# TITLE: Your Digital Privacy

**by Howard Fosdick © 2023** 

This is a transcript for the two-hour seminar entitled **"Your Digital Privacy".**

The current version of the accompanying slides are at:

www.RexxInfo.org/Howard_Fosdick_Articles/Privacy_Seminar_Slides.pdf

This transcript is at: www.RexxInfo.org/Howard_Fosdick_Articles/Privacy_Seminar_Transcript.pdf

Contact me via: **webmasterA** at-sign-goes-here **RexxInfo** a-period-goes-here **org**

---

**TITLE: This is Creative Commons licensed...**



---

**TITLE: Who am I ?**

I've been an independent computer consultant for many years.

Hands-on I work as a Database and/or Systems Administrator. I've also done management consulting.

And I enjoy spending time on various projects that interest me, such as writing books, technical articles … and this seminar.

I've studied privacy for decades, and have been involved in many computer projects that relate to matters of privacy and security.

---

**TITLE: Agenda**

Here's the agenda for this seminar.

First we'll define privacy.

Then we'll wander through various technologies and how they impact your privacy. There are far too many technologies to cover them all, so we'll just focus on a handful that surface important privacy principles.

(Let me add that privacy is a vast topic, and I don't pretend to have "the answers." The goal here is to inspire you to do your own research.)

Then we'll talk about government surveillance.

We'll wrap up with my privacy recommendations. These apply to both corporations and governments.

---

**TITLE: What is Privacy?**

The big trend of this century is the way the world has transitioned from analog to digital technologies.

Today all your communications – your emails, texts, tweets, phone and video calls, etc – are digitized.

As are all your purchases, internet activity, streaming entertainment, where you go, and everything else.

And of course, your posts to social media, blogs, forums, and more.

You generate an ***absolute ton*** of digital data every day. It describes you and your life ***in intimate detail***.

**Privacy** is about **who controls all this data about you**. If you control this data, you have privacy.

If it is controlled by others – corporations, governments, or other individuals (like hackers) – you lack privacy.

---

**TITLE: Privacy is Power**

That's a traditional definition of privacy.

What it doesn't make explicit is that **privacy is power.**

Why? Because information is power. Give the correct answers on a test, and you pass. Get detailed information about a job opening prior to your interview, and you're more likely to win the job.

**Privacy is about who controls information about you.** Therefore, privacy is power.

If you control your personal information (or "**PI**"), you have some degree of power. If others control it – if you have no privacy – you've lost that power to others.

This diagram shows that three entities – individuals, governments, and corporations – all require some degree of privacy.

Privacy is an attribute of the relationship between any two of them.

If one party to any such relationship violates or negates the privacy of the other side, they have accumulated some degree of power in that relationship.

---

**TITLE: Privacy is Power**

Here's an example of how privacy is power. Let's say you're negotiating your salary for a new job.

If you lack privacy concerning your salary and your potential new employer knows what it is, you'll rarely be able to negotiate a big salary increase. You leverage is limited because you lack privacy.

On the other hand, if the potential employer knows nothing about your salary, they have to guess what you might accept. Now you have more negotiating power.

Now imagine the inverse situation. You've violated your potential employer's privacy and know exactly what they pay everyone in the department. But they don't know your salary. In this case, you should be able to negotiate a maximum salary increase.

The bottom line is that individuals, corporations, and governments all need some degree of privacy. Otherwise they lack power and become vulnerable to those who have obtained their "private" information.

BTW, you might be interested to know that the salaries of most of you in this room are contained in a database you've probably never heard of called "The Work Number."

Companies contribute your "private" work and salary history to this database, typically without your knowledge or consent. Then other companies use that information against you when you switch jobs and try to negotiate a better salary.

Neat trick, eh? Hard to believe this isn't prosecuted under one of the anti- labor market collusion laws.

(You'll notice links at the bottom of many of my slides. These provide supporting references for facts or claims made in the slides, as well as starting points for your own investigations into these topics. I also recommend useful books by displaying their covers.)

---

**TITLE: Privacy is a Human Right**

Psychologists universally agree that some degree of privacy is necessary for the development and preservation of the self. Without it, you have no *agency* or *autonomy*.

For this reason, organizations like the United Nations, the European Union, and the Organization for Economic Co-operation and Development (OECD), all recognize privacy as a **fundamental human right**.

The United States is an exception. Our foundational documents touch on privacy only in very specific contexts, not as a fundamental human right. We'll see what this means soon.

---

**TITLE: Is Your Privacy Protected From Corporations?**

This slide has been around a while, but it's still accurate.

The countries colored blue and green – virtually all the world's developed nations – have in place decent privacy protections for individuals when they deal with corporations. This group includes the EU, Canada, and Australia.

As you would expect, privacy protections for individuals are lacking in dictatorships like China and Russia. So these countries are colored orange and red.

Now here's what will strike you. While local laws vary, overall the US is orange, too. Instead of giving its citizens the privacy vis-a-vis corporations you see in nearly all other developed nations, individual privacy in the US is much more akin to what you see in countries like China and Russia.

---

**10. TITLE: Why?**

Goodness, how could that be?

The simple answer is that the US recognizes no fundamental privacy right for individuals, unlike other developed nations.

And US laws are a patchwork that do not provide adequate privacy protections.

The result is a huge industry called ***Data Brokering*** that collects, uses, and sells your personal information (**PI**). It's a **$230 billion dollar** per year industry.

Companies have discovered the power in seizing – ***appropriating*** – your personal data. With or without your consent, it doesn't matter.

Why? Because they can leverage the power this gives them to make money. For example, they can use it in targeted advertising, setting prices, tailoring their sales pitches, and the like.

The goal is to gain such an intimate understanding of you that they can manipulate you.

Dr Shoshana Zuboff argues that we've entered the age of ***Surveillance Capitalism***, in which a data "gold rush" is on. Tons of data about you helps companies create very intimate profiles of everything about you. Not only what you buy and wear and do, but who you are. How you think, and your most intimate thoughts.

That power yields profits.

That's *surveillance capitalism*.

---

**TITLE: Is Your Privacy Protected from the Government?**

Here's another aging but accurate slide.

It shows that, as you might expect, many advanced democracies have good or at least adequate privacy protections for their citizens versus their government.

But of course, China and Russia, the world's two great dictatorships, do not. So they're colored red, meaning that they are **"Endemic Surveillance Societies."**

Now, here's a shocker. Two of the world's premier democracies, the US and the UK, are colored red just like China and Russia!

In the US, we give our citizens little more privacy from their government than do the world's two most notorious dictatorships.

One very important distinction needs to be made between the US and the UK.

In the UK, laws were passed through the normal parliamentary processes to approve mass surveillance of the citizenry. So you can look up the various acts of parliament and their debates to understand the general parameters and legal underpinning of government surveillance.

In the US, government surveillance was implemented by our Presidents entirely in secrecy. So it becomes very difficult to figure out exactly what your government is doing.

---

**TITLE: US Government Surveillance**

In the US, mass public surveillance was initiated by the federal government in secret by the executive branch under George W. Bush. Not only the public, but Congress and the Judiciary were kept in the dark about these programs.

Much of the surveillance is conducted by the **NSA** (the **National Security Administration**). The NSA intercepts digitized communications – such as emails, texts, tweets, video calls, VoIP, etc. (We'll get into details later.)

After the Edward Snowden revelations a decade ago, the *Washington Post* tried to get an idea of the size and scope of governmental surveillance. The result appeared in their report called *"Top Secret America."*

Their conclusion was that federal surveillance consisted of a huge conglomeration of budget, technologies, employees, and contractors working on a range of secret projects that are run directly by, and known only to, the executive branch of the federal government.

This is the secret mass surveillance unmasked by Edward Snowden. (And others such as Mark Klein, Russell Tice, William Binney, Thomas Tamm, Thomas Drake, James Risen, Laura Poitras, James Bamford, etc.)

In the words of former NSA director Keith Alexander, the federal government's goal is to *"Collect it all."*

As he explained, *"In order to find the needle in the haystack, you need to collect the whole haystack."*

Hence the mass surveillance and its huge data collection effort.

---

**TITLE: Status**

The *New York Times* launched an investigation similar to the *Washington Post*'s in 2019.

It ultimately concluded that: *"We in the west are building a surveillance state no less totalitarian than the one the Chinese government is rigging up."*

---

**TITLE: How US Surveillance Happened**

Yikes! We're like *China* when it comes to government surveillance? How could that happen?

This slide is highly simplified, but it will at least get you oriented. (We'll fill in more details later.)

In the 1970s, the basic rules for government surveillance were established in response to Watergate and the revelations of the FBI's secret illegal actions against American citizens.

An agreement was struck. A reformed FBI would handle investigations inside the US, while the NSA would restrict its communications intercepts to overseas.

After being caught by surprise by 9/11, the George W Bush administration terminated this arrangement. Leaders like Vice President Cheney claimed that there were **thousands** of al-Qaeda "sleeper agents" in the US, poised to strike and continue the violence of 9/11.

The Bush administration knew this to be true – in spite of a lack of evidence – in the same way that they knew that Iraq had weapons of mass destruction.

