Engineering, Ethics and Society: Computing Ethics 4 - Databases and Surveillance

Dr. Gershon Weltman
Engineering 183EW, UCLA SEAS
Lecture 14

Copyright Gershon Weltman, 2020

Lecture Contents

- Database & Privacy Overview
  - Societal Issues: Availability, privacy, security
  - Personal Information: Voluntary & Otherwise
  - Information Sources
- Ethical Case 1: Database Use & Abuse
  - Technology
  - Ethical Test
- Ethical Case 2: Government Surveillance
  - 4th Amendment Protection & Expectation of Privacy
  - Technology & Programs
  - Benefits of Surveillance
  - Ethical Analysis
    - Societal Security vs. Personal Security
    - Public Reactions
    - Trust in Government vs. Protection against Tyranny
- Ethical Case 3: The Right to Information
- Ethical Status: Current and Future

Copyright Gershon Weltman, 2020

Societal Issues

The societal issues and ethics of databases and surveillance center on *Internet Information -- availability, privacy and security*:

- What do you WANT others to know about you?
- What do you NOT WANT others to know about you?
- Is there a RIGHT to personal privacy?

- What do others ALREADY know about you?
- What are others DOING with your information? Is this for private gain or for the common good?
- What PROTECTION is there or should there be available? For individuals? For information itself?

- Is there a RIGHT to Internet Information?

Copyright Gershon Weltman, 2020

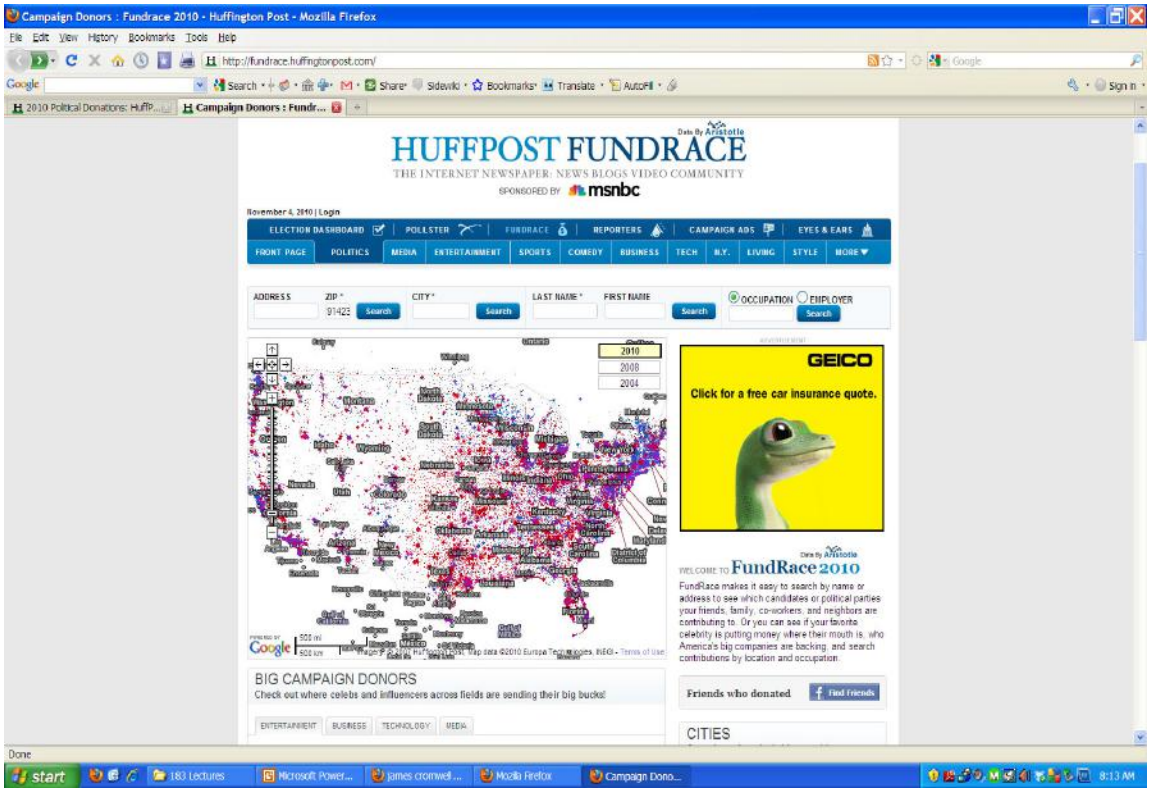
Personal Information: Good and Bad News

Good News

- Gigantic amount of information available
- Ultra easy access
- Many positive uses

Bad News

- Difficult to control
- Many chances for abuse and misuse!

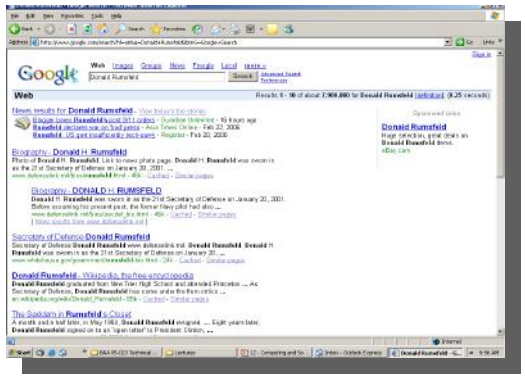


Copyright Gershon Weltman, 2020

Example: Building an eDossier

"John Doe"
"Jane Doe"

Google.com
Bing.com
MSN.com

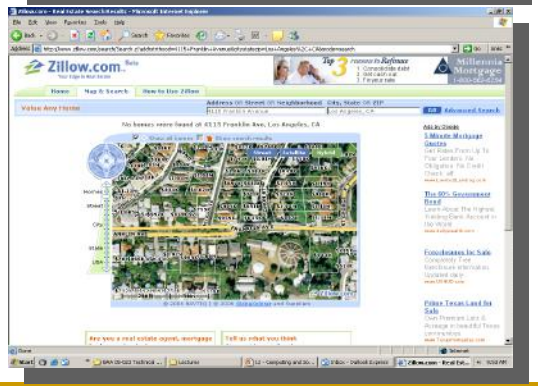


- Employment
- Education
- Memberships
- Publications
- News Events
- Contact Info

