TRANSCRIPT - TECHNICALLY OPTIMISTIC - SEASON 2 - EP. 5

> **CLIP [Anchor]:** *It started with a loud knock on the door of a Detroit house.*
> **[Porcha Woodruff]**: *Like, whoa. Wait a minute. That's loud. It was police officers at the door.*
> **[Anchor**]: *Porcha Woodruff, the homeowner, spent 11 hours in jail for a crime she didn't do.*

RAFFI VO: In February of 2023, Porcha Woodruff was 32 years old, and 8 months pregnant.

> **CLIP [Anchor]:** *They told her she was under arrest for carjacking and robbery.*
> **[Porcha]:** *Who am I gonna carjack? I'm pregnant.*
> **[Anchor]:** *They frisked and handcuffed her as her children watched.*

RAFFI VO: Porcha was innocent. And now, she's suing the city of Detroit and the Detroit Police Department.

> **CLIP [Anchor]:** *According to the lawsuit, facial recognition software mistakenly matched her mugshot, from an arrest eight years ago, to this video of a suspect.*

KASHMIR HILL: The suspect in the case, the person was not visibly pregnant. Clearly was not the same person.

RAFFI VO: This is Kashmir Hill, who covers technology and privacy for the New York Times. She's also written a book, *Your Face Belongs to Us*, about a particularly secretive facial recognition company that we'll hear more about in a few minutes. But, about Porcha…

KASHMIR HILL: She'd been identified with facial recognition technology and an eyewitness who agreed with the computer that it was her. And she ended up getting charged. She had to hire a lawyer. She ended up in the hospital that night because she was dehydrated and stressed out from being arrested. I mean, it has a real toll when you are arrested. And, you know, the Detroit police chief said, he said it's not the facial recognition technology that was wrong here. It was our police detective, we did a bad investigation. We shouldn't be arresting anyone based on just a facial recognition match.

RAFFI VO: Facial recognition technology is here. And it's in the hands of law enforcement and government agencies all across the U.S. right now.

And that's despite the fact that there are major problems with how this technology works. For one thing, it is demonstrably worse at identifying dark-skinned people.

CLIP [NEWS REENACTMENT]: *Study after study has shown facial recognition software misidentifies Black, Native American, and Asian faces anywhere ten to one hundred times more often than white faces.*

RAFFI VO: That's also despite the fact that the very algorithms powering this technology can often replicate the same biases we observe throughout the criminal justice system.

CLIP [NEWS REENACTMENT]: *There's still enormous bias in these systems, because there's bias in the data that goes into these systems.*

RAFFI VO: And, it's in spite of the fact that today's newest facial recognition software uses images pulled down from the public Web. Including photos posted to social media. And this technology will have huge implications not just for data privacy but legally.

In the U.S., the Fourth Amendment to the Constitution prevents people from being subject to illegal searches or seizures by government officials, including police.

But can it protect us from facial recognition technology?

CLIP [Andrew Ferguson]: *I am a law professor who studies the intersection of big data policing and Fourth Amendment freedoms. The Fourth Amendment will not save us from the privacy threat posed by facial recognition technology.*

RAFFI VO: Facial recognition is one thing, but the broader issue that this technology raises is even bigger than that. We've talked about how much data social media companies have on you, and we've talked about how political campaigns can get ahold of your data, but this episode, we're asking a different question: Is your data at risk of being accessed, taken, and used by your government? We're used to thinking about having a baseline right to privacy, but how does this right extend to our digital data?

I'm Raffi Krikorian. And from Emerson Collective this is Technically Optimistic.

THEME MUSIC

KASHMIR HILL: There's just this bigger question of how comfortable we are as a society with facial recognition systems. And do we, you know, how much do we want them used?

RAFFI VO: Kashmir Hill often reports for *The New York Times* on new developments in tech that raise a lot of questions about our privacy. But, in a piece that was published in January of 2020, she introduced readers to an obscure little startup.