And they knew that mass surveillance of American citizens would protect the nation – in spite of a lack of evidence – in the same way that they knew that torture was an important new tool in this effort.

So the Bush administration – without the knowledge or approval of either Congress or the courts – secretly implemented programs of mass surveillance on American citizens.

At one point, in 2003, Bush attempted to legalize his surveillance through his Total Information Awareness proposal. But Congress voted it down. Bush ignored the rejection and continued in secret.

In 2008, candidate Obama ran on a platform of "transparency," saying he would bring unauthorized surveillance under control.

But as President, he did the opposite. He expanded the use of NSA data to many other federal agencies by an executive order.

The result is that we now have programs for government mass surveillance that were first implemented under a perception of terrorist threat that has long since been proven incorrect.

And these systems provide your personal information to many federal agencies that have nothing to do with terrorism.

Which mass surveillance programs are in place a decade after Snowden's reveal? We the public aren't told. It's a safe bet some are operating today.

As we'll explain later, government mass surveillance of the US citizenry is unconstitutional as per the 4th amendment to the US Constitution.

---

**TITLE: Why You are Losing Privacy**

To summarize so far, your entire life – nearly everything you do, communicate, and everywhere you go -- is now digitized.

Governments and corporations gain power by appropriating this data about you. They join together in what some call the ***Surveillance-Industrial Complex.*** The make common cause in seizing information about you to increase their power.

---

**TITLE: Privacy Misconceptions**

Let's wrap up this part of the talk by dispelling some common privacy myths.

***I'm not important, they won't bother with me –***

So why is appropriating and selling your data a $230 billion per year business? They're investing huge sums of money in "bothering" with you because they seek the power your personal data gives them.

The huge amounts of data you generate just by going about your everyday life plus modern computer processing yields this power. And they're taking it.

***They won't notice me, I'll hide in the crowd –***

You can hide from a person in a crowd, but it doesn't work this way with computers. A computer gives the same attention to the billionth record in a database as it does to the first one.

I'm always surprised when I hear programmers promulgate this myth. If you think your personal data can hide in a crowd from a computer, you have a fundamental misunderstanding of how computers work.

***I don't care if they target me for ads –***

This is about **power**. Targeting you for ads is just one possible use of that power. Others include the hacker who stalks you, the Cambridge Analytica scandal that tried to secretly manipulate your vote, the company that uses your data to charge you more for a product that they sell to someone else for less, etc, etc.

***You have no privacy, get over it –***

Scott McNealy, founder of Sun Microsystems, famously said this years ago. Many still believe it today.

It's plain wrong. The EU proves it. They started where we are today, and passed laws that dramatically increased personal privacy.

We can gain back privacy in the US if we want to. It just requires willpower and appropriate law.

***If you have nothing to hide, you have nothing to fear –***

*"Hi, I'm Mark Zuckerberg and these are my friends Elon Musk and Jeff Bezos. Please give us all your most personal information, including your social security number and everything else, so that we can do whatever we want with it."*

*"What? You won't give us all your personal data? What do you have to hide? What's wrong with you? WHAT ARE YOU HIDING? What are you afraid of?"*

Sometimes you'll hear people make this statement to justify government surveillance. *"Trust us,"* they're saying.

Unfortunately, in the US, government surveillance does not operate with adequate oversight. It's not a trustworthy system.

Surveilling citizens without oversight is inimical to democracy.

---

**TITLE: II. Technologies**

Okay, let's discuss a few technologies and how they are used to appropriate your personal information, steal your privacy, and reduce your personal power.

Let me emphasize that no one knows all these technologies in detail... I certainly don't.

The purpose is to inspire you to your own investigations into these topics.

---

**TITLE: Tracking Your Location**

Many devices track your real-time location. They include new cars, wearable devices, license plate readers, and many more.

Cell phones track your location through several technologies. They broadcast your location tens of thousands of times per day (depending on your use of your cell).

The GPS in your cell places you to within an accuracy of about a 16 foot radius. So whoever accesses this data can tell which building you're in, for example.

The photo on this slide shows use of a cell phone location tracking tool by a *Law Enforcement Agency* (or ***LEA***).

There are very few restrictions on who can access your locational data or how they use it.

---

**TITLE: Why Do You Care?**

The reason you should care about your location being tracked is that this information exposes oodles about your life. Much more than you would ever suspect.

Here we introduce the principle of ***Big Data*** (also known as *Data Aggregation*).

(Throughout this talk, I'll put important principles like Big Data inside tan boxes to emphasize them.)

Big Data says that even though we have but a single data point – your location – if we collect enough of these data points, modern algorithms can figure out all sorts of things from this data you would never imagine.

The blue box lists just some of the things the users of your location data can deduce about you and your life.

Take the first item in the list. How could just your location disclose if you're gay, for example?

Well, the algorithm could see if you attended the Gay Pride parade. It could see if you frequent social clubs or bars known to favor gay patrons. It could determine if you attend a gay-friendly or anti-gay church. It could see where your cell sleeps every night, and if it's co-located with a cell owned by another person thought to be gay.

See what I mean? With millions upon millions of data points – even if it's but a single item like your location – modern algorithms can decode your life.

I have a gay acquaintance who lives in a community in Texas who doesn't want his sexual orientation known. He's a minor. He feels he could suffer physical abuse if others knew he is gay. Shouldn't he be able to keep this information private? Shouldn't that be **his** decision?

In today's America, it's not. Companies can collect and disseminate this personal data without restriction. Our lack of a fundamental right to privacy means that your private life is available to any company or government agency willing to buy it.

Data collectors called ***Data Brokers*** specialize in selling all your personal info. They don't care how personal that information seems to you. Or if you object to their selling it. That's too bad for you.

The basic question we face is: do we want private lives? Or do we want corporations to appropriate and sell them?

So far, our nation has chosen the latter.

---

**20. TITLE: Tracking You: Facial Recognition**

Facial recognition – or "**FR**" – could also be used to track you. It has other uses, too.

FR starts with a massive database of facial photos. The photos are then compared to individuals for matches.

As shown by the blue boxes in this slide, the simplest form of FR is **static comparison**. The subject stands still, and his or her face is matched against photos in the FR database. You might see static FR used at an airport check-in, for example.

More complicated is **real-time FR**. This tries to identify individual subjects who are moving or in a crowd. For example, it could be used to identify people attending a political rally. Real-time FR makes **lots** of errors with current technology.

The ultimate goal is ***Video Analytics***. This is where the computer derives conclusions about the subject using FR. In the case of the photo of the young lady you see here, the algorithm has determined that the woman is happy, based on her facial status. Video analytics is just in its infancy.

You might ask: where do they get the photos to create the huge FR databases needed to make this work?

The answer is that companies and governments *appropriate* your photos (typically without your knowledge or permission).

They get them from government IDs like passports, government badges, and military records. Also, the internet and social media posts, and of course from those states that still sell drivers license information.

For example, a company called Clearview AI grabbed 30 billion facial photos from such sources and sold them to everyone in sight.

Whoa! Is all that legal?

Yes. The principle we're talking about here is ***Data Cross-use***.

Cross-use is where data is collected for one purpose, then used for others.

For example, of course you must pose for a state drivers license, government ID, military ID, or employee badge. But did you know that that data may then be used for other – completed unrelated – purposes as well?

Well, that's data cross-use. One big reason we have so little privacy in the US is that data cross-use is so widely practiced.

Companies and governments collect your PI for perfectly valid, legitimate reasons. But then they misuse it in a thousand unrelated ways. That's cross-use.

What about future use of your PI? Data others collect about you for legitimate reasons today could be used in the future for purposes absolutely no one can foresee today, even those who collect it.

This is another reason corporations and governments are so eager to collect all your personal information.

---

**TITLE: (1) Over-collection (2) Cross-use (3) Ineffective Laws**

This slide emphasizes three key principles.

To discuss them, we'll use the example of your drivers license. It contains lots of your vital PI.

These include your *biometrics* – your physical characteristics. Including your photo and signature. Plus your home address. And also your unique ID numbers for Real ID and your state Drivers License Number.

That's great information for any hacker or stalker! And just as useful to corporations and governments.

One big way you lose privacy is through ***Data Over-collection***. Bars, for example, have a legitimate need to see your license to check your birth date.

But many of them insist on scanning your license. They use their legitimate need to verify your age as an excuse to over-collect data. You're forced to give up all the other valuable PI on your license by this tactic.

Same thing happens when you return an item at many major retail stores, or when you check into a hotel, or when you mail an express package. Corporations scan your license and over-collect your PI at every opportunity.

You'll notice that none of those organizations hands you a Privacy Policy when they scan your license.

So by the principle of cross-use, your license PI can sold and used for all sorts of other purposes. Most will have nothing at all to do with the original reason they demanded to "see" your drivers license.

Who knows if your PI will be stored securely? Who knows who will buy it, or how they will use it?

You have no power in the situation. Your lack of privacy makes you vulnerable.

You'd think there would be a law to protect us, wouldn't you?

