false info?

### **Copyright and Artificial Intelligence**



The Copyright Office has launched an initiative to examine the copyright law and policy issues raised by artificial intelligence (AI) technology, including the scope of copyright in works generated using AI tools and the use of copyrighted materials in AI training. After convening public listening sessions in the first half of 2023 to gather information about current technologies and their impact, the Office will publish a notice of inquiry in the *Federal Register*.

#### Announcements

March 16, 2023 - Copyright Office Launches New Artificial Intelligence Initiative

#### **Upcoming Events**

April 19, 2023 – Literary Works Listening Session May 2, 2023 – Visual Arts Listening Session May 17, 2023 – Audiovisual Works Listening Session May 31, 2023 – Music and Sound Recordings Listening Session

#### Past Events

Fall 2021 – Copyright Law and Machine Learning for AI: Where Are We and Where Are We Going? Winter 2020 – Copyright in the Age of Artificial Intelligence

#### Past Statements and Announcements

Fall 2021 – Artificial Intelligence: The Copyright Connection

## Al can be a catalyst, but can't be relied on

THE SHIFT

# A Conversation With Bing's Chatbot Left Me Deeply Unsettled

A very strange conversation with the chatbot built into Microsoft's search engine led to it declaring its love for me.

- My own experiences
  - ChatGPT puts George Cayley, inventor of seat belt in 19<sup>th</sup> century, in 20<sup>th</sup> century
  - ChatGPT tells me that an acquaintance was executive producer of another's movie. Both tell me that it was wrong.

### But there are plenty of good uses for AI ...

Thank you in many languages

Danke

អរកុណ

Gracias Medaase

شکر آ raieminderit Рахмат Terima kasih Gracias

Баярлалаа

धन्यवाद

Dankjewel

Gracias

Salamat

Mulțumesc

Ďakujem



# Prof. Lance J. Hoffman lancehoffmancyber.com

# ADDITIONAL RESOURCES on cybersecurity and privacy

ТҮРЕ	AUTHOR	TITLE	LINK
Ν		The Cybersecurity 202 (Washington Post)	https://www.washingtonpost.com/newslette rs/the-cybersecurity-202/
Ν	Prof. Dan Solove, GWU	Privacy and Security Blog, country whiteboards	https://teachprivacy.com/privacy-security- training-blog/
Ν	Bruce Schneier	Schneier on Security	https://www.schneier.com/crypto- gram/subscribe/
Ν	Brian Krebs	Krebs on Security	Krebsonsecurity.com
В	Shoshana Duboff	The Age of Surveillance Capitalism	
В	Bruce Schneier	A Hacker's Mind: How the Powerful Bend Society's Rules, and How to Bend them Back	
В	James Grimmelbaum	Internet Law Cases and Problems	https://semaphorepress.com/InternetLaw_o verview.html
А	Noam Chomsky	The False Promise of ChatGPT	https://www.nytimes.com/2023/03/08/opini on/noam-chomsky-chatgpt-ai.html
D	Council on Foreign Relations	State-sponsored attacks (Cyber Operations Tracker)	https://www.cfr.org/cyber-operations/
D	Responsible AI Collaborative	Al Incident Database	incidentdatabase.ai

#### N newsletter, B book, A article, D database

- Classic concerns about privacy and surveillance
- How countries address privacy and surveillance
- Cybersecurity awareness, training, and education
- How institutions are challenged and react
- Regulation
- Cybersecurity, national security, and war
- Some current and future challenges
- Q&A and Discussion