Zabasearch.com
Whitepages.com
Spokeo.com

- Criminal Record
- Lawsuits
- Judgments
- Tax Liens
- Bankruptcies

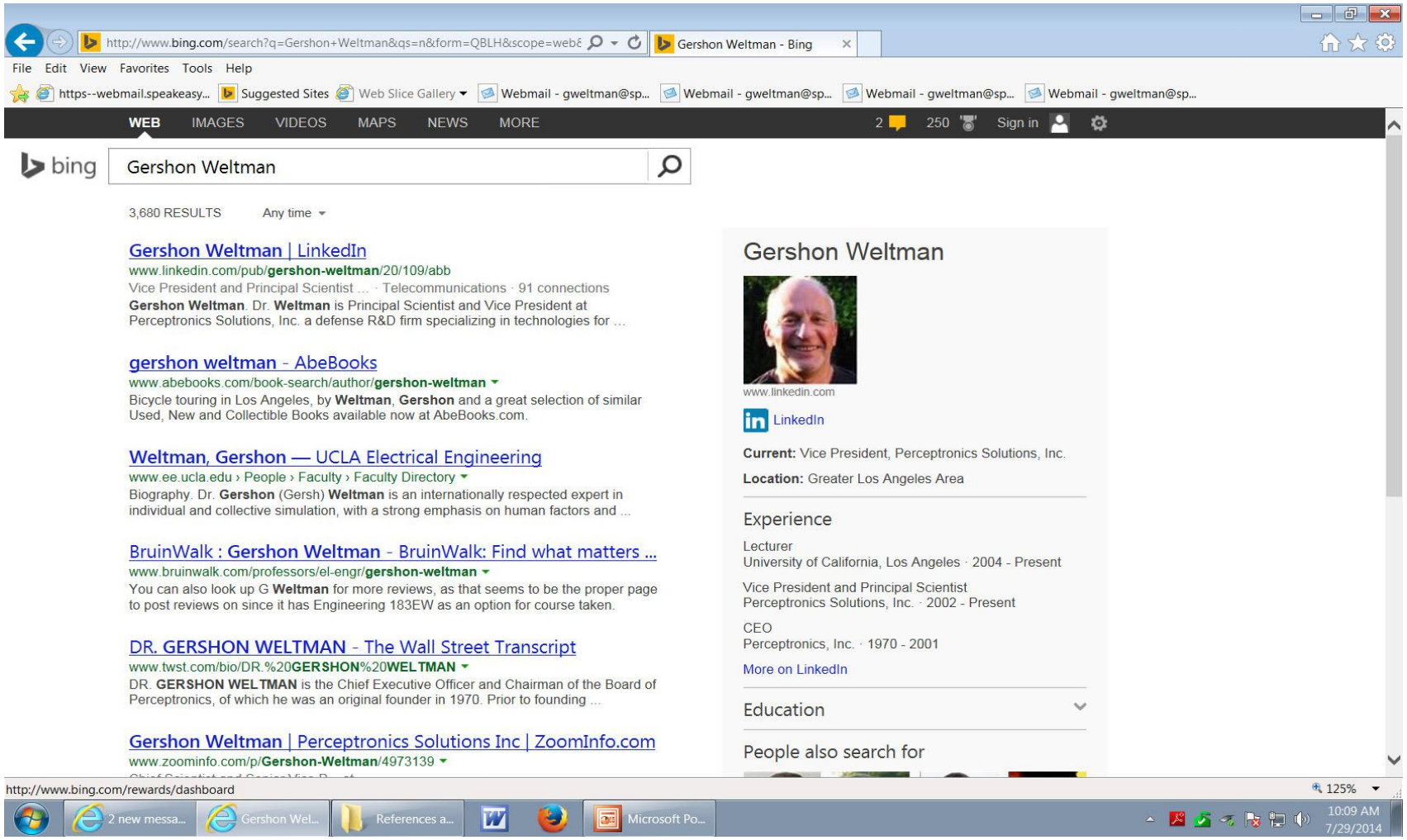
Zillow.com
Trulia.com
Redfin.com



- Home Size
- Home Value
- Neighborhood

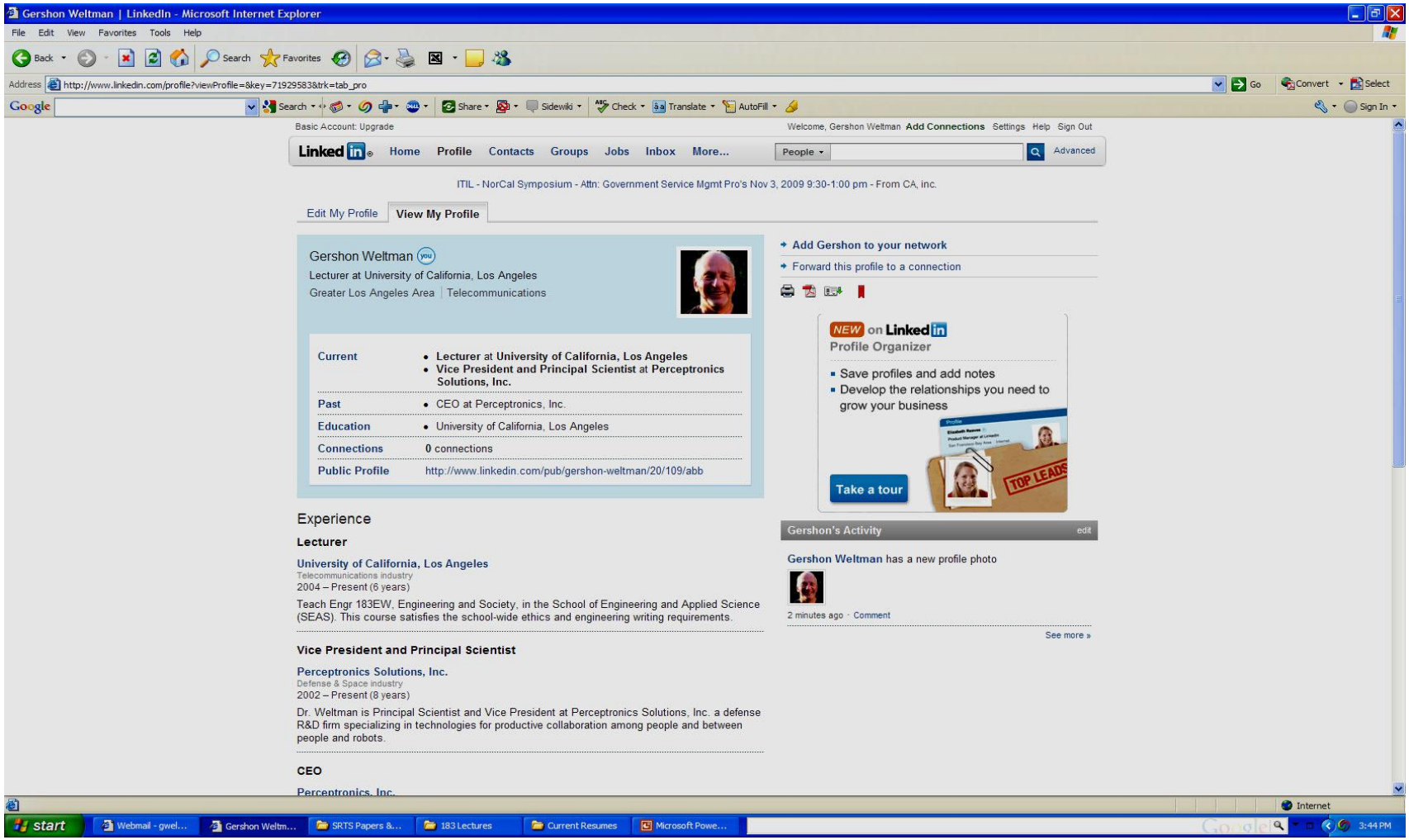
Copyright Gershon Weltman, 2020

Personal Information: General Search



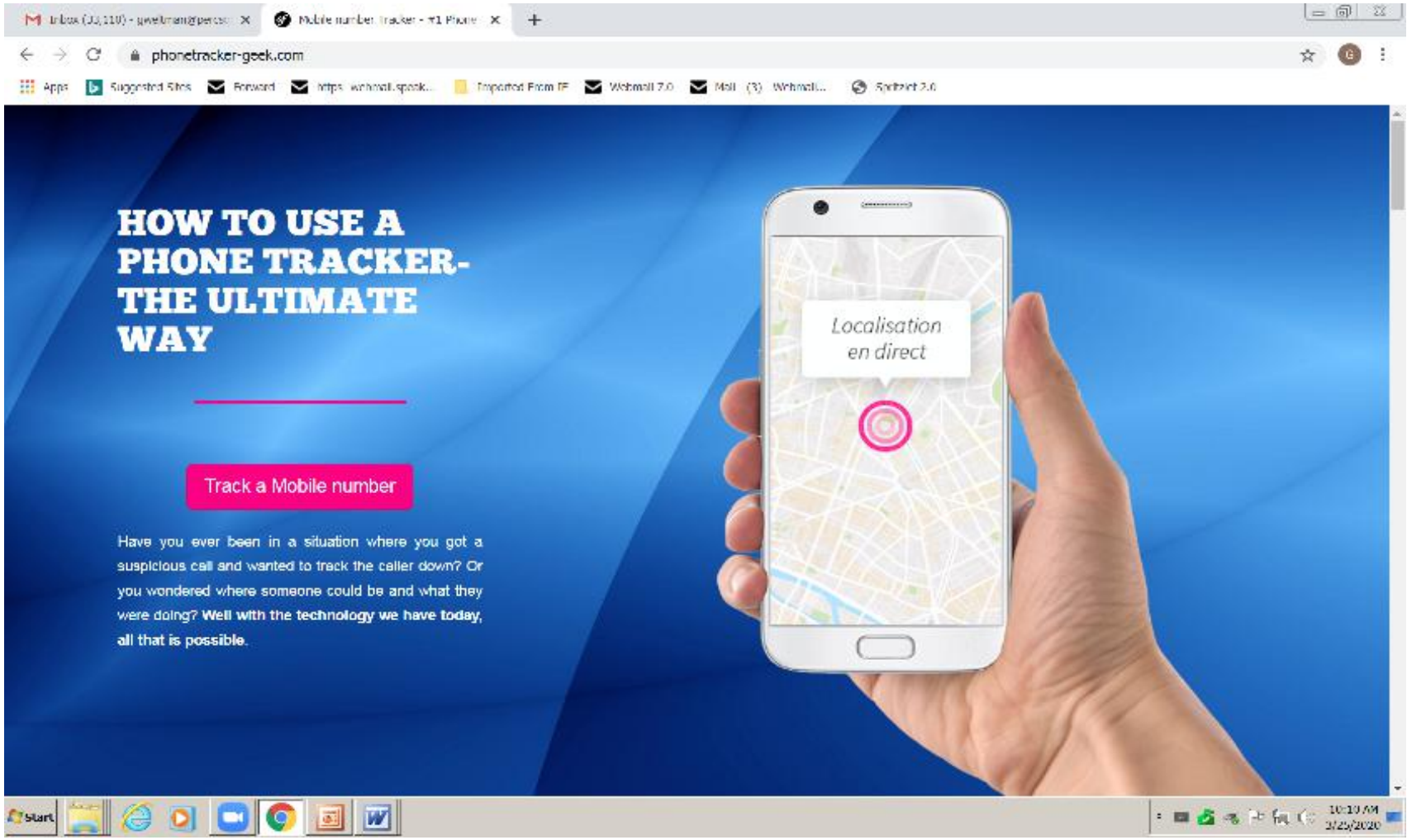
Copyright Gershon Weltman, 2020

Personal Information: Social Media



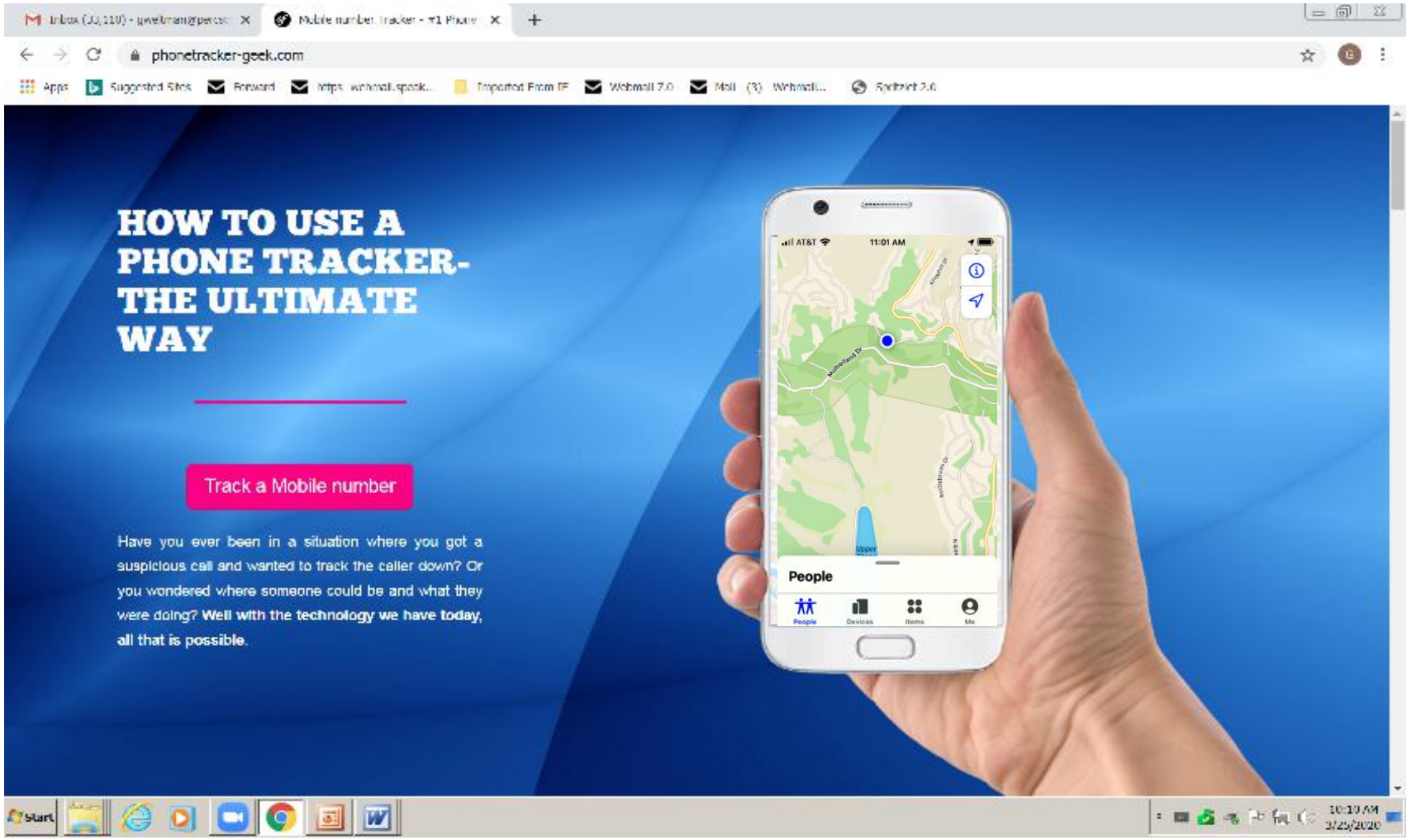
Copyright Gershon Weltman, 2020

Personal Information: Individual Location



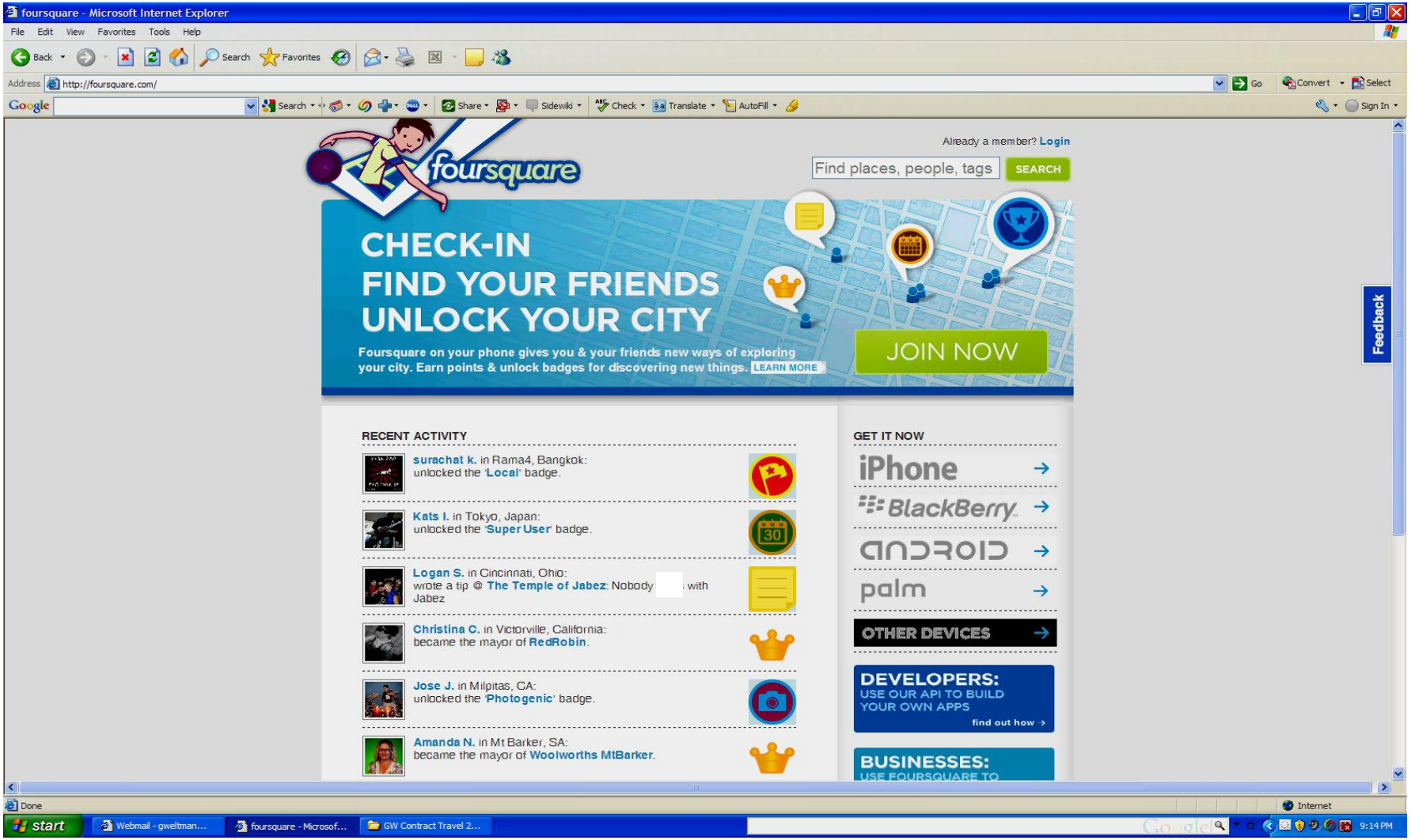
Copyright Gershon Weltman, 2020

Personal Information: Individual Location



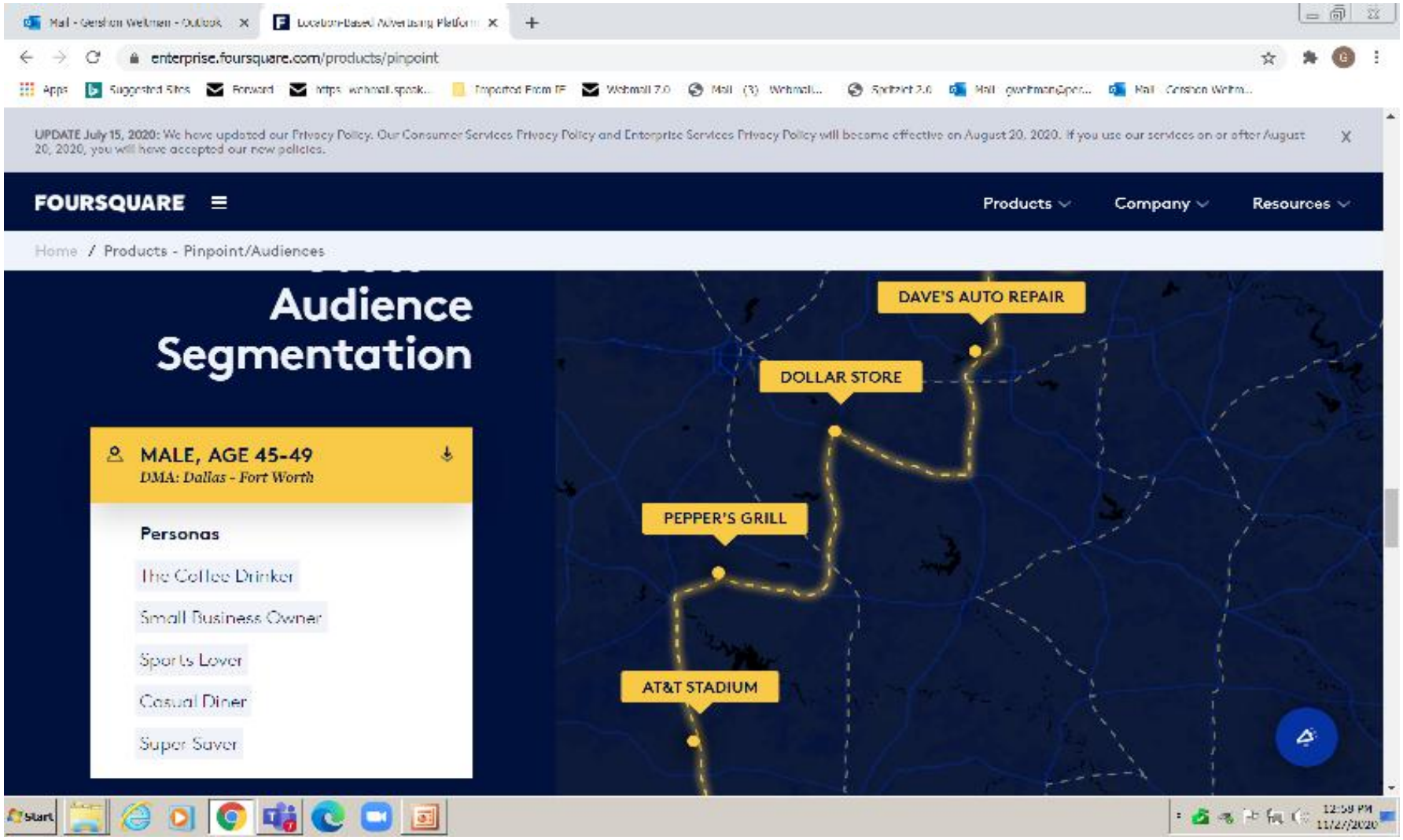
Copyright Gershon Weltman, 2020

Personal Information: Friends' Location



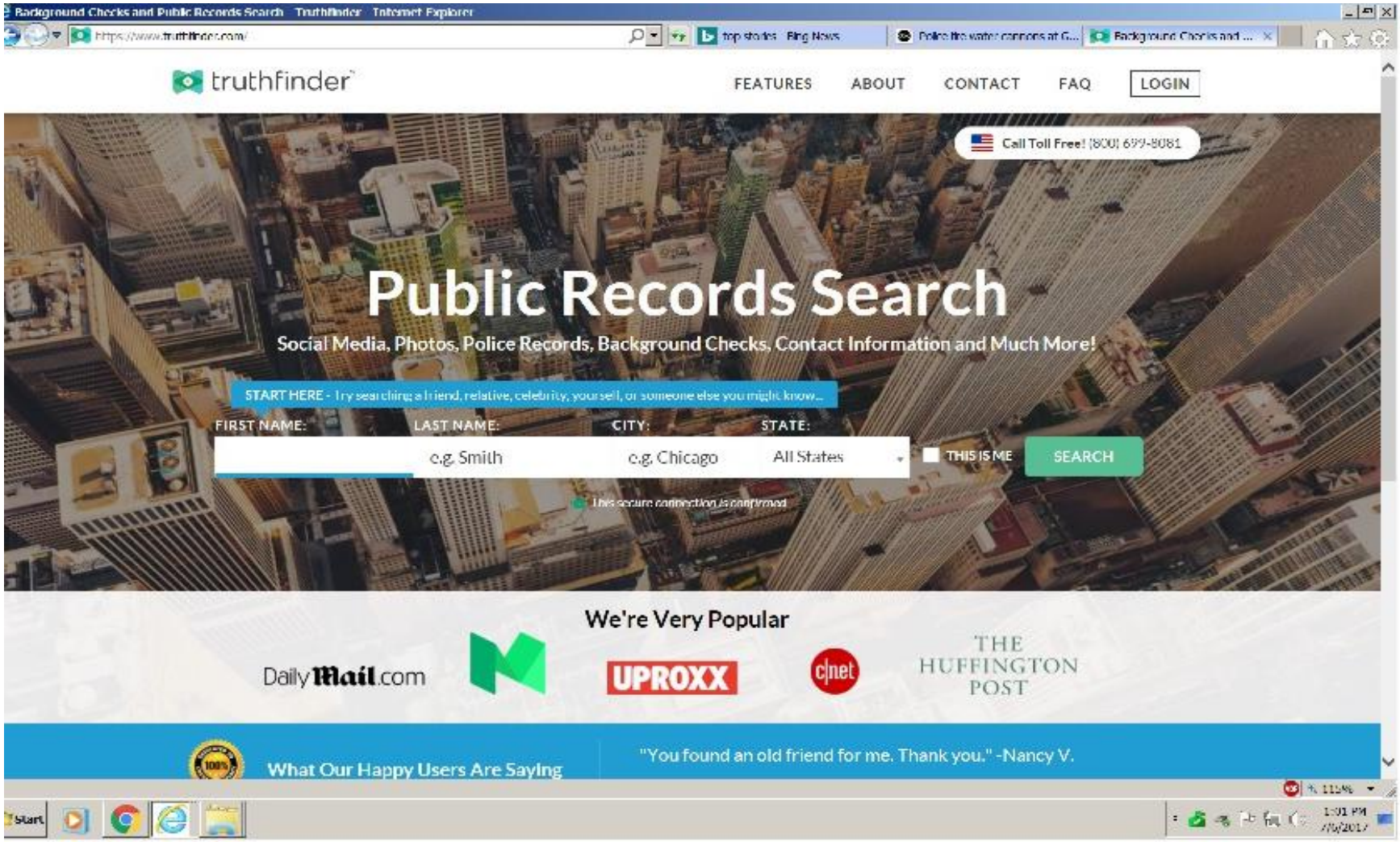
Copyright Gershon Weltman, 2020

Personal Information: Customers' Locations



Copyright Gershon Weltman, 2020

Personal Information: Public Records



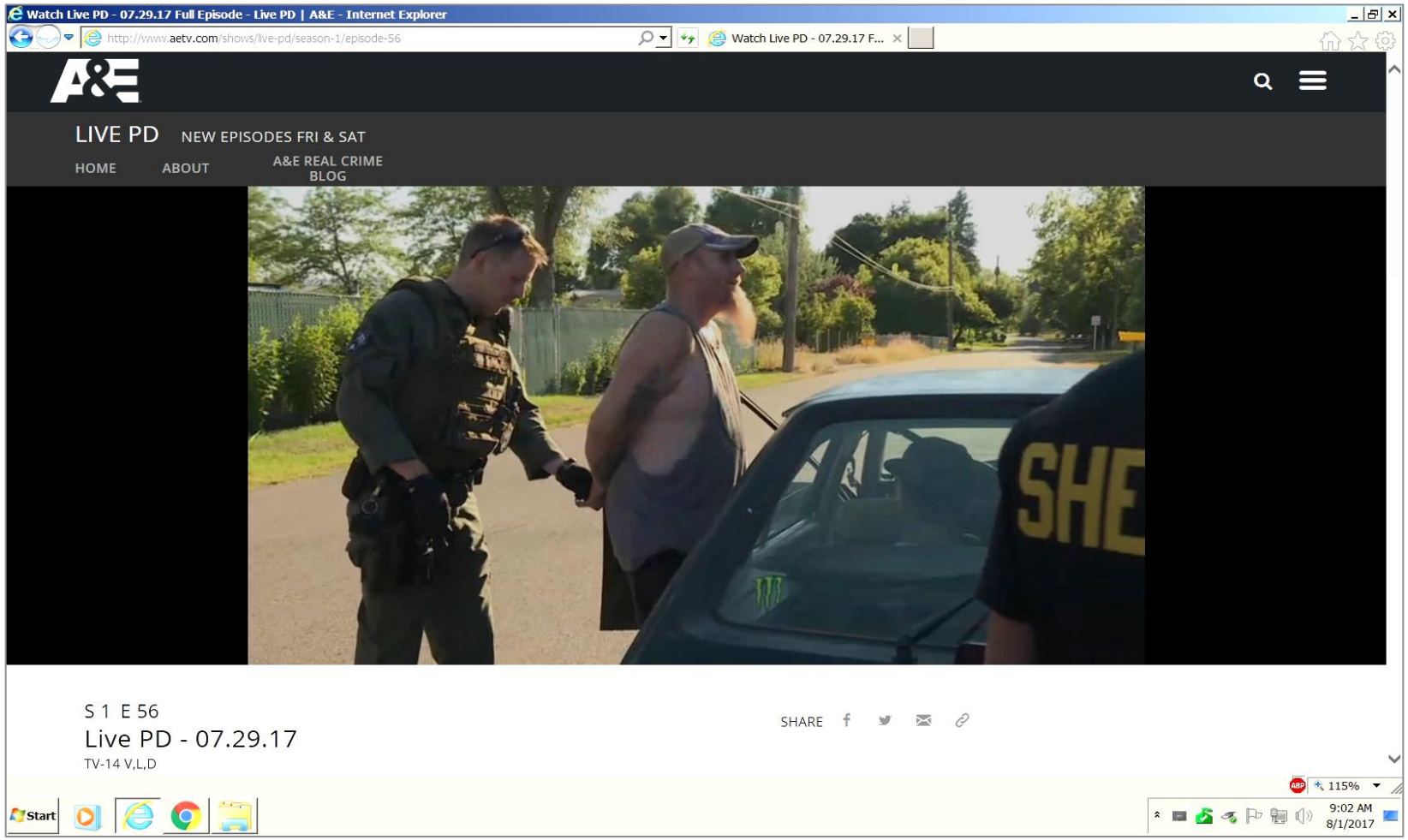
Copyright Gershon Weltman, 2020

Personal Information: Photos and Videos

Internet widely circulates pictures and transcriptions of arrests, deaths, and other compromising events that become part of the public record

Copyright Gershon Weltman, 2020

Personal Information: Photos and Videos



And the public record quickly becomes part of the reality TV industry.

Copyright Gershon Weltman, 2020

Personal Information: Mug Shots

findmugshots.com

BACKGROUND CHECKS

Easy access to Background Check databases with just 1 click.

GOVERNMENT RECORDS

One click access to third part sources for additional government records.

BOOKING RECORDS

List of charges related to the specific mugshot and arrest record

PREMIUM SUPPORT

Premium members get premium support :)

What is FindMugshots.com?

FINDMUGSHOTS.COM IS A COMPLETELY FREE SERVICE TO SEARCH FOR MUGSHOTS

FIND MUGSHOTS PROVIDES REAL TIME SEARCH TO ARRESTS AND MUGSHOTS.

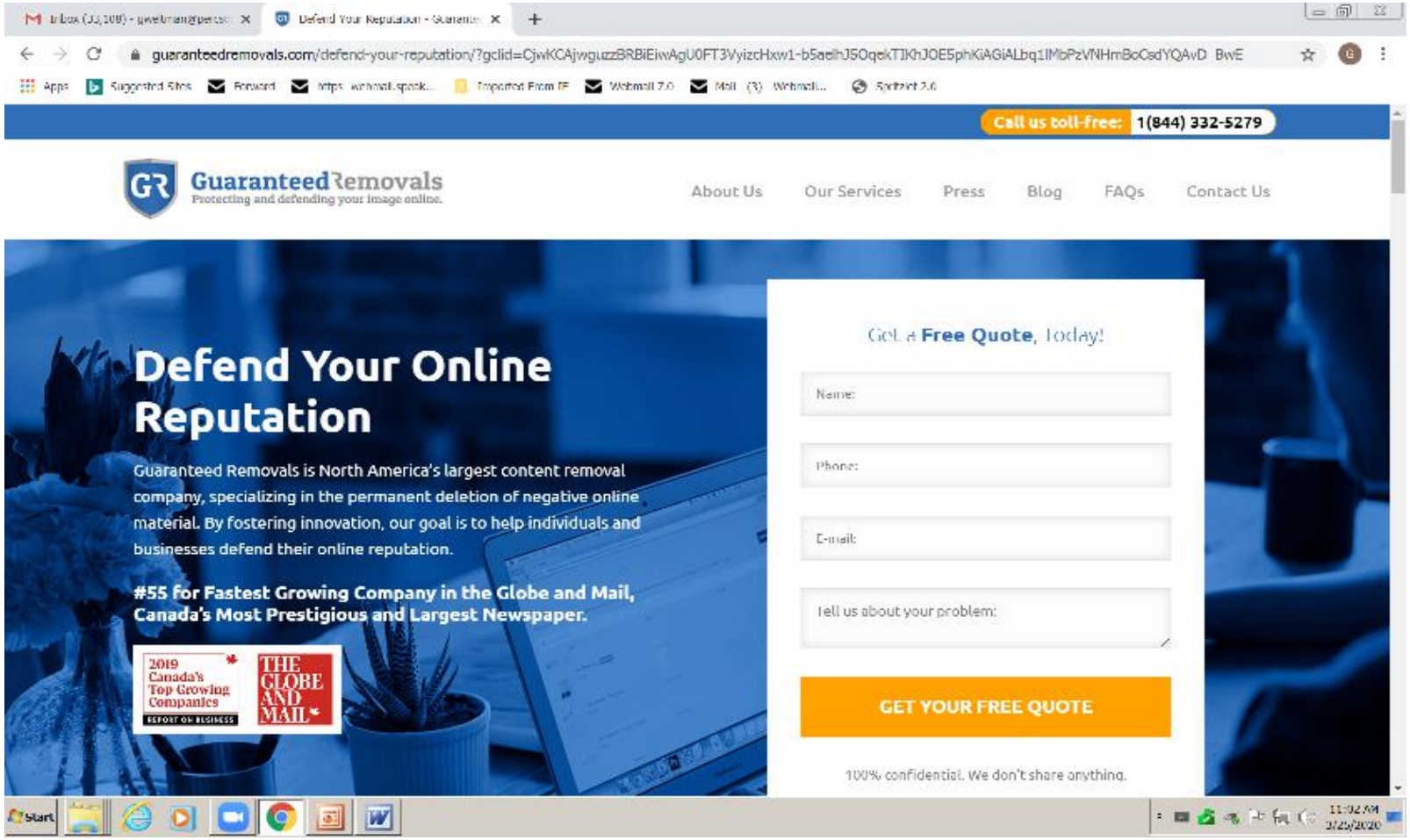
FindMugshots.com presents information that is sources from records made freely and publicly available by state and local law enforcement agencies or departments.

FindMugshots.com collects thousands of arrest records and mugshots a day. Our current database is over 1 billion records.

Our goal is to provide you with the most recent and even historic mugshots and arrest information for completely free of charge. You may want to use our partners for additional information about a person or the specific arrest record.

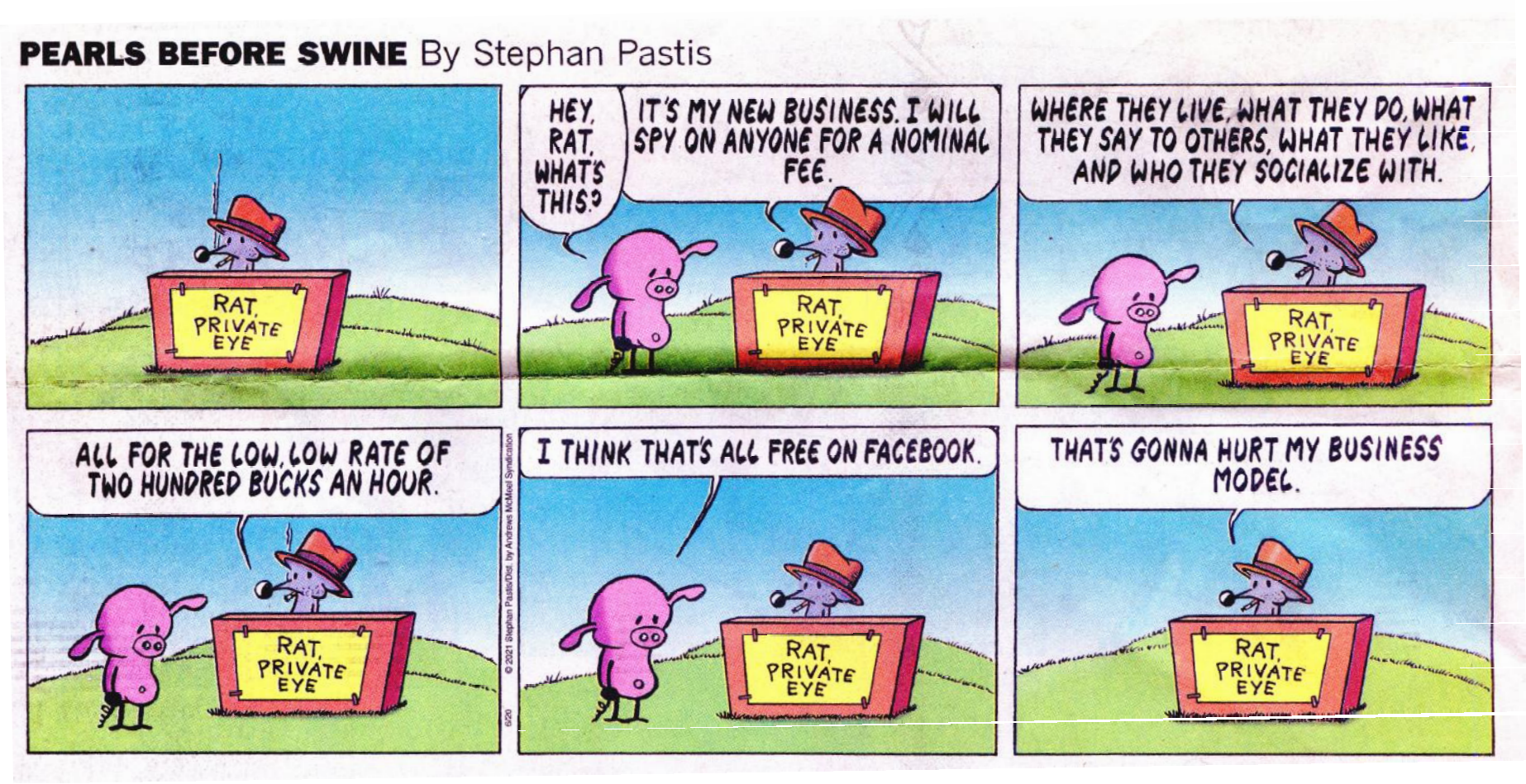
Copyright Gershon Weltman, 2020

Editing Your eDossier



Copyright Gershon Weltman, 2020

In Summary



Los Angeles Times, June 20, 2021

Copyright Gershon Weltman, 2020

The Importance of Information

- Key Factor

  Information will be the *main determinant of power, influence and security* in the 21st century (Alvin Toffler and others).