Well, there's the *Drivers Privacy Protection Act of 1994*, amended in 2020. Like most of our privacy laws, it's easy to circumvent and provides little protection. We'll go into more detail about why our "privacy" laws are so ineffective later.

---

**TITLE: 5 Principles**

The way privacy works in the US is like this.

The more you give out your PI, the greater the chances harm will come to you because of that.

Yet rarely do you have the power to refuse to divulge your PI.

Then your data gets fed into the *data brokerage* business and it gets spread it all over the place.

When harm comes to you because of the loss or misuse of your PI, you have no way to trace that harm to how it happened. The entire system is opaque to you.

This is why so many people don't understand the importance of privacy. They can't trace the harms they suffer because of their lack of privacy to its causes.

---

**TITLE: Public Surveillance – Ring**

Okay. Time to discuss another privacy-invading technology.

They're called "doorbell cameras", but most I've seen surveil a good deal more than your doorstep. As the photo shows, many monitor the street outside and even houses on the other side.

Amazon's Ring links to its Neighbors app. And the company conducts a nationwide program in which they've enrolled thousands of police forces to promote and use the product.

That's great for Amazon, and it's fantastic for law enforcement agencies (LEAs). How else could they build a nationwide network of surveillance cameras?

Laws vary by locality, but I've never heard of a single case where an LEA couldn't get a hold of Ring surveillance recordings when they wanted to. Ring is effectively a government surveillance network.

Expect Ring and its competitors to eventually add FR and video analytics to their products.

---

**TITLE: Public Surveillance – More**

There is one public surveillance camera for every four Americans. (Add in cell phones, and the ratio is way higher.) And, the surveillance network is rapidly growing.

Cameras are at homes, corporations, and public venues. Over 90% of high and middle schools use them.

We're building a comprehensive public surveillance network.

With little public recognition of this fact. And no public debate.

With full LEA and government access to the network.

The irony is that, if you asked Americans if they thought it would be a good idea to have all public spaces monitored by the government or the police, they'd probably say "no".

But that's exactly what we're doing.

It's a little like cell phones. Tell the average American to wear a government tracking device, and he'd say "no."

Disguise it in the form of a cell phone, and he'll loyally carry it everywhere.

---

**TITLE: The "Gorgon Stare" – Mass Aerial Surveillance**

Here's another surveillance technology you've probably never heard of.

The *Gorgon Stare* was developed for our military use in the Mideast wars. Like many of those technologies, it's been brought home for use on American civilians.

The technology allows a single airborne vehicle to surveil **an entire city.** Down to the resolution of an individual license plate.

It's been used on an experimental basis over several American cities without notifying the public. And without public debate.

There is no evidence the Gorgon Stare reduces crime, nor has there been any kind of community input.

The book *Eyes in the Sky* tells you more.

---

**TITLE: Why Don't Courts Protect Privacy?**

By now you're probably wondering: Don't the courts protect my privacy?

Shouldn't they be doing that?

The US judicial system puts great emphasis on *precedents* – prior judicial decisions.

Unfortunately, some major judicial precedents concerning privacy date from the 1960s and 1970s, well before modern technology. These decisions make little sense today, yet their dead hand hovers over us all.

One precedent is that **"You have no expectation of privacy in a public place."**

That made sense with 1960s technology. But not today.

This precedent legalizes public surveillance through such personal tracking technologies such as cell phones and license plate readers. And facial recognition and the Gorgon Stare.

Today I'd rephrase this precedent to ask: **Do we live in a free society when we are required to submit to comprehensive surveillance?**

Another old precedent is called the ***3rd Party Doctrine***. It states that once you give out your data, you lose any control over it.

This made sense fifty years ago, but today it means there are few limits on use of your personal information. It forms the basis of today's $230 billion data brokering business, permits data cross-use, and guarantees your loss of privacy.

Lastly there is the 4th amendment to the US Constitution. It forbids mass government surveillance of US citizens, because it requires a *specific warrant* to search specific citizens.

A special court called the FISA court killed the 4th amendment. We'll discuss this in detail later.

---

**TITLE: FAIL! US Privacy Laws**

Now, there have been thousands of laws passed since those old judicial precedents. So obviously I'm vastly simplifying the situation!

So let's talk for a few minutes about US privacy laws. This slide enumerates some of the most important federal privacy laws.

One key point is how we pass privacy laws.

Since the US does not recognize a fundamental right to privacy, our privacy laws tend to address specific situations as they arise.

In other words, a "privacy scandal" gets publicized, the public gets worked over it, and our legislators then pass a law to "fix it."

The trouble is that these laws are topic-specific. They apply only narrowly to the situation that caused the public furor.

As a result, often they can easily be circumvented. And as technology advances, their value is compromised over time.

Take the first law on the list as an example: HIPAA. We all know that **"HIPAA protects our personal medical data"**, right?

Actually, no. HIPAA imposes privacy restrictions on only "covered entities": *medical insurers, medical providers,* and *companies that directly service them*.

HIPAA does not apply at all to any other companies.

So, we go to our doctor or hospital and we see that they take HIPAA very seriously, and try to protect our medical PI, just as the law requires.

But that doesn't stop corporate collection of your medical data.

Here's an example. Let's say you develop type 2 diabetes and you don't want potential future employers to know. You buy some test strips on the web.

Well, the company you bought the test strips from now knows about your condition. As does the issuing company for the credit or debit card by which you paid. As does the email service through which you got your sales confirmation. As may your internet service provider through which you make your web connection.

HIPAA does **not** apply to any of these companies. All are free to sell info about your diabetic condition to anyone, including potential future employers.

The link on the slide provides an article that tells how an entire industry has evolved to circumvent HIPAA and collect your medical PI.

Welcome to the world of American privacy law.

I could tell you how companies and governments circumvent **every law listed on this slide**. I'm not exaggerating. This is how it works.

Later, I'll tell how we can alter our country's fundamental bias in favor of privacy in the recommendations at the end of this seminar.

---

**TITLE: The Internet: Surveillance is it's Business Model**

Okay, let's get back to surveillance technologies.

Here's one you use every day: the internet.

As privacy expert Bruce Schneier states, ***"Surveillance is the business model of the internet."***

Everything you do on the internet, from your searches to your posts, from your web surfing behavior to your communications, is tracked. The internet is a surveillance machine.

Your loss of privacy is huge, and those taking it intend to know you *intimately*.

---

**TITLE: Tracking You: 3 Hours Online**

Here's what tracking you on the internet looks like. This map shows all the tracking that can occur when you're online for only 3 hours and 20 minutes.

Each circle in the diagram is an event, and every dot is a tracker.

Imagine how much data companies gather from you over the space of a year!

---

**30. TITLE: Use VPNs or TOR for Privacy**

How do you stop all this tracking?

You can't. But you can minimize it.

First off, don't be logged into any service while you web surf (eg, Facebook, Google, Microsoft, Yahoo, Apple, Amazon, Disqus ...).

Second, use a *Virtual Private Network* or ***VPN***.

Your internet service provider (ISP) sees **everything** you do on the internet. After all, your connection to the web goes through them. Some – such as AT&T – sell this data. It provides a comprehensive picture of who you are and what you're about.

With a VPN, your computer connects to the VPN, which then connects to the websites you actually want to get to. So all your connections go through the VPN. And they're all encrypted.

This gives you privacy and security. **I believe everyone should use a VPN**.

Select a VPN you trust not to look at your data, and that will not slow down your connections.

Those with more expertise or special needs might look at using *TOR*. TOR – or *The Onion Ring* – is a free computer browser designed to protect your privacy.

The diagram shows how it works. By routing your connection through a random series of servers, it provides you with privacy and anonymity. TOR is sometimes slower than VPNs because it passes you through those extra servers.

Neither TOR nor VPNs can protect your anonymity from an "*omniscient surveillor*" like the NSA.

---

**TITLE: What Do They Know About You?**

So, from all this tracking, what do they know about you?

It all depends on your how you interact with the web.

For those who log in to Google during their web session, this slide lists all the things Google knows about you.

That's rather breath-taking, isn't it?

---

**TITLE: What Do They Know About You?**

Here's what I ask you to do after this seminar. If you normally log in to Facebook or Google, go see how much data they've collected on you.

I've supplied the URLs to do that in this slide.

You'll be stunned – absolutely floored – when you see how much data they've collected about you. It's more intimate than if you kept a *very thorough* diary.

They might well have stored hundreds of gigabytes of data on you. (How much depends on your behavior and how long you've used your Facebook or Google login.)

For comparison, a few hundred gigabytes is how much data was required to run an *entire* Fortune-500 company 30 years ago.

Now they have that much data **just on you!**

(Keep in mind, you're only allowed to see the ***raw data*** they've compiled on you… not the analysis or profiles they've created about you. After all, that's **their** private data, upon which decisions are made about **your** life!)

---

**TITLE: Emails and Texts Could Expose Your Life**

Emails and texts are two more privacy-challenged technologies.

Many people unthinkingly send their most personal financial and medical data by email. So these are useful for harvesting that data.

People send their most personal thoughts and emotions via texts. So companies scan these to build their profiles of how you act and think.

