

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

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

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

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 UNIVERSAL RIGHT to Internet Information?

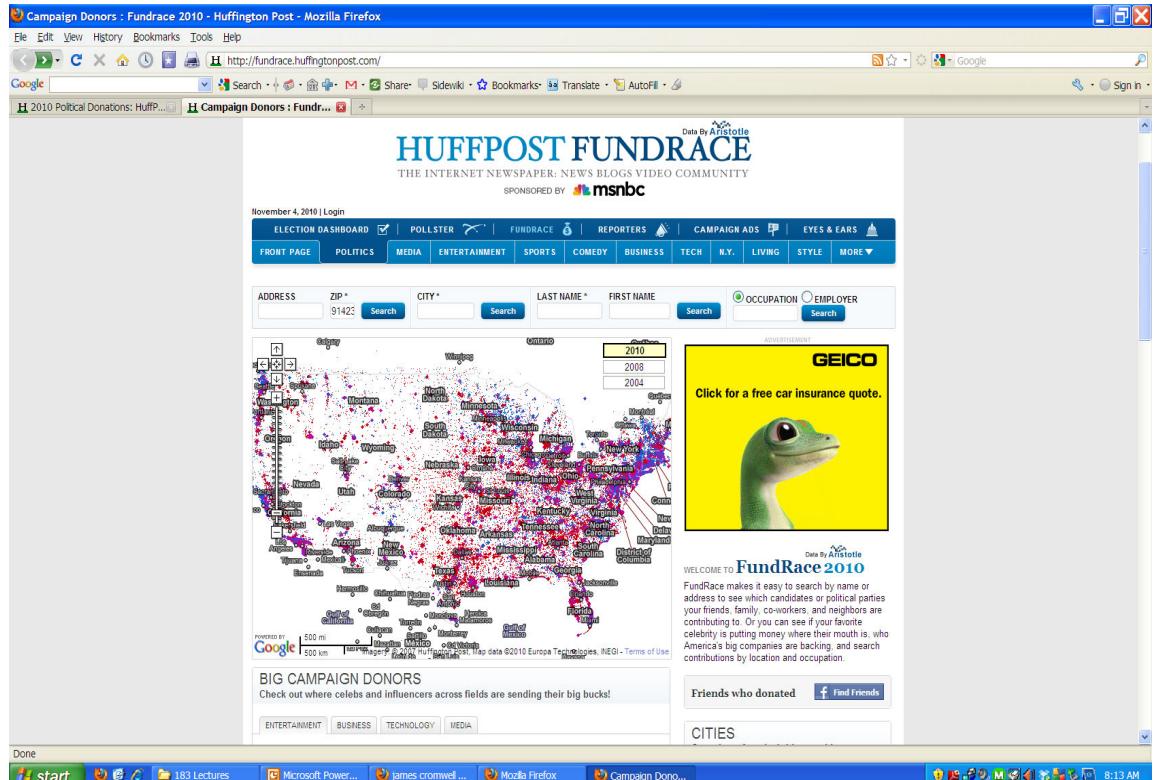
Personal Information: Good and Bad News

Good News

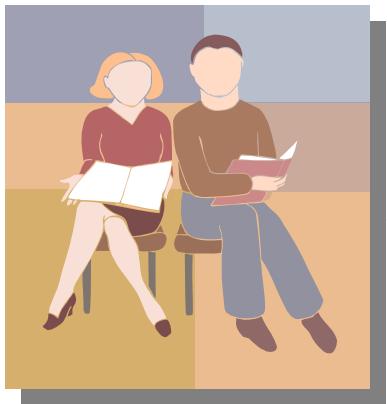
- Gigantic amount of information available
- Ultra easy access
- Many positive uses

Bad News

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



Example: Building an eDossier

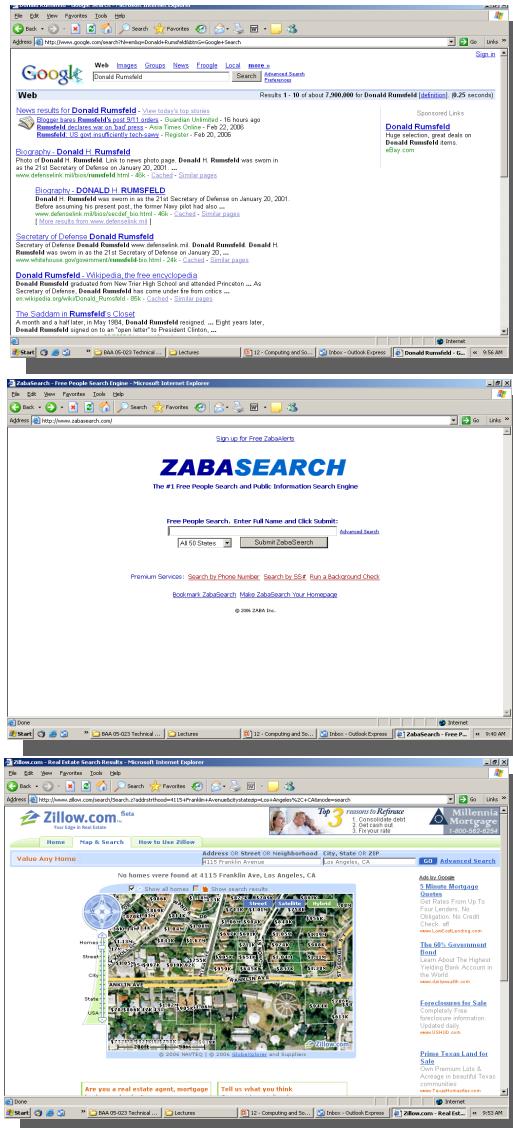


“John Doe”
“Jane Doe”

Google.com
Bing.com
MSN.com

Zabasearch.com
Whitepages.com
Spokeo.com

Zillow.com
Trulia.com
Redfin.com

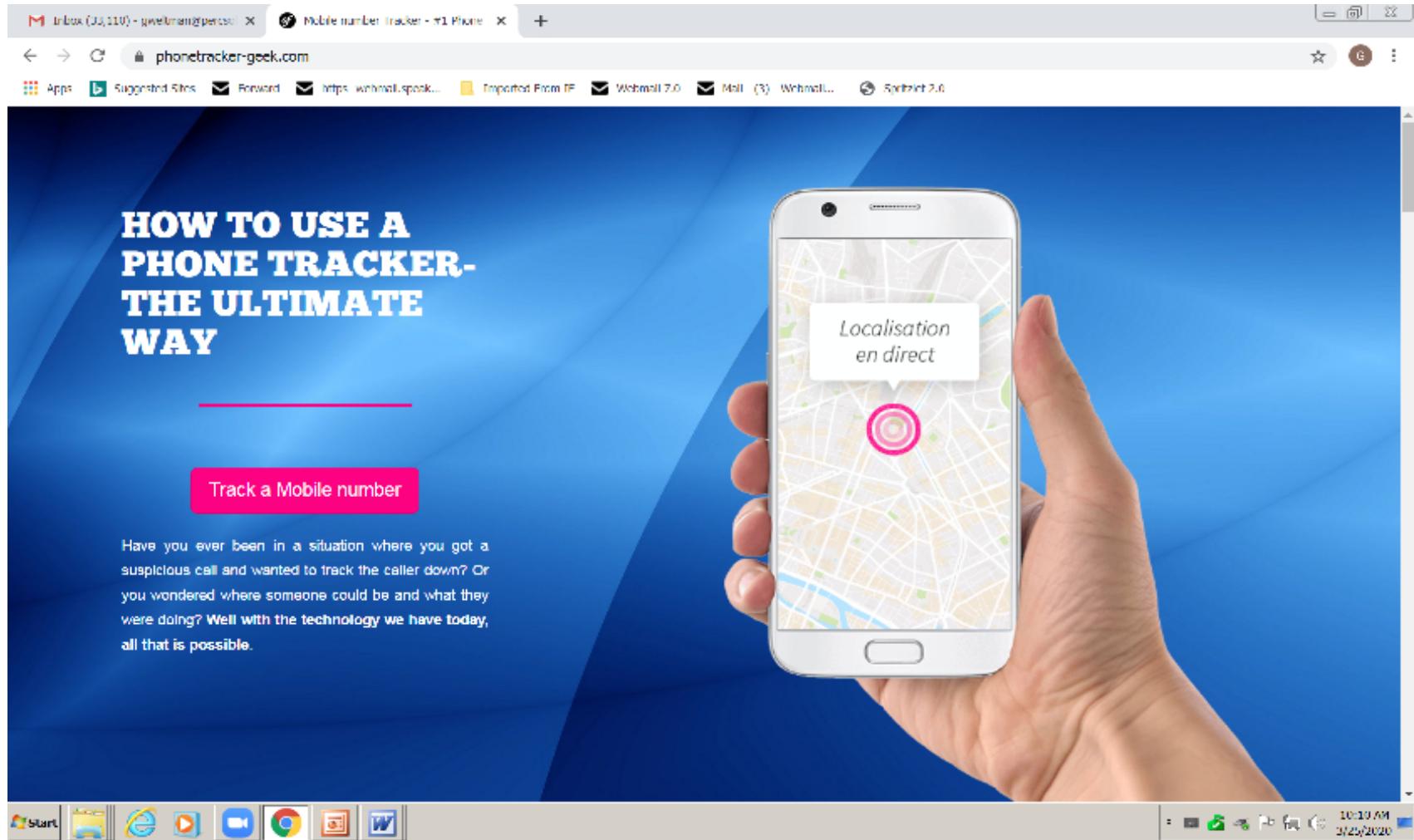


- Employment
- Education
- Memberships
- Publications
- News Events
- Contact Info
- Criminal Record
- Lawsuits
- Judgments
- Tax Liens
- Bankruptcies
- Home Size
- Home Value
- Neighborhood

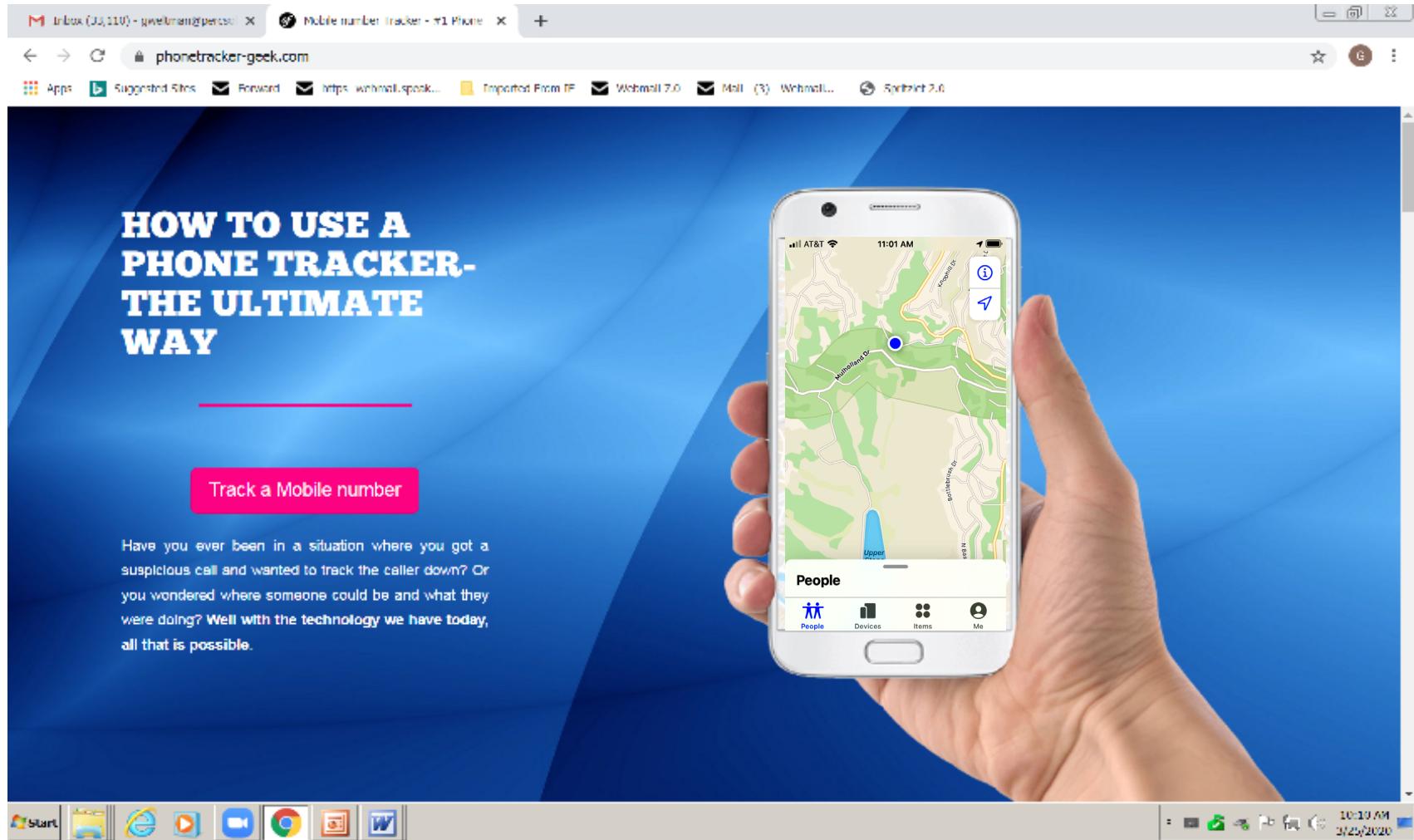
Personal Information: General Search

The screenshot shows a Bing search results page for the query "Gershon Weltman". The search bar at the top contains the text "Gershon Weltman". Below the search bar, there are 3,680 results. The first result is a LinkedIn profile for "Gershon Weltman". The profile includes a photo of a man, the URL www.linkedin.com/pub/gershon-weltman/20/109/abb, and a brief description: "Vice President and Principal Scientist ... · Telecommunications · 91 connections". The second result is a link to "AbeBooks" for "gershon weltman". The third result is a link to "UCLA Electrical Engineering" for "Weltman, Gershon". The fourth result is a link to "BruinWalk" for "Gershon Weltman". The fifth result is a link to "The Wall Street Transcript" for "DR. GERSHON WELTMAN". The sixth result is a link to "ZoomInfo.com" for "Gershon Weltman". The bottom of the screen shows the Windows taskbar with various pinned icons.