- Critical Influence

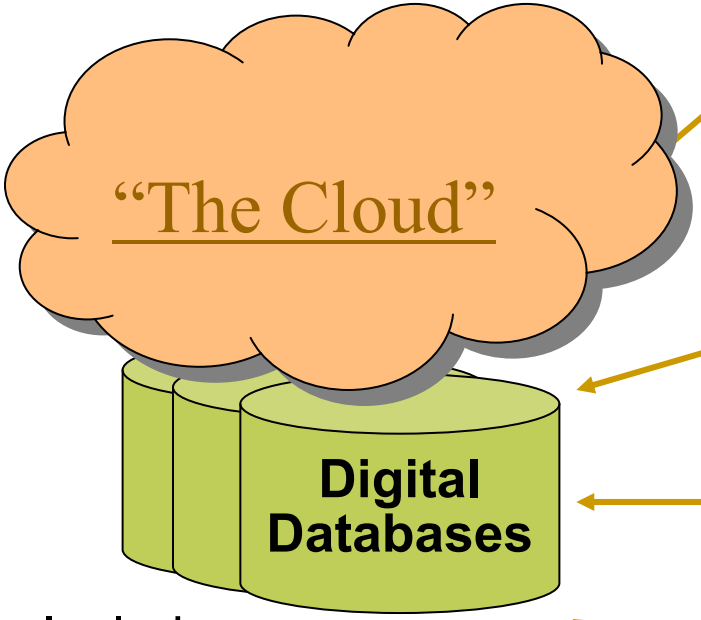
  Power, influence and security are *critical societal issues*, therefore information technologies will be central to society now and in the future.

- Logical Conclusion

  The technologies by which information is acquired, stored, distributed and used or misused will be major sources of *ethical and legal controversy.*

Copyright Gershon Weltman, 2020

Ethical Case 1: Database Use and Abuse



Include
- Messages
- Documents
- Images
- Videos
- Web Pages
- Web Clicks
- Etc.

Created by:
- Everyday Transactions
- Specialized Transactions
- Internet Activity
- eMailing and Texting

Owned by:
- Government
- Businesses and Institutions
- Individuals

Used for:
- Records & Statistics
- Information Gathering
- Strategic Decision Making

Involve Technologies for:
- Acquisition
- Security
- Integration
- Analysis

Copyright Gershon Weltman, 2020

Data Acquisition

Older Technologies:

- Records: Written transactions, photographs, recordings, movies
- Personal Traces: Fingerprints, blood type, belongings
- Movements: Eyewitness reports, bills. travel documents

Newer Technologies:

- Viewpoints: Satellites, cellular nodes, videocams, drones
- Records: Digital computer & phone data: files, emails, texts, messages
- Personal Traces: DNA
- Movements: Phone/GPS, credit card, license plate, facial recognition
- **Interconnection and Distribution: Broad networks of companies, Internet users, bloggers, hackers, and *government agencies***

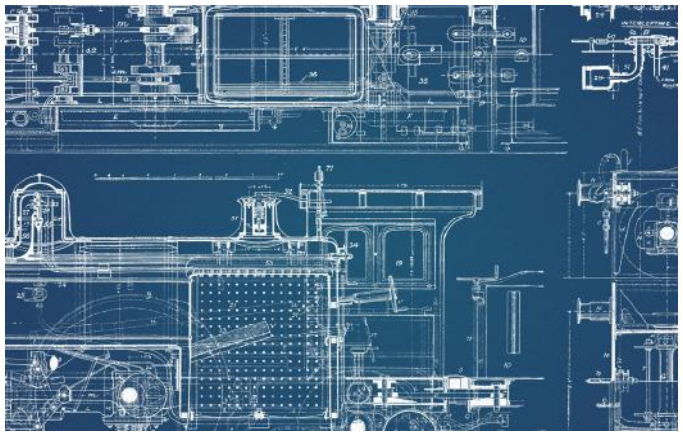
Copyright Gershon Weltman, 2020

The Chances for Abuse and Misuse

- Privacy: *Adding to Databases Personal*
  - Information (e.g.. medical records)
  - Sensitivities (e.g., sexual identity)
  - Actions (e.g. arrests, bankruptcies)
  - Associations (e.g. memberships)
  - Communications (e.g. embarrassments)


Donald Sterling and Maria Perez

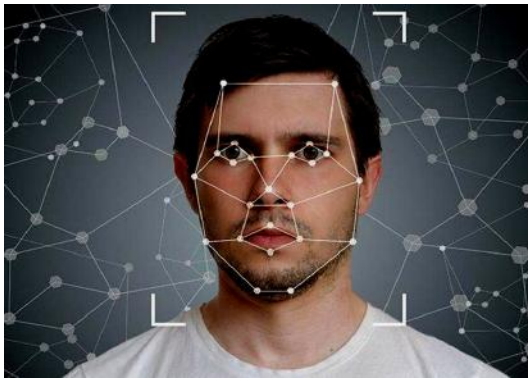
- Piracy: *Taking from Databases*
  - Secrets (e.g., plans, formulas)
  - Intellectual Property (e.g., technologies)
  - Identities (e.g., individual, corporate)
  - Site functionality or operability



Copyright Gershon Weltman, 2020

Protection Before: User Authentication

- What's Protected
  - Brick & Mortar Sites
  - Virtual Storage Sites
  - On-Line Transactions
- Technical Modalities
  - Something you have – Card, key
  - Something you know – PIN, passwor
  - Something you are – Biometrics
- Biometric Identification/Verification
  - Fingerprint
  - Handprint
  - Iris or Retinal Pattern
  - **Facial Recognition**
  - Movement – Signature, Gait



Copyright Gershon Weltman, 2020

Protection Today: Cyberspace Invasions

May 9, 2011 | Log In | Sign Up

Peter S. Goodman
pgoodman@huffingtonpost.com
Become a fan of this reporter
GET UPDATES FROM Peter
Like
256

Sony Hack Speaks To Proliferating Threat

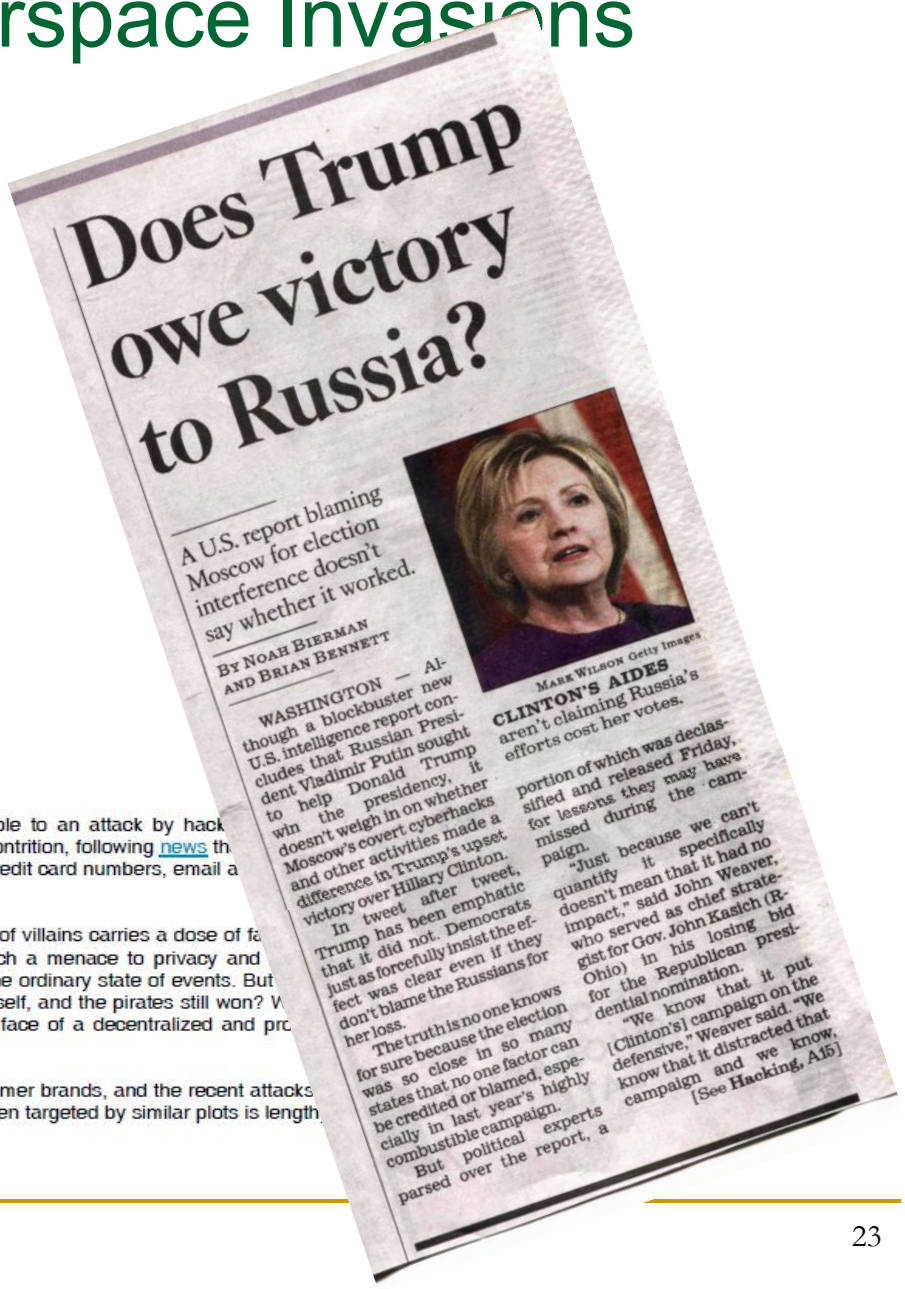
First Posted: 05/ 9/11 08:46 AM ET Updated: 05/ 9/11 08:51 AM ET

React

Sony is run by a bunch of greedy morons who stupidly left their systems vulnerable to an attack by hack
conventional explanation of how the company finds itself bent into a familiar pose of contrition, following news th
breached its defenses, potentially gaining access to troves of valuable information -- credit card numbers, email a
more than 100 million customers.

If only life were so soothingly simple. The Sony data hack and the predictable pursuit of villains carries a dose of fa
implicitly affirming the assumption that someone must have fouled up to create such a menace to privacy and
someone must have failed in a readily identifiable way, because this surely can't be the ordinary state of events. But
narrative masks an unsettling question: What if Sony did the best it could to protect itself, and the pirates still won? W
company employed the best defenses available, yet they proved inadequate in the face of a decentralized and pro
threat?

Sony has captured headlines because it is one of the world's most conspicuous consumer brands, and the recent attacks
network have been both brazen and successful. But the list of companies that have been targeted by similar plots is length
growing.



Does Trump owe victory to Russia?

A U.S. report blaming Moscow for election interference doesn't say whether it worked.

By Noah Bierman and Brian Bennett

WASHINGTON — Although a blockbuster new U.S. intelligence report concludes that Russian President Vladimir Putin sought to help Donald Trump win the presidency, it doesn't weigh in on whether Moscow's covert cyberhacks and other activities made a difference in Trump's upset victory over Hillary Clinton. In tweet after tweet, Trump has been emphatic that it did not. Democrats just as forcefully insist the effect was clear even if they don't blame the Russians for her loss.

The truth is no one knows for sure because the election was so close in so many states that no one factor can be credited or blamed, especially in last year's highly combustible campaign. But political experts parsed over the report, a portion of which was declassified and released Friday, for lessons they may have missed during the campaign.

"Just because we can't quantify it specifically doesn't mean that it had no impact," said John Weaver, who served as chief strategist for Gov. John Kasich (R-Ohio) in his losing bid for the Republican presidential nomination.

"We know that it put [Clinton's] campaign on the defensive," Weaver said. "We know that it distracted that campaign and we know,

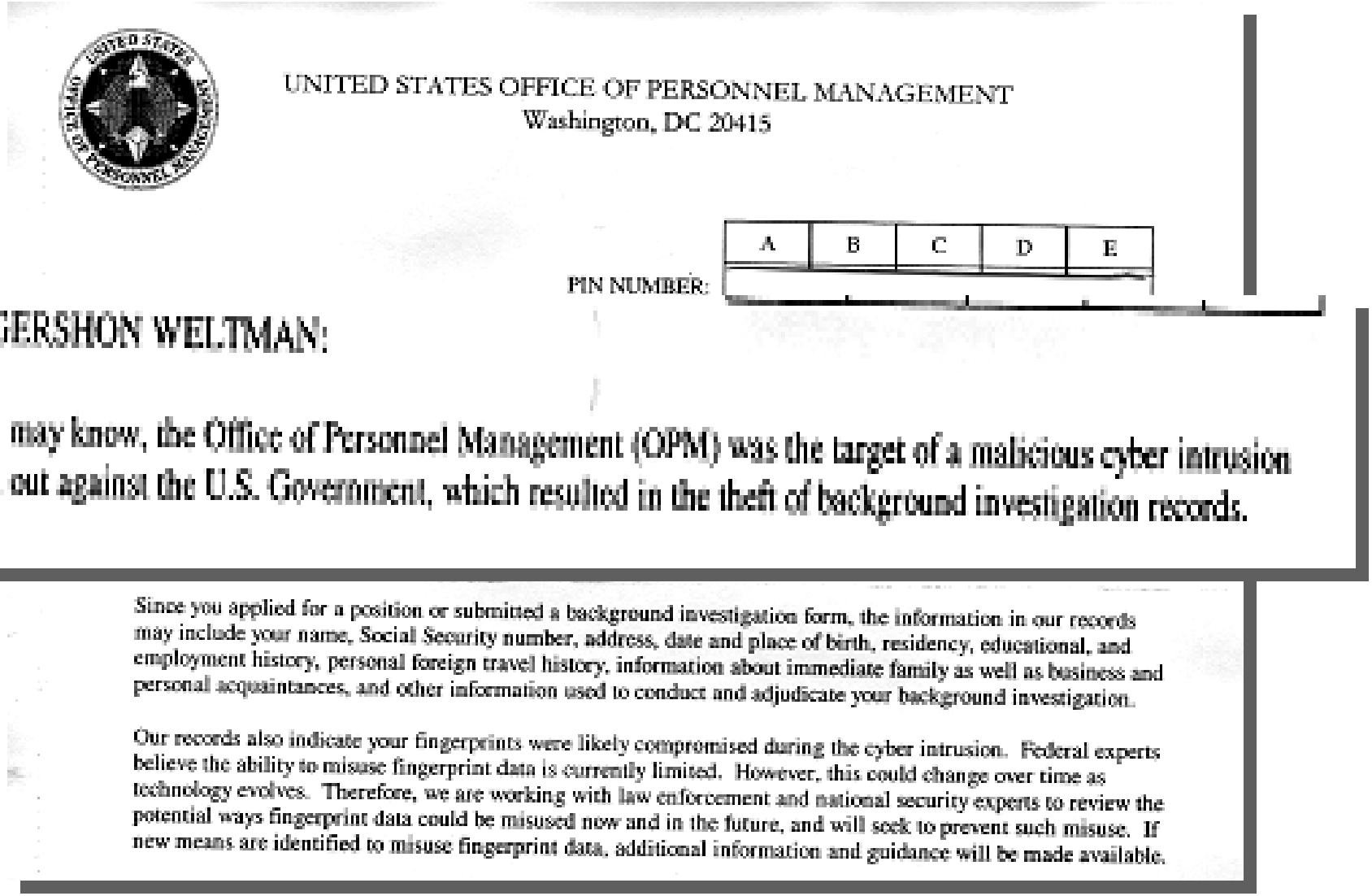
[See Hacking, A15]

Mark Wilson Getty Images

CLINTON'S AIDES aren't claiming Russia's efforts cost her votes.

Copyright Gershon Weltman, 2020

It Gets Personal…



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

A	B	C	D	E

PIN NUMBER:

Dear GERSHON WELTMAN:

As you may know, the Office of Personnel Management (OPM) was the target of a malicious cyber intrusion carried out against the U.S. Government, which resulted in the theft of background investigation records.

Since you applied for a position or submitted a background investigation form, the information in our records may include your name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate your background investigation.

Our records also indicate your fingerprints were likely compromised during the cyber intrusion. Federal experts believe the ability to misuse fingerprint data is currently limited. However, this could change over time as technology evolves. Therefore, we are working with law enforcement and national security experts to review the potential ways fingerprint data could be misused now and in the future, and will seek to prevent such misuse. If new means are identified to misuse fingerprint data, additional information and guidance will be made available.

Copyright Gershon Weltman, 2020

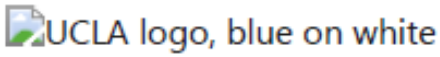
…Institutional…

UC Cyber Security Incident

UCLA Chief Information Security Officer David Shaw <security@ucla.edu>

Wed 3/31/2021 7:26 PM

To: gweltman@ee.ucla.edu <gweltman@ee.ucla.edu>



Information Technology Services

Dear Bruin Community:

I wanted to make you aware of a cyber security incident that may have impacted members of our community and provide you with information and resources to help anyone who might have been affected. Please know that UCLA is committed to the security of your personal information and is working to address this.

Beginning this past Monday, many UCLA email accounts started receiving messages stating that their personal data had been stolen and would be released. These emails contained a link to a public website where a sample of personal information from UC employees was posted.

Copyright Gershon Weltman, 2020

…and National

JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

TLP:WHITE

Product ID: AA22-047A

February 16, 2022

Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology

SUMMARY

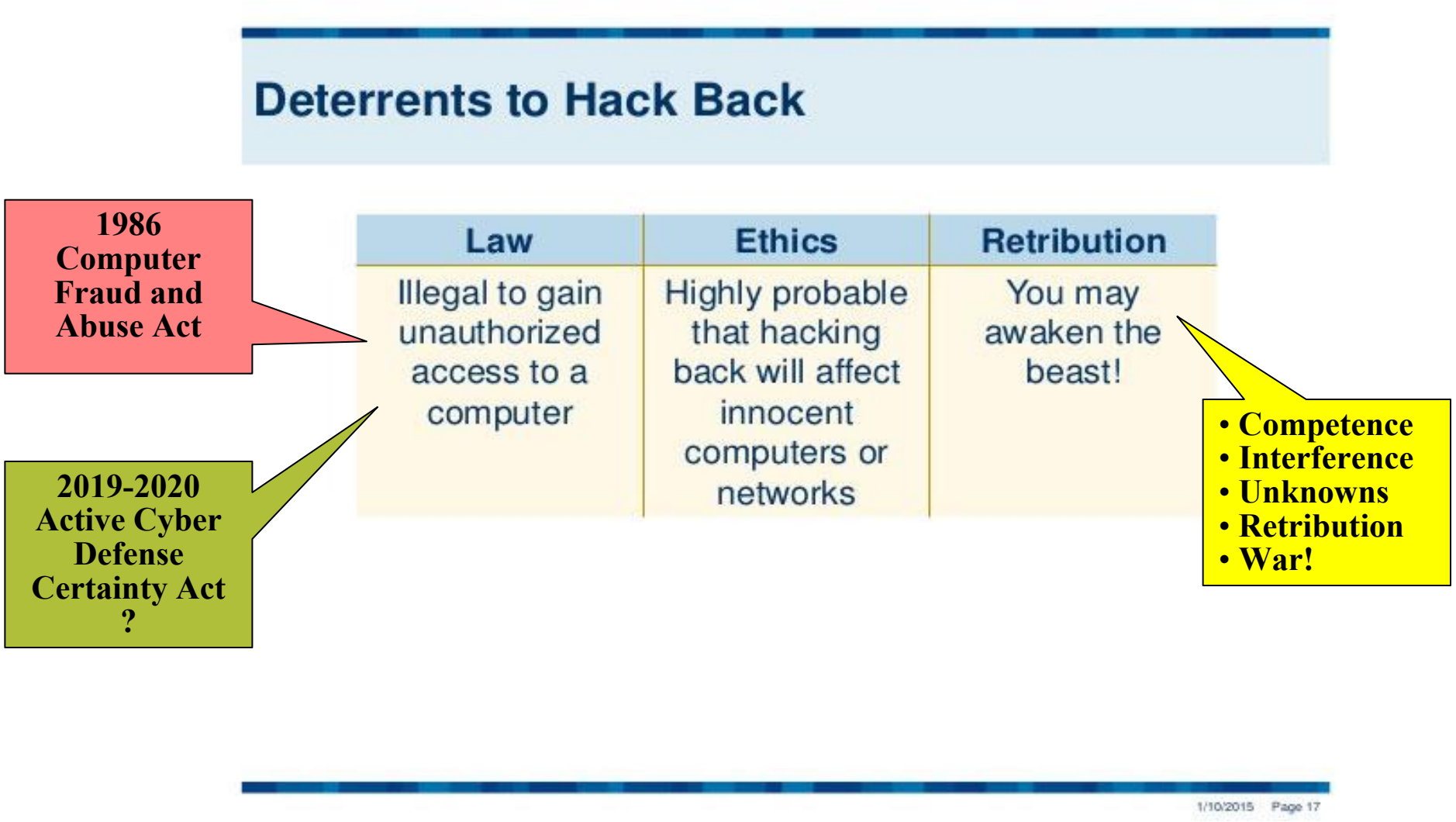
From at least January 2020, through February 2022, the Federal Bureau of Investigation (FBI), National Security Agency (NSA), and Cybersecurity and Infrastructure Security Agency (CISA) have observed regular targeting of U.S. cleared defense contractors (CDCs) by Russian state-sponsored cyber actors. The actors have targeted both large and small CDCs and subcontractors with varying levels of cybersecurity protocols and resources. These CDCs support contracts for the U.S. Department of Defense (DoD) and Intelligence Community in the following areas:

Actions to Help Protect Against Russian State-Sponsored Malicious Cyber Activity:

- Enforce multifactor authentication.
- Enforce strong, unique passwords.
- Enable M365 Unified Audit Logs.
- Implement endpoint detection and response tools.

Copyright Gershon Weltman, 2020

Private Response Can be Dangerous



Copyright Gershon Weltman, 2020

The Problem Has Become Evident..

In the cloud, a hazy grasp of security risks

Data protection is increasingly an issue as more companies rely on remote servers to store their files, a consultant says

BY PARESH DAVE

When Thomas Trappler talks clouds, companies listen.

But he's not warning about rain. Rather, Trappler is a "cloud" consultant, who tells attorneys, executives and fellow information technology experts what to look out for when they put company databases in the so-called cloud.

As more companies rely on remote cloud servers to store their files, Trappler has become a highly sought-after security advisor, a celebrity of sorts in the rapidly growing cloud computing industry.

"No one's teaching people about this," Trappler said. "At the moment, I don't think there are very many people like me."

Trappler is the director of software licensing at UCLA — a job that opened the door to his lucrative moonlighting.