When an email is sent across the web, it's broken up into data units called *packets*. These are sent from sender to recipient through a series of random servers.

Ten or twenty years ago, nearly all emails were unencrypted (or sent in ***clear text***). They could be read by anybody who could intercept them.

Today the majority of emails travel by way of encrypted communications tunnels. But the emails themselves are **not** encrypted. So they are protected when "in transit" via communications, but could be read when "at rest" at servers.

This is today's default for personal Gmail and Outlook emails.

To address this shortcoming, you want full **end-to-end encryption** of your emails (called **E2EE**). The trouble is that there is no universally compatible way to do this, so the burden is on you to figure it out.

Some possible solutions are:
- – Use the advanced/optional E2EE features of Gmail or Outlook
- – Use an E2EE browser extension to protect your emails (like Mailvelope)
- – Switch to an email service that promises E2EE by default (like Proton Mail)

The ultimate solution is for vendors to agree to a common standard so that everyone could communicate using E2EE **regardless of which email product they use**. This would remove the burden of figuring out E2EE from you. We need this solution for both emailing and texting.

For texts, most recommend **Signal** as the best E2EE solution. Telegram E2EE encrypts if you enable it.

Standard SMS text messages are **not** encrypted. Apps like WhatsApp, Facebook Messenger, Instagram, and SnapChat encrypt E2EE under most – but not all – circumstances. If you use them, please read current info on how to use their encryption.

---

**TITLE: How to Stop Their Tracking**

So far, we've discussed a range of tracking technologies and techniques.

People often ask how to avoid them.

Hence, this slide.

There's too much to talk through here, so if you're interested, you can review this slide later.

Meanwhile, here's a conclusion. There's no way you can achieve privacy on your own in today's world, no matter how much you expertise you have, or how hard you work at it.

We need a societal solution – that is, a fundamental right of privacy. And enabling laws on top of that. More on that later.

---

**TITLE: Device Fingerprinting**

Companies are well aware that there are some folks who fight back against corporate efforts to appropriate their privacy.

They need ways to track you *without your knowing.*

Here's a good one: ***device fingerprinting***.

With **DF**, programs interrogate your computer or cell phone and collect a list of its software and hardware characteristics.

Take together, all these parameters define a ***device fingerprint***. The chart shows what level of uniqueness DF provides for different configurations.

Combined with other techniques, DF can be powerful in identifying you without you knowing.

Another clever way to identify and track you without your knowing is to secretly collect your biometrics (physical characteristics). Companies could monitor your unique typing style, for example.

---

**TITLE: Shadow Profiles**

How about all those who defend their privacy by not logging into Facebook or Google? And who insist on *informed consent* before giving away their privacy?

For them, companies like Facebook create ***shadow profiles***.

Companies build their shadow profile of you through your contacts with those they can track. Plus from purchased data and data combined from other sources.

Even if you've never logged into Facebook, you can bet they've built an extensive profile of you anyway. Your very own shadow profile.

---

**TITLE: The Secret Life of Your iPhone**

You may have heard that iPhones are "much more private" than other phones.

Well, this slide is based on a *Washington Post* article where a reporter saw that his iPhone was *exfiltrating* – or sending out – his personal data **all night long.**

How could *that* happen?

The blue boxes show that privacy-killing software can be installed at any of five different levels on your cell phone.

**Apps** are the most common offenders. Those technologies lower in the chain are harder to defeat (you can't just uninstall your carrier or your cell firmware, like you can an app.)

Generally speaking, installing fewer apps enhances your privacy. But that's hardly realistic. We need a societal agreement to protect your privacy when using a cell.

---

**TITLE: Apps and Browser Extensions Steal Your Privacy**

When you install a cell phone app or a browser extension on your PC, they hit you up with a "Privacy Panel" to ask permission to collect your data.

As a privacy mechanism, these panels are of little value. Look at those shown in this slide. Do they actually give you the information you need to know about what will happen to your private data if you click Install?

Nope.

It gets *much* worse news. Over the years, studies have shown that thousands of apps just plain lie about the data they collect. Even with Apple's "*Ask App Not to Track"* panel!

The whole thing is a sham. It's "privacy theater," a farce designed to give you the illusion of privacy.

The solution is to pass laws that remove this unrealistic privacy burden from the consumer, and place it squarely on the corporations and software vendors where it belongs.

This requires an enforcement mechanism, and sufficient penalties to make it stick.

---

**TITLE: The "Data Brokering" Industry**

So where does all that data corporations collect on you go?

*Data Brokering* is the $230 billion dollar industry that collects and sells your data.

It's largely unregulated. Though brokers often claim to sell your PI only to "qualified buyers," that's bunk. They have no way of knowing what happens to your PI once they've sold it.

Data of the most personal kinds can be purchased. Just look at this list.

A bad guy could buy data on police officers, rape victims, confused seniors, or defenseless children. Any harm that could result is not a consideration to the data broker industry.

Our government is a major data buyer. This allows them to circumvent laws that prevent them from collecting data on US citizens. Nice dodge, eh? They don't violate the law by collecting your personal data. Instead, they just rent access to it.

The solution to all this is laws that impose obligations on data collectors, sellers, and buyers. In short, impose regulation on the data brokering industry.

The EU's *General Data Privacy Regulation* (*GDPR*) and the US government report *"A Call for Transparency and Accountability"* are good places to start. We'll discuss them later.

---

**40. TITLE: The Bogus "Consent" Industry**

Corporations that destroy your privacy claim, *"Wait a minute, you're consenting to all this! You people voluntarily hand over your PI. We provide privacy agreements* ***that you've signed!****"*

Baloney.

In few cases do the public voluntarily provide informed consent. Only **informed consent** truly respects the right to individual privacy.

Two slides ago, we saw how apps and browser extensions appropriate your privacy through the sham mechanism of "privacy panels." Studies have shown that many companies just plain lie about their data collection. And there's no system in place to prevent this.

There's more. You know those "privacy agreements" you're often confronted with? The ones designed by lawyers and written in small type, that you're constantly forced to agree to?

Many do not bind those who give them to you at all! Just scan for words like "alter" or "change" or "update" and you'll see that many agreements say that they issuer has the right to alter the terms at any time.

That's not a contract at all! It's "data appropriation agreement," not a "privacy agreement."

Many companies force you to sign away your privacy under time pressure. For example, you scheduled your knee operation months ago, and now, just before they wheel you in to the operating room at the hospital, they present you with a pile of "consent forms."

How could you not sign them? What kind of consent is that?

Similarly, in today's America, many industries are dominated by just a couple suppliers. You have to sign their agreements to get service.

For example, according to the *FCC's National Broadband Map*, the majority of Americans have only one or two internet service providers (ISPs) they can select from.

So, what choice does the public have when it comes to agreeing to whatever privacy agreement their ISP forces upon them?

Because the US has declined to enforce anti-trust law for four decades, many industries are now dominated by two or three large companies. So you often have little choice. You're forced to sign whatever data use agreement they shove at you.

And then there are ***Dark Patterns***. Dark patterns are computer interfaces or wording purposely designed to fool you.

The average “privacy agreement” is a dark pattern to most of us.

Back in the 1970s, our society came to a consensus that **informed consent** was our goal. Today, by any measure, the goal of most corporations is to avoid that. The techniques listed on this slide are just a few of the many they employ.

The best solution is to make **Opt-out** the legal default. By default your data will not be sold or shared. And then we must get rid of these techniques used to trick you or force your “consent.”

Ultimately, we must shift the burden of “consent” from helpless consumers to privacy rules for the corporations and governments that appropriate their personal data.

---

**TITLE: The “Software Tools” Scandal**

The recent “software tools” scandal is a great example of how privacy works in America.

Over the past couple years we’ve been treated to a barrage of exposés that detail how hospitals, pharmacies, banks, tax preparation firms, and government agencies have been sharing your most personal data with companies like Facebook/Meta and Google/Alphabet Inc.

This directly violates laws like HIPAA and the GLBA financial data privacy act.

How could this happen?

Well, when most companies write code for their websites they use software tools to help them do this.

Facebook/Meta eagerly supplies a tool called *Meta Pixel*. This code can collect your PI from the website into which it’s embedded.

So hospitals and banks that sincerely intend to protect your personal data find it appropriated by Facebook.

Meta gives hospitals and banks the same kinds of bogus consent forms they do to you and me. So many sincere law-abiding institutions are duped into sending your data to Meta. Many didn’t even realize they were doing it.

Who’s at fault? Dozens of lawsuits are right now deciding that. Meta claims that the companies that used their Pixel tool voluntarily signed “privacy” agreements. They claim the companies who used their tools are at fault. The companies respond by claiming they were duped.

This is typical of how privacy works in America.

Here’s another example. We’ve all run into the CAPTCHA panels that try to verify that you are human. Companies use this to ensure that internet scanning programs don’t harass or rip-off their websites.

Google/Alphabet has supplied several versions of their CAPTCHA tool to many millions of websites.

What you might not know is that this tool enables Google to capture your personal data from those websites, similar to Meta Pixel.