KASHMIR HILL: So Clearview AI is a facial recognition technology company.

RAFFI VO: And Clearview wasn't just raising *questions* about privacy. They were, it seems, tearing it apart.

KASHMIR HILL: What Clearview did was to scrape billions of photos from the public web, including social media sites such as Facebook, Instagram, LinkedIn, Venmo, to build this app where you can upload the photo of somebody you might not know, and then see all the places on the internet where their face appears, as determined by the app. So you might learn their name, their social media profiles, and you might even find photos of them on the internet that they don't know about.

JONATHAN ZITTRAIN: When I think of a Clearview AI, that's a company that started out necessarily as a one person startup with nothing to lose and everything to gain.

RAFFI VO: That's Jonathan Zittrain, professor of international law, public policy, and computer science at Harvard. He also runs the Berkman Klein Center for Internet and Society.

JONATHAN ZITTRAIN: Now you can't be anonymous in the world. And I mean, and that's I mean the new normal now, thanks to Clearview. It was shocking when it happened. And I remember my reaction was, this should be stopped immediately. This is like a huge sea change in privacy, and this company should be, you know, put into another line of work, and the earth above their servers salted.

RAFFI: How did they get away with this?

KASHMIR HILL: Well, I mean, part of how they got away with it is that it is pretty easy to scrape information off of the Internet. And Clearview, you know, specifically was looking for faces. And so they sent, you know, scrapers out onto the Internet, you know, collecting faces.

One of the first sites scraped was Venmo.com. And this was funny to me as a privacy reporter for more than 10 years, I remembered the kind of outrage from the privacy community about the way that Venmo was architected to be public by default. When you signed up for Venmo, all of your transactions where you're paying somebody else were public by default, including your profile photo.

RAFFI: So like if we bought a pizza together, in effect I gave you five dollars, it shows up on my profile.

KASHMIR HILL: Yeah, it would show, you know, Raffi pays Kashmir and maybe there's a little pizza slice. And privacy activists at the time said, "Hey, Venmo, you shouldn't do this. You know, defaults are very powerful. Most people aren't going to change this. And so they're going to be broadcasting kind of who they're paying and what they're buying to the world." And so he built a little scraper that would hit the site every few seconds and download all the profile photos that

were displayed at that moment. And so, he collected, you know, like, more than a million faces this way. And that is how scraping works.

RAFFI VO: The legality of this process, scraping the internet for publicly available content, was dealt with in a court case that ultimately resolved in 2022. In hiQ Labs versus LinkedIn, a U.S. Federal Appeals Court said that scraping didn't violate the Computer Fraud and Abuse Act, a 1986 anti-hacking law.

But it was a narrow ruling. For now, Clearview's database is technically legal. And you are almost certainly in it.

KASHMIR HILL: I mean, I'm in the database, you're in the database. Probably most people listening to this podcast are in the database. If you have photos on the public web, there's a likelihood you're in the database. Clearview has 40 billion faces, they say, in their database.

RAFFI VO: So, if building a massive facial recognition database is such a great idea, why haven't big tech companies done it themselves? After all, Clearview's scraping their platforms to get your images in the first place.

KASHMIR HILL: When I first heard about Clearview AI, I thought that they must have had some kind of technical genius there. Like I thought it was a technological breakthrough. Because, yeah, why wouldn't Facebook or Google do this first? So it was a surprise to me in my reporting for the book to find out that actually Google and Facebook did get there first. They did develop technology internally, like Clearview AI, where you could take a photo of somebody and it would find other photos of them. It was a way to identify them. Google, as early as 2011, had a product like this. Both companies decided not to release the technology. They just thought there were too many downsides, that there were, you know, too many legal risks, ethical risks, probably.

What Clearview AI did was not necessarily a technological breakthrough, it was an ethical breakthrough that they were willing to do something that other companies weren't willing to do.