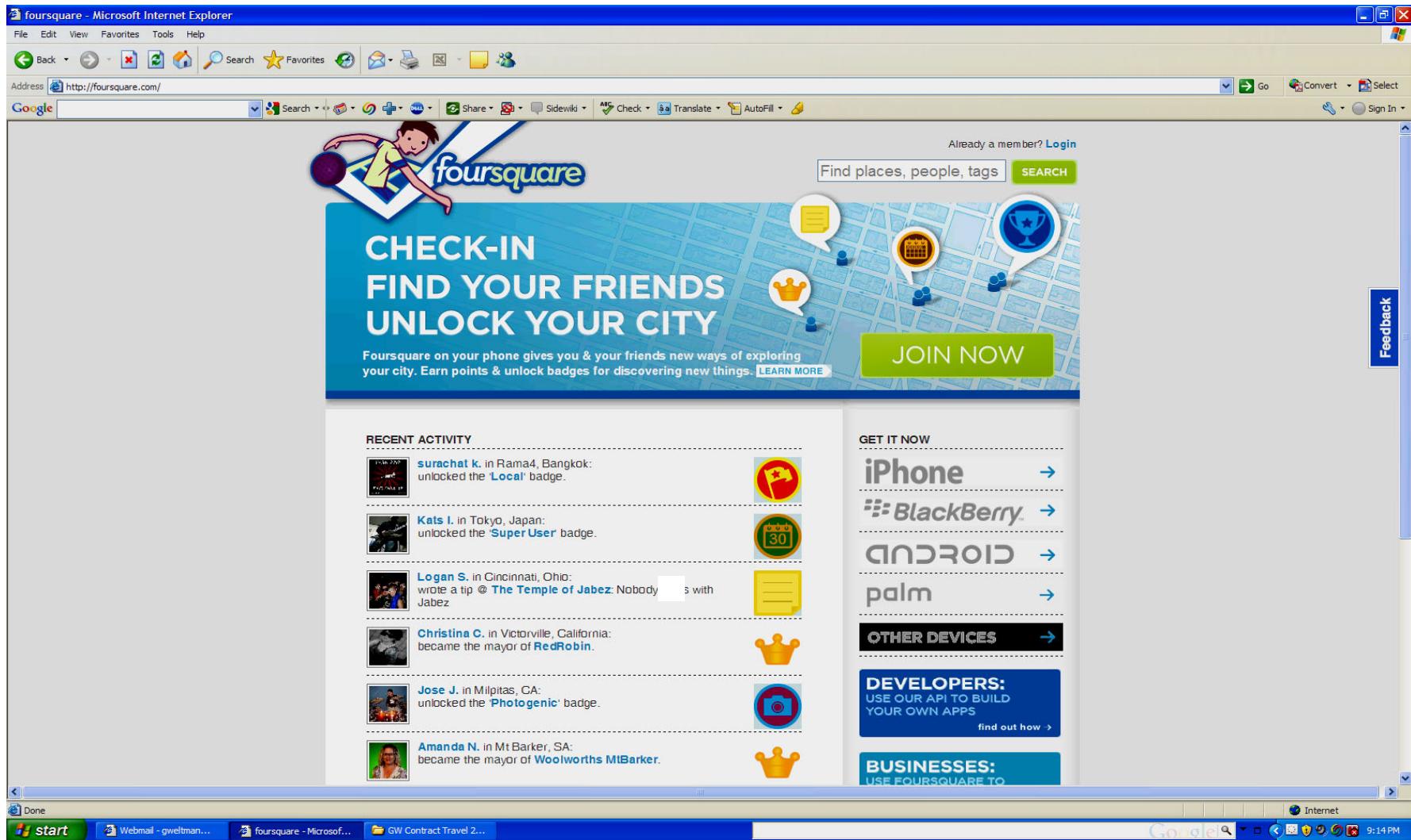
Personal Information: Individual Location



Personal Information: Individual Location



Personal Information: Friends' Location



Personal Information: Customers' Locations

Mail - Gershon Weltman - Outlook F Location-Based Advertising Platform

enterprise.foursquare.com/products/pinpoint

Apps Suggested Sites Forward https://whmmail.speak... Imported From IF Mail (3) Whmmail... Search 2.0 Mail gershon@per... Mail Gershon Weltma...

UPDATE July 15, 2020: We have updated our Privacy Policy. Our Consumer Services Privacy Policy and Enterprise Services Privacy Policy will become effective on August 20, 2020. If you use our services on or after August 20, 2020, you will have accepted our new policies.

FOURSQUARE Products Company Resources

Home / Products - Pinpoint/Audiences

Audience Segmentation

MALE, AGE 45-49
DMA: Dallas - Fort Worth

Personas

- The Coffee Drinker
- Small Business Owner
- Sports Lover
- Casual Diner
- Super Saver

DAVE'S AUTO REPAIR

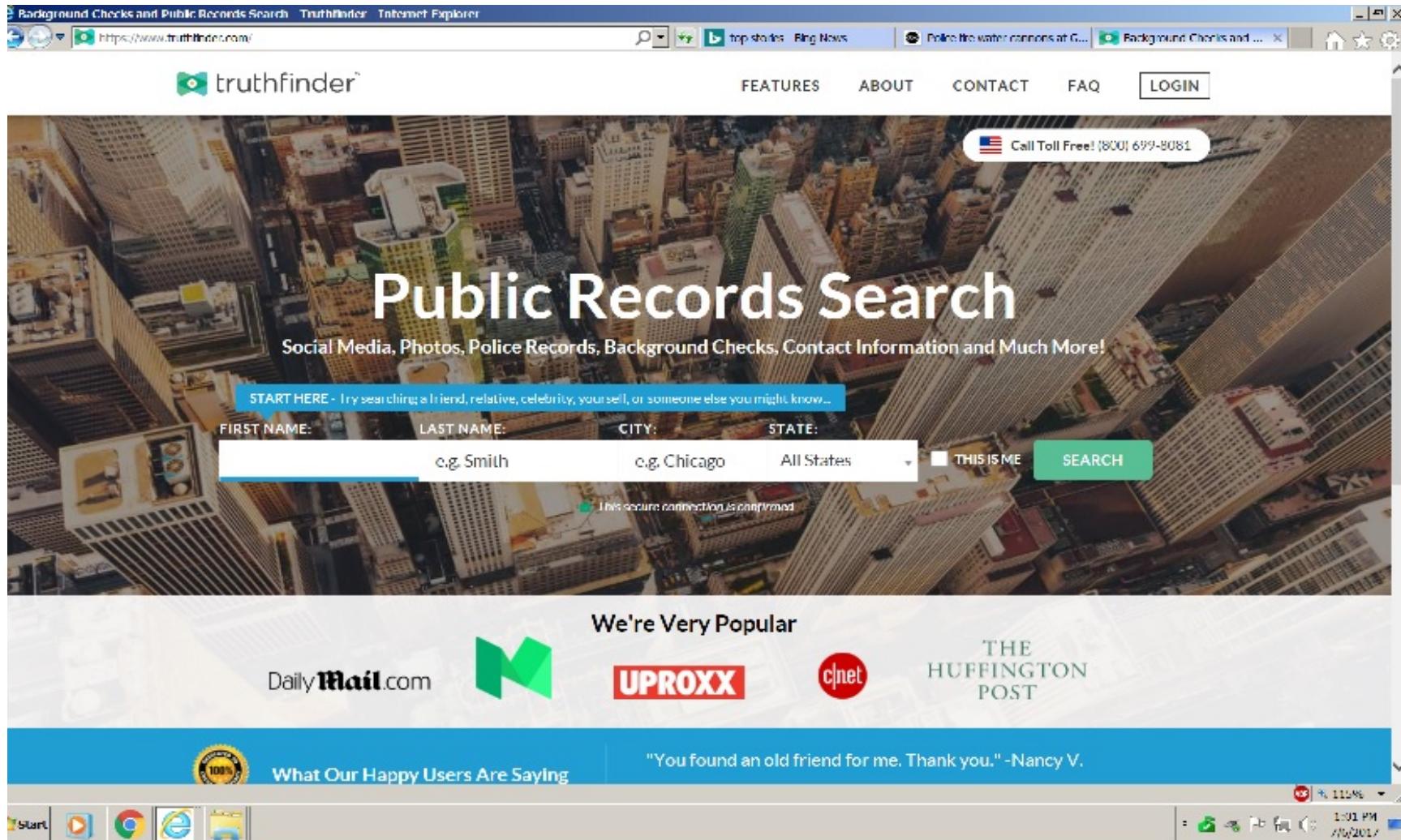
DOLLAR STORE

PEPPER'S GRILL

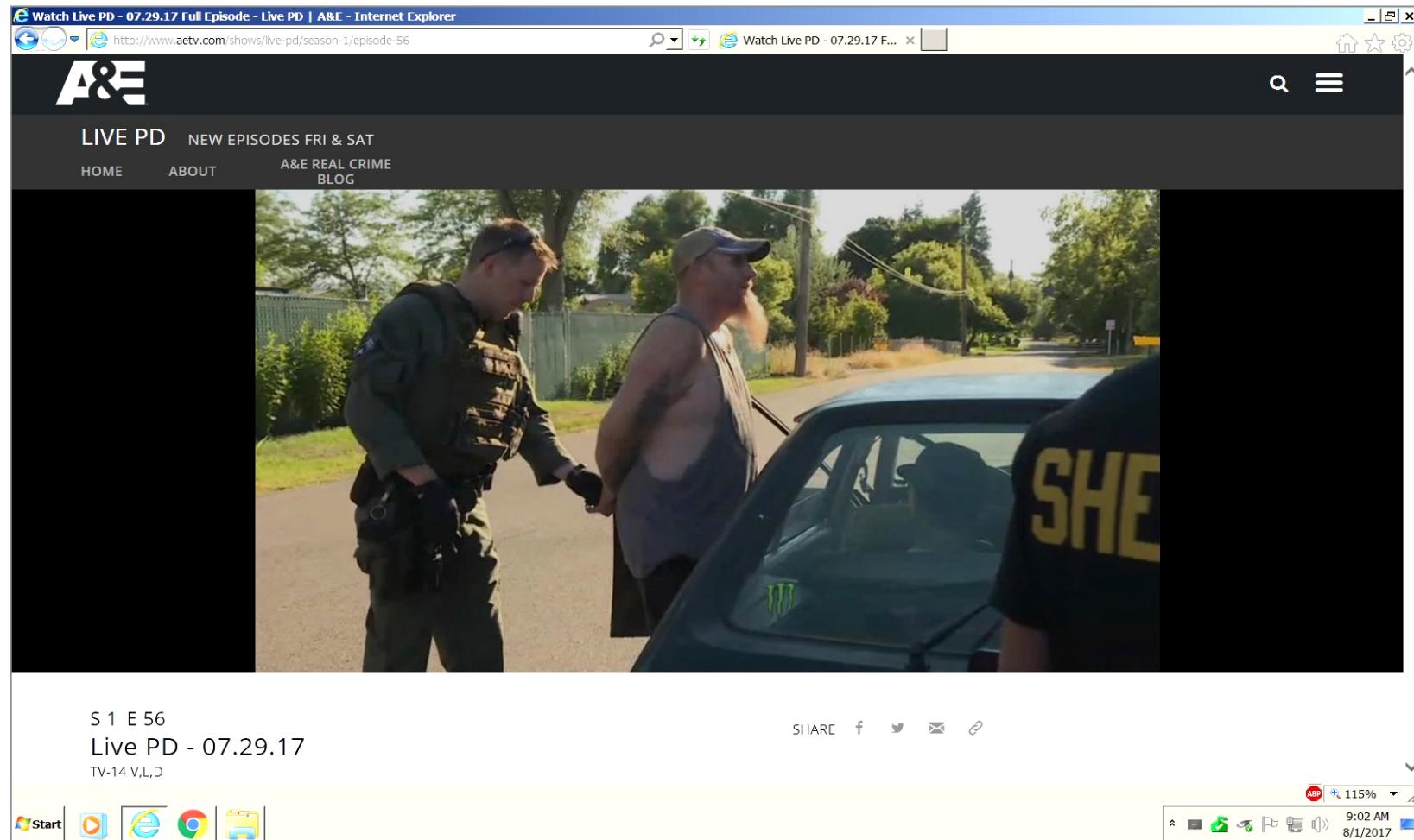
AT&T STADIUM

12:59 PM 11/2/2020

Personal Information: Public Records



Personal Information: Photos and Videos



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

Personal Information: Mug Shots

The screenshot shows a web browser window with the URL [findmugshots.com](https://www.findmugshots.com). The page features four main service icons: 'BACKGROUND CHECKS' (file folder icon), 'GOVERNMENT RECORDS' (building icon), 'BOOKING RECORDS' (checkmark icon), and 'PREMIUM SUPPORT' (globe icon). Below these are descriptive text blocks and a large central heading.

What is FindMugshots.com?

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

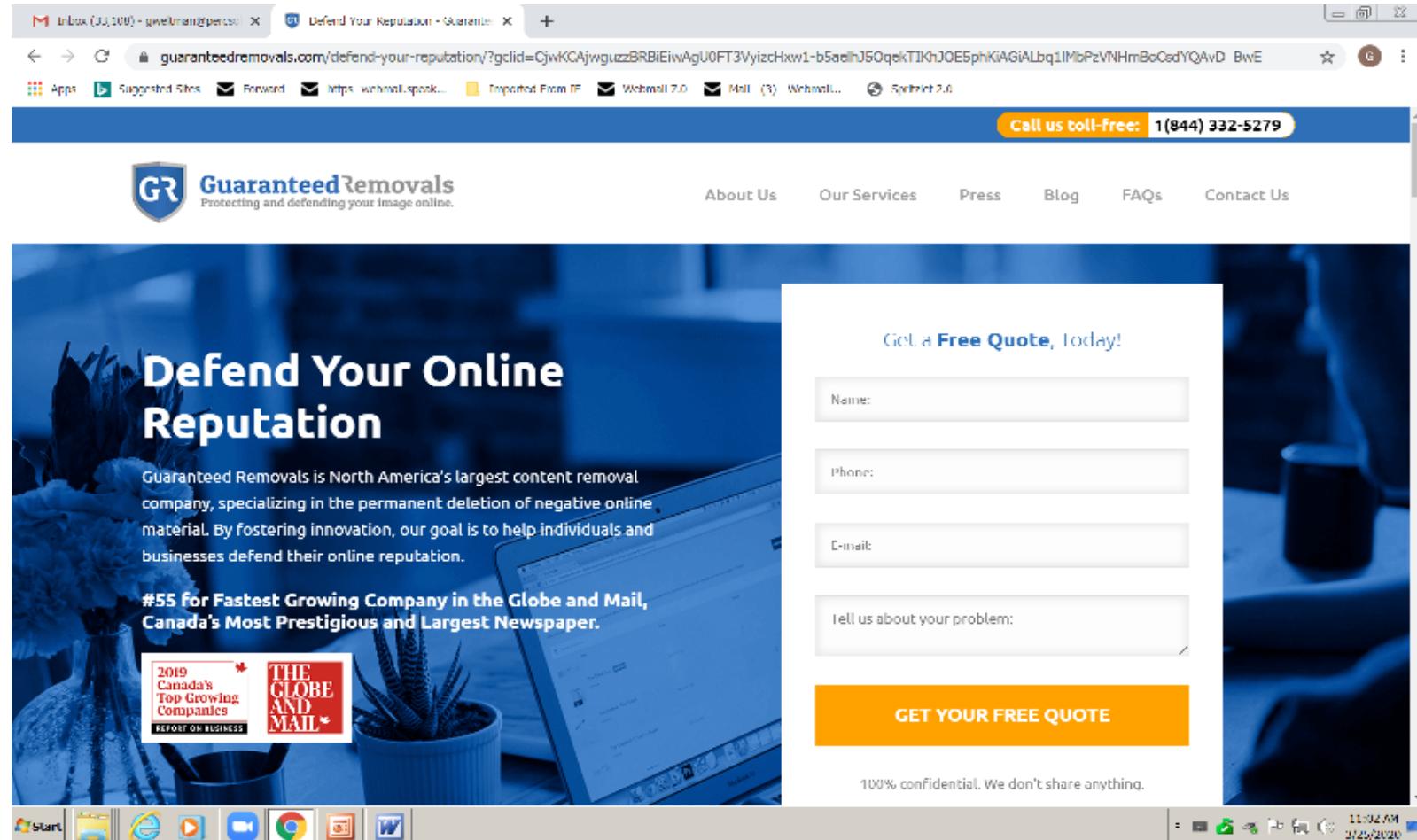
FIND MUGSHOTS PROVIDES REAL TIME SEARCH TO ARRESTS AND MUGSHOTS.

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.