Google can collect your device fingerprint, your personal behavior in interacting with the website, and more. Some versions captured a screenshot. This is a **huge** privacy and security exposure if that screen contains sensitive PI.

I visited one state police website where the CAPTCHA took a screen print that included your login, your social security number, your drivers license number, and more.

I highly doubt that the state police did this on purpose or understood the security risk at which they were putting their users.

Did Google even know they collected this sensitive information? Did they encrypt when they stored it? Doubtful.

Legislation with teeth is the only solution to these scandals. Not the patchwork of ersatz laws we have today.

---

**TITLE: Bubbles (of Data Breaches)**

Each of these bubbles represents a data breach.

A group called the Privacy Rights Clearinghouse tracks them. They offer a wealth of background on the scope of the problem and why it occurs. (They are also your best single resource for information on data brokers.)

Something over 13 **billion** records have been lost since 2005.

In 2022 alone, there were over 1,800 breaches that impacted the privacy of 422 million people, according to Statista. There are 1.9 breaches of health PI **per day**.

Investigating data breaches shows that – even today – **many** of these breaches could have **easily** been avoided.

**In many cases, the companies didn't even encrypt your personal data!** Companies are often not under any legal obligation to do so, so they don't. Just a single law addressing that one exposure could greatly reduce this problem.

---

**TITLE: Data Breach**

A ***Data Breach*** is where a company or government appropriates your data – then they lose it!

Companies are often fined over this, but it's really **you** who pays the price.

The law requires companies to report data breaches. But the hard fact is, sometimes they don't even know when they've lost your data.

Sometimes companies don't keep a good inventory of your PI, or they don't log access to it so they can't trace if or when a hack occurs.

Companies that store your personal data should be required by law to follow certain security and privacy standards. For example, **data encryption** and **logging**. Limits on cross-use and sales should apply. There should be regulations to prevent over-collection, and for the deletion of aging data. And lots more we'll go into later.

**Data breaches continue to multiply because we have not taken even the most basic steps to counteract them.**

Criminal organizations and potentially hostile states like Russia and China just love our inaction on this issue.

---

**TITLE: Equifax Lost PI of 147 Million**

In a single breach, Equifax – one of the Big Three credit companies -- lost the PI of 147 million Americans. The data included social security, credit card, and drivers license numbers for most.

How did Equifax respond? They gave the victims a limited-time subscription to a personal data monitoring service **that they own.** Yes, Equifax saw the loss of your PI as a marketing opportunity!

If you go to check if your PI was compromised by the breach, you'll see that Equifax asks for your social security number. They see the loss of your PI as an opportunity to verify SSNs.

In an FTC settlement, Equifax was forced to commit "up to" $425 million to help people recover from the damage they caused.

A mere fine is not a solution to the problem of data breaches and will not prevent them. We need laws that require secure storage and management of your PI.

---

**TITLE: Identify Theft**

With corporations largely free to be irresponsible with your PI, it's not surprising that identity theft cases continue to increase.

As we'll talk about in the "Recommendations" portion of this seminar, **solutions are well known and have been proven useful in other countries. But we haven't adopted them here.**

Meanwhile, *you* pay the price for corporate misbehavior.

---

**TITLE: Biometrics**

*Biometrics* are your physical characteristics.

Some are relatively easy to change, such as your hair color, or your eye color (by colored contact lenses).

Others are very difficult to change, such as your face.

And others are impossible to change, such as your DNA. (This is why the US government built a database that contains the DNA of every American, according to a former NSA director.)

Many see biometrics as the ultimate in personal identification, so corporations and governments appropriate them whenever possible.

The federal law called GINA prevents discrimination based on your DNA in *only two areas*: health insurance and employment. GINA is of minimal value.

Illinois passed a much more stringent law called BIPA. It's a good template for a more effective anti-discrimination law.

---

**TITLE: Anonymity**

If you've ever given your DNA to one of those ancestry DNA firms, doubtless they allayed your privacy concerns by saying that they only sell your data after anonymizing it.

But data anonymization processes vary in effectiveness (just like passwords do).

In fact, almost any anonymized data can be de-anonymized, according to the *Harvard Business Review.*

So how did the government build their DNA database of all Americans?

Maybe from the ancestry DNA firms… maybe from hospitals or blood testing firms because you signed a waiver about removed "body parts"… maybe from your military or government required physical… maybe from that envelope you licked before you sent it in… maybe from….

Your personal data is incredibly valuable. Corporations and governments appropriate it through all possible means.

---

**TITLE: K to 12 Panopticon ...**

Our school systems monitor children in every way imaginable. We're training them to submit to comprehensive life-long monitoring.

Over 90% of high and middle schools monitor kids through surveillance cameras, for example. Expect FR soon.

Many schools monitor childrens' social media posts, their writing assignments (for plagiarism), their internet interactions, and everything they type into their laptops.

The schools don't do this themselves, of course. They outsource it all to private companies. These private companies thus collect and store tons of the most personal information about our children.

Do privacy policies adequately protect the kids?

You'd have to an expert in contract law to know. It varies in every school district.

What is clear is that we've contracted out 24 by 7 monitoring of our children to private companies.

Will this personal data follow kids around for the rest of their lives?

Some think that's a great idea. See the diagram from the Western Interstate Commission of Higher Education.

We're raising a generation under constant surveillance. By age 18 most children have never typed a private thought.

Welcome to your future.

(Or if you're a kid, your present.)

One solution is voluntary nationally-recommended ***standards for Ed Tech privacy***, as argued in this study. Some say we have them. I'd argue that, if we do, they are not working. Nor are FERPA and COPPA.

*Privacy licensing bodies and procedures* are another option.

---

**TITLE: Your Shopping Experience**

This slide shows how one company, the giant foodstore chain Kroger, collects, compiles, analyzes, and sells your data.

As shown, their activities go ***way beyond*** your purchases. Shopping data is combined with tons of other PI from multiple sources and then sold to 1,400 purchasers.

All this occurs without your knowledge or consent.

Grocery chain Kroger owns *84.51*, *Kroger Personal Finance*, and *Kroger Precision Marketing* as part of this effort.

So what you might consider a typical consumer chain is deeply involved in selling your data.

---

**50. TITLE: Employer Surveillance**

In most states, as long as it's in the Employee Handbook, employers can monitor you however they like.

Many studies show that some small amount of surveillance can help achieve corporate goals. But too much is often counter-productive.

The problem is that our employment and our private lives often intersect.

Did you order your holiday presents using the corporate laptop? Do you use your corporate-issued phone for an occasional private conversation?

Something more sophisticated than a statement in the Employee Handbook is needed to sort this out. Employees deserve a right to a private life.

---

**TITLE: Wearables – Let's Monitor Your Body!**

Here's another way companies get around that pesky HIPAA law.

Why not just have the subjects collect the data for you? Unless you're a health care insurer or provider, HIPAA does not apply to your company.

Wearable watches, activity trackers, exercise monitors, and other devices aid in this effort.

The trouble for **you** is, as always, you have no idea where your PI is going or how it will be used.

And what about future use of this data? Will you one day find you can't get your mom into a senior care facility because of what her Fitbit told Google/Alphabet?

Will you discover your auto insurance rates climb because they've concluded you're not a good health risk?

There's no real way for you to judge whether a wearable is worth its PI cost.

---

**TITLE: Let's Monitor You at Home!**

All the devices pictured here gather data about you, often without your knowledge or consent.

They include baby monitors, children's toys, video games, TVs, and even mundane appliances like garage door openers, doorbells, refrigerators, and washing machines. And devices to tie them altogether, like Google's Nest.

The home was once your castle. Today it's the best opportunity ever to invade your privacy.

---

**TITLE: The Internet of Things (IoT)**

Our world increasingly consists of internet-connected devices. Sensors and data collection electronics are everywhere.

This world of internet-connected devices is called *The Internet of Things* (or *IoT*).

In the US, with our lack of rights, this is a privacy nightmare.

Think about security, too. Will any of these devices be automatically updated if vulnerabilities surface? How many will not be?

The result could be what I call ***Internet Pollution***. That's a world of insecure devices available for bad players to assemble into bot networks, eager to do their bidding in denial of service attacks, as spam bots, in bitcoin mining, rigging AdSense, and for other harmful activities.

Fortunately, the US recently announced a *Cyber Trust Mark*. It's kind of like the EPA's Energy Star program, a stamp of approval for IoT product security, based on NIST standards (National Institute of Standards & Technology). This is a big step towards reducing Internet Pollution.

But it only covers **security**. How about a Trust Mark for **Privacy**?

We still need privacy solutions like Opt-out as the default, and the users' ability to disable the internet connection and data exfiltration.

---

**TITLE: Hacking IoT: From Fish Tank to Casino**

Here's an example of how IoT can hurt us.

Thieves hacked into an internet-connected fish tank at a casino. Now on the internal network, they were then able to get into other, more important parts of the casino network to steal data.

This is the world we face unless we change our privacy and security laws for the better.

---

**TITLE: TikTok – a Red Herring**

You may recall that TikTok was in the news a while back. Should we ban TikTok so that the Chinese can not get our personal data?

The question shows ignorance. The Chinese can easily get our PI by buying it from any of many data brokers.