RAFFI VO: At first, it was difficult for Kashmir to reach anyone at the company, which began working on facial recognition back in 2016.

KASHMIR HILL: They are a small team, it was kind of astounding to me to find out just how small the company was for the kind of astounding technology they built.

RAFFI VO: And the leader of that team was a man named Hoan Ton-That. He's a Vietnamese Australian engineer, and one-time model, who, at the time of Kashmir's exposé, was 31 years old. This is him, talking with a CNN business reporter.

> **CLIP [(CNN Business YT 3:56-4:09) Hoan Ton-That]:** *You know, we really think, and we can give you the demonstration, that we've, you know, really broken the sound*

barrier for facial recognition. So, it's gotten to a point where we think it's better than the human eye, and it works on different poses, different angles, all kinds of stuff like that…

KASHMIR HILL: Before he built Clearview AI, his track record included making Facebook quizzes, iPhone games, and an app called Trump Hair.

RAFFI VO: Yeah…Trump Hair. That app is exactly what you think it is. Feed it a photo and it would put Trump's hair on a person's head. [SIGH]

KASHMIR HILL: He did not want to talk to me at first. And part of the book is kind of the detective story of trying to figure out who's behind the company. They were a bit hidden. But once he did start talking to me, I asked him about the implications of building a technology like this and releasing it into the world and the kind of threat it poses to anonymity if everybody starts using an app like this. And he kind of said, the first time I asked him, that's a good question I'll have to think about it.

RAFFI VO: Clearview did have some high-profile funders, according to Kashmir's reporting, including a former adviser to Rudy Giuliani, and the venture capitalist Peter Thiel. But, by Silicon Valley standards, the 7 million dollars that Clearview had raised through 2019 was…not huge.

KASHMIR HILL: In the beginning, Clearview, it was kind of a product in search of a customer. And they assembled this big database and they weren't actually sure who would pay for it. So some of the earliest users I talked to were billionaires and investors that they were pitching.

One of my favorite stories was John Katsomatidis. He's a billionaire who owns grocery stores in New York City. And so Clearview pitched him on putting their technology into his grocery stores to try to identify shoplifters. And he did not ultimately use their technology in his stores, but he had the app on his phone. And one night he was in a Italian restaurant. His daughter walked in with a man he didn't recognize. So he sent a waiter over to take a photo of them and then ran the photo through Clearview AI and identified her date as a, I believe it was a San Francisco venture capitalist. He said he was reassured that he was not a Charlton. I said, are you sure?

RAFFI: Yeah, exactly.

KASHMIR HILL: But who Clearview AI wound up settling on as their main customer — now they say their only customer — is law enforcement agencies and government agencies.

RAFFI VO: That's right. Today, Clearview AI only makes their database available to police and government agencies. There's a reason for that. And it has to do with what happened after Kashmir broke the story about Clearview, and people learned what they were up to.

KASHMIR HILL: So when I first wrote about Clearview in the New York Times, there were a bunch of lawsuits from people who said, "Hey, this company has violated our privacy." And a lot

of those lawsuits got consolidated in Illinois because Illinois has this really unique state law called the Biometric Information Privacy Act. It was passed in 2008. It's the rare law that moved faster than the technology. And it says that you can't use people's biometric information, including their face print, without their consent, or you face a up to $5,000 fine. There's a private right of action. So people are allowed to sue companies directly that they think have violated the law.

So Clearview's dealt with a couple of lawsuits there and one was from the ACLU. And to settle the lawsuit, Clearview said, “We're only gonna sell this database that we've made, these billions of faces to law enforcement and government agencies, we will not sell it to private companies or the public at large.” And so Clearview kind of tied its hands in a way.