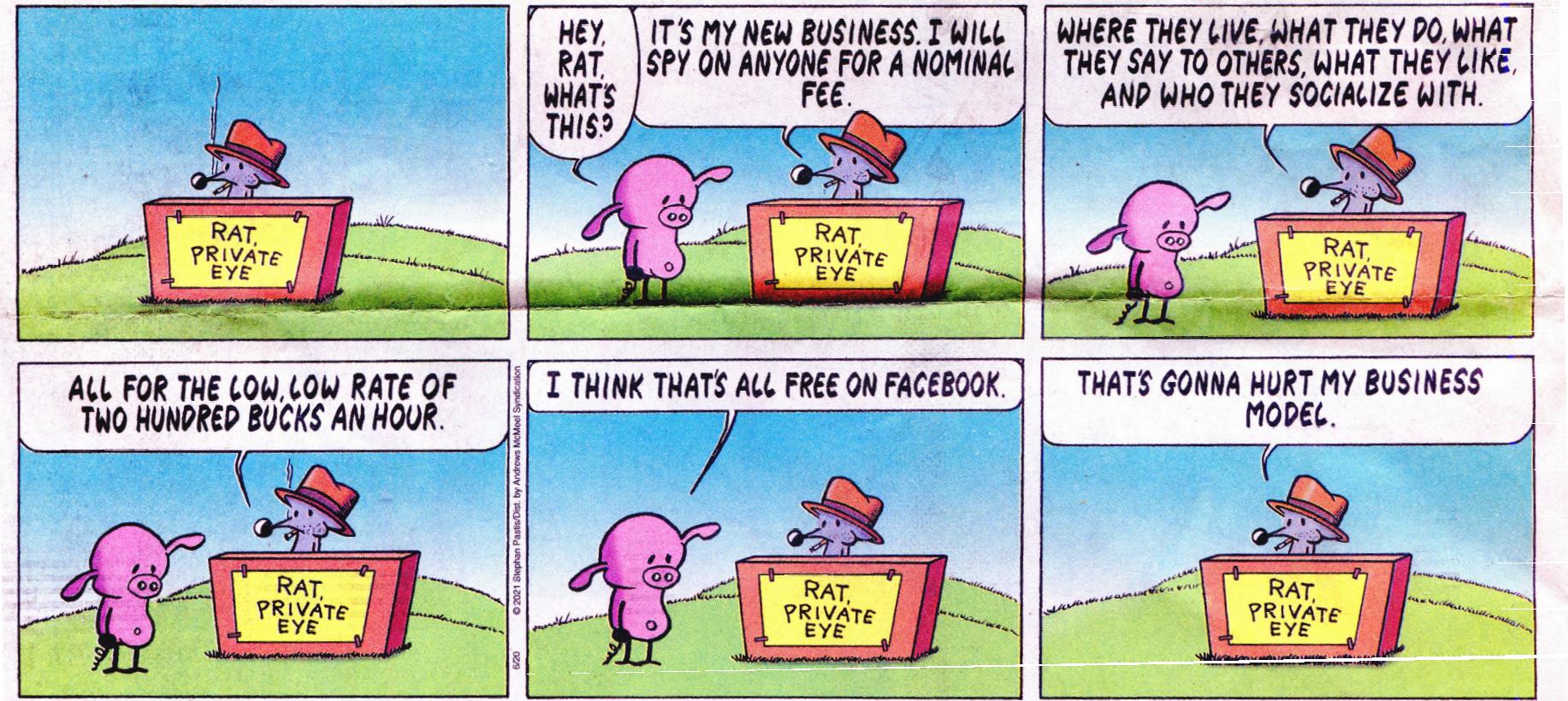
Our goal is to provide you with the most recent and even historic mugshots and arrest information for completely free of charge. You may want to use our partners for additional information about a person or the specific arrest record.

Editing Your eDossier



In Summary

PEARLS BEFORE SWINE By Stephan Pastis



Los Angeles Times, June 20, 2021

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).

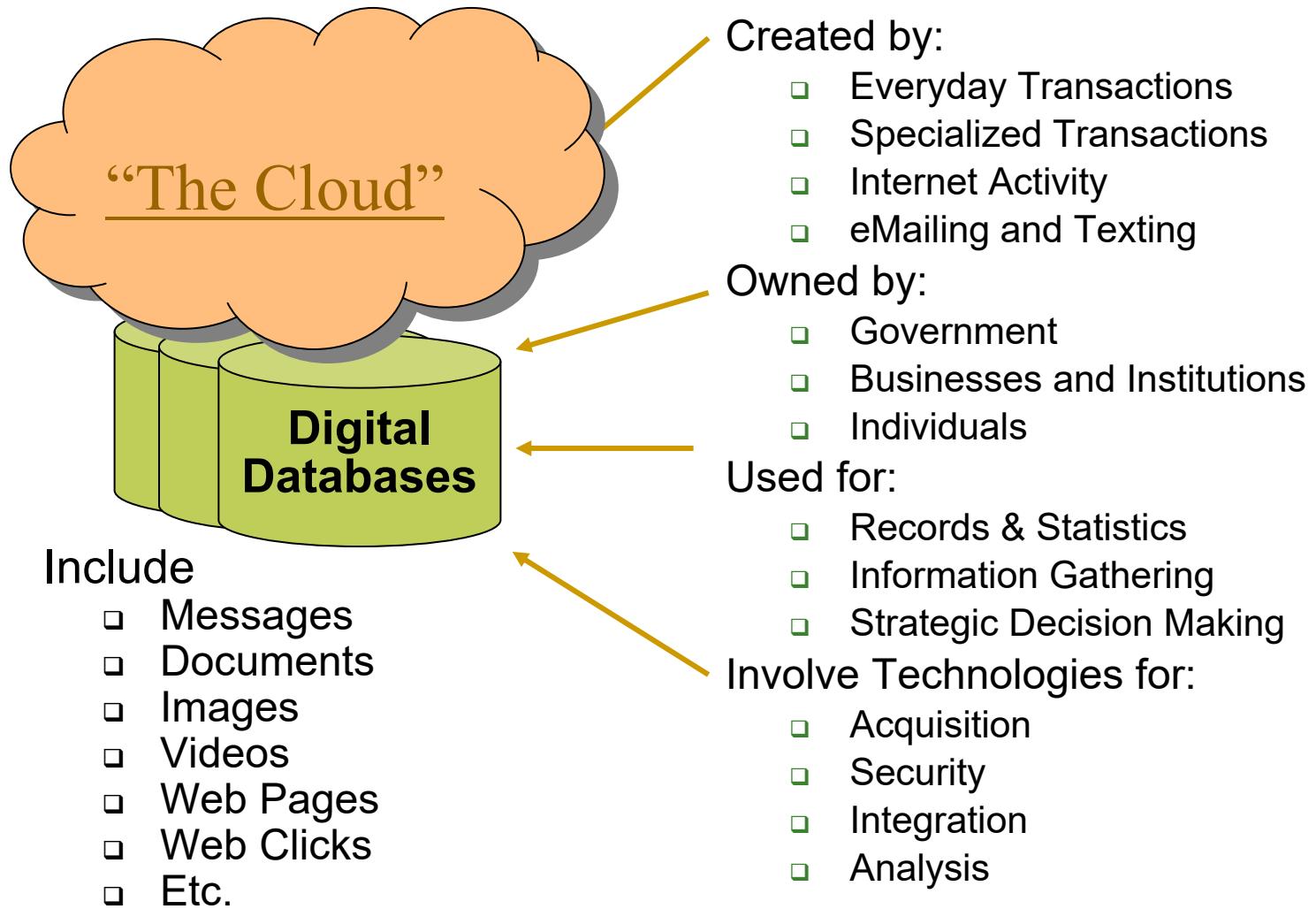
- Critical Influence

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.

Ethical Case 1: Database Use and Abuse



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**

The Chances for Abuse and Misuse

■ Privacy: *Adding to Databases Personal*

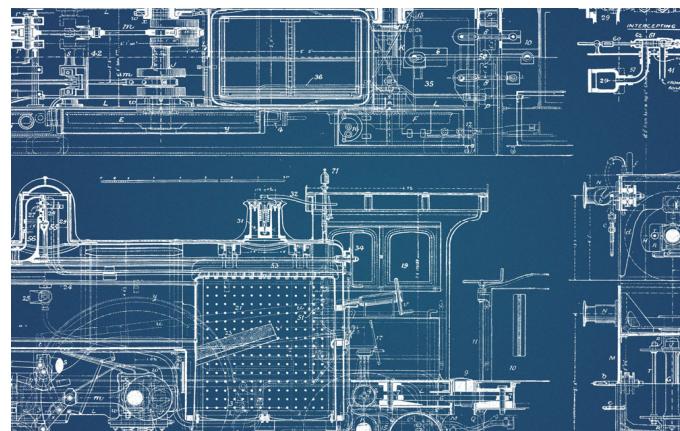
- Information (e.g.. medical records)
- Sensitivities (e.g., sexual identity)
- Actions (e.g. arrests, bankruptcies)
- Associations (e.g. memberships)
- Communications (e.g. embarrassments)



Donald Sterling and Maria Perez

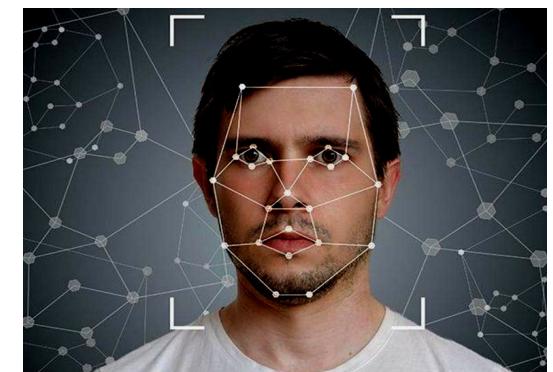
■ Piracy: *Taking from Databases*

- Secrets (e.g., plans, formulas)
- Intellectual Property (e.g., technologies)
- Identities (e.g., individual, corporate)
- Site functionality or operability



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, password'
 - **Something you are – Biometrics**
- Biometric Identification/Verification
 - Fingerprint
 - Handprint
 - Iris or Retinal Pattern
 - **Facial Recognition**
 - Movement – Signature, Gait



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](#). A conventional explanation of how the company finds itself bent into a familiar pose of contrition, following [news](#) that breached its defenses, potentially gaining access to troves of valuable information -- credit card numbers, email accounts and 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 fatuity, 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? What if the company employed the best defenses available, yet they proved inadequate in the face of a decentralized and proliferating threat?

Sony has captured headlines because it is one of the world's most conspicuous consumer brands, and the recent attacks on its network have been both brazen and successful. But the list of companies that have been targeted by similar plots is lengthening and 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 cyberattacks and other activities made a difference in Trump's upset victory over Hillary Clinton. In a tweet after the election, Trump has been emphatic that it did not. Democratic just-as-forcefully insist the effect was clear even if they don't blame the Russians for their 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 (Ohio) in his losing presidential nomination.

"We know that [Clinton's] campaign on the defensive," Weaver said. "We know that it distracted that campaign and we know [See Hacking, A15]

It Gets Personal...



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

PIN NUMBER:

A	B	C	D	E

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.

...Institutional...

A third of Americans could have had data stolen in big health care hack



By Sean Pyles, CNN

3 minute read · Published 5:53 PM EDT, Wed May 1, 2024

[f](#) [X](#) [✉](#) [⎙](#)



UnitedHealth CEO Andrew Witty testifies before the Senate Finance Committee on Capitol Hill in Washington, DC, on May 1, 2024. In February, hackers stole health and

MORE FROM CNN



Member of ransomware gang sentenced to more than 13 years in prison over 2021 ...



Far-right network OAN retracts false story about Michael Cohen affair with Stormy Daniels



Donald Trump fined \$9,000 for violating gag order in hush

In hours of hearings in the Senate and House Wednesday, UnitedHealth apologized and admitted that hackers broke in through a poorly protected computer server and confirmed that they authorized a \$22 million ransom payment to the hackers.

...and National



JOINT CYBERSECURITY ADVISORY

Co-Authored by:

FBI
DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

Cybersecurity & Infrastructure Security Agency

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](#).

Private Response Can be Dangerous

Deterrents to Hack Back

1986 Computer Fraud and Abuse Act	Law	Ethics	Retribution	?
	Illegal to gain unauthorized access to a computer	Highly probable that hacking back will affect innocent computers or networks	You may awaken the beast!	
2019-2020 Active Cyber Defense Certainty Act				<ul style="list-style-type: none">• Competence• Interference• Unknowns• Retribution• War!

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 every-

thing'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 Rack-space Inc.

What troubles Trappler is that not [See Cloud, B4]

...but the Solution is Often Not Simple...

Web freedom vs. Web piracy

The Internet flexes its muscles

Thousands of websites darkened

Congressional opposition to anti-piracy bills

for the day, while others such as Craigslist and Google blacked out

**ANDREA CHANG
REPORTING FROM LOS ANGELES**

**JIM PUZZANGHE
REPORTING FROM WASHINGTON**

In cutting thousands of websites darkened, the tech industry flexed its political muscle. The don't-mess-with-us campaign took on its vast reach and不可靠 became.

The switch from protest to support of the bills sparked confusion and anger. The bills had their own supporters.

SIGNING 1.19.12

PHOTO: DAILY NEWS

CAMPAIN \$ from HOLLYWOOD

CAMPAIN \$ from GOOGLE, etc.

SIGNE WILKINSON Philadelphia Daily News

Thousands of websites darkened

Congressional opposition to anti-piracy bills

for the day, while others such as Craigslist and Google blacked out

ANDREA CHANG
REPORTING FROM LOS ANGELES

JIM PUZZANGHE
REPORTING FROM WASHINGTON

In cutting thousands of websites darkened, the tech industry flexed its political muscle. The don't-mess-with-us campaign took on its vast reach and became.

The switch from protest to support of the bills sparked confusion and anger. The bills had their own supporters.

SIGNING 1.19.12

PHOTO: DAILY NEWS

CAMPAIN \$ from HOLLYWOOD

CAMPAIN \$ from GOOGLE, etc.

SIGNE WILKINSON Philadelphia Daily News

...but the Solution is Often Not So Simple



“Big Data” Further Complicates Things...

The infographic features a central title "THE POWER OF BIG DATA." above a large illustration of a person surrounded by various data icons like charts, graphs, and social media symbols. To the left, a quote reads: "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." Below this is a section with a sun icon and the statistic "80% of the data currently produced is unstructured — coming from sources like images, videos, tweets, posts and e-mails." To the right, a section titled "MINING MOTIVATION." discusses IBM Smarter Analytics, stating it helped XO Communications predict customer defections and reduce churn. A "Share" button is at the bottom right.