For years, he had been buying licenses for programs, such as Microsoft Office, so that UCLA faculty, students and staff could use them. But the rules started to change five years ago as these programs moved into the cloud, turning into apps such as Office 365. Trappler studied until he became a go-to expert nationwide.

"It's easy to overlook security because of the virtual nature of the cloud, but really your data is going over the Internet to another computer and not to some magical world where everything's going to be fine," he said.

The $40-billion cloud industry, as measured by the research firm IDC, is attractive to companies. By transferring files via the Internet to a hard drive located in a data center or server farm, users can access the data from any Internet-connected device.

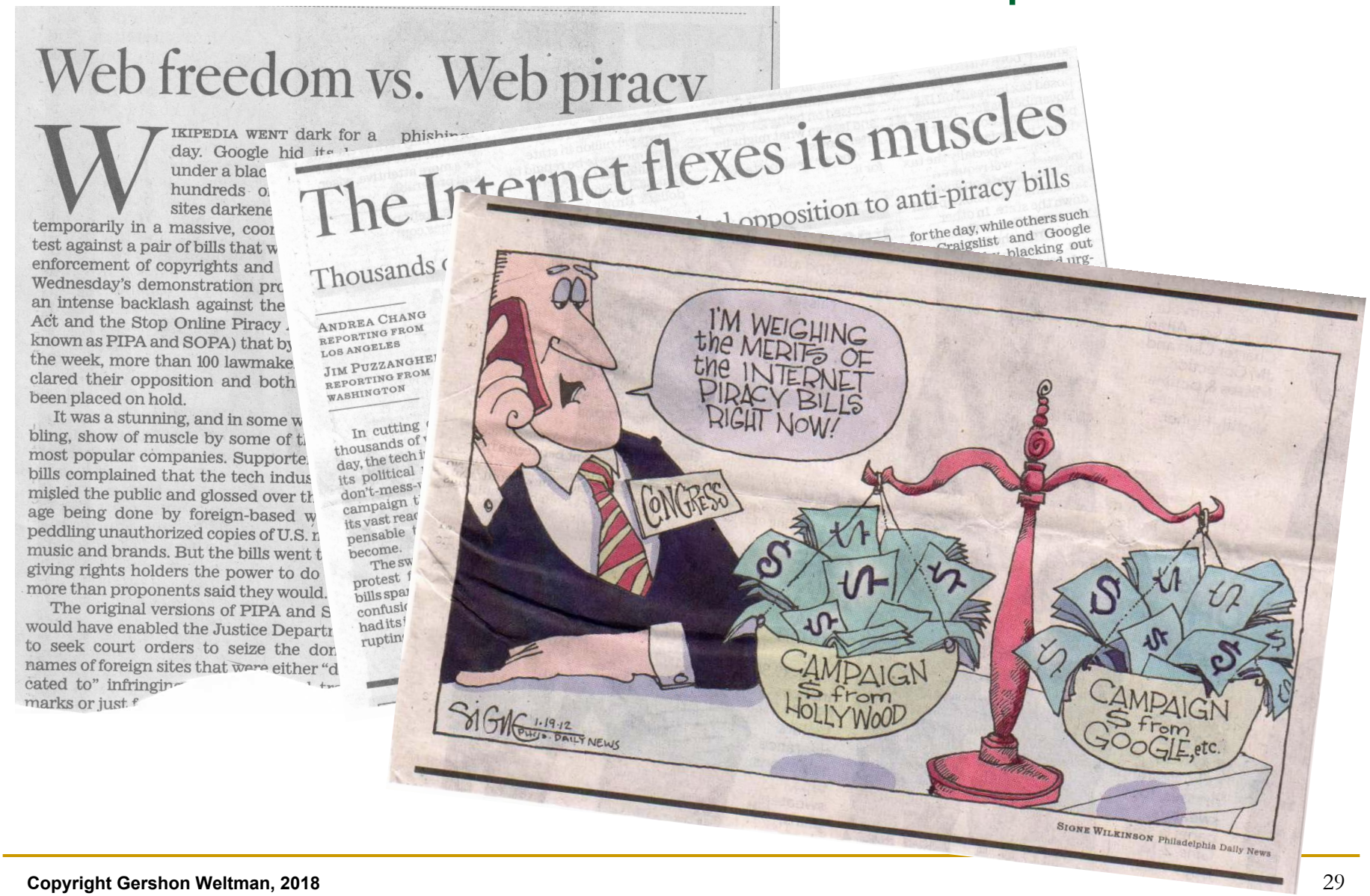
Online retailer Amazon.com Inc. is one of the largest data center providers, housing data on behalf of thousands of companies including Netflix Inc., Dropbox Inc. and Autodesk Inc. Other large cloud providers are Google Inc., Microsoft Corp. and Rackspace Inc.

What troubles Trappler is that not

[See Cloud, B4]

Copyright Gershon Weltman, 2020

…but the Solution is Often Not Simple…



Web freedom vs. Web piracy

WIKIPEDIA WENT dark for a day. Google hid its under a blac hundreds o sites darkene temporarily in a massive, coor test against a pair of bills that w enforcement of copyrights and Wednesday's demonstration pro an intense backlash against the Act and the Stop Online Piracy known as PIPA and SOPA) that by the week, more than 100 lawmake clared their opposition and both been placed on hold.

It was a stunning, and in some w bling, show of muscle by some of t most popular companies. Supporte bills complained that the tech indus misled the public and glossed over th age being done by foreign-based w peddling unauthorized copies of U.S. r music and brands. But the bills went t giving rights holders the power to do more than proponents said they would.

The original versions of PIPA and S would have enabled the Justice Departr to seek court orders to seize the dor names of foreign sites that were either "d cated to" infringin marks or just f

The Internet flexes its muscles

Thousands

ANDREA CHANG REPORTING FROM LOS ANGELES

JIM PUZZANGHE REPORTING FROM WASHINGTON

In cutting thousands of day, the tech i its political don't-mess- campaign t its vast reac pensable become.

The sw protest bills spa confusi had its ruptin

opposition to anti-piracy bills

for the day, while others such Craigslist and Google blacking out urg-

I'M WEIGHING the MERITS OF the INTERNET PIRACY BILLS RIGHT NOW!

CONGRESS

CAMPAIGN $ from HOLLYWOOD

CAMPAIGN $ from GOOGLE, etc.

SIGNE 1.19.12 PHILLY DAILY NEWS

SIGNE WILKINSON Philadelphia Daily News

Copyright Gershon Weltman, 2018

…but the Solution is Often Not So Simple

Copyright Gershon Weltman, 2018

“Big Data” Further Complicates Things…

expect a company to know why they're buying. Or why they aren't. Because when a company knows what motivates customers, it can serve them better.

THE POWER OF BIG DATA.

Combining big data with company data paints a better picture of the customer.

80% *of the data currently produced is unstructured —coming from sources like images, videos, tweets, posts and e-mails.*

MINING MOTIVATION.

Enter Smarter Analytics from IBM—software, systems and strategies that help companies combine their own enterprise data with their consumers' unstructured data to see a fuller

communications carrier, XO Communications was able to predict likely customer defections within 90 days, reducing churn by 35 percent the first year.

With IBM Smarter Analytics,

Share

Big Data is the totality of information about a person and his or her personal finances, memberships, activities, interests and inclinations.
Political campaigns use Big Data to understand voters, companies use Big Data for marketing, public organizations use Big Data to gage public opinion, and *Government agencies use Big Data for surveillance*.

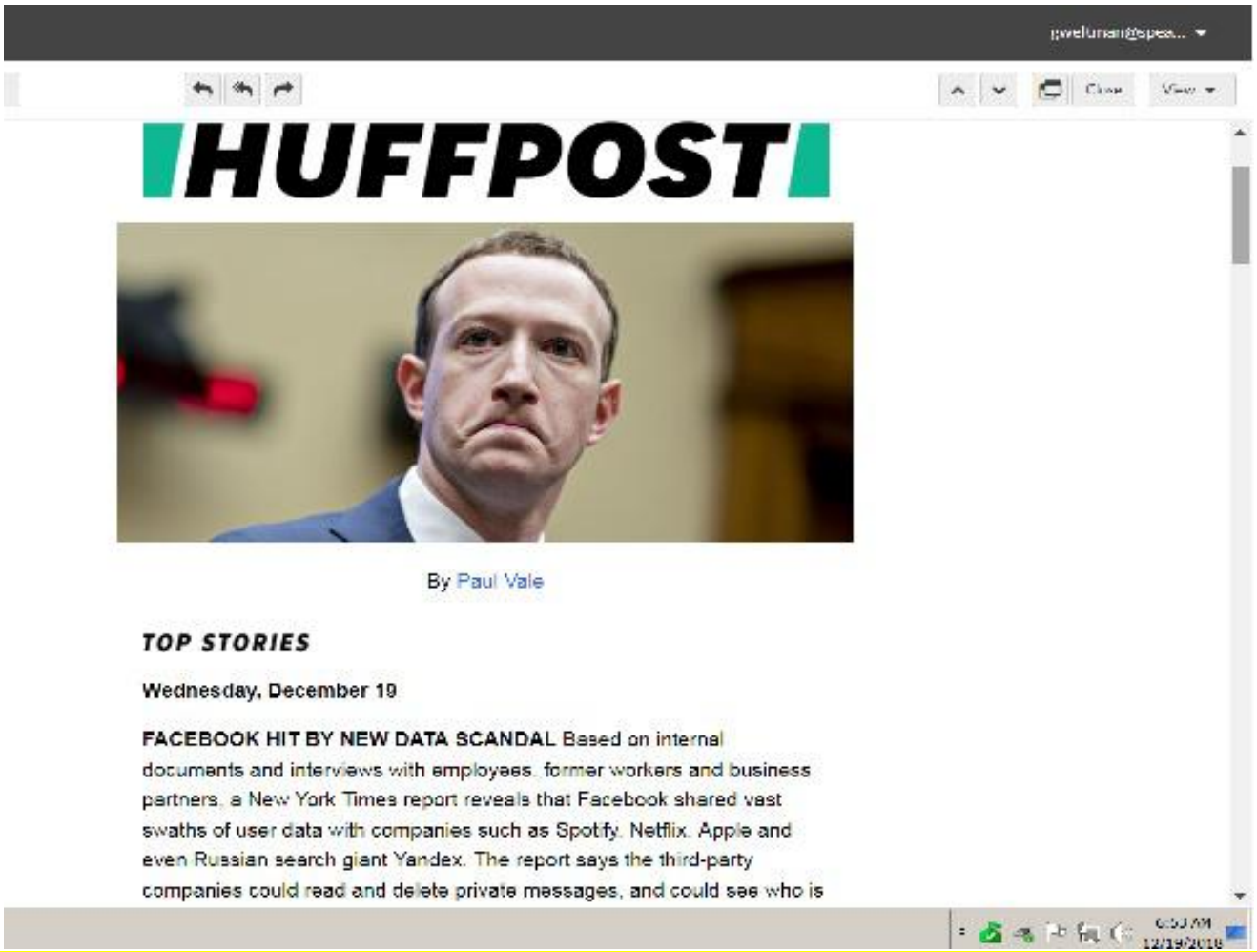
Copyright Gershon Weltman, 2018

…and Creates Its Own Forms of Abuse…

Social media creates an immense worldwide database of detailed personal information and preferences as well as of "friends and family" connections

Copyright Gershon Weltman, 2018

…with Facebook as a Major Culprit…



HUFFPOST

By Paul Vale

TOP STORIES

Wednesday, December 19

FACEBOOK HIT BY NEW DATA SCANDAL Based on internal documents and interviews with employees, former workers and business partners, a New York Times report reveals that Facebook shared vast swaths of user data with companies such as Spotify, Netflix, Apple and even Russian search giant Yandex. The report says the third-party companies could read and delete private messages, and could see who is

Social media information is sold as Big Data to businesses and organizations.

Copyright Gershon Weltman, 2018

…Its Data Maybe Even Affecting Elections

PULLING BACK THE CURTAIN

Cambridge Analytica's Real Role in Trump's Dark Facebook Campaign

Now new data has opened a small window into Trump's social-media machinery, and in particular the role played by the now-defunct Cambridge Analytica.

Kevin Poulsen 12.10.18 5:06 AM ET

Copyright Gershon Weltman, 2018

…Its Data Maybe Even Affecting Elections

THE FACEBOOK SCANDAL DEEPENS "Disturbing undercover interviews with executives from U.K.-based political research firm Cambridge Analytica have revealed admissions of bribery, entrapment and the use of sex workers to sway political elections around the world, according to an investigative series airing Monday." U.K. authorities have taken over the investigation into Cambridge Analytica. The blowback is "pummeling" Facebook's stock. Facebook's data security chief is also leaving over a dispute on the handling of "Russian ploys." And turns out it's harder to delete your Facebook account than you'd think. [Huffpost. March 20, 2018]

Copyright Gershon Weltman, 2018

Facebook Said It Would Change

BY ELIZABETH DWOSKIN

Facebook Inc. Chief Executive Mark Zuckerberg announced sweeping changes to his company's services Wednesday, saying he would spend the next several years reorienting the social media giant's apps toward encryption and privacy.

500 2,771.45 ▼ 18.20 | NASDAQ 7,505.92 ▼ 70.44 | GOLD $1,284.90 ▲ 2.90 | OIL $56.22 ▼ 0.34 | EURO $1.1308 ▲ .0005 | U.S.

MARCIO JOSE SANCHEZ Associated Press

CEO Mark Zuckerberg likened the change to transforming Facebook from a town square into a living room.

Beleaguered Facebook vows a shift to privacy

Promise to refocus is likely to be met with skepticism

Copyright Gershon Weltman, 2018

But It's Not Just Facebook…

Grindr, other dating apps leak data, group finds

They share users' info — including sexual orientation — with other companies, a report says.

BY SARAH SYED, NATALIA DROZDIAK, NATE LANXON AND SUHAUNA HUSSAIN

Grindr is sharing detailed personal data with thousands of advertising partners, allowing them to receive information about users' location, age, gender and sexual orientation, a Norwegian consumer group said.

Other apps, including popular dating apps Tinder and OkCupid, share similar user information, the group said. Its findings show how data can spread among companies, and they raise questions about how exactly the companies behind the apps are engaging with Europe's data protections and tackling California's new privacy law, which went into effect Jan. 1.

Grindr — which describes itself as the world's largest social networking app for gay, bi, trans and queer people — gave user data to third parties involved in advertising and profiling, according to a report by the Norwegian Consumer Council that was released Tuesday. Twitter Inc. ad subsidiary MoPub was used as a mediator for the data sharing and passed personal data to third parties, the report said.

"Every time you open an app like Grindr, advertisement networks get your GPS location, device identifiers and even the fact that you use a gay dating app," Austrian privacy activist Max Schrems said. "This is an insane violation of users' [European Union] privacy rights."

The consumer group and Schrems' privacy organiza-

[See Dating, C5]

HASSAN AMMAR Associated Press

A WOMAN checks the Grindr app. "Every time you open an app like Grindr, advertisement networks get your GPS location, device identifiers and even the fact that you use a gay dating app," one activist says.

LA Times 1/15/20

Copyright Gershon Weltman, 2018

…and Not Just Social Media

A8 FRIDAY, JULY 23, 2021 Los Angeles Times LATIMES.COM

BUSINESS

Big Tech in a race for your health data

As companies rush to get monitoring devices in homes, lawmaker pushes medical privacy bill

DAVID LAZARUS

There's a race on between the tech industry and lawmakers over your medical privacy.

Big Tech is moving as fast as it can to embed its increasingly intrusive devices into people's homes before policymakers can summon the political will to put much-needed consumer protections into place.

The latest example of such intrusiveness, as I reported last week, is Amazon receiving federal approval to equip its Alexa devices with radar sensors capable of "capturing motion in a three-dimensional space."

Amazon

AMAZON has been cleared to develop devices with radar sensors that can capture "motion in a three-dimensional space" to monitor sleep. Above, an Echo Dot.

share that stream of data with Amazon.

I asked the company last week for some details about how the radar technology will work and what Amazon will do with the information. No one responded.

I asked again this week and also requested some comment on Chau's medical-data bill. No one responded.

Chau, on the other hand, said he read my column about the radar technology and found the idea "creepy."

"The tech industry keeps coming up with technologies that are more and more intrusive to consumers," he said.

Chau's bill says that any company offering "a personal health record system" to consumers "shall not knowingly use, disclose, or permit the use or disclosure of personal health record

availability and cost of everyday health products for Californians," the chamber says.

For the Apples and Amazons of this world, that's not ideal. For the rest of us, well, a little disruption is precisely what's needed.

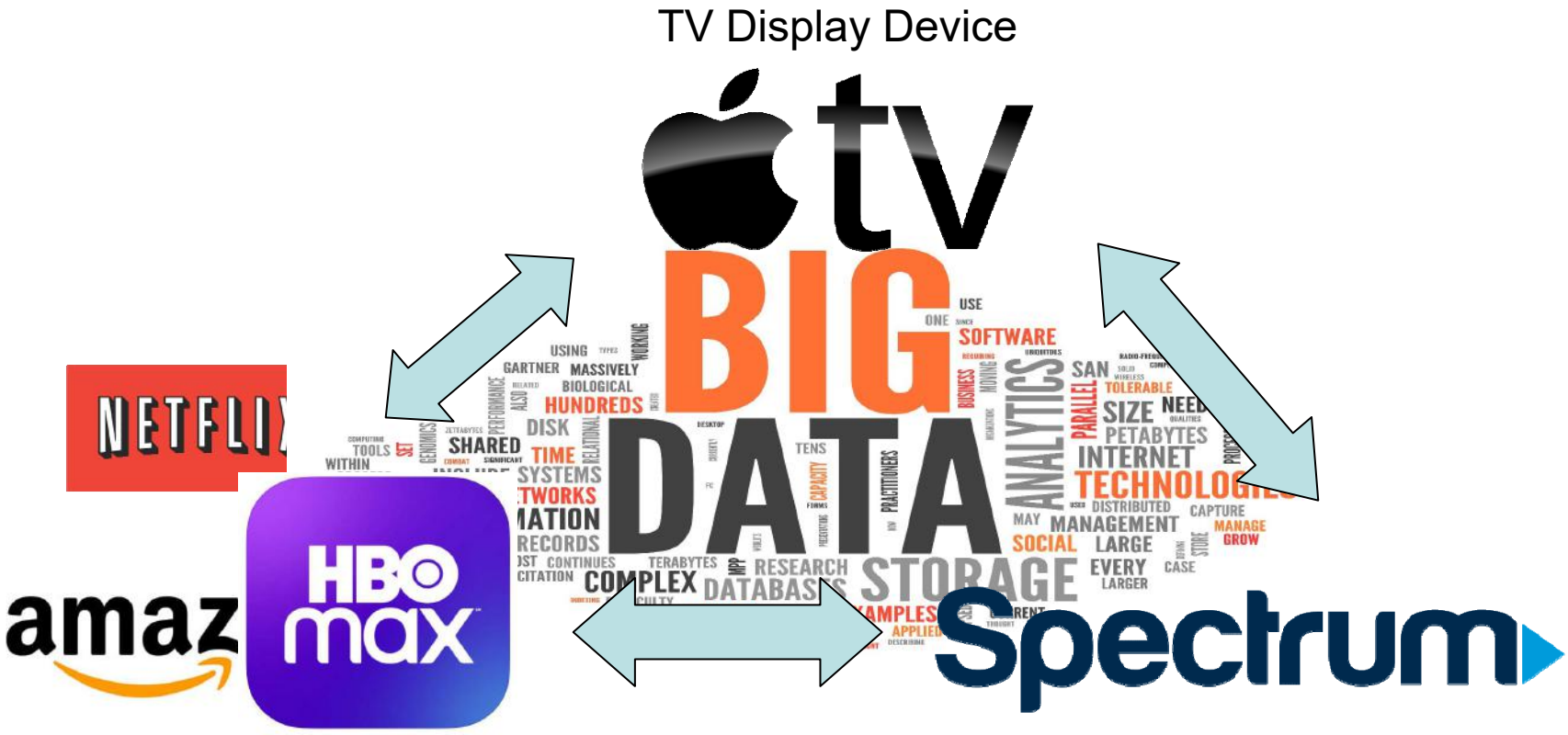
Chau also suspects a larger purpose at work among opponents of AB 1436.

He observed that if California passes a law making tech companies accountable for people's medical data, this could prompt Congress to similarly amend the main federal medical privacy law, the Health Insurance Portability and Accountability Act.

The federal law, known as HIPAA, is embarrassingly out of date. Amazon was still just a startup bookseller when the law was enacted in 1996. Apple was

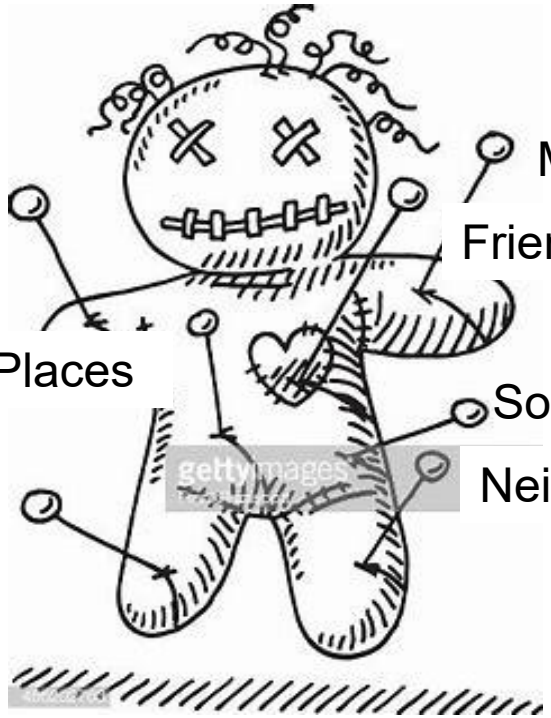
Copyright Gershon Weltman, 2018

Plus, Databases Connect…



Copyright Gershon Weltman, 2018

…So the Outlook Can Be Worrisome



Commentators have said that Big Data is creating a "voodoo doll" so you can be manipulated with personally targeted messages and also by ***fear tactics***. Harvard Prof. Shoshana Zuboff has called the result "Surveillance Capitalism."

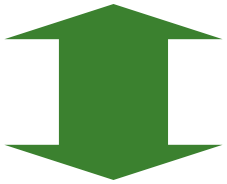
Doll image from gettyimages.com

Copyright Gershon Weltman, 2018

Ethical Case 2: Surveillance

- Data Acquisition:

  Data and information acquired on a broadly defined population in the course of normal activities



Today there is significant overlap

- Surveillance:

  Data and information acquired on selected individuals or groups of individuals for a specifically defined purpose, for example:

  1. *Investigation* of past illegal and/or dangerous activities
  2. *Prevention* of future illegal and/or dangerous actions
  3. *Anticipation* of potentially dangerous behavior patterns

Copyright Gershon Weltman, 2020

Constitutional Protection: The 4th Amendment

"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*."