> **CLIP [(CNN Business YT 14:38-14:44; 14:51-15:03) Hoan Ton-That]:** *I can understand people having concerns around privacy. So the first part to remember: it’s only publicly available information. Two, it’s what you use it for. We’re not just making technology for its own sake. There has to be a vision, a purpose, and a reason for this to exist. And the reason and purpose that we’ve found is to really help law enforcement solve crimes.*

KASHMIR HILL: Clearview in the early days was trying to sell it to anybody who would buy it. And now the fact that they work only with law enforcement has been kind of a get out of jail free card for them in a lot of different jurisdictions because people kind of feel, if we're gonna use facial recognition technology, I think a lot of people feel like this is the best use case.

RAFFI VO: But we’ve already heard a little bit about what can happen when this technology is used by law enforcement. Porcha Woodruff was not a criminal, and justice was not done when she was arrested.

But police officers were smitten by this new piece of tech.

KASHMIR HILL: When I first started talking to police officers, the police officers raved about the tool and said it just worked like nothing they had used before, that it was so much more powerful than the kind of state facial recognition systems that they had access to.

RAFFI VO: In the past, facial recognition databases consisted of official government photos, like drivers license pictures and mug shots. But by using scraped images from all over the web, Clearview’s database is huge by comparison.

But of course, it’s not just the size of the database that makes Clearview so powerful. It’s the fact that now there’s an algorithm that’s been trained on this huge pile of faces.

And this algorithm has led to some real success stories.

KASHMIR HILL: One of the detectives I talked to is a child crime investigator. And he described kind of incredible use case of Clearview to me. He works for ICE, in their child crime investigations unit. And he was working on a case where Yahoo had found a photo of child exploitation in a foreign user's account. And they forwarded it on to the Department of Homeland Security. They knew that the abuse was somewhere in the US. They could tell from the electrical outlets in the background of the photo. But they had a photo of the abuser, they had a photo of the child, and they just had no idea who these people were.

So he ended up running this photo through Clearview. It got a hit for the abuser's face. And he was in the background of an Instagram photo. And he was standing behind a counter for a workout supplements company. And so this officer ends up calling that company, just following these kind of digital breadcrumbs. And he identifies the guy.

He lives in Las Vegas. He goes to his Facebook account. He's able to see photos of the room where the original photo was taken, and photos of the child. And so they end up arresting this guy.. And he just said there's no way that they would have solved that case without Clearview AI. And based on that case, Department of Homeland Security decided to get an annual subscription. They just re-upped in September for almost a million dollars per year.

RAFFI VO: But, the way that this tool was just immediately put in service, without any kind of review process, raised some red flags. For one thing, as we've seen, there were problems with how it worked in practice.

KASHMIR HILL: What troubled me is Clearview was being actively used by police officers, but it hadn't been tested by an outside agency for how accurate it was, or if it had any problems with bias. Did it work as well on women as men, on people of different ethnicities?

RAFFI VO: Porsha Woodruff wasn't misidentified by the Clearview database. But Randal Quran Reid was.

KASHMIR HILL: The Clearview AI incident that I've reported on involves a man named Randal Quran Reid who lives in Atlanta. They pulled him over and told him he was under arrest for larceny in Jefferson Parish. And he said, "Where's Jefferson Parish?" And they said, "It's in Louisiana." He said, "I've never been to Louisiana." And he spent a week in jail because it took a week to kind of clear it up that it was not him.

If you're going to run a search with Clearview AI, it includes 40 billion people. So even though it's a crime in New Orleans, it's going to include this guy who lives in Georgia.

RAFFI VO: The presence of this powerful tech in the hands of law enforcement raises a ton of big questions, about a number of things here. First, about police.

KASHMIR HILL: Do we want police working with a big database like this? Should all of the people whose faces are in the database be part of a lineup every time a crime is committed?

You know, how often do they result in the arrest of the right person? How well do they work on kind of grainy surveillance camera stills? Like we need a more robust analysis of the tools.