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 picture. A big data platform, 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, companies are gathering big

Share

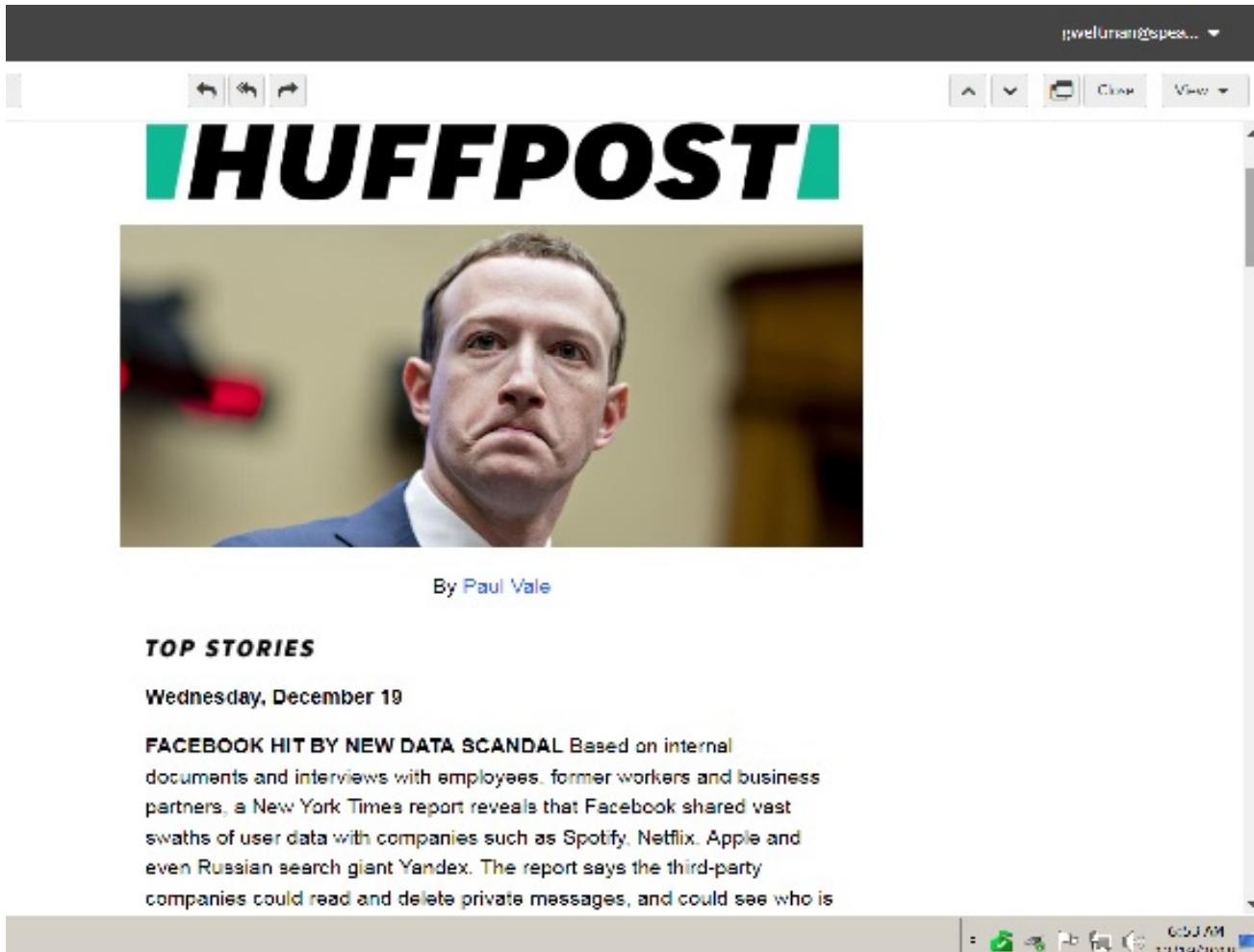
Big Data is the totality of information about a person and their personal finances, memberships, activities, interests and inclinations. Political campaigns use Big Data to understand voters, companies use Big Data for marketing research, public organizations use Big Data to gage public opinion, and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

...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

...with Facebook as a Major Culprit...



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

....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



....Its Data Maybe Even Affecting Elections

PULLING BACK THE CURTAIN

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

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]

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.

THURSDAY, MARCH 7, 2019 :: LATIMES.COM/BUSINESS

• **S&P 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

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.

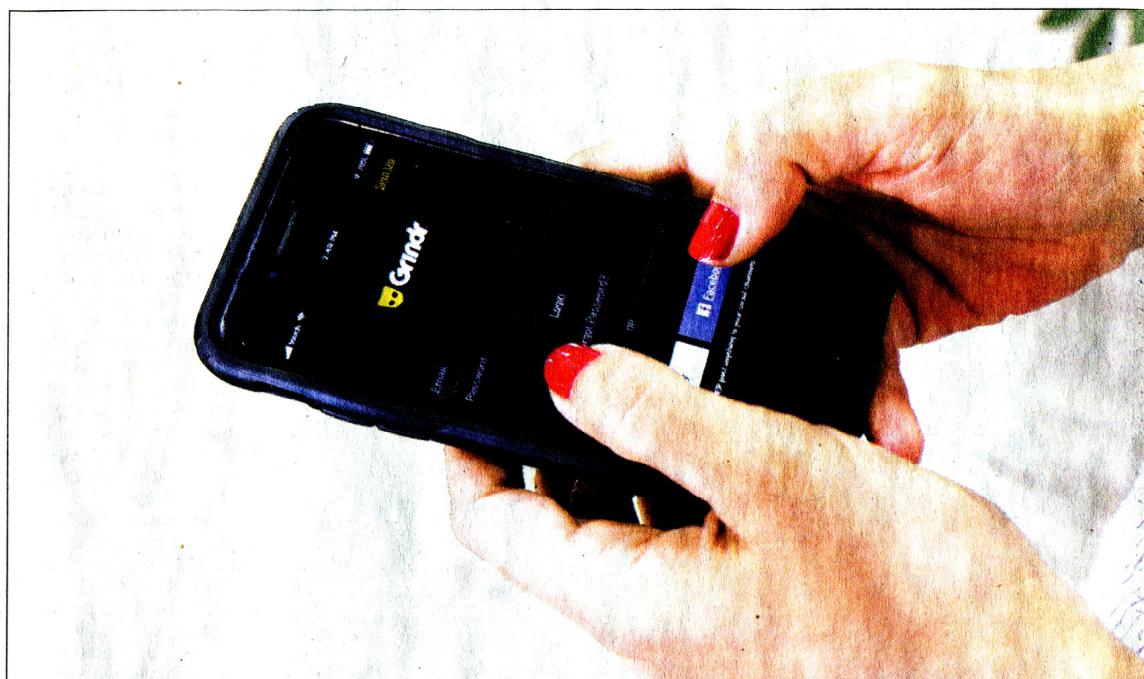
Other apps, including popular dating apps Tinder and OkCupid, share similar user information, the group said. Its findings show how data can spread among companies, and they raise questions about how exactly the companies behind the apps are engaging with Eu-

rope'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 organization [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

...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."

The idea according to



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. Photo: AP

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.

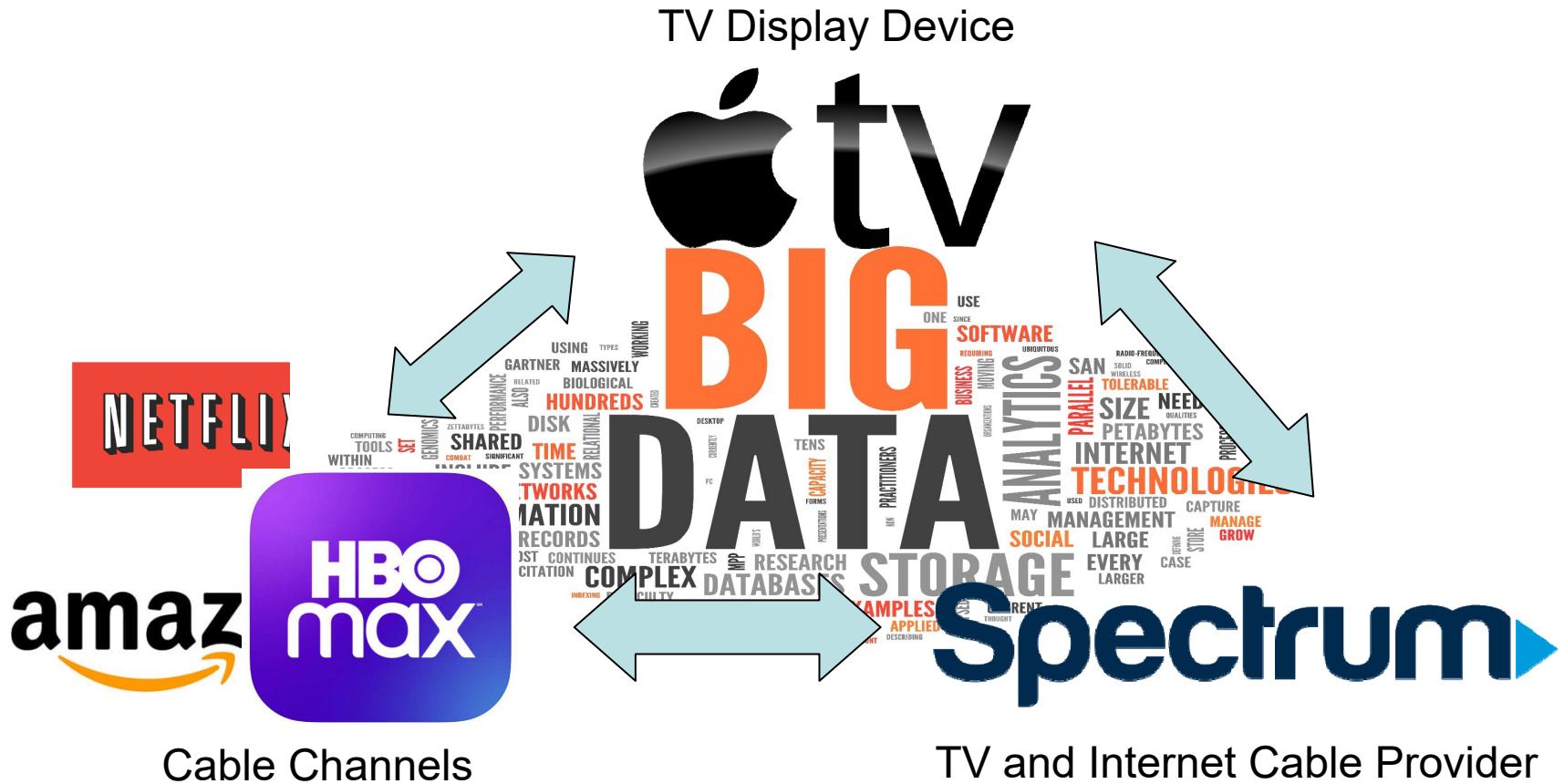
For the Apples and Amazons of this world, that's not ideal. For the rest of us, well, a little disruption is precisely what's needed.

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

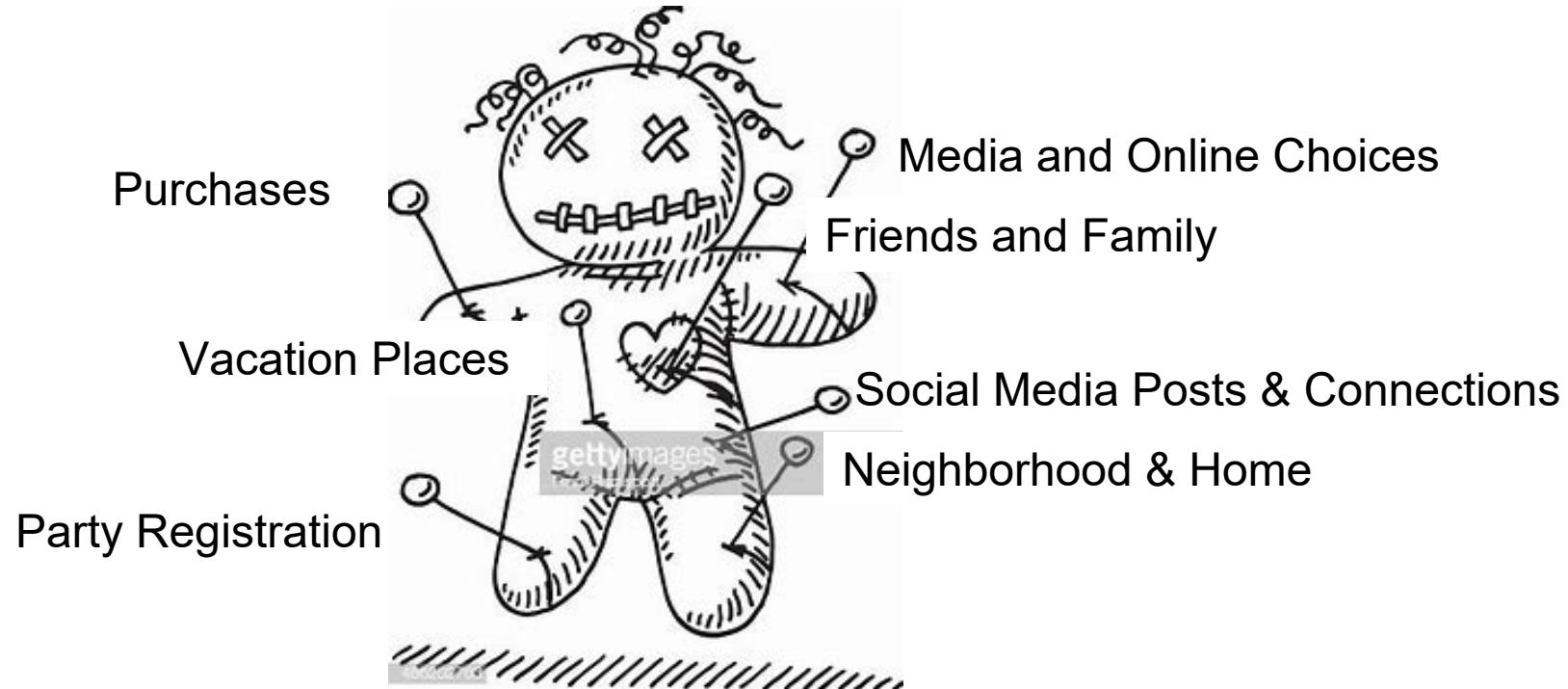
He observed that if California passes a law making tech companies accountable for people's medical data, this could prompt Congress to similarly amend the main federal medical privacy law, the Health Insurance Portability and Accountability Act.

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

Plus, Databases Connect...



...So the Outlook Can Be Worrisome



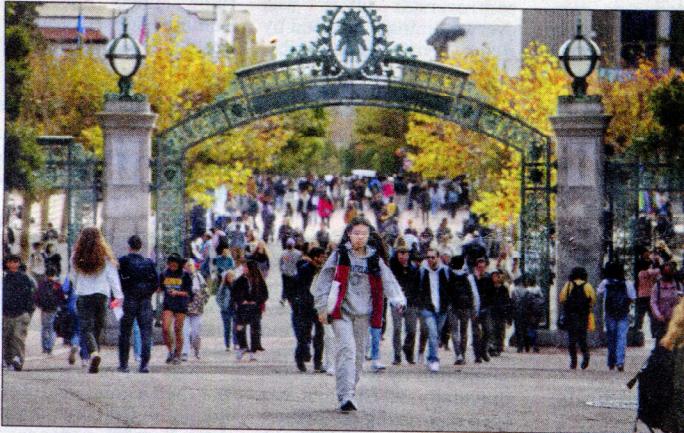
Commentators have said that Big Data is creating a “voodoo doll” so you can be manipulated with personally targeted messages and also by fear tactics.

Harvard Prof. Shoshana Zuboff has called the result “Surveillance Capitalism.”

Doll image from [gettyimages.com](https://www.gettyimages.com)

On the Other Hand

At UC Berkeley, spreading the gospel of data science



MARLENA SLOSS Washington Post

STUDENTS walk on the UC Berkeley campus in November.

‘We want to expand access to computing and the possibilities of how people can learn these skills that will get them a better job.’

— ERIC VAN DUSEN, data sciences faculty member

Campus aims to increase access to high-demand and high-paying field with a new college and free curriculum.

BY TERESA WATANABE

They comb through troves of legal records and video evidence to challenge wrongful convictions. They organize medical data to help personalize health treatments for better care. They scrutinize school test scores to investigate inequities. Finding safe drinking water is easier thanks to an analysis tool they created.