The 4th Amendment was prescient in framing the general issue of individual security as it relates to the actions of Government.

Copyright Gershon Weltman, 2020

The Right to be Secure

- Expectation of Privacy

  The principle underlying the 4th Amendment and many subsequent laws and regulations

- Historical Understanding

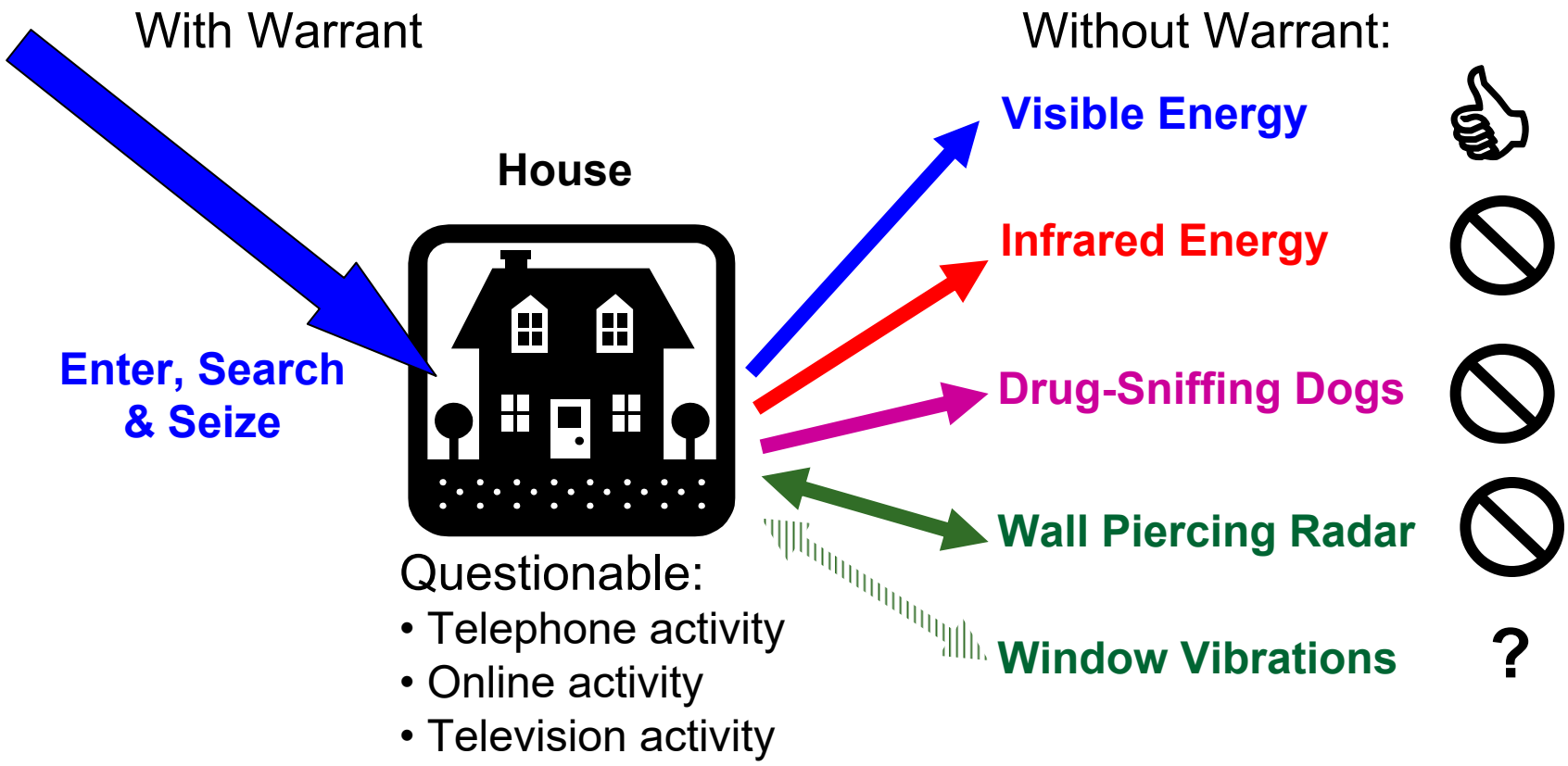
  Under usual circumstances homes, personal objects, and personal actions are private and not public.

- Effect of Internet Connectivity

  What is our expectation of privacy in the Internet age, with the new widespread availability of personal information?

Copyright Gershon Weltman, 2020

Example: Inside/Outside Your House



Copyright Gershon Weltman, 2020

Example: Above Your House

People are concerned that the unique vantage point and low flying capabilities allow drones to violate previous expectations of visual privacy.

Copyright Gershon Weltman, 2020

Example: Inside Your House

"*We are living in an always on, always connected world. We are creating records that have never existed before*."

Joel Reidenberg
Director, Fordham University Center on Law and Information Policy

Copyright Gershon Weltman, 2020

Real People are Listening

THE AGENDA: PRIVACY

HOWARD LIPIN San Diego Union-Tribune

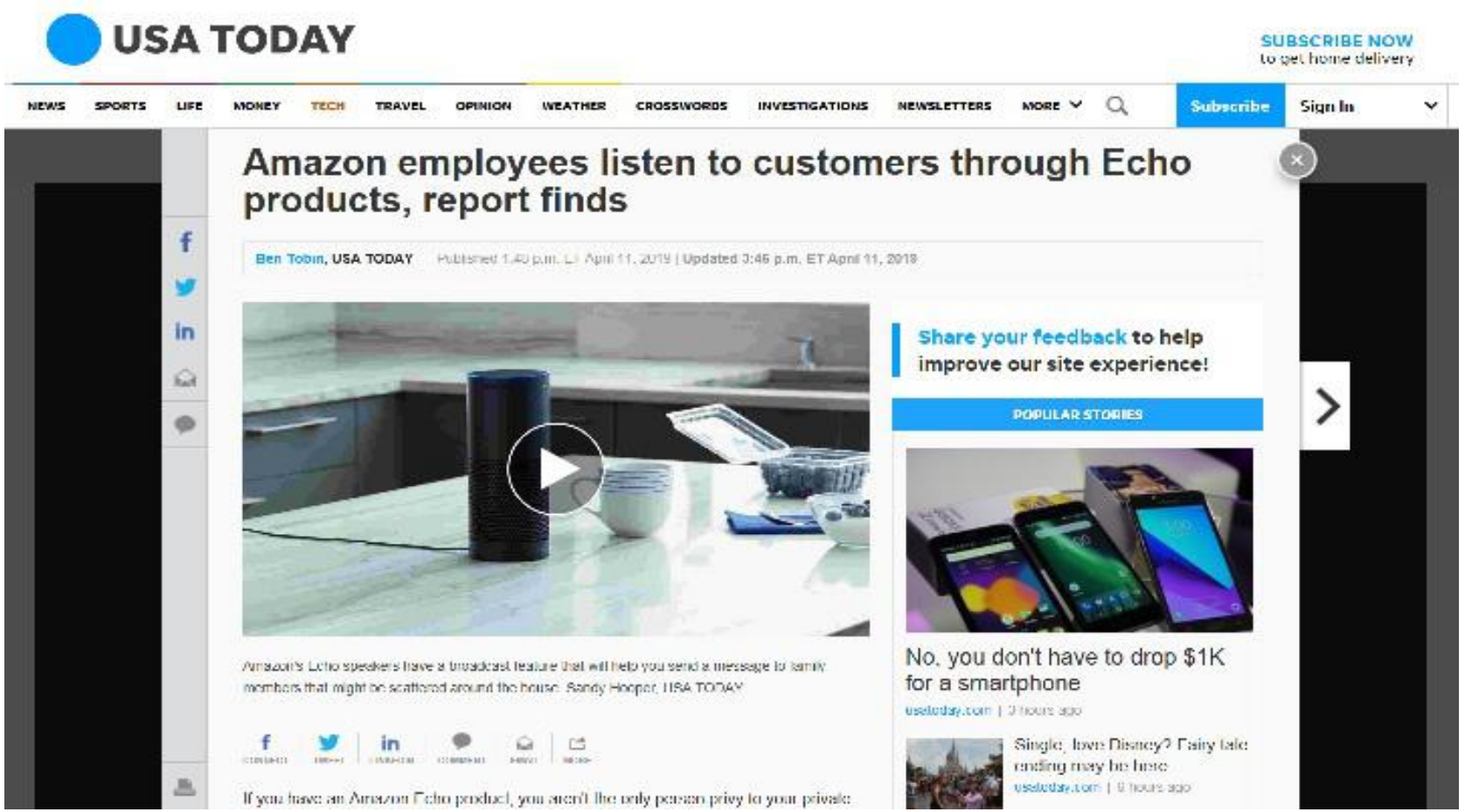
DEBUTING IN 2014, Amazon's Echo popularized the voice-activated home smart speaker. Globally, consumers bought 78 million smart speakers last year.

Alexa, and strangers, are listening

Amazon employees review and transcribe audio clips to help improve the digital assistant

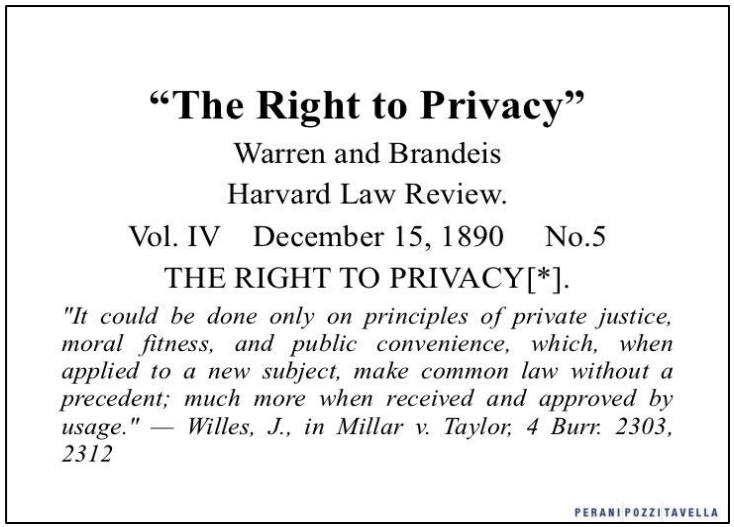
Copyright Gershon Weltman, 2020

Real People are Listening



Copyright Gershon Weltman, 2020

Privacy Can Be Complicated



"The Right to Privacy"

Warren and Brandeis

Harvard Law Review.

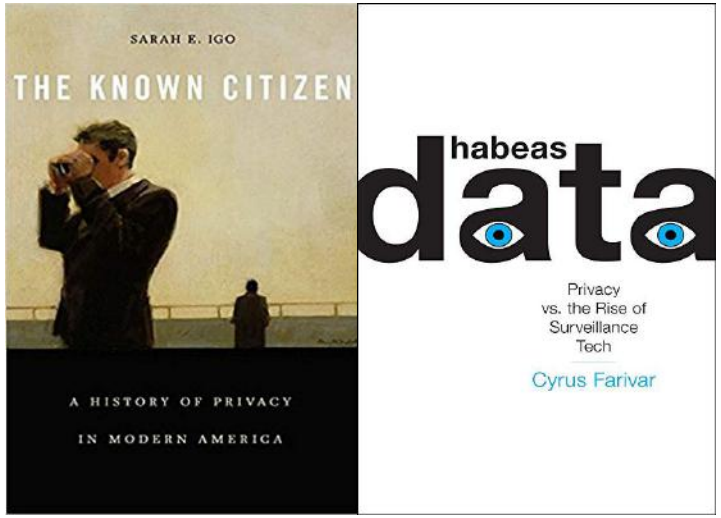
Vol. IV December 15, 1890 No.5

THE RIGHT TO PRIVACY[*].

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage." — Willes, J., in Millar v. Taylor, 4 Burr. 2303, 2312

PERANI POZZI TAVELLA

In 1890 the legal scholars Samuel Warren and Louis Brandeis state that privacy is basically "*the right to be let alone*" by Government as well as by other individuals.



In 1997 University of South Wales professor Roger Clarke says there are four privacies:
1) Privacy of the person (bodily privacy)
2) Privacy of personal data
3) Privacy of personal behavior
4) Privacy of personal communication

In 2018 commentator Sarah Igo says:
"Privacy has value, sometimes the value is received by hoarding it, and sometimes it's realized by cashing it out."

Copyright Gershon Weltman, 2020

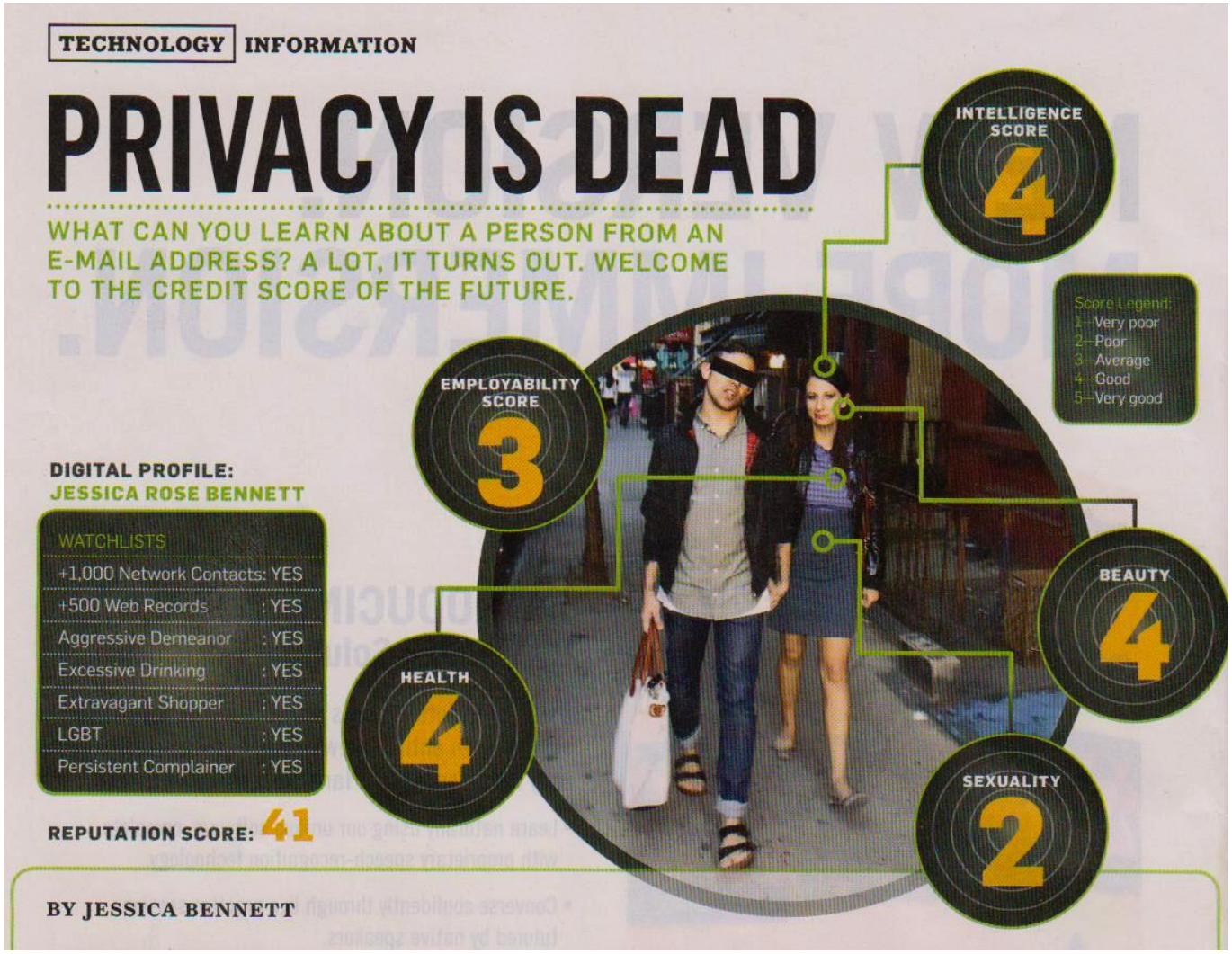
13 Years Ago Prof. Kleinrock Was Cool

"I'm very relaxed about privacy because there is none left. John Perry Barlow, a former lyricist with the Grateful Dead, was one of the founders of the Electronic Frontier Foundation. His life is public. He says that's the only way to have privacy – expose it all and you have nothing to hide."

UCLA Professor Emeritus Leonard Kleinrock
Computer Scientist and Internet Founder
Los Angeles Times, October 24, 2009

Copyright Gershon Weltman, 2020

And One Year Later Newsweek Agreed



Newsweek, November 1, 2010

Copyright Gershon Weltman, 2020

Government Had Taken a Similar Position

"Protecting anonymity isn't a fight that can be won; anyone that's typed in their name on Google understands that….

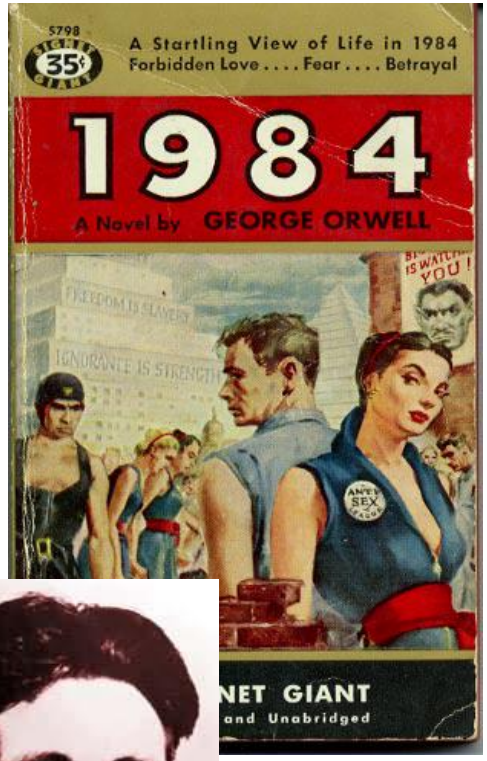
….Privacy is a system of laws, rules and customs with an infrastructure of inspectors general, oversight committees and privacy boards on which our intelligence community's commitment is based and measured."

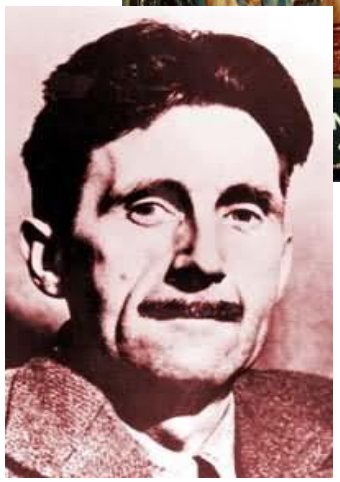
Donald Kerr
Principal Deputy Director of National Intelligence
October, 2007

The above was the position of President George W. Bush's administration. Commentators called this an "*Orwellian outlook*" because it seemingly put government agencies above basic constitutional rights.

Copyright Gershon Weltman, 2020

Orwell's Predicted This…





George Orwell 1949

"Benevolent" Surveillance

"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized."

Copyright Gershon Weltman, 2020

…and “The War on Truth” As Well

In Orwell’s 1984 novel, the slogans of ‘The Party’ showed that truth was only what the Government said it was. A warning that certainly resonates today.

Copyright Gershon Weltman, 2020

Surveillance Tech: Wire Tap vs. SIGINT

- Wire Tap

  Interrupting an established hard-wired communication channel

- Signal Intelligence (SIGINT)

  "A category of intelligence information comprising all communications intelligence (COMINT), electronics intelligence and telemetry intelligence. Electronics intelligence is amplified as "Technical and intelligence information derived from foreign non-communications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. Also called ELINT.“

DOD Dictionary of Military and Associated Terms, January 1986

Copyright Gershon Weltman, 2020

SIGINT Military Origins

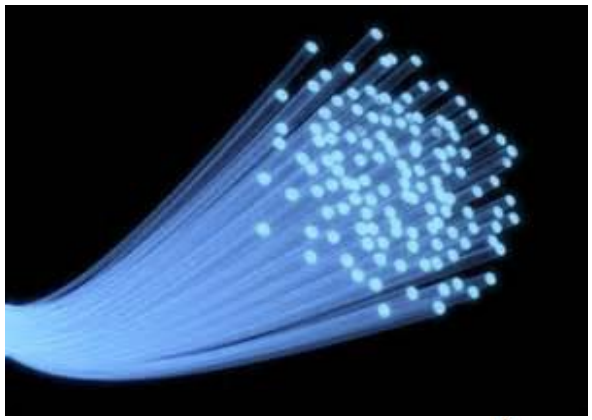
Image from L3 Communications

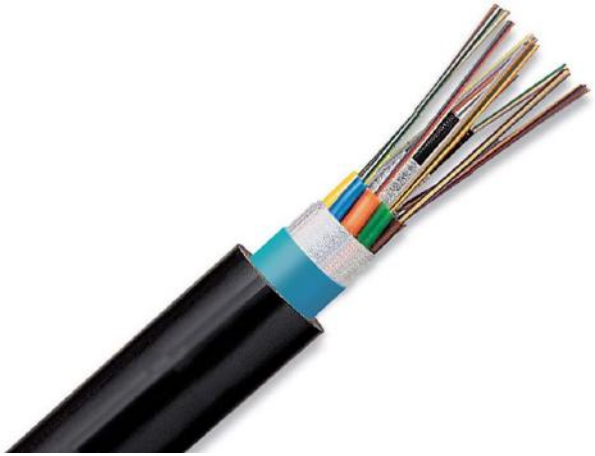
COMINT/ELINT Detection Equipment

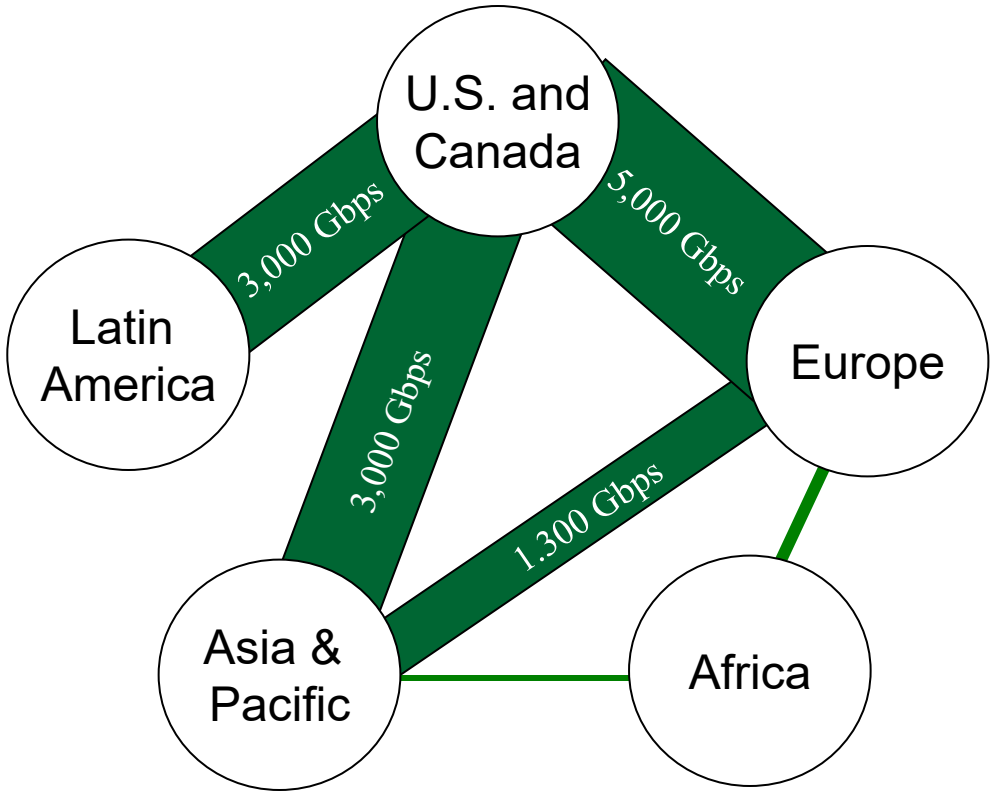
We and other countries use sophisticated and powerful detection systems for continuous SINGINT monitoring.