Should it be used for all crimes, you know? Every shoplifting crime or only serious crimes? That's what they decided in Detroit. They're only using it for violent crimes and home invasions. If it is used, do we have a robust way to audit police and make sure that they're pairing this with a robust investigation as opposed to this thing can happen where a computer says, yeah, it's this person. And then they fall prey to automation bias where they think it has to be right.

RAFFI VO: And it raises even bigger questions about the Constitution. Specifically, whether or not a system like Clearview AI actually violates our rights.

KASHMIR HILL: Is this an unreasonable search? Some civil liberty activists say if the police had built this database, it would have been unconstitutional and that they're kind of circumventing constitutional protections by buying the service from a private company like Clearview AI. So, there's just a lot of concerns.

RAFFI VO: Clearview AI was able to assemble this massive facial recognition system because of a lack of data privacy protections. The company claims that they only used images that were publicly available, but that's not really the same as getting permission.

No one really posts a photo with the understanding that it'll be used to train a powerful algorithm for the police. Even if that use case might technically be kosher under the obscure terms of a social media privacy policy.

And photos of our faces are just one example. Tons of our data is out there on the public web, with the potential to be used, appropriated, or exploited in ways we can't even think of right now. So, what rights do we have here?

JENNIFER LYNCH: There's technology all around us that could never have been contemplated when the Constitution was written, when the early Supreme Court cases were decided, uh, or even last year.

RAFFI VO: This is Jennifer Lynch, general counsel at the Electronic Frontier Foundation, or EFF.

JENNIFER LYNCH: The Electronic Frontier Foundation is a 30 year-old digital nonprofit and we work to protect privacy and civil liberties and new technologies. We do a lot of advocacy about consumer privacy. We have a whole team of lawyers and we litigate our own cases and we also partner on other people's cases and we file amicus briefs. And, somewhat unique to organizations, we have a whole team of technologists who design privacy-enhancing technologies, and then roll those out to the world. They also help the lawyers to understand the technologies.

RAFFI VO: And don't underestimate how important it is to train lawyers on this stuff. If we need the Courts to weigh in on how new technologies fit into our legal framework and the Constitution then it's really important that they understand the tech.

Because as we've seen over the past couple decades, from some of the highest courts in the nation, lack of familiarity with technology can be a major impediment to progress.

CLIP [SCOTUS via Oyez, ABC, Inc. v. Aereo, Inc., Oral Argument, 5:17-5:27]:

J. Sotomayor *I mean, Justice Breyer has already said he's troubled about the phonograph store and, and the Dropbox and the iCloud. . . .*

CLIP [SCOTUS via Oyez, Riley v. California, Oral Argument, 5:08-5:15)]:

[Michael Dreeben]: *So if you have an iPhone, Justice Breyer, and I don't know what kind of phone you have—*

[J. Breyer]: *I don't either because I can never get into it because of the password. [LAFF]*

JENNIFER LYNCH: And technology is moving so quickly that the courts can't keep up, legislators can't keep up in passing these rules. That is the real challenge that we're dealing with today.

RAFFI VO: The EFF fights to protect civil liberties in the face of new technology. But their work on data privacy, beyond just facial recognition, is central to their mission.

JENNIFER LYNCH: It might feel like you have no control over where your data goes, and that's pretty much because you don't have a lot of control, unfortunately, over where your data goes. It may be collected by private companies. The private companies may sell data directly to the government. They may sell to other private companies. They may sell to data brokers. The whole sort of pathway of where your data goes is pretty opaque, I think, to most people, even people like me a lot of the time. We are at this place where we have a patchwork of privacy laws. And so when you click OK, it might mean one thing in one place and it might mean something else in another place.

RAFFI VO RT: Yeah, I mean like one of my favorite things to talk about is how a lack of a national data privacy law makes everything, just worse, and so I get your point about the patchwork of state laws.

But what about the 4th Amendment? That's already in the Constitution, we don't have to pass anything new. Does the Fourth Amendment do anything to protect our data privacy?