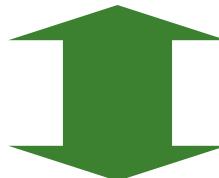
UC Berkeley’s faculty and students are marshaling the vast power of data science across myriad fields to address tough problems. And now the university is set to accelerate those efforts with a new college, its first in more than 50 years — and is providing free curriculum to help spread the gospel of data science to California community colleges, Calif. [See UC Berkeley, A14]

Access to the Web database can help solve many societal problems, say the disciples.

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

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.

Constitutional Protection: The 5th Amendment

“No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.”

The 5th Amendment also protects against inadvertent self-incrimination.

The Right to be Secure Involves:

- **Expectation (and Right) of Privacy**

The principle underlying the 4th and 5th Amendments and many subsequent laws and regulations

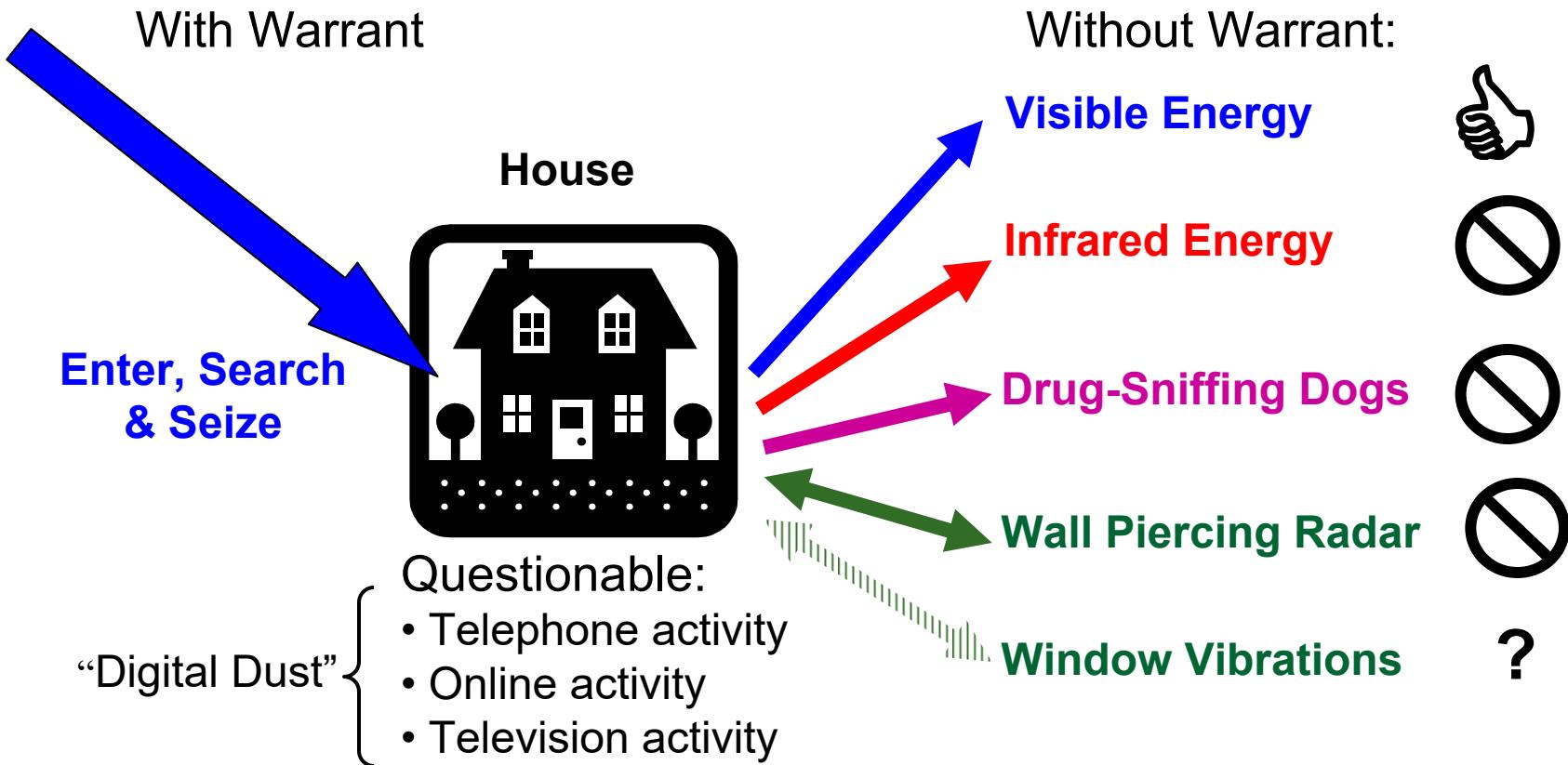
- **Historical Understanding**

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?

Example: Inside/Outside Your House



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.

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

Real People are Listening

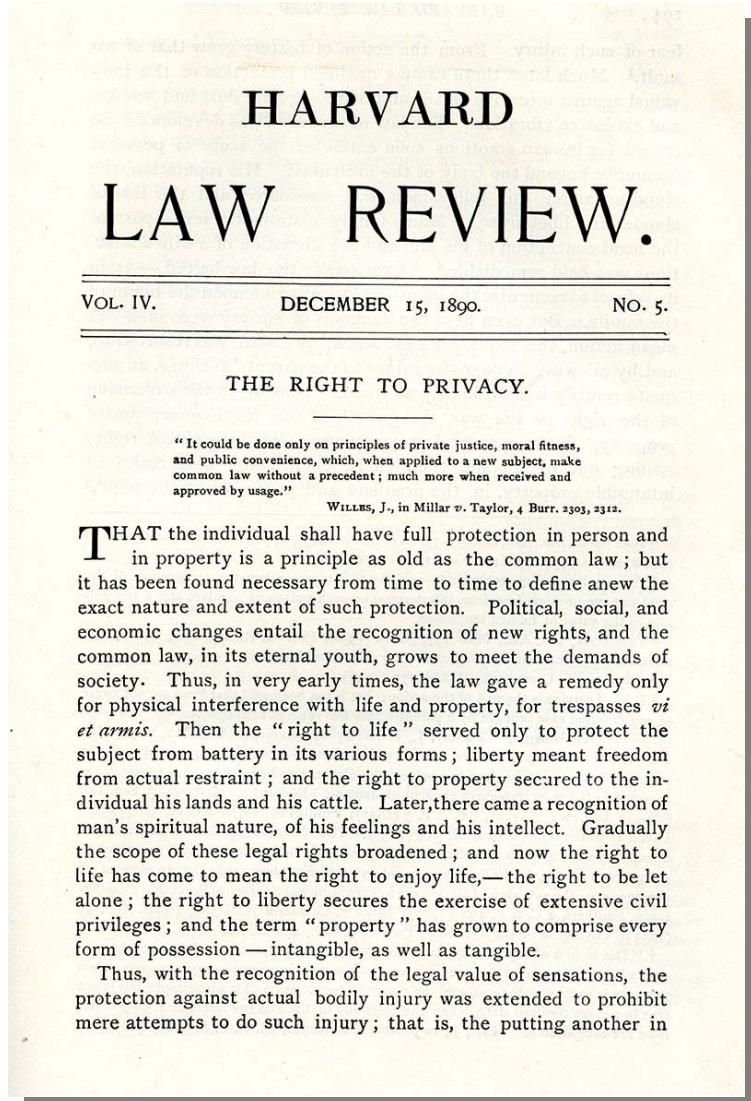


DEBUTING IN 2014, Amazon's Echo popularized the voice-activated home smart speaker. Globally, consumers bought 78 million smart speakers last year.

Alexa, and strangers, are listening

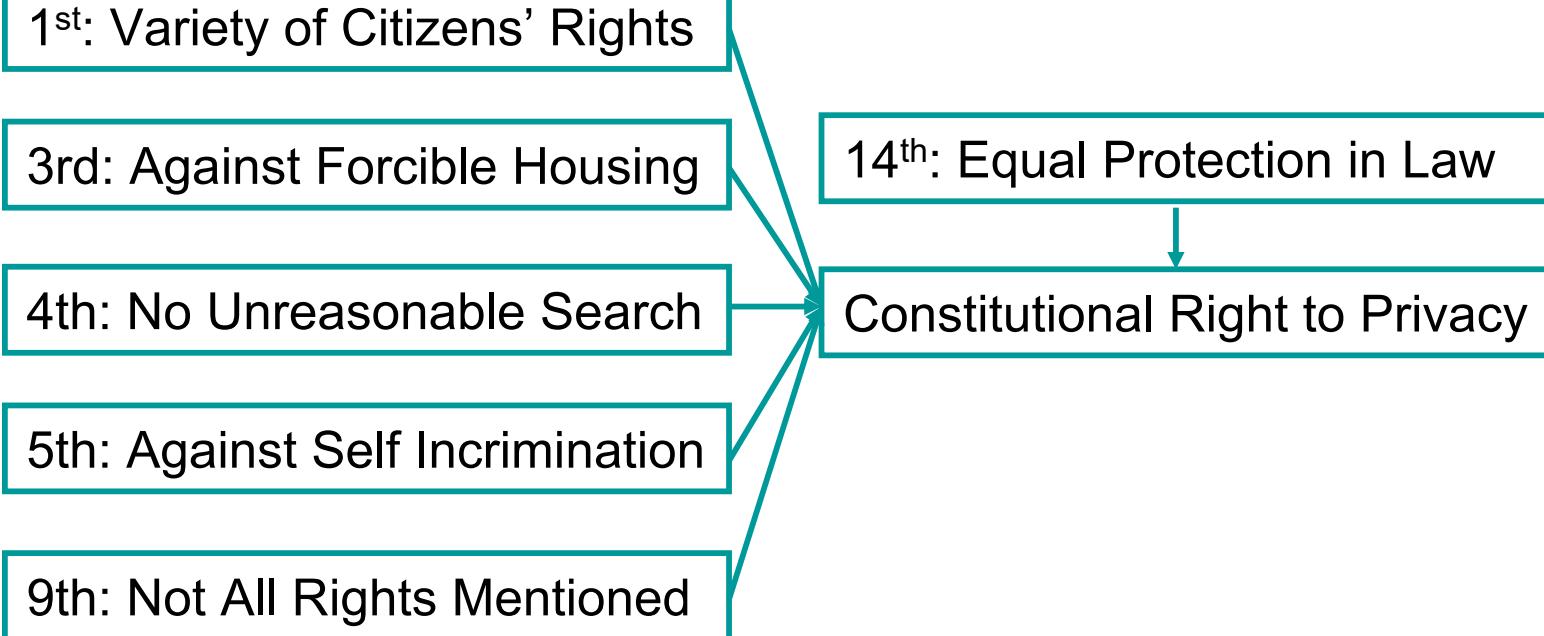
Amazon employees review and transcribe audio clips to help improve the digital assistant

Privacy Can Be Complicated



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

A Constitutional Rationale



In a 1961 contraception case, Justice William Douglas wrote for the 7:2 majority that these Constitutional Amendments create a “Zone of Privacy.”

But after many judgments affirming an implied right to privacy in the Constitution, the US Supreme Court seems to be backtracking on this line of reasoning, and opening more personal actions to legal prohibition by states.

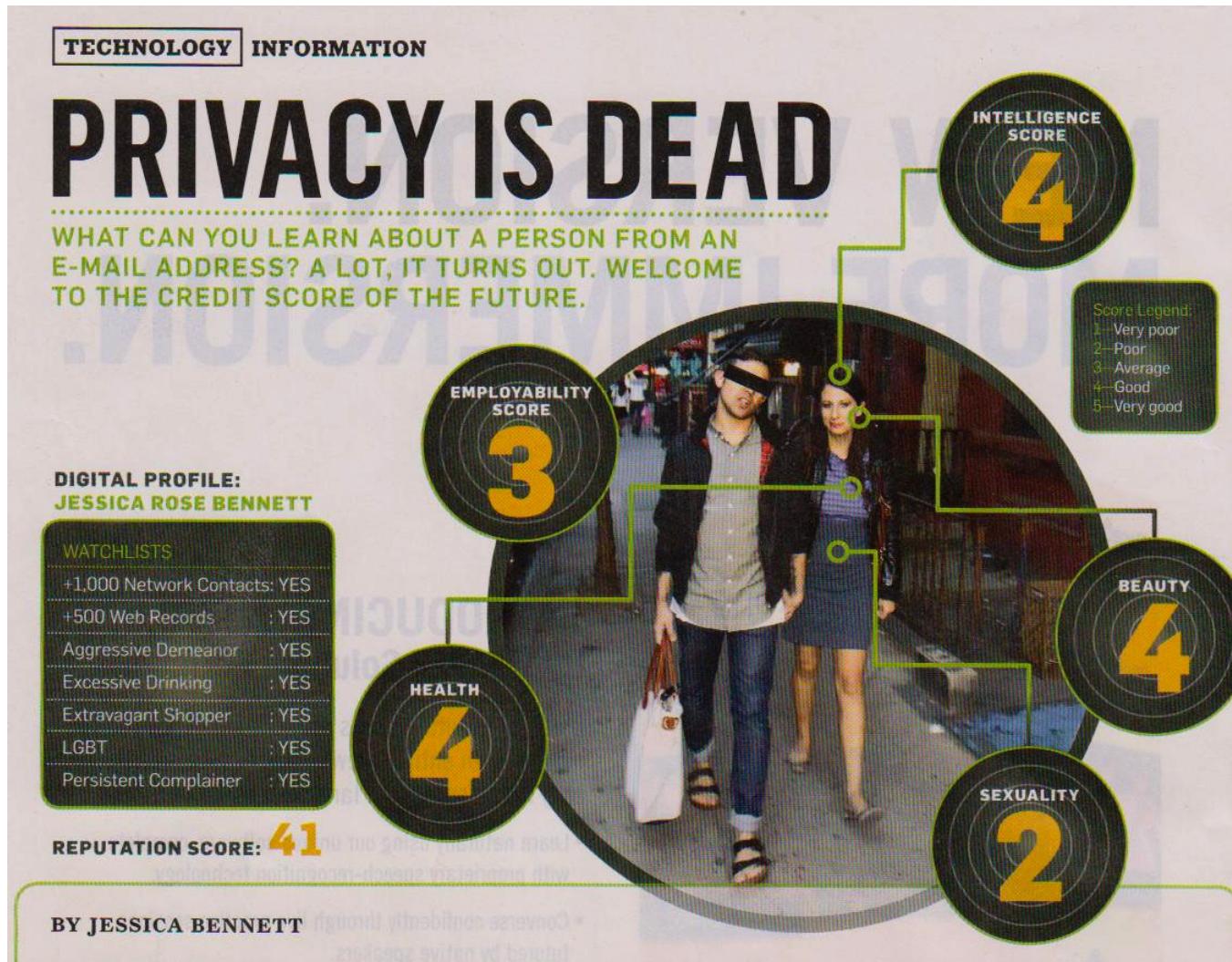
15 Years Ago Prof. Kleinrock Was Cool



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

"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."

And One Year Later Newsweek Agreed



Newsweek, November 1, 2010

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 were deeply disturbed because it seemingly put the arbitrary actions of Government agencies above basic guaranteed constitutional rights and opened up new avenues of [Government surveillance](#).