The Chinese could also harvest data from the many devices they sell us. (For example, Lenovo was caught with spyware in its firmware some years ago, and Chinese Huawei and ZTE computer equipment were recently banned in the US.)

Finally, the Chinese could just steal the data. They're thought to be behind the big data breaches listed here. (Notice that these include the **huge** Equifax breach, as well as some **very sensitive** personal data from the US Office of Personnel Management.)

So, banning TikTok is not a solution. We need to get our privacy & security act together, or else suffer the consequences.

---

**TITLE: Sweden – a Cashless Society**

Corporations and the government would **LOVE** to switch us over to a cashless society! That way, **all** sales and transaction taxes would be collected. Companies could *completely* monitor every purchase you make. And they could make money from transaction fees, too.

It's a surveillance dream for them. And a privacy nightmare for you.

Sweden has completely eliminated cash. Instead, you pay either with a specific cell phone app called *Swish*, or by a card (debit or credit).

Swish was designed as a cooperative effort between the country's major banks, and the national government.

The corporate/government surveillance alliance is pushing hard for a cashless America. Some local and state governments are pushing back by outlawing cashless stores.

Unless we greatly alter our privacy landscape, a cashless America would be a disaster for our fundamental human rights.

---

**TITLE: Your Life-Long Personal Database**

A big question I've emphasized several times is: how could your personal data be used against you in the future?

No one knows. All we know for certain is that we have no privacy protections against bad things happening.

Your personal information is now collected throughout your life: by schools, employers, devices, the internet, and in all your digital communications. That's a LOT of data.

This data could follow you around for the rest of your life.

If you're unlucky, it could place a permanent millstone around your neck.

Ever heard of Dog Poop Girl? A young South Korean woman didn't pick up her dog's poop from the floor of a commuter train. She was photographed and put on the web by other passengers. The result was internet vigilantism that wrecked her career hopes and impacts her life to this day, over 15 years later.

Do we live in a free country if your life can be derailed by ***forever data***?

We've haven't even created a decent privacy regimen for our nation, much less wrestled with these deeper issues.

---

**TITLE: III. Government Surveillance**

Now let's talk about federal government surveillance.

---

**TITLE: I support our government employees …**

Let me level-set with a personal opinion, if I may.

Employees in government security agencies -- like the NSA, DHS, FBI, and local LEA – all work for us. They're our employees, working on our behalf.

Just like any other group of employees in any other industry, the great majority of them work hard and want to do a good job.

I thank them for their service.

I'm going to make some critical comments in this section. Everyone needs to understand that these comments are about our national **policy choices** – *not* about our federal employees.

---

**60. TITLE: National Security Versus Personal Security**

Sometimes there is a trade-off between our ***national security*** of our country and the ***personal security*** of 330 million individual Americans.

For example, government agencies have fought hard against encryption of cell phones, emails, texts, etc, so that they can easily access your personal information.

But this devastates your *personal security*. It unnecessarily exposes you to malicious actors. Some sort of balance here would make much more sense.

Another example: the NSA keeps any software backdoors and zero-day exploits they discover to themselves, so that they can use them. But how much does that cost the millions of us who could be affected by bad actors using these exploits?

As security expert Bruce Schneier has said, "*The NSA is willing to compromise the security of everything to get what they want."*

The NSA takes their extreme approach because we've asked them to. They're tasked **solely** with our national security, and since 9/11 they've been expected to protect us from terrorists *at all costs*.

We need to reconsider these choices in light of the current threats to Americans individually as well as our nation as a whole.

---

**TITLE: Mass Search is Unconstitutional**

The 4th amendment to the US Constitution states that ***"The right of the people to be secure in their persons, houses, papers, and effects … shall not be violated … but upon probable cause ... describing the place to be searched, and the persons or things to be seized."***

You need a court-ordered warrant to search an American citizen. It has to specify the person you're searching and what you expect to find.

Mass surveillance constitutes mass search. It's done by a **general warrant**, rather than the **specific warrant** the Constitution demands.

It is unconstitutional.

These two charts from the Snowden revelations show that the US government is violating the Constitution through mass search:

(1) ***Cable intercepts*** that capture **all** communications data directly
(2) The ***PRISM program*** that captures your personal data directly from all the major US service providers (including Microsoft, Google, Facebook, Yahoo, Skype, Youtube, and Apple.)

As US representative Jim Sensenbrenner claims, "***Washington is violating the privacy rights guaranteed to us by the 4th Amendment."***

Rep. Sensenbrenner should know. He's the primary author of the Patriot Act, the very law the federal government claims as its authority to perform these mass searches!

Sensenbrenner says the surveillance agencies read powers into the Patriot Act that he never put there. So mass surveillance is not only unconstitutional, it also has no apparent basis in US law.

---

**TITLE: Data Mining All Your Communications**

The charts on this slide further illustrate the NSA's mass surveillance programs.

Like those on the previous slide, they were released by Edward Snowden. They are a decade old.

Are these programs still in place today? Have they been terminated, altered, or expanded?

We citizens are not allowed to know. Most in Congress still don't know either, much less the judiciary.

My belief is that unconstitutional mass surveillance of US citizens continues. That's based on the words and actions of our national security leaders and Presidents, the continuing growth of the NSA's huge Utah data center, the work of groups like the EFF, ACLU, POGO, PBS, EPIC, CDT, ProPublica, The Markup, Vice, theRegister, Wired, and various researchers and investigative journalists.

But don't just accept my view. Do your own research and make up your own mind.

And if you learn something, please let me know!

---

**TITLE: Where Does Gov't Get This Authority?**

How could we come to this, where our federal government engages in unconstitutional mass surveillance of American citizens?

Part of the answer is that some government agencies purposely misinterpret laws like Patriot Act section 215, FISA 702, and Executive Order 12333 to claim authorizations they really don't have.

---

**TITLE: FISA Court**

The other part of the answer is the *FISA court*.

This special court was established in the mid-1970s in response to the revelations of the illegal spying that the FBI and Richard Nixon and other federal agencies were engaged in at that time.

FISA stands for the Foreign Intelligence Surveillance Act. FISA (and its amendments) set the ground rules for government surveillance.

A special "FISA court" was created to decide upon any government request for surveillance.

Unfortunately, the court was born defective. Unlike all other courts, it heard only one side to the argument: the government's side.

Only a single judge heard any case. He or she did not have any investigative ability by which to verify or disprove the government's claims.

And the court met in secret. It never reported its findings to anyone. **It made secret law in secret session.** That's exactly what you don't want in a democracy.

Not surprisingly, the chart shows that government surveillance requests were routinely approved (with a negligible rejection rate of 0.03%).

Congress eventually caught wind of this. They tried to address some of these defects by replacing the Patriot Act with the USA Freedom Act of 2015.

But the FISA changes were largely cosmetic. I highly doubt they've proved effective in controlling unconstitutional mass surveillance.

So, the well-intentioned FISA laws of the 1970s set up a system – outside of the regular Supreme Court and Congressional oversight – that has utterly failed to protect the 4th amendment.

---

**TITLE: Mass Surveillance Doesn't Work**

From public data, it appears that government mass surveillance has proved ineffective in stopping terrorists – and school shootings, for that matter.

The Phone Call Metadata Program is an example. This program collected the *metadata* of your phone calls – their timing, duration, participants, etc.

Here the principle of Big Data surfaces once again. As stated by former NSA director Michael Hayden, ***"With enough [phone call] metadata, we don't need content."***

**They don't have to monitor your phone conversations to destroy your privacy!** The metadata is sufficient.

President Obama claimed that this program uncovered 50 terrorists. He later changed this to "a number of terrorists." Then he changed it to the actual number – 1 person. That person was not a terrorist. He had only made a financial contribution to a group designated as terrorist in a national list.

That's it! All that surveillance of all of us to uncover a single financial contribution.

The additional sources at the bottom of this slide verified that this program stopped no terrorists.

Our instincts tell us that mass surveillance helps keep us safe. Actual data informs us differently.

---

**TITLE: Why Failure? The Percentage Fallacy**

Why do mass surveillance programs fail? One reason is the ***Percentage Fallacy***.

Assume we have a magical system that finds terrorists with 99% accuracy. Sounds great, right?

Further assume that 1 out of every 100,000 people in the US is a terrorist.

Out of a population of 323 million people, that means we have 3,230 terrorists among us we need to find.

With 99% accuracy, 1% of those terrorists will be missed. That's 32 terrorists that remain entirely unknown to us (they are *false negatives*).

The system will also identify 1% of 323 million as positives. In other words, a system with 99% accuracy will incorrectly identify about 3.23 million people as terrorists (*false positives*).

The actual set of 3,198 identified terrorists will be hidden in a false positive population the size of the state of Oklahoma.

That's hardly helpful.

Charlie Savage reported how the poor FBI was forced to waste their time chasing down all these false leads for some time before the powers that be finally figured out how all this works.

For mass surveillance, a system with 99% accuracy is not enough.

While instinct tells us that mass surveillance is useful, actual data informs us differently.