JENNIFER LYNCH: Yeah, so the Fourth Amendment is our right against unlawful or unreasonable searches and seizures. That right only applies to the government. So it only applies to police searches, some administrative searches, but you have to have a government. entity doing the search. It doesn't apply against a company, for example.

And so the Fourth Amendment also requires at a baseline, a warrant. Now, there are some searches that the Supreme Court has held don't require a warrant for various reasons. There are some exceptions to the Fourth Amendment. But in general, um, searches require a warrant.

RAFFI: What is the extent of the government's power to get my data either from me or from one of the services that I might be using? And then what protection do I have given the Fourth Amendment in those situations?

JENNIFER LYNCH: Yeah, so courts tend to look at older technology, if we might call it technology, when they, when they try and decide how to apply the fourth amendment to digital data. And by that, I mean, courts are looking at, uh, letters that we mail or paper that we write on, right? And, um, and trying to make an analogy between, for example, the sealed letter and the data that we're communicating to other people or sharing with a company.

So in that context, if you look at an email, for example, the body of the email has been compared to the text that's inside a letter. And courts have said that police need a warrant to access that body of the email, the text that's inside the email. And that's true even if you're using Google to send your email. So theoretically Google can scan all of your email. And theoretically you have accepted that by clicking yes to those terms of service. But the court has said that this is just like giving your letter to a letter carrier. You're still expecting privacy in your email communications. And so the government needs a warrant.

It does get a little bit more confusing, though, if we're talking about, the digital data that we share with our credit card company, for example. Now that data could be extremely revealing. I mean, I could learn so much about a person's life just by knowing that they've purchased diapers at Target, for example, right?

RAFFI: Totally.

JENNIFER LYNCH: But unfortunately, we have some older cases where the Supreme Court has looked at financial records and said, well, those financial records are shared with a third party and because you've given them up to your bank, your bank has seen them, then you no longer have an expectation of privacy in those financial records.

RAFFI VO: This idea that, when you share data with a third party, you can no longer maintain an expectation of privacy around that data is part of what's known as the "third

party doctrine." Professor Zittrain can explain.

JONATHAN ZITTRAIN: The third party doctrine began as a way of saying that if you entrust something, including something bearing information about you, like a notebook full of your scribbles or something like that, to someone else, if the authorities in the United States want to demand that of that third party, they don't get to make the kind of Fourth Amendment privacy claim you would, because it's not their privacy being invaded if your journals are read. And you may not have the same defensible constitutional interests in it, because you entrusted it to someone else. And in doing so, you were indicating something about your expectations of privacy.

And what that would mean is, the difference, say, between an old-fashioned answering machine with a cassette recorder that would record people's calls for you and voicemail, there might be differential legal protections depending on whether you used voicemail or a home answering machine, with the home answering machine getting more protection because it's in your house and they'd have to get a warrant to let themselves in and seize the cassette tape.

RAFFI: Mm-hmm.

JONATHAN ZITTRAIN: Whereas voicemail might just be an administrative order. And as so much of our worlds moved into the cloud, whether through backup or just through direct access, for all sorts of reasons of convenience and price, it bore with it this sort of unnoticed change in the level of constitutional protection one could get.

RAFFI VO: A lot of our digital data today is shared with a third party. Even data we think of as very personal, like the content of our text messages, or our online shopping history…it all goes to the platforms, who store our data on their servers.

And somewhere in some long privacy policy that we didn't read, we probably consented to their possession of this data.

So, if the contents of our digital life deserve the same amount of privacy protection as our paper letters do, it seems like the Courts might need to acknowledge that the "third party doctrine" is in need of an update.

JENNIFER LYNCH: What I'm hoping is that we will get to a point where courts will accept that. The data that we're generating today from our purchases is very, very different from my bank statement in 1975, because we're not using cash for anything anymore. Every single purchase is revealing something private about us.

RAFFI VO: How will the Courts interpret our data privacy rights in the future? One big piece of that puzzle came in a landmark Supreme Court decision from 2018, which was specifically about location data.