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

SIGINT Military Origins



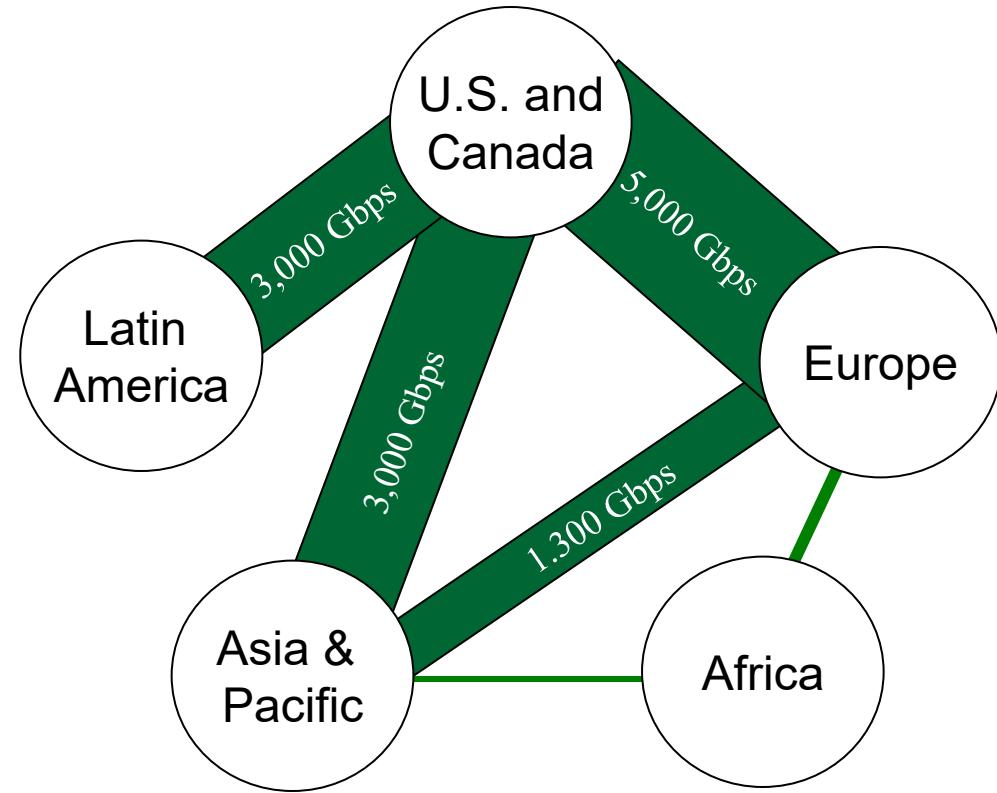
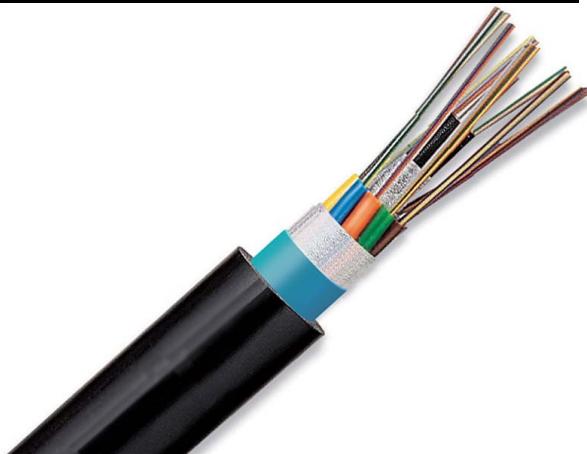
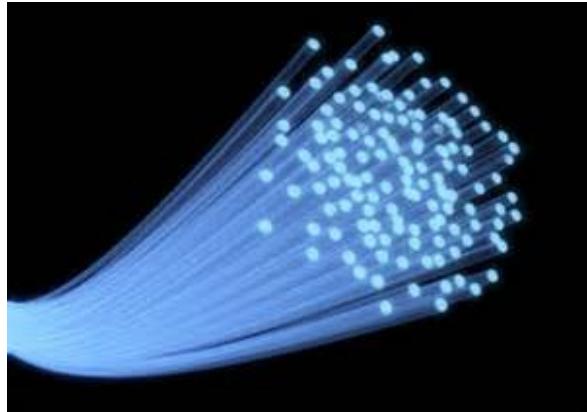
Image from L3 Communications

COMINT/ELINT Detection Equipment



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

More COMINT: Fiber Cable Networks



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

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

Total Information Awareness: An Early Trial

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**.



A Real 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**.



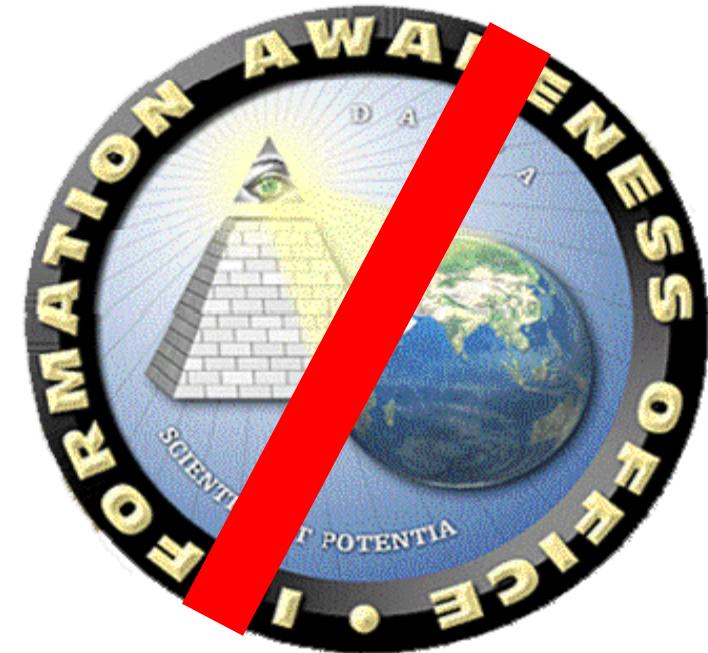
A Real Trial: Total *Information Awareness*

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)**.

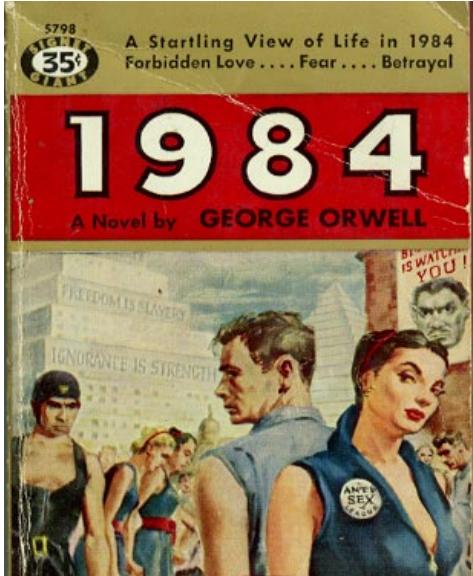
The stated mission of the IAO was to "*imagine, develop, apply, integrate, demonstrate and transition information technologies, components and prototype, closed-loop, information systems that will counter asymmetric threats by achieving total information awareness.*"

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**.

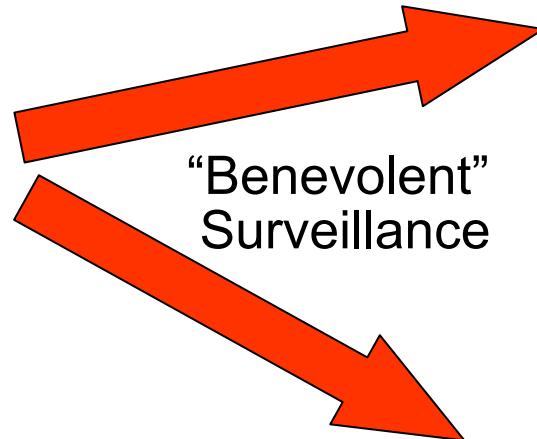
The goals and proposed technology of the *Total Information Awareness* program so disturbed Congress that it ordered DARPA to discontinue it.



Orwell Had Predicted This



George
Orwell
1949



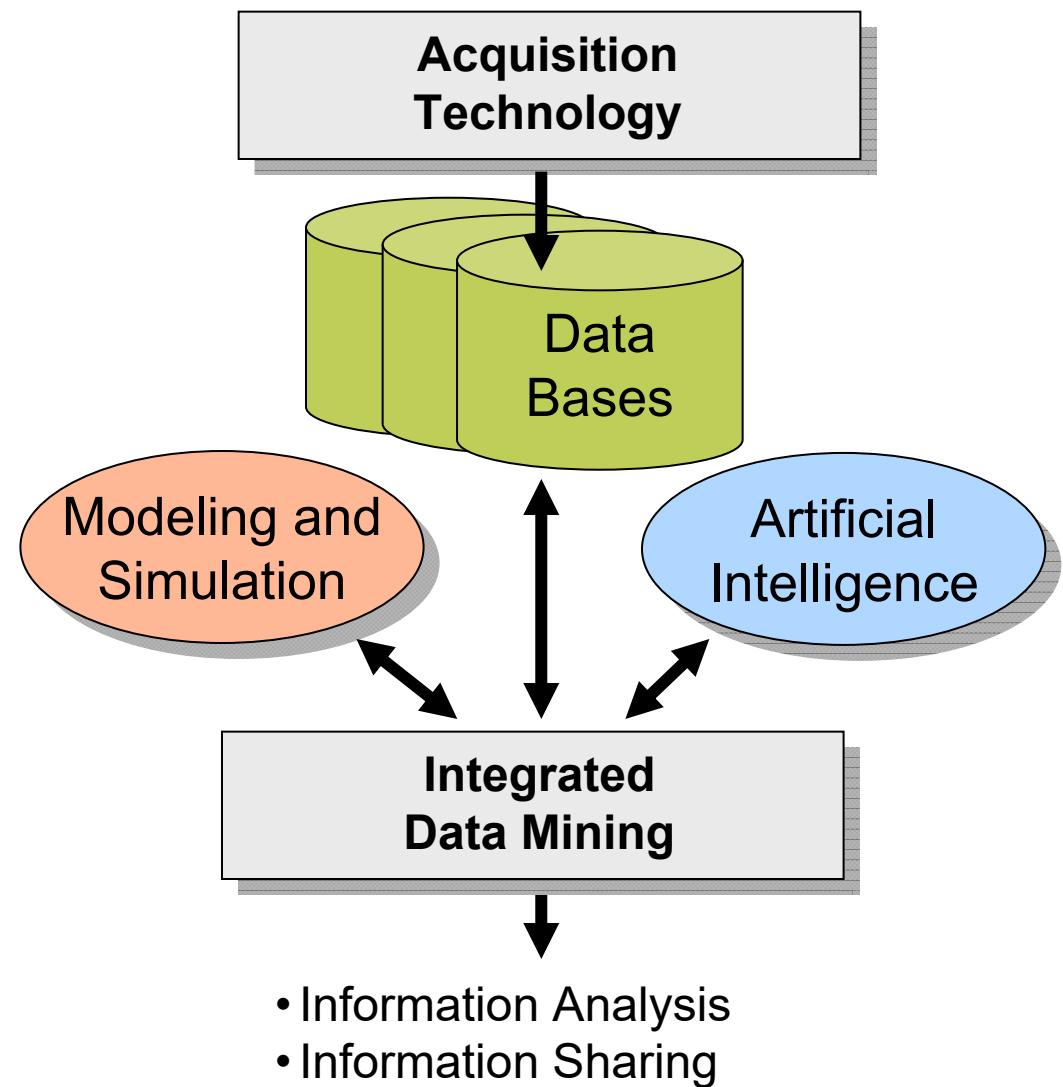
"There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate they could plug in your wire whenever 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."

As Did “Person of Interest”



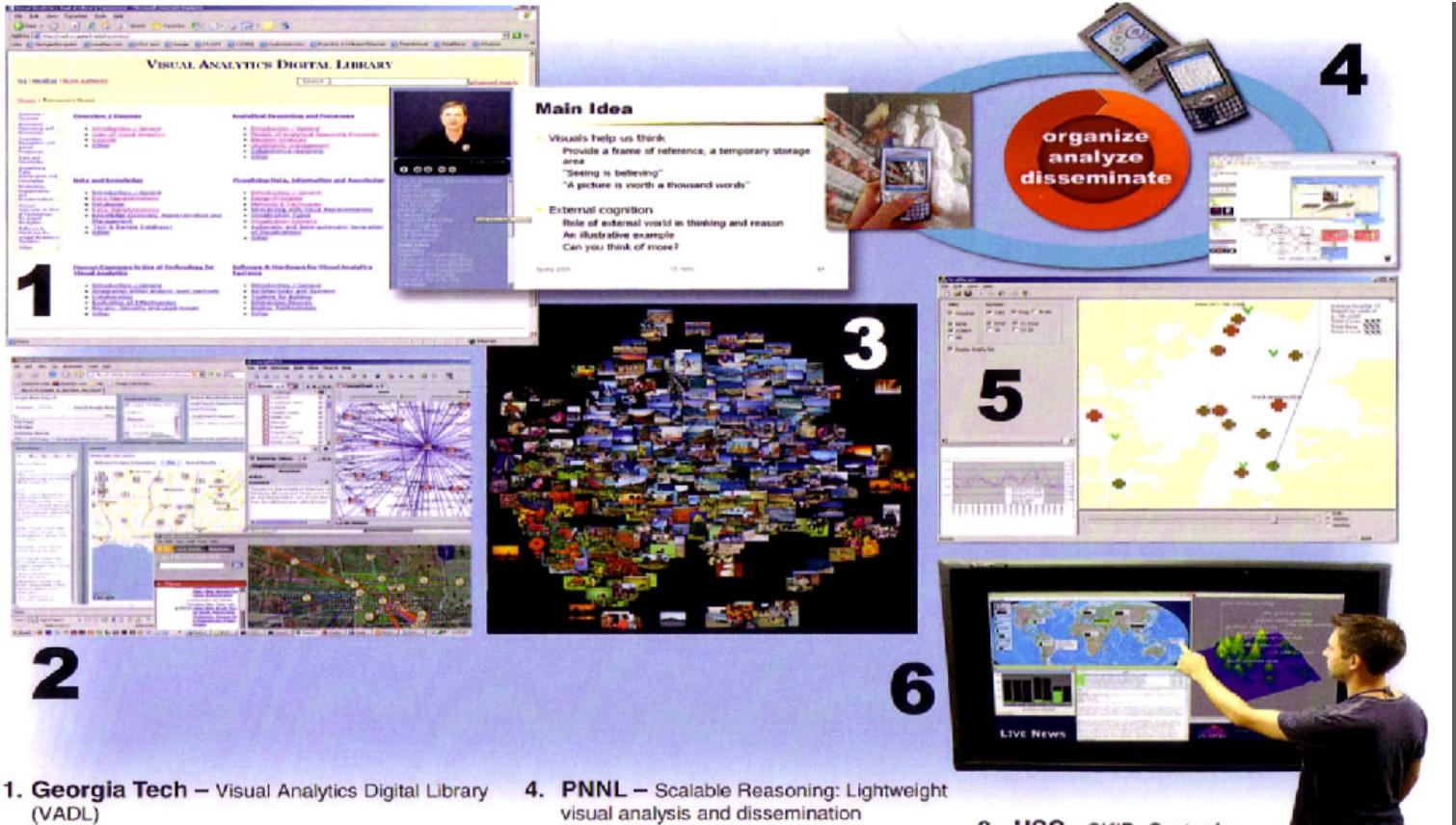
This 2011-2016 TV series postulated a universal program that used pattern recognition to identify individuals who would soon be involved in violent crimes and needed quick help.