---

**TITLE: Surveillance Erodes Freedom**

Some might say – *"Well, even if surveillance catches only one terrorist, it's worth it."*

This ignores the costs of surveillance. Besides the financial cost, there is also a very real cost to society. And to your freedom.

I recommend watching the film called *"The Feeling of Being Watched."* You can find it on PBS.

It shows how an innocent community was torn apart by intrusive, unwarranted, and ineffective federal surveillance.

The chart shown here verifies that huge numbers of innocent people change their behaviors due to surveillance. Is that what we would call a "free country"?

Freedom isn't free. And neither is surveillance.

---

**TITLE: Democracy Requires Privacy**

Democracy requires privacy. It can not function without it.

The Watergate scandal was basically a privacy case. Under President Nixon's orders, thieves violated the privacy of the Democratic party by stealing their campaign plans.

Nixon also harassed political opponents by cross-using their tax data for persecution. Another privacy violation.

What Watergate shows is that you can't have a democracy without privacy.

And that surveillance based on “trust us” doesn’t work. That’s why our government splits power among three branches, has checks and balances, judicial review, Congressional oversight, informed voter accountability, and all the rest.

---

**TITLE: Democracy Requires Privacy**

Here’s another example of how violating privacy wrecks democracy.

Long-time FBI director J Edgar Hoover violated the privacy of Presidents and Congressional representatives by compiling data on their personal lives.

Then he would use this PI to blackmail them.

Presidents Kennedy and Johnson both wanted to fire Hoover but couldn’t. He knew their secrets (Kennedy – womanizing, Johnson – the Bobby Baker scandal.)

Lacking oversight, Hoover employed his powers to direct the FBI to commit many illegal acts against American citizens. Examples are the COINTELPRO program, and the FBI’s attempt to get Dr Martin Luther King to kill himself.

Can you imagine what Hoover would do with today’s digital surveillance capabilities?

Or what one of our political parties might do with them today in our over-politicized environment?

Surveillance without oversight undercuts democracy.

---

**70. TITLE: IV. Solutions**

Let’s discuss solutions to the US privacy dilemma.

---

**TITLE: We are “Digital Peons”**

Start with the fundamental fact. We are all what I call ***digital peons***.

Your entire life is digitized. You can not live in the US otherwise.

Yet you have very few *digital privacy rights*.

Your data is *appropriated* – seized, typically without our knowledge or informed consent.

You don’t what data they have describing you. Or whether it’s accurate or secured.

And, you don’t know who accesses it, or how they use it.

**Decisions critically affecting your life are made based on data you’re not even aware of.**

---

**TITLE: Your “Digital Doppelganger” Determines Your Life!**

There are two “you’s” – the real you, and the you that exists in computer databases.

Companies and governments don’t know the real you. They only know your “***Digital Doppelganger***.” They make decisions that critcally effect your life based on your digital doggelganger.

Every human being is worthy of dignity and respect. But that often doesn’t happen when decisions that impact your life are made based on a digital doppelganger over which you no control and few rights.

---

**TITLE: Solution: A Privacy Architecture**

The wrong way to ensure privacy is what we're doing today – passing random laws to address specific privacy issues.

Instead, we need to create what I call a ***Privacy Architecture***.

It starts by establishing a fundamental right to privacy for all American Citizens.

Pass a generalized law that forms the philosophical basis of privacy as the default right of Americans. This becomes our nation's default orientation on privacy.

With that bias towards privacy in place, pass individual laws like we do today. But couch them within the privacy architecture and generalize them as much as possible.

What I've described here is exactly what the EU has done.

They have two foundational documents that ensure a fundamental human right to privacy, their Charter and their Convention.

On top of this they passed their generalized privacy law, the **General Data Protection Regulation** (**GDPR**).

Then individual laws are created, couched in terms of implementing these underlying privacy principles.

---

**TITLE: General Data Protection Regulation** (**GDPR**)

This slide lists the data Processor Obligations under the GDPR, and the Subjects' Rights.

Processor Obligations include security and encryption standards, limitations on data collection and cross-use, data anonymization, and more.

Subjects have the right to review, correct, transfer, and delete data. Opt-out is the default, in an attempt to move from bogus consent to informed consent.

The GDPR went into effect in 2018. The laws passed on top of it since then continue to work off its rough edges and improve privacy for EU citizens.

---

**TITLE: California Consumer Protection Act (CCPA)**

As of 2023, 8 states have passed their own Privacy Acts in the face of federal inaction.

California's CCPA dates from 2018 and is best known.

This slide lists some of its key provisions.

The list highlights the law's weaknesses. It only applies to large companies, it only applies to collected (and not purchased) data, consumers must approach each company to opt out, Opt-in is still the default, etc.

Everyone acknowledges the CCPAs weaknesses (even after its amending in 2020).

Some consider the CCPA a great first step towards better privacy. Others consider it a failure that doesn't do the job.

What this tells you is that it falls short unless supplemented by further law.

---

**TITLE: GDPR vs CCPA**

This slide compares the GDPR versus the CCPA.

Both have their advantages, but there's little question that the GDPR – while far from perfect – is stronger in its privacy rights.

---

**TITLE: Solutions – Corporate**

This slide lists my recommendations for improving individual privacy versus corporations.

Obviously, to start, we need a fundamental right to individual privacy. All laws should be nestled within the context of that *Privacy Architecture*.

This will shift the burden of privacy from individuals to corporations and governments. A degree of privacy and security requirement must be imposed on software vendors, too.

Opt-out should become the default.

We must eliminate techniques that defeat informed consent – bogus "privacy" policies, duress signings, misleading app privacy panels, and all the rest of those data appropriation tricks. The burden for consent must be removed from the consumer and placed on corporations through consumer protection.

Any organization storing PI must form to a number of security standards (including ***encryption*** and ***logging***). Holding PI will become a serious responsibility subjecting the holder to certain standards, with corrective penalties if necessary.

Subjects will have the right to review their data, ask for its correction and deletion, restrict its cross-use, and demand that it be aged out.

The landscape of the data broker industry will be fundamentally altered through regulations such as these.

Concerning the Internet of Things, the US government recently took a major step forward in devising a **security** "seal of approval" for these products. They should devise a **privacy** "seal of approval," too. Consumers should have the option to turn off the internet connections for such products, and forbid sending their PI if desired.

There must be a simple, obvious way for consumers to avoid personal collection of their data when they buy or use such consumer devices as cars, TVs, computers, cell phones, and appliances. The default should **not** be massive personal data collection.

Software products should enable encryption *by default*. For example, E2EE standards should be promulgated for email that work seamlessly *across different vendors' products.* Texting should use E2EE across products, too. Operating systems should default to encrypted storage for personal computers and cell phones. All computers, phones, and disks should be required to have a "secure erase" feature.

There are many more points I could list, but these are a decent start.

---

**TITLE: Solutions – Government**

Here are my recommendations to improve your privacy versus the federal government.

We have to stop mass surveillance of the American public because:

1. It breaks the 4th amendment
2. It has no valid basis in law (the Executive interpretations of 215, 702, and 12333 are highly questionable)
3. It has been proven ineffective (in the cases we know about)
4. It can easily be misused because it lacks oversight
5. Its very existence undercuts our freedoms and democracy

We must fix oversight mechanisms related to surveillance powers including:

1. Real Congressional oversight
2. Eliminate the FISA court and replace it with an actual judicial oversight mechanism
3. Eliminate National Security Letters (NSLs) and gag orders (they require no judicial review)
4. Increase the role and authority of the Privacy Civil Liberties Oversight Board (PCLOB)
5. Prevent security agencies from purposely misinterpreting laws to give them surveillance capabilities

We must ensure "due process" in all government operations that directly impact the lives of American citizens. Examples would include the various government blacklists such as the Do Not Fly List, and government programs such as civil asset forfeiture.

We must balance *national security* with the *personal security* of 330 million Americans. The government should stop opposing encryption for email, texting, personal computer operating systems, cell phones, personal data storage, and the like. The government should report, rather than hoard, any backdoors and zero-day exploits it discovers to protect us.

We should stop the **"3rd party dodge"** wherein government circumvents laws about data collection and use by renting the data from the private sector or by accessing it through foreign entities like GCHQ or other Five Eyes nations.

Our government has legitimate needs for information on its citizens for many specific purposes. We should be able to accommodate this aboveboard, legally, and with Congressional assent (as in the UK). Secret surveillance is not the way.

There are many more points I could list, but these are a decent start.

---

**TITLE: "Privacy" Legislation?**

Individuals want privacy, personal security, and some degree of control over their PI.

Often they can't connect the harms that happen to them to the privacy losses that caused those harms.

Corporations and governments would like to keep the status quo – with a few tweaks. They collect and control your data, and you have few rights. It works for them.

Their ultimate goal for a privacy law would be to legitimize much of their current activity.

They'd also like to override and curtail those pesky state privacy laws that are increasingly popping up and getting in their way. In fact, it is these state privacy laws that are generating increasing pressure to pass national legislation.

Key parts of today's privacy landscape that corporations and governments want to retain are:

1. Opt-in as the privacy default
2. Bogus consent
3. Unlimited data cross-use

Ultimately, our political system will decide whether you win back some degree of privacy. So far, corporations and governments have won in a walk.