Copyright Gershon Weltman, 2020

More COMINT: Fiber Cable Networks







The U.S. is the World's telecommunications backbone

The temptation is to intersect the massive amount of communications in search for information that *might* be important to national security.

Copyright Gershon Weltman, 2020

Early Trial: Total Information Awareness

Total Information Awareness was a 2001 R&D program within the new Information Awareness Office (IAO) of DOD's **Defense Advanced Research Projects Agency (DARPA).**

The stated mission of the IAO was to *"imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness."*

The DARPA program was headed by ***Adm. John Poindexter***, former **National Security Advisor** in the **Reagan Administration** and a pardoned architect of the Reagan-era ***Iran-Contra Affair.***

Copyright Gershon Weltman, 2020

Early Trial: Total *Information Awareness*

Total Information Awareness was a 2001 R&D program within The new Information Awareness Office (IAO) of DOD's **Defense Advanced**

To ensure individual privacy, ADM Poindexter proposed that: "[It] would lock private information away in a kind of electronic safe that might only be opened upon order of a judge. The judge would have to find that the government has a reason for thinking that this anonymous person might actually be a terrorist. Poindexter called this case-by-case approach to putting names to data 'selective revelation.'"

information awareness."

The DARPA program was headed by ***Adm. John Poindexter***, former **National Security Advisor** in the **Reagan Administration** and a pardoned architect of the Reagan-era ***Iran-Contra Affair*.**

Copyright Gershon Weltman, 2020

Early Trial: Total *Information Awareness*

Total Information Awareness was a 2001 R&D program within The new Information Awareness Office (IAO) of DOD's **Defense Advanced Research Projects Agency (DARPA).**

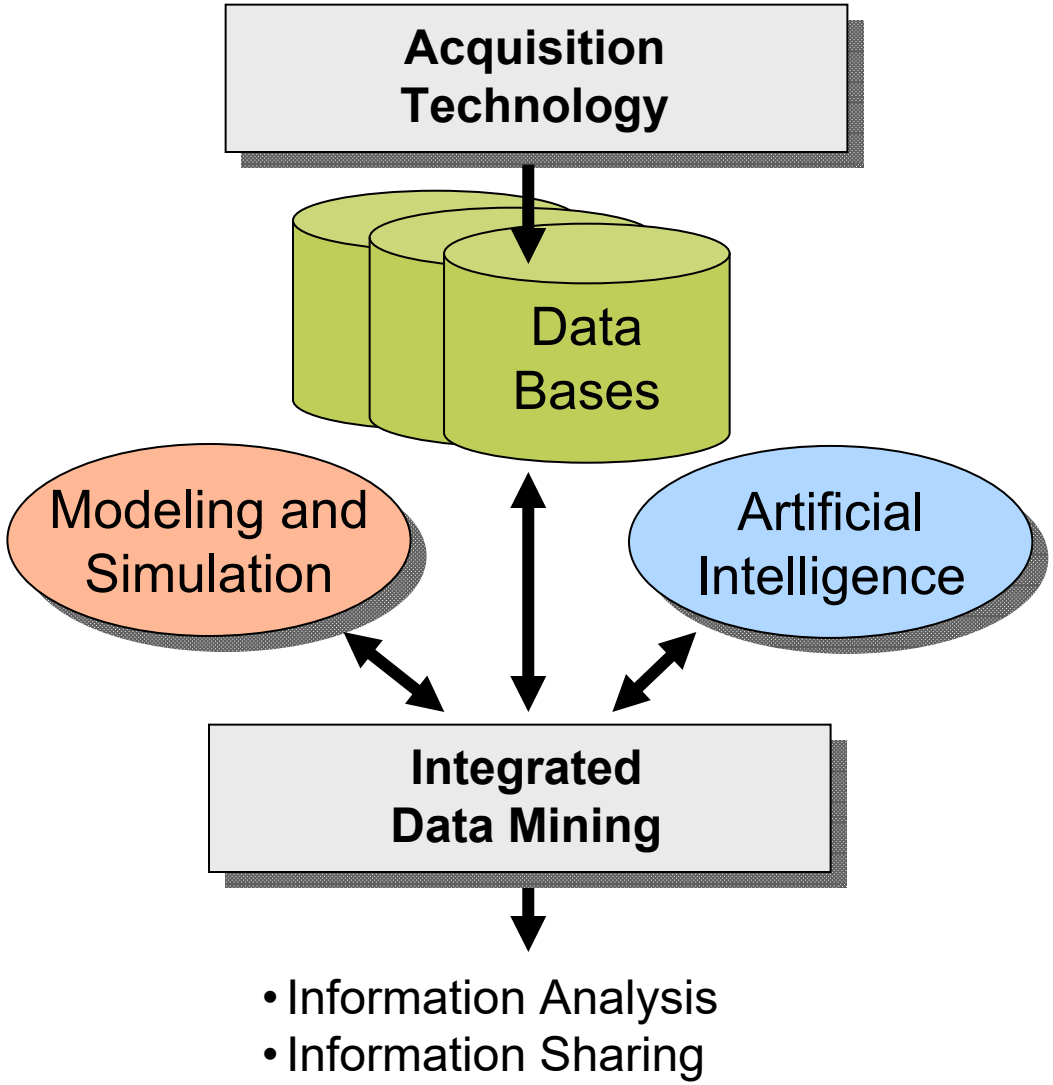
The stated mission of the IAO was to *"imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness."*

The DARPA program was headed by ***Adm. John Poindexter***, former **National Security Advisor** in the **Reagan Administration** and a pardoned architect of the Reagan-era ***Iran-Contra Affair*.**

The goals and proposed technology of the *Total Information Awareness* program so disturbed Congress that it ordered DARPA to discontinue it.

Copyright Gershon Weltman, 2020

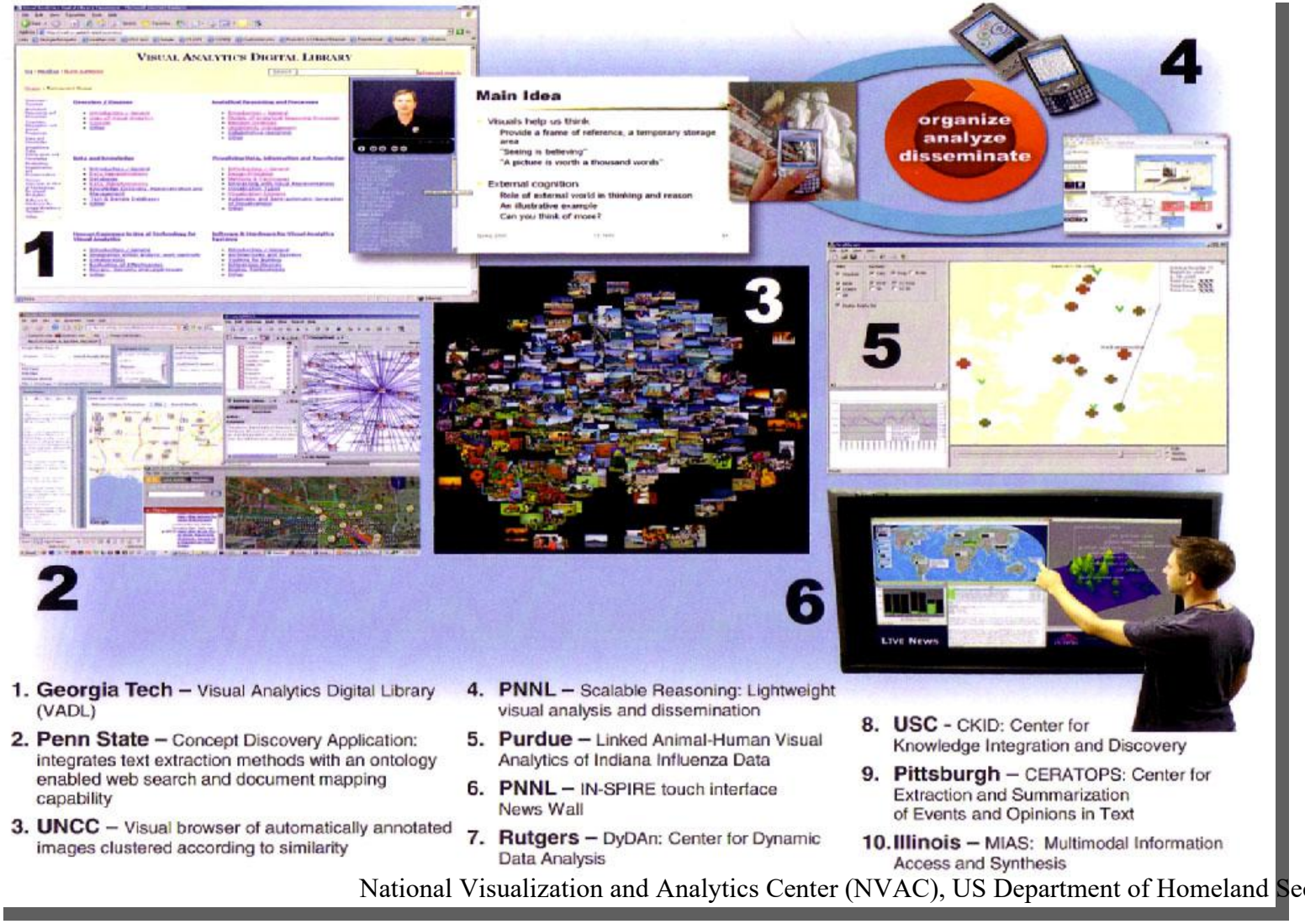
Post 9/11 Paradigm



www.snowbittlestoncom.verizonsupersite.com

Copyright Gershon Weltman, 2020

Continued R&D: Information Analysis



1. **Georgia Tech** – Visual Analytics Digital Library (VADL)
2. **Penn State** – Concept Discovery Application: integrates text extraction methods with an ontology enabled web search and document mapping capability
3. **UNCC** – Visual browser of automatically annotated images clustered according to similarity
4. **PNNL** – Scalable Reasoning: Lightweight visual analysis and dissemination
5. **Purdue** – Linked Animal-Human Visual Analytics of Indiana Influenza Data
6. **PNNL** – IN-SPIRE touch interface News Wall
7. **Rutgers** – DyDAn: Center for Dynamic Data Analysis
8. **USC** - CKID: Center for Knowledge Integration and Discovery
9. **Pittsburgh** – CERATOPS: Center for Extraction and Summarization of Events and Opinions in Text
10. **Illinois** – MIAS: Multimodal Information Access and Synthesis

National Visualization and Analytics Center (NVAC), US Department of Homeland Security

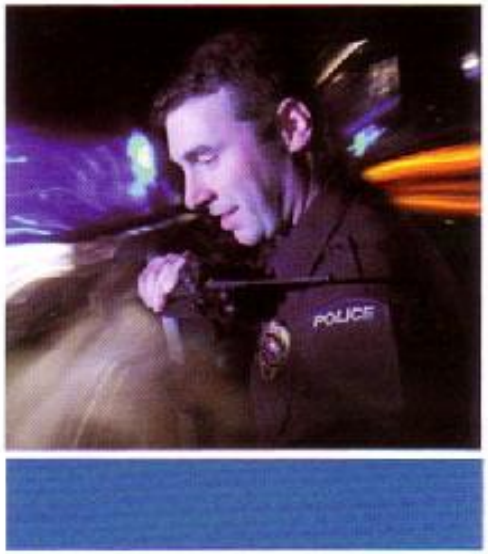
Copyright Gershon Weltman, 2020

Continued R&D: Information Sharing

Information Sharing

DHS Lead: Office of Intelligence & Analysis

Representative Technology Needs



- Data fusion from law enforcement, intelligence partners, and other sensors to support the common operating picture (COP)—*In particular, technologies to correlate and fuse sensor data into a comprehensive representation* (Command, Control, & Interoperability Division)
- Management of user identities, rights, and authorities—*In particular, technologies and standards to enable external identity adjudication* (Command, Control, & Interoperability Division)
- Distribution of intelligence products—*In particular, technologies and techniques to automate the distribution of unclassified or lower classification portions of intelligence information to DHS mission partners* (Command, Control, & Interoperability Division)
- Information sharing within and across sectors on terrorist threats—*In particular, analytic capabilities for structured, unstructured, and streaming data* (Command, Control, & Interoperability Division)

High-Priority Technology Needs, US Department of Homeland Security, June 2008

Copyright Gershon Weltman, 2020

Surveillance Positives: Connect the Dots…

s Angeles Times

IGHER 158 PAGES © 2014 WST ¹ SUNDAY, MAY 25, 2014 latimes.com

Rampage in Isla Vista

Student dies of gunshot after killing 6, wounding 13

IRFAN KHAN Los Angeles Times

THE ATTACKER'S CAR is cordoned off in Isla Vista, where seven people, including the killer, were slain. He was found slumped in the BMW, three handguns and more than 400 rounds of ammunition at his side.

BY ADOLFO FLORES, KATE MATHER AND SCOTT GOLD

ISLA VISTA — At first, when it began, it was lost to the soundtrack of another Friday night in this bluff-top college town: screeching tires and what sounded like fireworks.

But then — shattered glass. Sirens. Screams.

Within 10 minutes, it was done — seven dead, 13 wounded, a tormented young man slumped at the wheel of a shattered BMW, a gunshot wound to his head, three semiautomatic handguns and more than 400 rounds of ammunition at his side.

Behind him, there were 10 distinct crime scenes in a single square mile — skateboarders and bikers run down and tossed into the air; bullets bursting through the windows of shops; police officers tackling pedestrians and hauling them indoors to protect them; two young women dying on the lawn of a sorority.

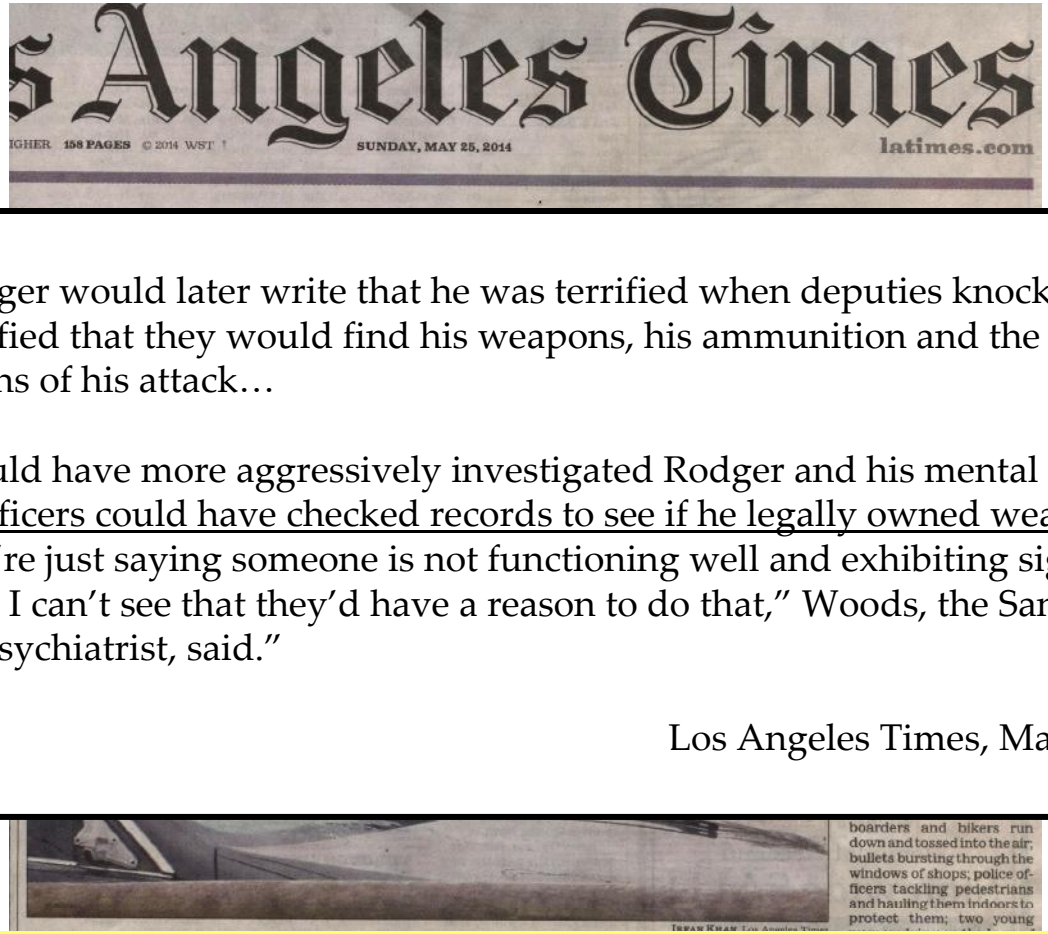
For months, Elliot Rodger, 22, had posed behind the wheel of that same BMW, posting videos of himself on social media.

The son of a Hollywood director, he was born to a

Killer's videos reflect cold rage

Copyright Gershon Weltman, 2020

…Connect the Dots…



"(Elliot) Roger would later write that he was terrified when deputies knocked on his door – terrified that they would find his weapons, his ammunition and the detailed written plans of his attack…

Officers could have more aggressively investigated Rodger and his mental state. <u>For instance, officers could have checked records to see if he legally owned weapons.</u> 'But if they're just saying someone is not functioning well and exhibiting signs of depression, I can't see that they'd have a reason to do that," Woods, the San Francisco psychiatrist, said."

Los Angeles Times, May 25, 2014

Knowing that a very disturbed individual owed three automatic pistols and a large amount of ammo would likely have changed response and events

Copyright Gershon Weltman, 2020

….Anticipate Terrorist Acts…

U.S. issues a worldwide travel alert

By Paul Richter and Ken Dilanian

WASHINGTON — The State Department issued a worldwide travel alert Friday over the threat of a possible terrorist attack by Al Qaeda or its affiliates, which also prompted a decision to temporarily close 21 embassies and consulates in the Middle East and several predominantly Muslim countries elsewhere.

The greatest risk of attack is in the Middle East and North Africa, the department said, and it warned that the attack could emanate from the Arabian Peninsula.

The British government is closing its embassy in Yemen on Sunday and Monday but not missions in other Middle Eastern countries, suggesting that London believes the source could be Al Qaeda in the Arabian Peninsula. The group, centered in Yemen, is the only Al Qaeda affiliate that has recently shown sustained interest in attacking U.S. interests beyond its local base.

"There are concerns about a major Al Qaeda in the Arabian Peninsula plot," said Seth Jones, a terrorism analyst with Rand Corp. and former advisor to U.S. Special Operations Forces who speaks frequently to U.S. intelligence officials.

Gen. Martin Dempsey, chairman of the Joint Chiefs of Staff, said the warnings were based on "a significant threat stream, and we are reacting to it."

"It is an Al Qaeda and affiliated threat" to attack Western interests, Dempsey told ABC News.

Although the government often releases alerts involving specific countries, Friday's was the first worldwide alert since October 2011. Officials released few details about the threat, although several officials, speaking anonymously to discuss intelligence matters, emphasized the degree of anxiety involved.

"I've lived through a lot of threats, and this is a concerning one," said a State Department official, who noted that the department rarely closes embassies and consulates. "Part of the reason that you put out information like this is to let the terrorist know that you are aware," the official said, noting that publicity can have a deterrent effect.

An official of another agency said that the level of concern within the government was unusually high, but that there was "not a whole lot of detail."

The State Department plans to close embassies and consulates in a strip of countries stretching from northwest Africa east to Bangladesh, including Afghanistan, Iraq, Kuwait, Saudi Arabia, the United Arab Emirates, Israel and Libya.

The closings will begin Sunday, the first day of the workweek in Mideastern countries, and will continue for at least a few days, officials said.

Marie Harf, a State Department spokeswoman, said Thursday that the facilities were being closed out of "an abundance of caution." Officials said the threat could be tied to the Muslim holy month of Ramadan, which ends Wednesday.

The department's travel alert said:

"Current information suggests that Al Qaeda and affiliated organizations continue to plan terrorist attacks both in the region and beyond, and they may focus efforts to conduct attacks in the period between now and the end of August."

It didn't recommend that travelers stay away from any country, but urged them to take special precautions and to register with U.S. consulates.

The alert warned that private U.S. interests as well as government facilities could be targets. It said transportation systems and tourist sites were at risk and noted that previous attacks had struck subway systems, rail lines, airplanes and ships.

Rep. Ed Royce (R-Fullerton), chairman of the House Foreign Affairs Committee, told reporters that "we've had a series of threats."

Rep. C.A. Dutch Ruppersberger (D-Md.), ranking Democrat on the House Intelligence Committee, said the threat was more than "the usual chit-chat" picked up in communications intercepts.

The last worldwide travel alert nearly two years ago followed disclosure of an Iranian plot to kill the Saudi Arabian ambassador to the United States in Washington. That warning cited "the potential for anti-U.S. actions following disruptions of the plot." But no follow-up attacks took place.

U.S. officials may be especially sensitive to threats in the aftermath of the Sept. 11, 2012, attack on the U.S. mission in Benghazi, Libya, which killed the U.S. ambassador to Libya, J. Christopher Stevens, and three other Americans.

The attacks brought intense criticism of the State Department and led to a major in-house investigation, plans for reforms, and congressional hearings. Four State Department officials were removed from their jobs.

paul.richter@latimes.com
ken.dilanian@latimes.com
Brian Bennett in the Washington bureau contributed to this report.