Post 9/11 Paradigm



www.snowbittlestoncom.verizonsupersite.com

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

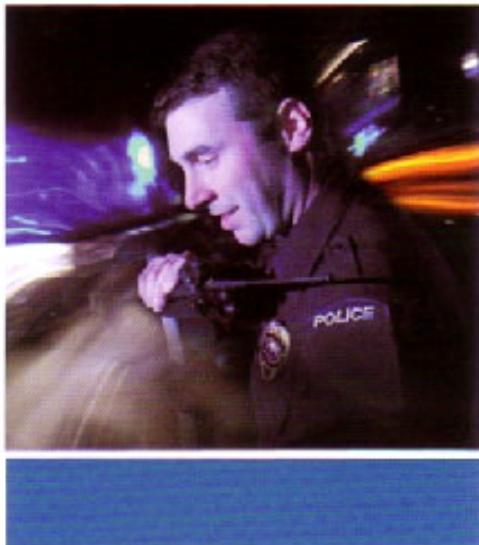
National Visualization and Analytics Center (NVAC), US Department of Homeland Security

Continued R&D: Information Sharing

Information Sharing

DHS Lead: Office of Intelligence & Analysis

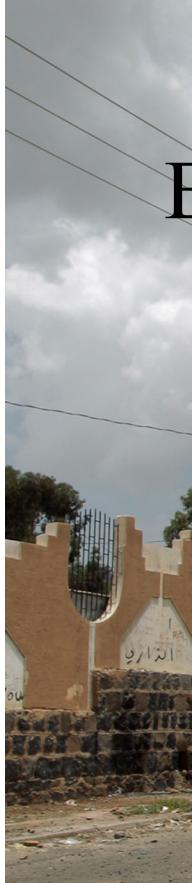
Representative Technology Needs



- 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

Surveillance Positives: 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 Afghani-

stan, 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-Fuller-

ton), 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.

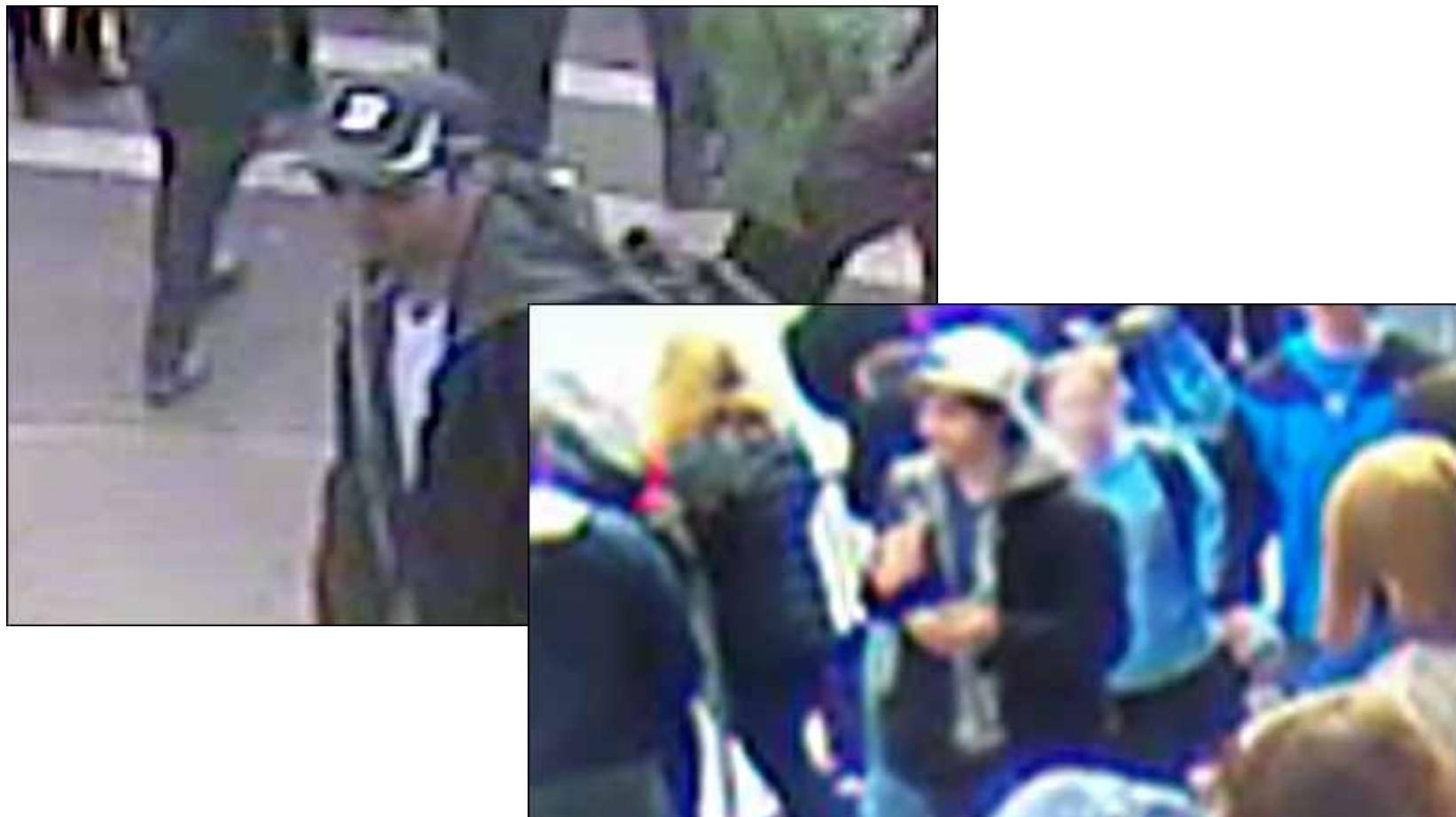
The attacks brought intense criticism of the State Department and led to a major in-house investigation, plans for reforms, and congressional hearings. Four State Department officials were removed from their jobs.

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



Los Angeles Times, August 3, 2013

...Identify Suspects...



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

...Possibly Prevent Mass Shootings

The screenshot shows a news article from CBS News titled "Can scanning social media help prevent a shooting? Some schools think so". The article discusses how schools are using social media monitoring to detect potential threats. It features a quote from Greg Boulanger, director of public safety in Bristol, Connecticut, who started a crisis team after the Sandy Hook shooting. The article also mentions Social Sentinel, a service that scans social media for threat indicators. The CBS News website interface is visible, including a sidebar with other news stories and a "Watch Now" section.

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

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.

CBS NEWS | November 27, 2016, 12:34 PM

Share / Tweet / Reddit / Flipboard / Email

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

Facebook Twitter YouTube RSS Instagram Email

11:10 AM 11/17/2016

2006 Public is Initially Unsure....



2013 Revealed NSA 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,

NSA surveillance programs revealed by defector Edward Snowden were surprising mainly because so many large corporations were shown to be cooperating. They were first justified under Section 702 of 2008 Foreign Intelligence Surveillance Act.

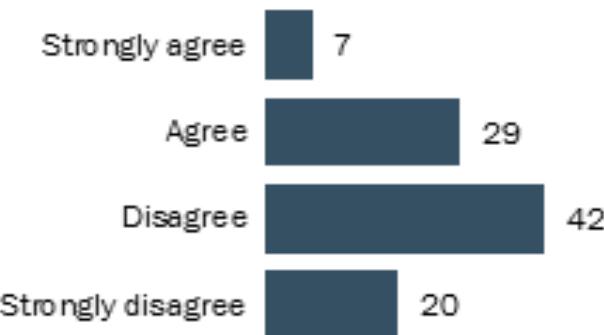
...But Found a Less Concerned Public....



...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.

The Courts Act in 2015....



The court ruling only stops NSA's warrantless surveillance of *American* phone data.

...and the Battleground Shifted...

1-14-20

FEBRUARY 19, 2016 :: LATIMES.COM/BUSINESS

S&P 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



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 approval the devices, Barr said in prepared remarks discussing the government's investigation.

Apple takes heat for locked phones

apple-fbi case pits privacy against national security

How far should encryption go?

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

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 anti-quated 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]

battle lines draw over encryption

tandoff with the FBI has tech firms, consumers weighing the limits of privacy

...and Has Shifted 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:

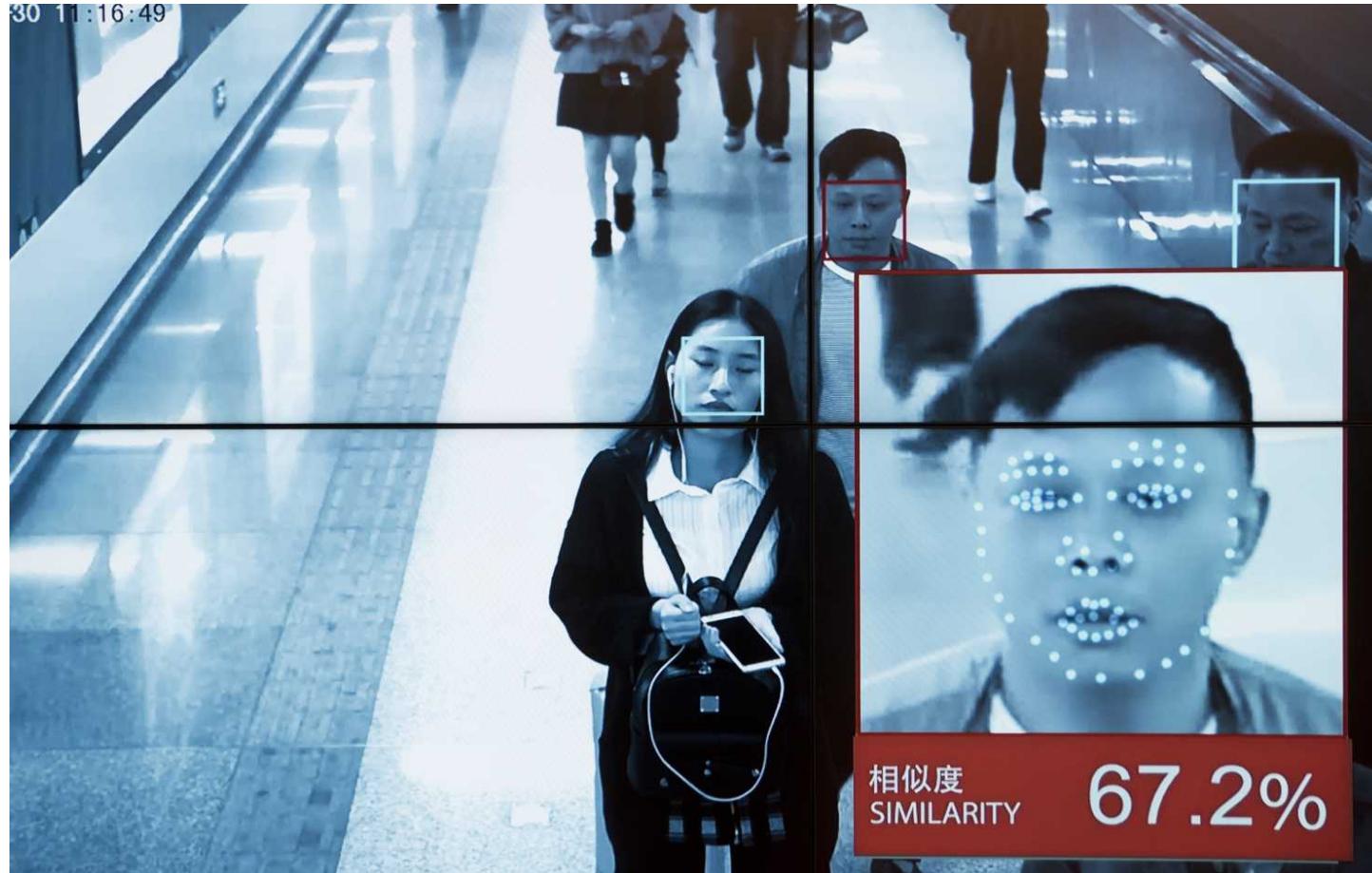
- ▶ Switch on a target's phone camera and microphone
- ▶ Access data on the device

Believed to have been 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

... while Surveillance Expands...



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

...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

...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 per-

sonnel 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 law

[See LAPD, A]

LAPD TECH RAISES PRIVACY WORRIES

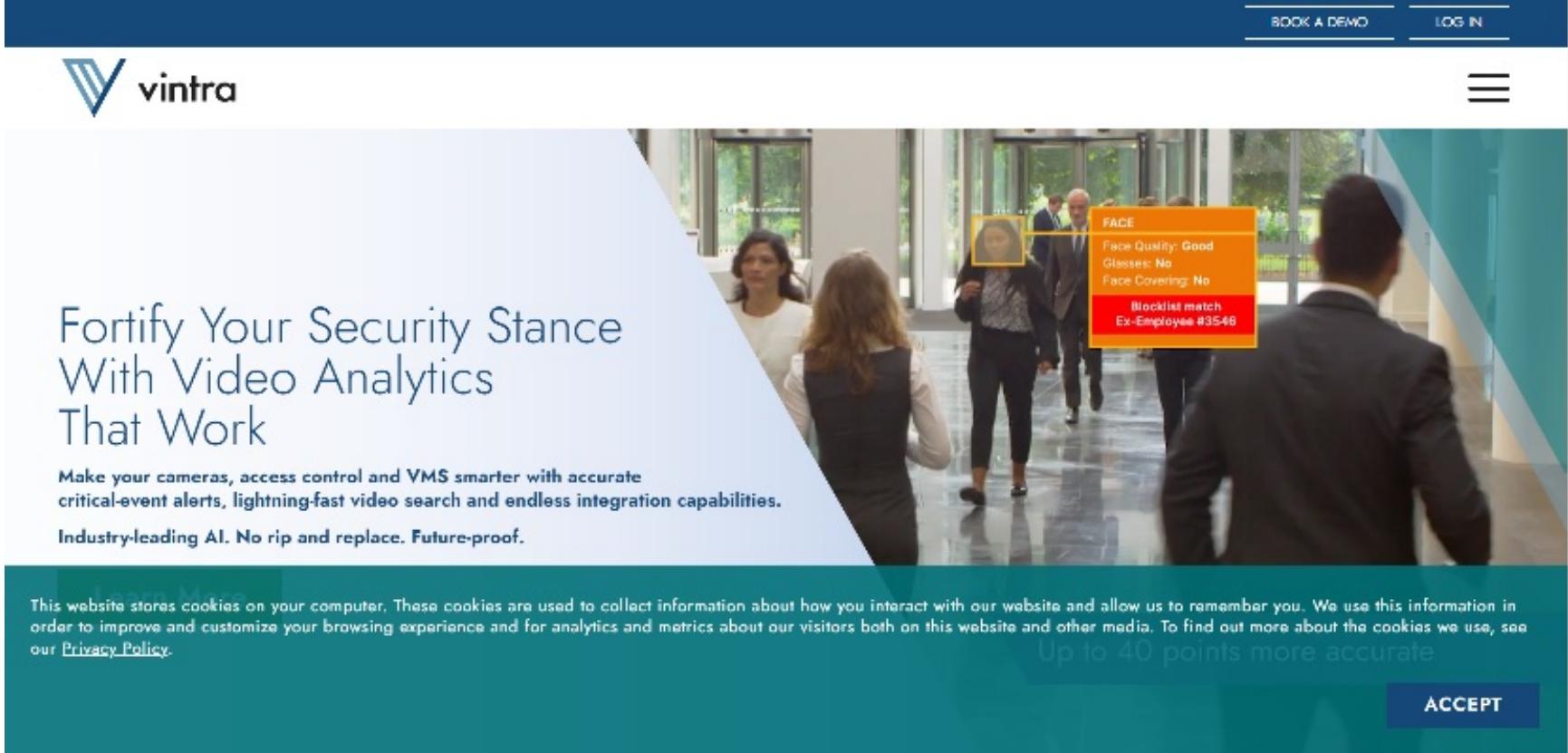
Police Commission will examine use of facial recognition software revealed in a Times report.

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

...Commercial Technologies Enable...