Substantial research – like the Gilens and Page study – indicate that the legislative preferences of the public have a near-zero effect on public policy.

Whereas, the elites get their way in legislation about half the time.

As former President Jimmy Carter says, the United States is no longer a democracy… we are an oligarchy.

I don't think you need an academic study to tell you this. 40 years ago, the Dow was at 3,000. Today it is at 33,000.

That's a thousand percent increase, or roughly 500% in real terms.

By any measure, those who work for a living have seen their wages go up less than 5% during that same period.

So who got all the rest of that money?

With that as your fundamental fact, it's a good bet to predict that the most likely privacy outcome will be weak national privacy legislation that overrides state legislation.

A fake law.

It will be called something like ***"The Great Privacy Act for All Americans!"***

It will contain some privacy concessions for the public. But ultimately it will serve corporate and government interests.

It will have little effect on the scandals of the Opt-in default, bogus consent techniques, unregulated data brokering, and massive data cross-use.

It will continue our tradition of privacy legislation that corporations and governments can circumvent.

I think this fate is likely. But it's not inevitable!

If people like you in this room push back and work for the real public interest, we can regain our privacy and our power.

---

**TITLE: Time to Update the Fairy Tale**

Thank you for listening.

**********

**80. TITLE: V. Extra Slides**

Here's good information that didn't fit into the allocated time.

---

**TITLE: Your Car is a Privacy Nightmare!**

Most of us are aware that cars automatically collect data on your driving. This data collection used to be about safety and ensuring cars functioned properly.

Now, new cars are internet-connected. Now it's all about monitoring **you** and **everything** you do and say while sitting in that car.

There's so much data collected that an entire new class of companies, called ***Vehicle Data Hubs***, have evolved to process and sell it.

The data collected, sold, (and often lost by the companies through hacking) includes your visuals, voice, health data, sexual activity and orientation, biometrics, driving behavior, location tracking, and more.

A Mozilla Foundation report labels new cars the worst devices for privacy loss they've ever seen.

Oh, and about consent? Simply buying the car is considered your "consent." Or sitting it as a passenger!!

---

**TITLE:  Your TV Monitors You**

You watch it, and it “watches” you back.

Your viewing habits tell companies a lot of valuable things about you, your preferences, your beliefs, and your personality.

So many companies have misrepresented their TVs’ data collection (and how to opt out of it) that the FBI issued a consumer warning about the scandal.

What you can do to protect yourself is to change the data collection settings to Opt-out, secure your router and your Wifi, don’t use your TV as an internet browser, and don’t use voice commands.

---

**TITLE: Your Job Interview – With an Algorithm**

You might find your next job interview is with a computer.

Several companies claim that AI programs that analyze your voice, your mannerisms, your word choice, and your facial movements can judge whether you should get a job. **They don’t analyze the job-related content of what you say!**

These companies provide absolutely **no** public data to support their claims (their algorithms are “private”).

Snake oil? Who knows?

What we do know is that some employers take these AI interviews seriously.

This is bad news for job-seekers because you have no idea what these programs are looking for. You could lose a job by an AI interview and you’ll never know why.

That interview might then be sold to other potential employers, **or even stored in an industry database.** That could blackball you.

What about consent? Sign their data release form or no job for you.

This is a privacy nightmare. It gives employers tremendous power with no guarantee they’ll use it responsibly.

If you get unlucky, this could derail your career.

---

**TITLE: Your Employer Sells Your Salary**

I touched on this privacy scandal back in one of the first slides.

The employers of about 190 million Americans send their job and salary data to an Equifax company called **The Work Number**. Almost always without your knowledge or informed consent.

This database is the perfect vehicle for denying you the leverage salary privacy would give you in future salary negotiations.

Equifax lost their data in a data breach that affected 147 million Americans. Including social security, drivers license, and credit card numbers for most of them.

This scandal epitomizes how privacy works in America today. We need to fix this.

---

**TITLE: Powerful Digital Monopolies**

A big factor working to deny you privacy is that our digital world is increasingly controlled by a few gigantic software corporations. I call them ***cyber-corps***.

This slide shows how Google grew into Alphabet, Facebook grew into Meta, and Amazon… just grew.

The problem is that such concentrations of digital and financial power create outsized political power.

This is what prompted the Sherman and Clayton anti-trust acts a century ago.

We've forgotten that lesson. Today industry is hugely concentrated in America because we've permitted continual consolidation through buyouts and mergers.

We haven't prosecuted anti-trust vigorously for four decades.

Part of the "privacy plan" has to be correcting this disproportional concentration of digital and political power.

---

**TITLE: Those Who Seize Your Privacy Know Its Value**

**The purpose of this slide is not to disparage the two individuals it depicts.**

It is to prove that the people in charge of the big companies that seize your privacy know perfectly well its potential effects on your life.

That's why they go to extreme lengths to protect their own privacy!

Could there be any better demonstration of the value of privacy?

---

**TITLE: Who Loses Their Privacy?**

While the wealthy spend tons to defend their privacy, the young, the old, the poor, and the uneducated are vulnerable.

Do we want to be the kind of society that takes advantage of them? For corporate profit?

---

**TITLE: 3 States of Surveillance**

When it comes to government surveillance, theoretically we could have a society with no surveillance. But that is a society that does not protect itself against threats that are very real.

At the other extreme, we could have a society with total surveillance, in which the state security apparatus applies penalties on law-breakers, political dissidents, or others they don't like.

That's a police state. It's where penalties are applied without a trial.

I think we all want to avoid that.

But we should understand that a some "police state behaviors" have occurred in our country. They could occur again if we're not vigilant. (For example, the illegal actions of the FBI prior to the death of J Edgar Hoover. Or today's secret Do Not Fly lists and civil asset forfeitures.)

This is why we always need real oversight of government agencies coupled with robust privacy protections for the public.

We need to refine our society's middle position in this chart. We need surveillance when it benefits **all of us** (not just corporations or off-the-leash security agencies). And we need better privacy protections otherwise.

---

**TITLE: China's "Social Credit"**

As a dictatorship that tries to control its people through mass digital surveillance, China offers an interesting talking point.

They're evolving a system of digital control called ***Social Credit.*** It's still in its formative stages, but it's growing into a comprehensive system of behavioral monitoring designed to control citizens.

Citizens get assigned scores based on how well they conform to whatever behaviors the government wants to encourage or discourage. Scores can deeply impact people's lives.

It's worth pondering if we might be sleepwalking into a society in which our behaviors are increasing rewarded or punished by corporations that know us intimately. While no one would assign the same malevolent intentions to corporations as to the Chinese government, companies that own our privacy still might well end up shaping our lives through a system of penalties and rewards.

---

**90. TITLE: Why the Secrecy?**

So, why have our political and security leaders tried to hide mass surveillance from Congress, the courts, and the public?

First, understand that our security agencies would face harsh blame if we suffered another high-impact terrorist attack. I sympathize with them 100%. They always get the blame if something bad happens. Rarely do they get the thanks they deserve for working for us day in and day out.

Another way to say this is: Deaths are quantifiable, but our loss of privacy is not.

Second, many of these leaders believe that program effectiveness depends on secrecy. But there's no good reason we couldn't be more like the UK, where the public understands the general outlines of government surveillance, and their elected representatives have debated and approved it.

Third, the "trust us" argument of many political and security leaders shows that they don't understand the political ramifications of extensive secret surveillance in a democratic society. We've built a democracy based on division of powers, checks and balances, and independent oversight. "Trust us" is for kings and dictators.

**Even if our current leaders have integrity, those who occupy their position in the future may not.** This is why we need a system of law and rules, rather than a system that depends on good men and women.

Fourth, our Presidents and security leaders know that when their secret surveillance systems have been uncovered (eg, Snowden), much criticism results. And they remember that Congress rejected Total Information Awareness back in 2003.

They fear that these programs would be shut down if understood by Congress, judicial review, or the public.

That decision is not theirs to make. Our democratic procedures should decide this.

---

**TITLE: A National Security State?**

James Madison wrote that **"*No nation could preserve its freedom in the midst of continual warfare."***

Barack Obama echoed the sentiment two hundred years later.

If you count our 1990s embargo of Iraq as an act of war – as the UN does – then you'll see from the list of our interventions on this slide that we have been at war – without end – since the fall of the Soviet Union.

That's **30 years** of non-stop war!

Could Madison's prediction be coming true?

---

It seems we've "brought the wars home" in the form of *security paranoia*. That means cameras everywhere, digital mass surveillance, location tracking the population, the panopticon classroom, and all the rest.

We have become a slightly paranoid ***National Security State.***

We broke our Constitution's 4th Amendment to do it. Our security services operate secretly. A secret court ~~oversees~~ approves their actions in secret sessions.

If thousands of years of human nature are any proof, it's not a matter of **if**, but rather a matter of **when** corruption seeps into such a system.

The world is a very dangerous place. We must always keep our guard up to protect our freedoms. But if we loose them at home, we've lost what makes America special.

---

The end.