Los Angeles Times, August 3, 2013

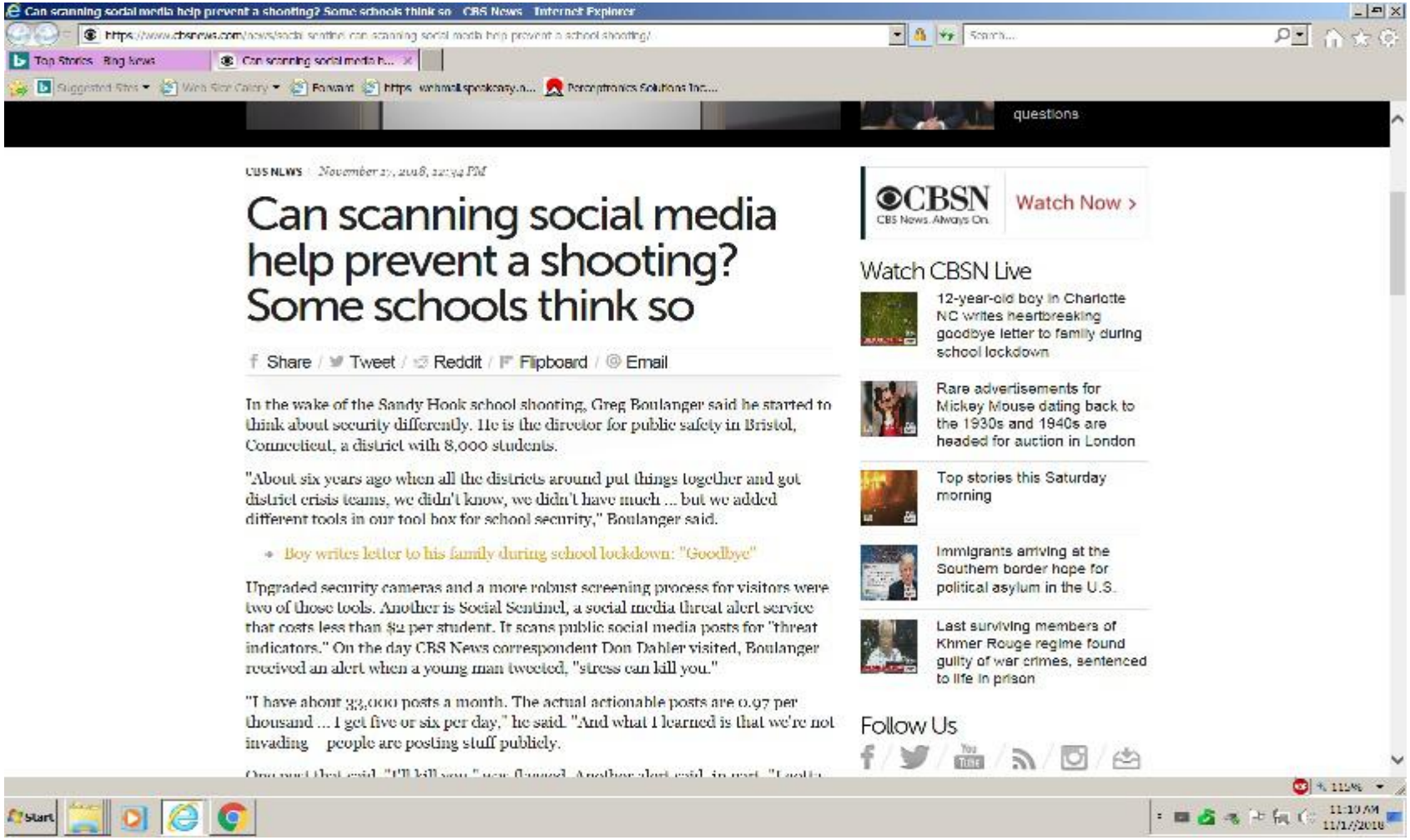
Copyright Gershon Weltman, 2020

…Identify Suspects…

Use of available surveillance information after the Boston Marathon bombing allowed authorities to quickly identify and capture the perpetrators.

Copyright Gershon Weltman, 2020

…Possibly Prevent Mass Shootings



Can scanning social media help prevent a shooting? Some schools think so - CBS News - Internet Explorer

questions

CBS NEWS November 27, 2018, 12:34 PM

Can scanning social media help prevent a shooting? Some schools think so

Share / Tweet / Reddit / Flipboard / Email

In the wake of the Sandy Hook school shooting, Greg Boulanger said he started to think about security differently. He is the director for public safety in Bristol, Connecticut, a district with 8,000 students.

"About six years ago when all the districts around put things together and got district crisis teams, we didn't know, we didn't have much ... but we added different tools in our tool box for school security," Boulanger said.

- Boy writes letter to his family during school lockdown: "Goodbye"

Upgraded security cameras and a more robust screening process for visitors were two of those tools. Another is Social Sentinel, a social media threat alert service that costs less than $2 per student. It scans public social media posts for "threat indicators." On the day CBS News correspondent Don Dahler visited, Boulanger received an alert when a young man tweeted, "stress can kill you."

"I have about 33,000 posts a month. The actual actionable posts are 0.97 per thousand ... I get five or six per day," he said. "And what I learned is that we're not invading people are posting stuff publicly.

CBSN CBS News. Always On. Watch Now >

Watch CBSN Live

12-year-old boy in Charlotte NC writes heartbreaking goodbye letter to family during school lockdown

Rare advertisements for Mickey Mouse dating back to the 1930s and 1940s are headed for auction in London

Top stories this Saturday morning

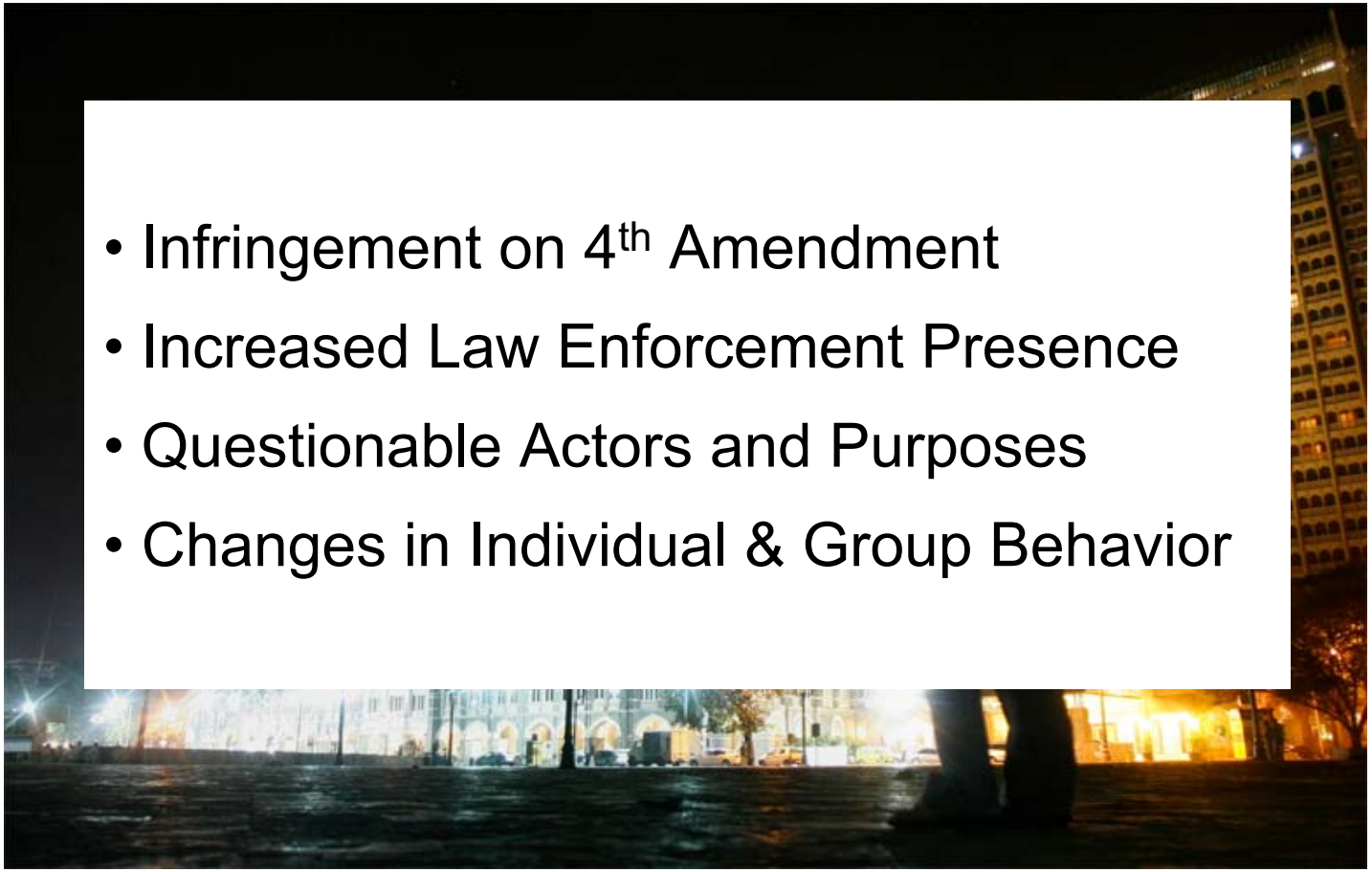
Immigrants arriving at the Southern border hope for political asylum in the U.S.

Last surviving members of Khmer Rouge regime found guilty of war crimes, sentenced to life in prison

Follow Us

Copyright Gershon Weltman, 2020

Surveillance Ethical Issues



Copyright Gershon Weltman, 2020

Ethical Analysis

- **Rights and Duties:** Which Prevail?
  - *Individuals' right* to be "secure in their persons" against:
    - Invasion of privacy
    - Fear of association
    - Unfounded accusations
  - *Society's right* to be secure by analysis of information
  - *Government's duty* to preserve both *rights and security*
- **Utilitarianism**: Measured Approaches to Regulation
  - Europe: Proactive, principles before technologies
  - USA: Reactive, technology restricted until crisis occurs
- **Pragmatism:** USA Changes Post 9/11
  - 2001 - Patriot Act: Expands Government powers
  - 2006 - Warrantless Surveillance: Look first, explain later
  - 2007 - Some roll-back of Patriot Act provisions
  - 2009 - New administration brings only small changes
  - 2013 - NSA revelations reopen the debate
  - 2015 - Congress effectively stops warrantless surveillance

Copyright Gershon Weltman, 2020

2006 Public is Initially Unsure….

REGARDING MEDIA

TIM RUTTEN

Public has to make the call

THE events of Sept. 11, 2001, were a watershed in this nation's history, but who would have suspected that they also would mark the beginning of an extraordinary era in American journalism?

Thursday's story in USA Today on

Copyright Gershon Weltman, 2020

2013 Revealed Surveillance Programs…

- **UPSTREAM**
  - Collection of *phone communications* on fiber cable and other infrastructure as data flows past
  - Data is collected from major U.S. communications companies including *AT&T, Verizon, etc.*
  - 'Meta data' (initial and final connections) only are stored for 5 years, but capability for content data may also exist

- **PRISM**
  - Collection of *Internet data* directly from servers of major U.S. Service Providers
  - Providers include *Microsoft (Hotmail, etc.), Apple, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL,*
  - Data include E-mail, chat, videos, photos, VoIP, stored data, file transfers, video conferencing, social network details,

Hidden NSA programs revealed by defector Edward Snowden were surprising mainly because so many large corporations were shown to be cooperating.

Copyright Gershon Weltman, 2020

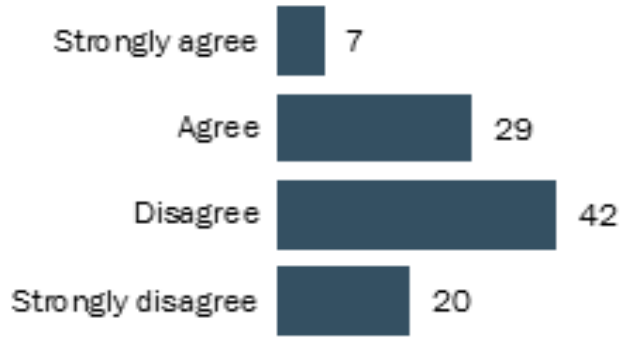
…Found a Less Concerned Public….

Copyright Gershon Weltman, 2020

…that Was Then Concerned Again..

Most do not think it's a good thing for society if people believe they are being watched online

Among all adults, the % who agree it is a good thing for society if people believe that someone is keeping an eye on the things that they do online



Source: Pew Research Privacy Panel Survey, January 2014. N=607 adults, ages 18 and older.

PEW RESEARCH CENTER

62% of respondents do not think online surveillance is good for society.

Copyright Gershon Weltman, 2020

The Courts Act….

5/8/15

washingtonpost.com • $1.50

NSA collection of phone data ruled unlawful

UNANIMOUS APPEALS COURT DECISION

Judges say program violates Patriot Act

BY ELLEN NAKASHIMA

A federal appeals court ruled Thursday that the National Security Agency's collection of millions of Americans' phone records violates the USA Patriot Act, marking the first time an appellate panel has weighed in on a controversial surveillance program that has divided Congress and ignited a national debate over the proper scope of the government's spy powers.

In a blistering 97-page opinion, a unanimous three-judge panel of the U.S. Court of Appeals for the 2nd Circuit overturned a lower court and determined that the government had stretched the meaning of the statute to enable "sweeping surveillance" of Americans' data in "staggering" volumes.

The ruling comes as Congress begins a contentious debate over whether to reauthorize the statute that underpins the NSA program or let it lapse. The court did not issue an injunction ordering the program to stop.

The NSA's mass collection of phone records for counterterrorism purposes — launched after the Sept. 11, 2001, terrorist attacks —

NSA CONTINUED ON A10

Copyright Gershon Weltman, 2020

…the Battleground Shifts…

1-14-20

Apple takes heat for locked phones

Attorney general criticizes company as U.S. struggles to crack devices used by Saudi shooter at Navy base.

BLOOMBERG

U.S. Atty. Gen. William Barr criticized Apple Inc. on Monday for not helping investigators unlock iPhones belonging to the alleged mastermind of a Dec. 6 terrorist attack at a Navy base in Florida.

The shooter had two iPhones, and the FBI quickly got court approval on probable cause to search the devices, Barr said in prepared remarks discussing the government's investigation.

EBRUARY 19, 2016 ▪ LATIMES.COM/BUSINESS

AQ 4,487.54 ▼ 46.53 | GOLD $1,226.10 ▲ 15.00 | OIL $30.77 ▲ 0.11 | EURO $1.1094 ▼ .0045 | U.S. T-NOTE (10-yr.) 1.74% ▼ 0.08

TIMOTHY A. CLAR

E chief Tim Cook said his company would fight a court order in the San Bernardino ter
ks the company for software to allow authorities to bypass the passcode on an encrypt

attle lines draw
er encryption

tandoff with the FBI has tech firms, g
umers weighing the limits of privacy p

Apple-FBI case pits privacy against national security

BY MAURA DOLAN AND VICTORIA KIM

SAN FRANCISCO — A court order requiring Apple to create a way to help law enforcement get access to a terrorist's smartphone amounts to an "unprecedented" stretch of an antiquated law — one that is likely to spark an epic fight pitting privacy against national security, legal scholars said Thursday.

Typically, law enforcement has filed for warrants under seal, and courts have issued orders under seal, to protect the confidentiality of ongoing criminal investigations.

But a federal judge in New York decided last fall to unseal portions of such a case. It revealed that Apple had turned over information to law enforcement about 70 times in recent years, according to the government, based on court orders citing an obscure 1789 law called the All Writs Act. The act, passed in the judiciary's infancy, allowed courts to issue orders if other judicial tools were unavailable.

This week's court order was different from those issued in the past, however. It requires Apple to create new software, experts said, not provide technology already at hand.

"This is a new frontier," said Jennifer Granick, director of civil liberties at Stanford Law School's Center for Internet and Society. "I know of no other statutory provision that would arguably create an obligation for device manufacturers to help out the government." Apple may not have fought orders in the past because "it was easy for Apple to give the data," she said. "But the architecture of

[See Apple, A17]

How far should encryption go?

Sealing off the personal information of phone customers extends to everyone — good guys and bad guys. BUSINESS, C1

Copyright Gershon Weltman, 2020

…and Shifts Again…

Pegasus is a super-powerful software suite used by hundreds of organizations to hack private phones; but it is only one of many such tools available for legal or illegal surveillance.

Controversial spyware

What is Pegasus?

Software made by Israel's NSO Group

Reportedly a highly invasive tool that can:

- Switch on a target's phone camera and microphone
- Access data on the device

Believed to have been in installed by spear-phishing techniques, as well as more advanced **"zero-click" attacks that don't require owners' interaction**

NSO claims its technology is sold solely to law enforcement and intelligence agencies of "vetted" governments

What's new?

May 2, 2022: Spain said the mobile phones of Premier Pedro Sanchez and Defence Minister Margarita Robles were tapped using Pegasus spyware in an "illicit and external" intervention

AFP

Copyright Gershon Weltman, 2020

… while Surveillance Expands…

China reportedly using facial recognition along with Big Data to track citizens...

Copyright Gershon Weltman, 2020

…in Purpose as Well as Scope…

…for the purpose of computing each person's Social Credit Rating, with a low Social Credit score causing loss of reputation as well as key benefits

Copyright Gershon Weltman, 2020

…and Here as Well as There…

Despite denials, LAPD uses facial recognition software

BY KEVIN RECTOR AND RICHARD WINTON

The Los Angeles Police Department has used facial recognition software nearly 30,000 times since 2009, with hundreds of officers running images of suspects from surveillance cameras and other sources against a massive database of mug shots taken by law enforcement.

The new figures, released to The Times, reveal for the first time how commonly facial recognition is used in the department, which for years has provided vague and contradictory information about how and whether it uses the technology.

The LAPD has consistently denied having records related to facial recognition, and at times denied using the technology at all.

The truth is that, while it does not have its own facial recognition platform, LAPD personnel have access to facial recognition software through a regional database maintained by the Los Angeles County Sheriff's Department. And between Nov. 6, 2009, and Sept. 11 of this year, LAPD officers used the system's software 29,817 times.

More than 300 LAPD personnel have access to the software.

Josh Rubenstein, an LAPD spokesman, said that he could not determine how many leads from the system have developed into arrests, but that the technology has helped identify suspects in gang crimes in which witnesses were too fearful to come forward and in crimes in which no witnesses existed.

He said it has helped officers solve crimes faster than they otherwise would, and confirmed that it was recently used by the Safe LA Task Force, a coalition of la

[See LAPD, A

LAPD TECH RAISES PRIVACY WORRIES

Police Commission will examine use of facial recognition software revealed in a Times report.

BY KEVIN RECTOR

The Los Angeles Police Commission on Tuesday said it would review the city Police Department's use of facial recognition software and how it compared with programs in other major cities.

Los Angeles Times, September 22&23, 2020

Copyright Gershon Weltman, 2020

…Causing Concerns…

Despite denial
facial recognit

BY KEVIN RECTOR
AND RICHARD WINTON

The Los Angeles Police Department has used facial recognition software nearly 30,000 times since 2009, with hundreds of officers running images of suspects from surveillance cameras and other sources against a massive database of mug shots taken by law enforcement.

The new figures, released to The Times, reveal for the first time how commonly facial recognition is used in the department, which for years has provided vague and contradictory information

Such technology has drawn criticism from civil liberties advocates and others, in part because of findings that it can produce more false results for people of color. Some critics also object to the use of mug-shot databases as the source of comparison photographs and say the lack of government transparency around the use of facial recognition is increasingly problematic as the technology becomes more powerful.

The city of San Francisco last year banned the use of facial recognition, including by its police, citing civil liberties concerns.

LAPD TECH RAISES PRIVACY WORRIES

Los Angeles Times, September 22&23, 2020

Copyright Gershon Weltman, 2020

…Promoting Countermeasures

Copyright Gershon Weltman, 2020

…and Creating New Ethical Policy

Lizabeth Rhodes, Director of LAPD's Office of Constitutional Policing and Policy, said in an email that *facial recognition technology* will not be used:

- **To establish any database**
- **To create suspect identification books**
- **As general identification tool**
- **When there is no investigative purpose**
- **In connection with body cameras**

A 2016 report issued by the Center on Privacy and Technology said the LAPD "May have the most advanced face recognition system in the country." Accordingly, LAPD principles and policies, if carried out, may influence other US and international law enforcement agencies.

Copyright Gershon Weltman, 2020

Abuse and Misuse: Preemption

- Privacy: *Adding to Database Personal*
  - Information
  - Sensitivities,
  - Actions
  - Associations
  - Personal communications
- Piracy: *Taking from Database*
  - Information
  - Secrets
  - Intellectual Property
  - Identities
  - Functionality or Operability
- **Preemption: *Inferring from Database..***
  - **Dangerous neighborhoods or locales**
  - **Dangerous Individuals**
  - **Likely criminal acts or terrorist activities**

Copyright Gershon Weltman, 2020

Public Reaction Against Preemption

WEDNESDAY, JULY 25, 2018 :: LATIMES.COM/

Photographs by IRFAN KHAN Los Angeles Times

JAMIE GARCIA, left, said at the Police Commission meeting: "Data will always be used to criminalize black, brown and poor people." She and Hamid Khan, right, are members of Stop LAPD Spying Coalition.

LAPD and activists at odds over data as tool

Cops call predictive policing effective; civilians say it's racist

Copyright Gershon Weltman, 2020

Public Reaction Against Preemption

WEDNESDAY, JULY 25, 2018 ⁝ LATIMES.COM/

Photographs by IRFAN KHAN Los Angeles Times

JAMIE GARCIA, left, said at the Police Commission meeting: "Data will always be used to criminalize black, brown and poor people." She and Hamid Khan, right, are members of Stop LAPD Spying Coalition.

LAPD and activists at odds over data as tool

Cops call predictive policing effective; civilians say it's racist

'We discontinued LASER because we want to reassess the data.... We're pulling back.'

—JOSH RUBENSTEIN, LAPD spokesman

The department also recently spiked a more controversial segment of LASER that identified and monitored so-called chronic offenders who were most likely to commit violent crimes. Once identified, they were included on lists of the worst offenders in a given area.

Amid outcery, the department in August stopped issuing the lists and using an offender database. The public did not learn about the decision until last month.

The department defended the data tools last summer, and Moore supported auditing them for possible problems.

Last week, the chief told commissioners that the department will not use programs that fail to produce results and will strive to "identify new or emerging ideas that hold promise."

"Crime reduction strategies are never static," Moore wrote in a memo to the Police Commission. "We will continue to learn and evolve in our work."