The screenshot shows the Vintra website homepage. At the top right are "BOOK A DEMO" and "LOG IN" buttons. The Vintra logo is on the left, and a menu icon is on the right. The main content area features a large image of a lobby where video analytics are being used to track people. A yellow box highlights a person's face with the text "FACE" and details: "Face Quality: Good", "Glasses: No", "Face Covering: No". Below this, a red box indicates a "Blacklist match" for "Ex-Employee #3546". To the left of the image, there is a white triangle containing text: "Fortify Your Security Stance With Video Analytics That Work". Below this is a paragraph: "Make your cameras, access control and VMS smarter with accurate critical-event alerts, lightning-fast video search and endless integration capabilities. Industry-leading AI. No rip and replace. Future-proof." At the bottom, a teal bar contains a cookie consent message: "This website stores cookies on your computer. These cookies are used to collect information about how you interact with our website and allow us to remember you. We use this information in order to improve and customize your browsing experience and for analytics and metrics about our visitors both on this website and other media. To find out more about the cookies we use, see our Privacy Policy." It also features a "Up to 40 points more accurate" claim and an "ACCEPT" button.

Vintra "...makes AI-powered video analytics solutions that transform video from any camera source into actionable, tailored and trusted intelligence, enabling our customers to build and maintain the safest and most productive organizations in the world." This includes "co-appearance" software to trace a person's contacts.

...Cause Public Concerns...

Despite denial, facial recognition

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 uses the technology. The LAPD tentatively denied related to facial recognition at time the technology was maintained.

The truth does not have recognition personnel have facial recognition through a maintained by the Los Angeles County Sheriff's Department. Nov. 6, 2019, this year used the 29,817 times.

More to come.

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.



Los Angeles Times, September 22&23, 2020

...Create 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.

...But Persist

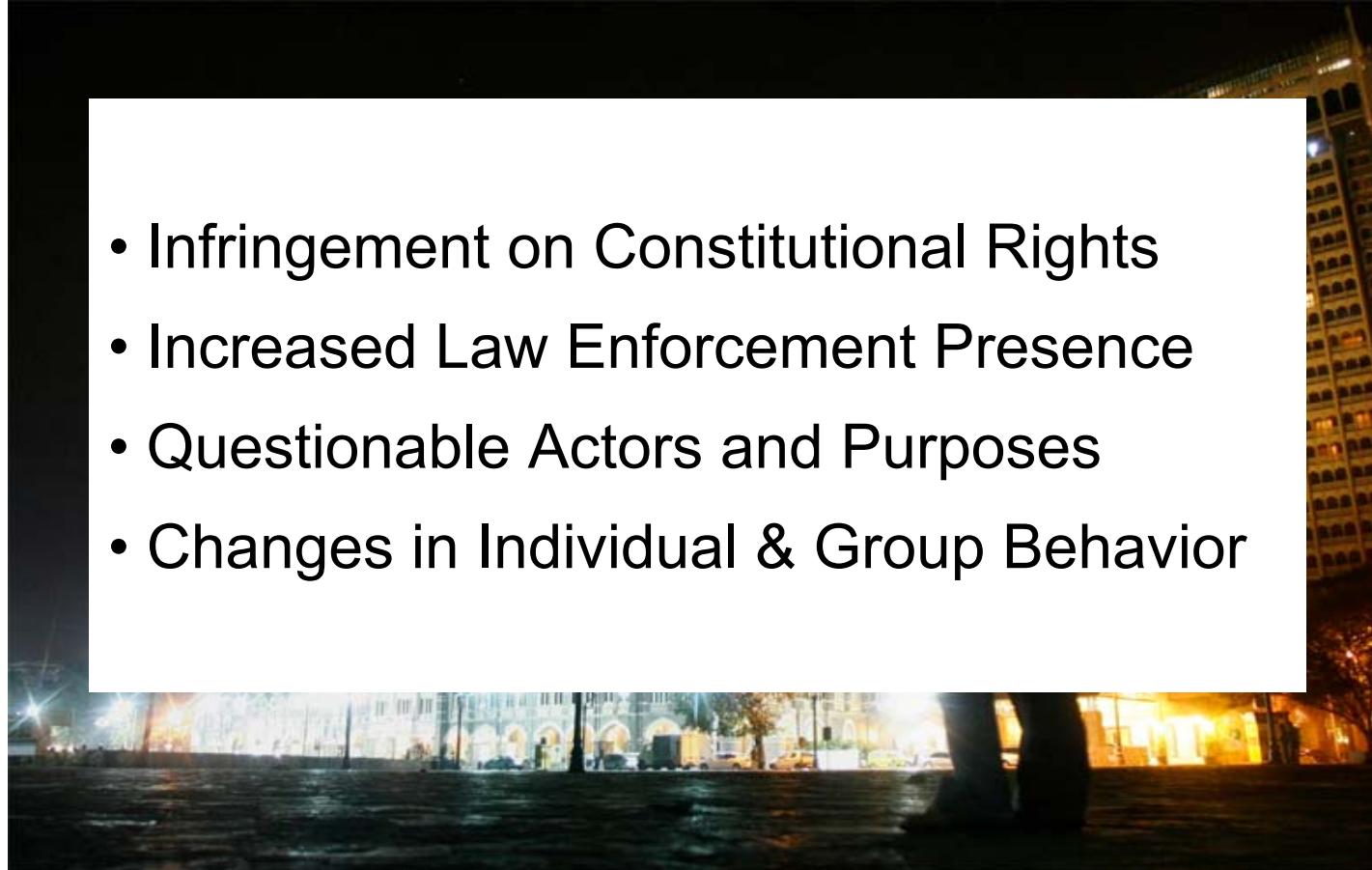


Ethical Analysis

- **Rights and Duties:** Which Prevail?
 - *Individuals' right* to be “secure in their persons” against:
 - Invasion of Privacy
 - Fear of Association
 - Self Incrimination and 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 Reactions Post 9/11
 - 2001 - Patriot Act: Expands Government powers
 - 2007 - Some roll-back of Patriot Act provisions
 - 2008 - Section 702 of Foreign Intelligence Surveillance Act
 - 2009 - New administration brings only small changes
 - 2013 - Snowden revelations on extent of NSA surveillance
 - 2023 - Supreme court declines challenge to 702 surveillance

Societal Issues of Broad Surveillance

- Infringement on Constitutional Rights
- Increased Law Enforcement Presence
- Questionable Actors and Purposes
- Changes in Individual & Group Behavior



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

Public Reaction Against Preemption



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

Public Reaction Against Preemption

LAPD ends data-driven policing program

[LAPD, from B1] raised by commissioners and the public, Rubenstein said. The department still plans to use data tools to fight crime and is "evaluating options" on how to move forward, he said.

LASER, or Los Angeles Strategic Extraction and Restoration zones, used data mapping to increase police presence in hot spots and identify specific "anchor points" such as liquor stores, parking lots and residences connected to certain crimes in an area.

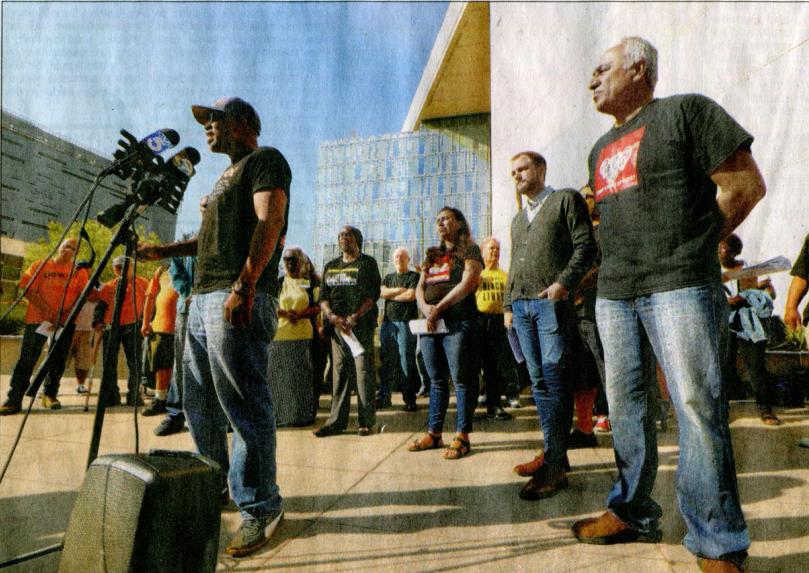
Analysts, not computers, identified where many crimes occurred and where to send more officers.

An inspector general audit released last month described LASER like this:

"The basic premise is to target with laser-like precision the violent repeat offenders and gang members who commit crimes in the specific target area. The program is analogous to laser surgery, where a trained medical doctor uses modern technology to remove tumors or improve eyesight."

But the audit found that the data programs lacked oversight and that officers used inconsistent criteria to label people who were likely to commit violent crimes. It also said the department lacked insufficient data to measure the programs' success.

Commissioner Shane Murphy Goldsmith applauded the LAPD for ending LASER, saying it was a



AL SEIB Los Angeles Times

PETE WHITE of Los Angeles Community Action Network, left, speaks at a protest against LAPD predictive policing programs Tuesday in L.A. as Hamid Khan of the Stop LAPD Spying Coalition, right, watches.

"recognition that the programs have eroded public trust."

"The department absolutely made the right decision," she said. "I absolutely appreciate the members of the community who have raised concerns for a long

time."

The Stop LAPD Spying Coalition hailed the decision Friday. The group sued the city to get more records on how the zones affected residents and homeowners.

A trial is scheduled for August.

"It's a great thing that LASER zones have ended," coalition member Jamie Garcia said. "It was a complete failure to not investigate this program. The fight is not over."

Proponents contend that much of the violent crime occurs in poor communities of color.

But Hamid Khan, another coalition coordinator, said the program led to excessive policing and increased surveillance in poor neighborhoods, adding, "we need to know the impact."

'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 outcry, 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."

The Basic 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.

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?

Information Access: A New Right?

■ People access

■ Chinese internet users employ the blockchain to share a censored news article

By Shannon Liao | @Shannon_Liao | Jul 24, 2018, 2:21pm EDT

f t SHARE



■ Blockchain

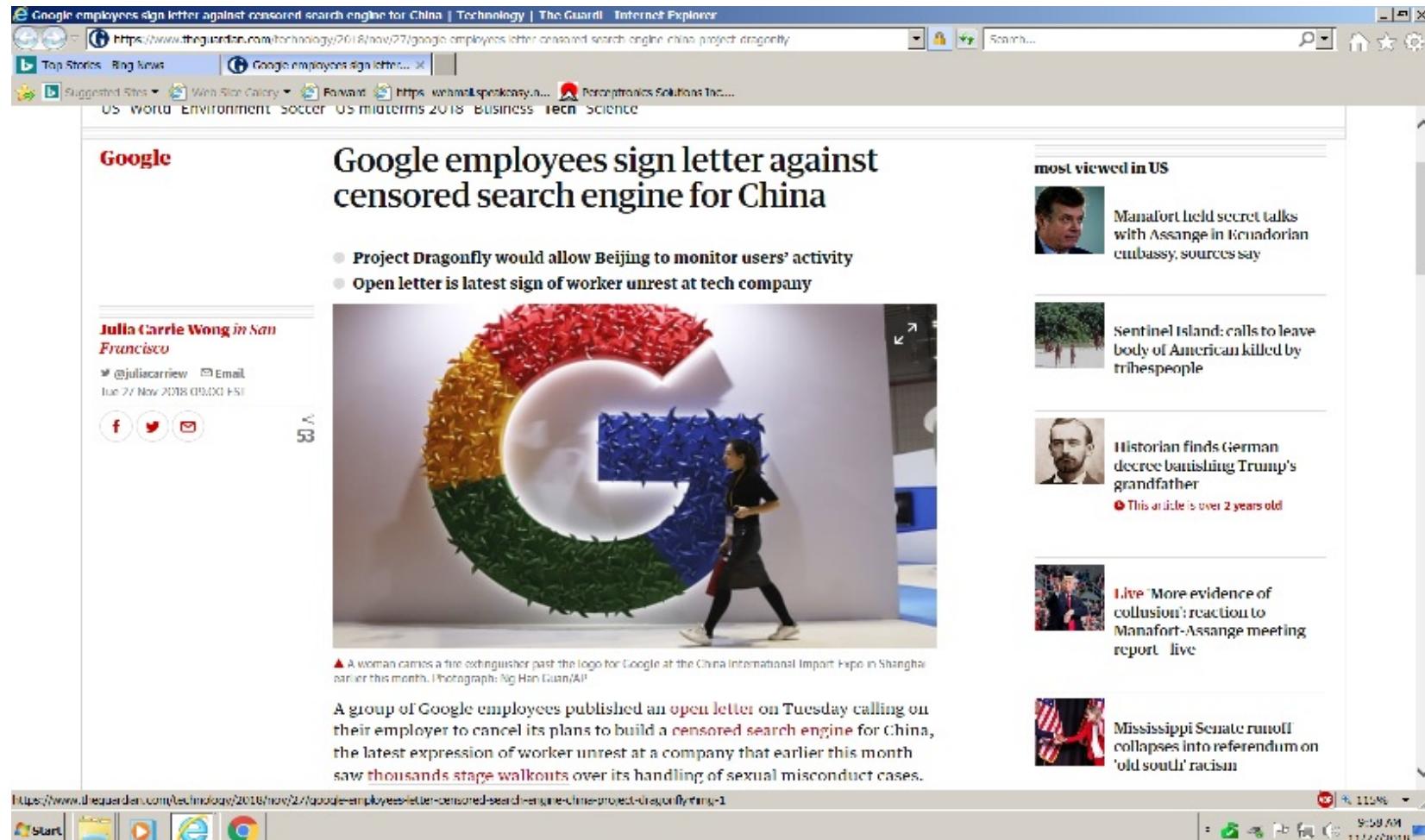
■ Unseen

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

Copyright Gershon Weltman, 2024

89

Information Access: A New Right?



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

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.

<https://www.theguardian.com/technology/2018/nov/27/google-employees-letter-censored-search-engine-china-project-dragonfly-tiny-1>

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

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?

12 Years After, 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

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

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

A Call for Ethical Self-Regulation

Tech needs ethics more than rules

By Mike Godwin

FACEBOOK IS to pay a \$1 billion fine with ongoing corners for privacy lapses, the vision of lies during the delivery of ads in ways along gender and race grapple with these problems to get ahead of the created), Chief Executive Mark Zuckerberg has proposed governments get together some laws and regulations Facebook to follow.

But Zuckerberg is aiming higher. The company just what rules should Facebook follow. The question is what all the tech companies' relationship with society should look like. This needed can't be crunched 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, developed codes of ethics —

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.

— 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

— 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 govern-

ment regulation. (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; it can enable people who care about the internet and its users to identify emerging trends and solutions quickly. None of this will end criticism of big internet companies. When they remove content — either by law or their own policies — they invariably get three reactions: You censor too much! You didn't censor enough! You censored the wrong

stuff. It's better to allow the companies to try to keep such issues from being overrun with national garbage. If we're lucky, 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

Status Quo and Status Futurus

- Data Bases Proliferating and Linking
 - Personal and business – Big Data
 - Institutional and Governmental
- Current Capabilities
 - Tracking known persons - Easy
 - Finding terrorists or criminals - Difficult
 - Acting preemptively – Legal and Ethical Issues
- Current Developments
 - DoD and DHS have been R&D leaders
 - AI Industry may be the new technology leader
 - Government surveillance interests include
 - New “Total Information Awareness”
 - Suspicious patterns of behavior
 - Big Data continues to feed commerce and Government
- Regulation: Industry ethics more than Government laws

Commentators have called today “The Surveillance Society.” Do you think it is?

The Cloud is Really..



Typical Server Room