JENNIFER LYNCH: So if you're looking at the government's access to data and specifically location data, we can look to a Supreme court case from a few years ago called Carpenter.

> **CLIP [SCOTUS viz Oyez, Opinion Announcement 0:01-0:06, J. Roberts]:** *I have the opinion of the Court in case 16-402, Carpenter versus United States.*

JENNIFER LYNCH: That case involved cell site location information data, which is the data that your phone generates or that the phone company collects every time your phone connects with a cell tower. And the Supreme Court said in that case, even though Mr. Carpenter was out in public for a lot of the time that his cell phone data was being collected, he still had an expectation of privacy in that data because it was the aggregation of data that was problematic.

> **CLIP [SCOTUS viz Oyez, Opinion Announcement 3:15-3:18; 3:22-3:28, J. Roberts]:** *We think that allowing government access to these location records enables all-encompassing government surveillance of the sort that troubled the drafters of the Fourth Amendment.*

JENNIFER LYNCH: This data is very revealing. In the aggregate, it tells us something about people's lives that the police shouldn't have access to without a warrant.

RAFFI VO: Carpenter was a huge victory for the EFF, and for privacy rights. Your location data is generated from your cell phone, and it passes through the hands of the phone company, as a third party. And still, the Supreme Court recognized: you have a Fourth Amendment right there. The government can't just up and take your location data when it wants to. They need a warrant, from a judge, and that requires probable cause.

But it's not just the phone companies who are third party recipients of our location data.

JENNIFER LYNCH: We all know that our phones generate a significant amount of location data, and they do this in several different ways. They create location information when they connect with a cell tower, and then the phone company knows where that cell tower is and can approximate our location based on that.

Our phones generate data when using GPS signals, connecting with Bluetooth, lots and lots of different ways. And the phone itself collects location data. Our apps on the phone collect location data. And in some cases, the companies that provide our services, whether that's Google or Apple or Facebook, they also collect location data.

RAFFI: So, like, a lot of people know where I am, is basically what you're saying.

JENNIFER LYNCH: A lot of people know where you are. Yeah. And, uh, our photos, uh, unless you turn off that feature, the photos are collecting location data. So if you're sharing a photo with

somebody or uploading a photo, we'll include that location information. So getting to access to that data really legally depends on where that data resides.

RAFFI: Mm hmm.

JENNIFER LYNCH: If it resides on your phone, then police need a warrant to access that data. If the data is stored with a service provider and it's linked to your account, then law enforcement needs to get a warrant to access that location data. And that is because of the Carpenter case. Even though Carpenter only applied to data that was collected by cell phone companies, courts have expanded it to cover location data that's stored with other service providers like Google.

Now, the real wrinkle in that, I think, is that for the last about six to ten years, police have also been able to ask Google in particular to give them information on everybody who was in a particular location at a particular time, regardless of whether there was any indication that an individual person committed any crime.

So police could say, there was a bank that was robbed. And that happened at three in the afternoon and so give us information on everybody who was in a hundred meter radius of that bank between say 30 in the afternoon.

RAFFI VO: And if a judge signs off on this sort of request, for law enforcement to obtain data on everyone in a certain geographic area, it's called a geofence warrant.

JENNIFER LYNCH: So a geofence warrant or reverse location warrant is the term for these warrants that are going mostly to Google to get access to the device identifiers for everybody who was in a given place at a given time. And in the past, Google was able to provide that information to the police and often that resulted in hundreds, if not thousands of people's identifiers being disclosed to the police and then police would eventually get information from Google revealing who those phones belong to.

RAFFI VO: But, in the opinion of the EFF, this doesn't seem super Constitutional.

JENNIFER LYNCH: And we have challenged those in the courts and courts have sort of gone different ways. But in general, courts have found that there are real issues with that because the way that the fourth amendment is set up is that police need to have an individual suspect or a group of suspects or even a suspect device before they can search that device.