Copyright Gershon Weltman, 2020

The Issue is Trust

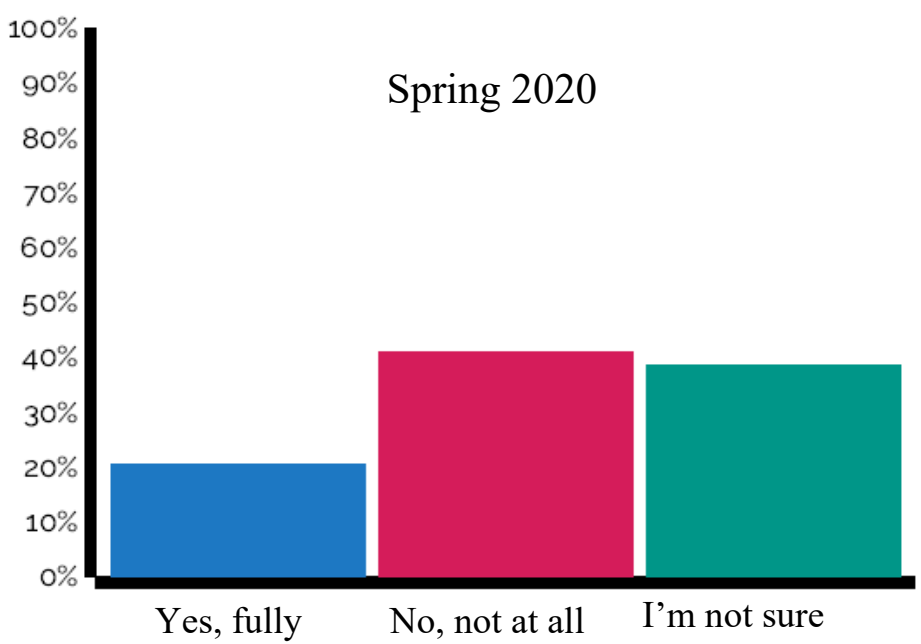
Senator Frank Church of Idaho (Dem) stated as early as 1975 with regard to NSA's growing technical capability:
"That capability at any time could be turned around on the American people and no American would have any privacy left, such [is] the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever becomes a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny…We must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that over that abyss."

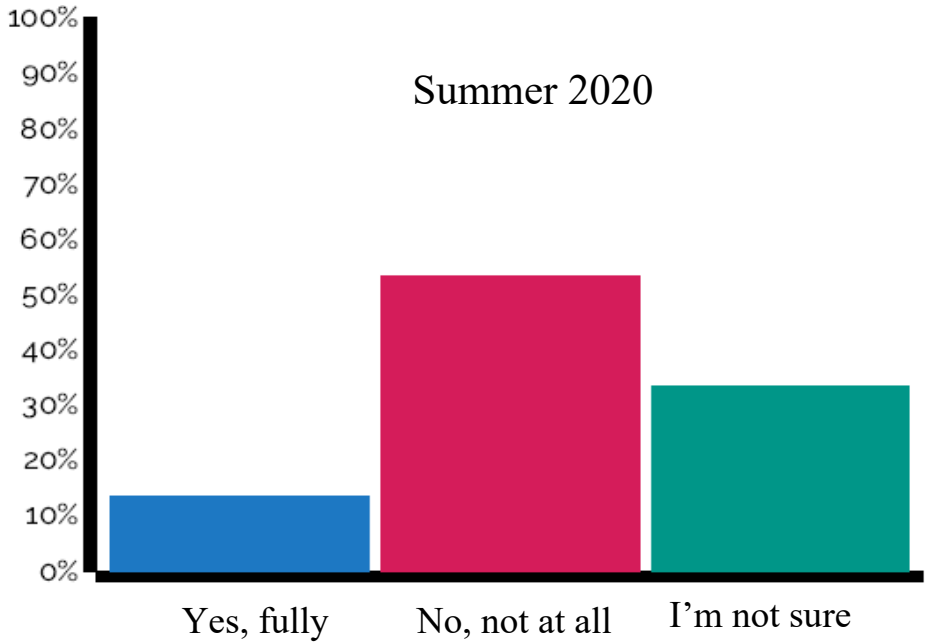
The central societal/ethical issue today may not be privacy or security, but peoples' basic trust that government will do the right thing. Even short of tyranny, surveillance technology opens the door to potential harm. If privacy today is essentially gone, we need to emphasize law, supervision and transparency.

Copyright Gershon Weltman, 2020

Online Poll: Trust in Government

Do you trust our Government to use your data ethically and for valid purposes?





Two years ago only 12% to 20% were fully sure data will be used ethically; while about 50% were fully negative and the "not sure" was about 40% – this reflected a lack of confidence in the ethicality and validity of Government surveillance.

Copyright Gershon Weltman, 2020

Ethical Case 3: A Right to Information?

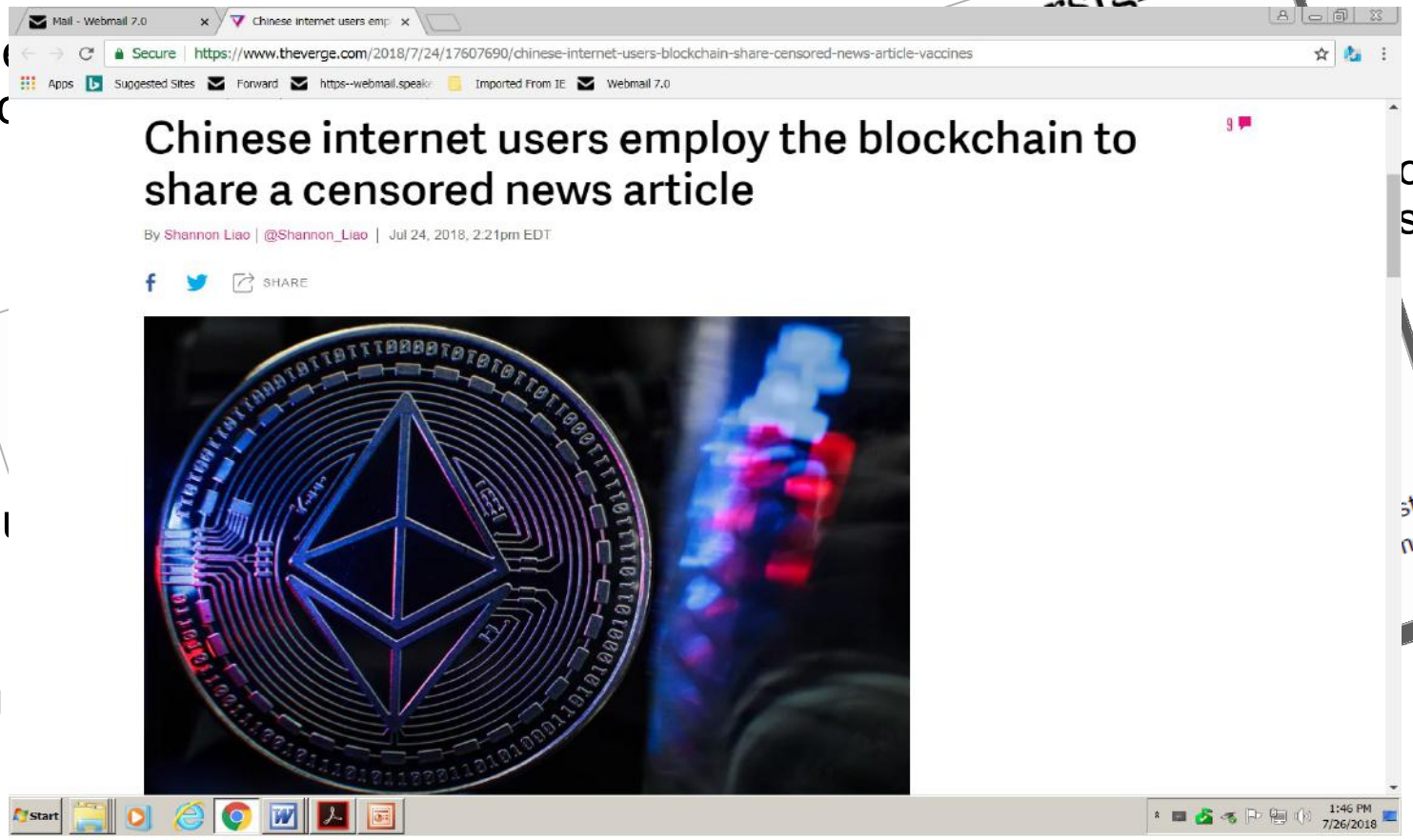
- People's Republic of China and other repressive governments want to limit access to data bases:
  - They demand that Google, Yahoo and other service providers restrict access to information about topics such as Democracy and to sites such as Twitter that they believe would cause societal unrest
- Google, Yahoo, et al weigh their ethical vs. business interests:
  - Adhere to their ethic of open access, possibly lose large market, vs.
  - Give in to countries' demands, lose a part of their ethical foundation
- Business trumps ethics for the time being -- with rationalization
  - Duty to shareholders outweighs founders' ethical ideals
  - Some information whets appetite for more information
- U.S. Congress could step in with regulation against restrictions:
  - Would get U.S. companies off the ethical hook
  - Might open door to greater international competition

Is there a general moral or ethical principle involved? If so, what is it?

Copyright Gershon Weltman, 2020

Information Access: A New Right?

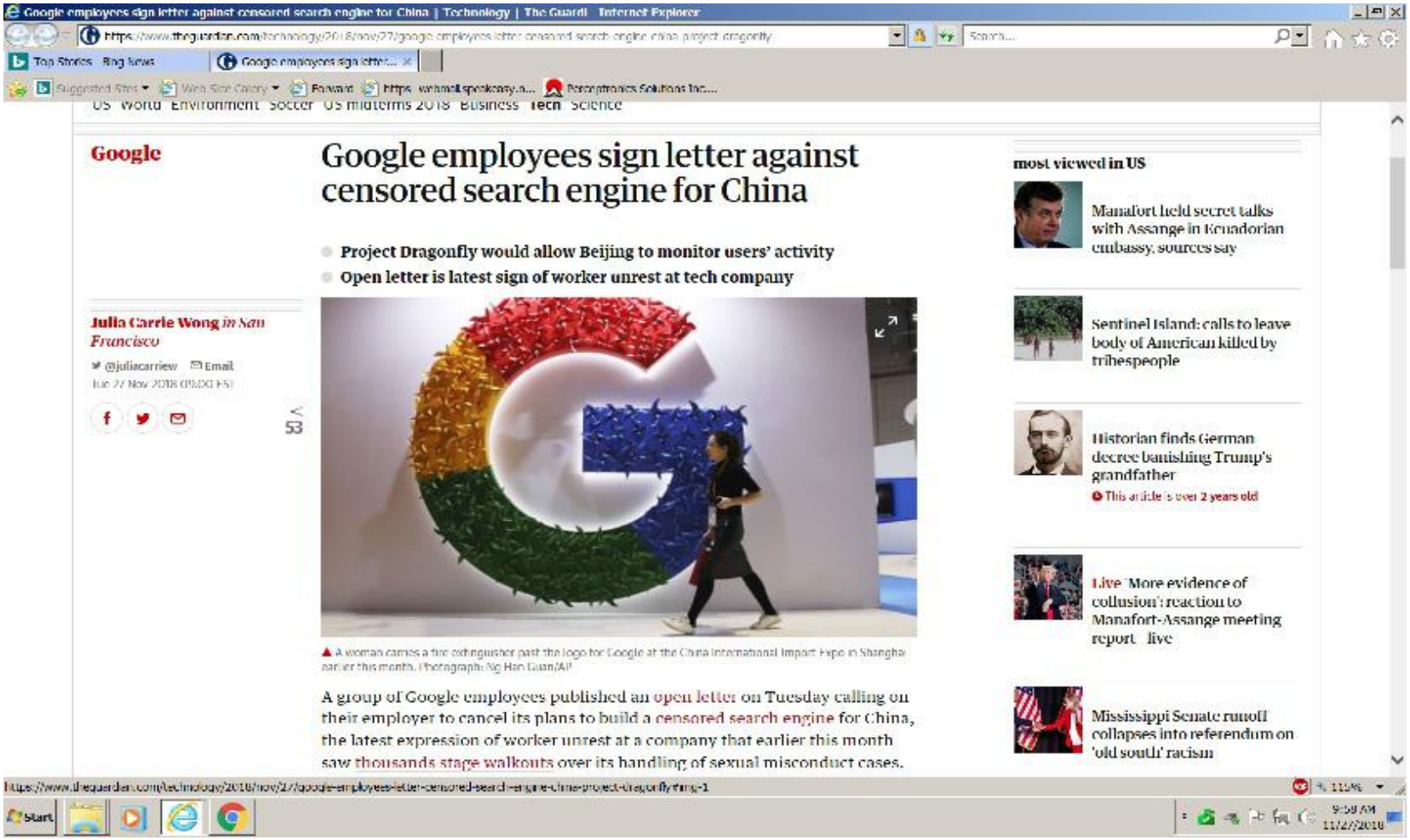
- P
  - ac
- B
- U



Chinese users find ways around the government's censorship policies.

Copyright Gershon Weltman, 2020

Information Access: A New Right?



Google employees sign letter against censored search engine for China | Technology | The Guardi - Internet Explorer

US World Environment Soccer US midterms 2018 Business Tech Science

Google

Google employees sign letter against censored search engine for China

- Project Dragonfly would allow Beijing to monitor users' activity
- Open letter is latest sign of worker unrest at tech company

Julia Carrie Wong in San Francisco

@juliacarriew Email

Tue 27 Nov 2018 09:00 EST

53

▲ A woman carries a fire extinguisher past the logo for Google at the China International Import Expo in Shanghai earlier this month. Photograph: Ng Han Guan/AP

A group of Google employees published an open letter on Tuesday calling on their employer to cancel its plans to build a censored search engine for China, the latest expression of worker unrest at a company that earlier this month saw thousands stage walkouts over its handling of sexual misconduct cases.

most viewed in US

Manafort held secret talks with Assange in Ecuadorian embassy, sources say

Sentinel Island: calls to leave body of American killed by tribespeople

Historian finds German decree banishing Trump's grandfather

This article is over 2 years old

Live 'More evidence of collusion': reaction to Manafort-Assange meeting report - live

Mississippi Senate runoff collapses into referendum on 'old south' racism

And the search engine employees see a duty to endorse the implied right.

Copyright Gershon Weltman, 2020

Freedom vs. Control: Which will Prevail?

- China's position reflects a serious disagreement on technological progress and societal values
  - US' Template: Rapid technical progress depends on a democratic society and broad distribution of information
  - China's Template: Rapid technical progress can be impeded by unchecked democracy, careful state control is needed -- of information as well as of technical emphasis
- If Information = Power, is free access more powerful than restricted access?
  - Totalitarian regimes can produce technologically advanced products -- for example, Soviet Union's atomic bombs and space satellites, and China's biotech and space programs
  - *But can they innovate* as successfully as democratic societies without free access to information?

Copyright Gershon Weltman, 2020

12 Years Later, Prof. Kleinrock Reassesses

"*When I was a young scientist working on the fledgling creation that came to be known as the Internet, the ethos that defined the culture we were building was characterized by words such as ethical, open, trusted, free, shared.*"

"We did not anticipate that the dark side of the Internet would emerge with such ferocity. Or that we would feel an urgent need to fix it."

"Scientists need to create more advanced methods of encryption to protect individual privacy by preventing perpetrators from using stolen data bases."

"If we work together to make these changes happen, it might be possible to return to the Internet I knew before."

UCLA Professor Emeritus Leonard Kleinrock
Computer Scientist and Internet Founder
Los Angeles Times, October 29, 2019

Copyright Gershon Weltman, 2018

A Call for Ethical Self-Regulation

Tech needs ethics more than rules

By Mike Godwin

FACEBOOK IS PREPARING to pay a multi-billion-dollar fine and dealing with ongoing ire from all corners for its user privacy lapses, the viral transmission of lies during elections, and delivery of ads in ways that skew along gender and racial lines. To grapple with these problems (and to get ahead of the bad PR they created), Chief Executive Mark Zuckerberg has proposed that governments get together and set some laws and regulations for Facebook to follow.

But Zuckerberg should be aiming higher. The question isn't just what rules should a reformed Facebook follow. The bigger question is what all the big tech companies' relationships with users should look like. The framework needed can't be created out of whole cloth just by new government regulation; it has to be grounded in professional ethics.

Doctors and lawyers, as they became increasingly professionalized in the 19th century, devel-

ANDREW HARNIK Associated Press

FACEBOOK'S Mark Zuckerberg testifies before Congress.

flect the same kinds of values.

Drawing on Yale law professor Jack Balkin's concept of "information fiduciaries," I have proposed that the tech companies develop an industry-wide code of ethics that they can unite behind in implementing their censorship and privacy policies — as well as any other information policies that may affect individuals.

Just like legal and medical practitioners, tech companies are

some degree can't help doing so.) Even if companies can't stop gathering user data, they certainly can be obligated to treat users and non-users alike. They should also be duty-bound to treat them with care (don't allow individuals' data to be used in ways that harm them; don't serve them content or ads that are false or misleading), loyalty (don't put company interests ahead of the well being of the individuals whose data you hold), and, perhaps most important, confidentiality. That last duty means, at a minimum: Don't share individuals' data with companies without their knowing, particular consent. And don't share individuals' data with governments unless the governments have sought that information consistent with international rights guarantees and norms of due process.

An industry-wide — and, ideally, society-wide — recognition of the tech companies' duty of confidentiality, care and loyalty has another benefit. It can give the companies legal standing to fight for user interests in the face of gov-

barriers to participation. (It follows that any tech-ethics framework should be open to amendment based on critical feedback from these forums or from elsewhere.) At worst, such a forum allows stakeholders to let off steam; at best, it can enable people who care about the internet and its services to identify emerging problems and solutions quickly.

None of this will end criticism of the big internet companies. When they remove content — abiding by either law or their own content policies — they invariably will get three reactions: You censored too much! You didn't censor enough! You censored the wrong stuff!

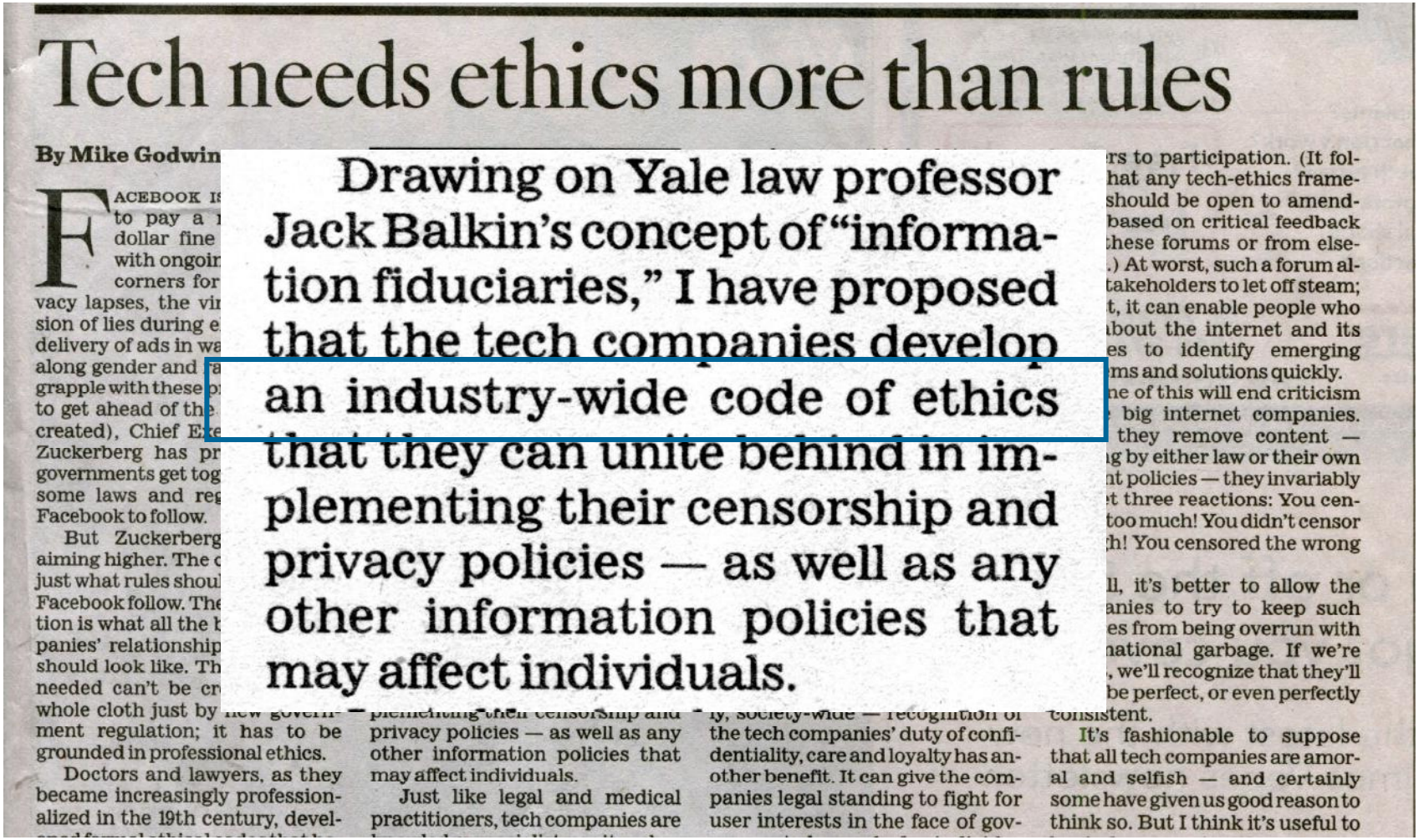
Still, it's better to allow the companies to try to keep such services from being overrun with informational garbage. If we're smart, we'll recognize that they'll never be perfect, or even perfectly consistent.

It's fashionable to suppose that all tech companies are amoral and selfish — and certainly some have given us good reason to think so. But I think it's useful to

Los Angeles Times, April 30, 2019

Copyright Gershon Weltman, 2018

A Call for Ethical Self-Regulation



Tech needs ethics more than rules

By Mike Godwin

Drawing on Yale law professor Jack Balkin's concept of "information fiduciaries," I have proposed that the tech companies develop an industry-wide code of ethics that they can unite behind in implementing their censorship and privacy policies — as well as any other information policies that may affect individuals.

Los Angeles Times, April 30, 2019

Copyright Gershon Weltman, 2020

Status Quo and Status Futurus

- Data Bases Proliferating and Linking
  - Personal and business
  - Institutional and Governmental
  - Secondary as well as primary sources
- Current Capabilities
  - Tracking known persons - Easy
  - Finding terrorists or criminals - Harder
  - Acting preemptively – Legal and Ethical Issues
- Current Developments
  - DoD and DHS are leaders
  - Government surveillance interests include
    - New “Total Information Awareness”
    - Suspicious patterns of behavior
  - Big Data continues to feed commerce and Government
- Regulation: Industry more than Government

Copyright Gershon Weltman, 2020

The Cloud is Really..

Typical Server Room

Copyright Gershon Weltman, 2020