They can't just say, well, a crime was committed and everybody in the area carries a cell phone, and so we can get access to information on everybody.

In the Carpenter case, the data only applied to one person, Mr. Carpenter. But in the geofence context, the data that Google is providing applies to hundreds or perhaps thousands of people, depending on the size of the geofence.

RAFFI VO: And the number of data requests from geofence warrants has been on the rise.

JENNIFER LYNCH: From the last reporting that we have from, I think, about 2021, Google revealed that geofence warrants constituted 25 percent of all warrants they received.

And, and Google is theoretically not set up as a company to conduct surveillance for the police. So, um, that probably costs the company quite a bit of time and money to respond to those warrants.

RAFFI VO: Whether as a result of the EFF's work in challenging this practice in Court, or maybe out of a desire to no longer have to comply with so many geolocation data requests, Google is changing their ways.

JENNIFER LYNCH: Just in January of 2024, Google announced that they will no longer be able to provide this data to the police.

RAFFI: And I'm assuming this, this change, this technological change, you support, that you, EFF supports.

Jennifer Lynch: We asked Google to make this change for years.

RAFFI: Even better.

RAFFI VO: So that's good news for our location data. But what about facial recognition? Well, the Supreme Court hasn't weighed in yet. But the EFF is fighting for a ban on its use by law enforcement. And we'll hear more about that later in the episode.

But first, since we've been talking about the Fourth Amendment, and protecting our private data from getting into the hands of the government, I think it might be fun to talk to some members of the government who are actually trying to make our digital data *more* secure.

That's coming up…after a short break.

MIDROLL

RAFFI VO: Welcome back to Technically Optimistic. I'm Raffi Krikorian.

We've been talking about the Fourth Amendment, which protects US citizens from illegal searches and seizures by the government, and we've been hearing about how new technologies might complicate this right to privacy.

But, right now, under the umbrella of the Department of Homeland Security, there's a new federal agency that is also super concerned about our privacy, and seems to have a pretty clear-eyed view about what tech is…and isn't.

JEN EASTERLY: Sometimes you get the argument, well, oh, tech is magic. You won't understand it. Just accept that product and then, you know, You know, there's a certain risk, but you'll be okay. And so the incentives are completely skewed.

RAFFI VO: That is Director Jen Easterly.

JEN EASTERLY: So part of what we are trying to do is to help inform the consumer, because consumers have to understand what to ask for so they can demand it.

RAFFI VO: After two decades in the Army, she has spent her career serving at high levels in the US government, in roles devoted to cybersecurity. Now, she is the head of CISA, spelled C-I-S-A.

JEN EASTERLY: It is the cyber security and infrastructure security agency. We love security so much. We had to have it twice in our name. Newest agency in the federal government. We were set up at the end of 2018 to play two key roles. The first is as America's cyber defense agency, and the second is is the national coordinator for critical infrastructure, security and resilience.

We're not a regulator. We don't do law enforcement, we don't collect intel, we're not a military agency, we were created entirely to be a partnership agency. And because that critical infrastructure is largely owned and operated by the private sector, everything we do is by, with, and through partners.

RAFFI VO RT: Okay so, from a national security perspective…why should American citizens be concerned about data privacy?

JEN EASTERLY: We are digital creatures, whether we like it or not. The fact that so much of our lives are lived online…I think we have to think very deliberately about what that means, both from a privacy perspective, but also from a fundamental safety perspective.

When you think about how much of our lives are data-driven, and how much of that data is now available, certainly from a cybersecurity perspective, we've seen data that's been weaponized in

some pretty nefarious ways, whether it's by adversary nation states or by cyber criminals. And so I think all of us need to be much more conscious and deliberate and intentional so that we can keep it safe and secure.

The great thing is, Raffi, if you do some very basic things, what we talk about is “cyber hygiene,” um, that prevents, the research shows, 98 percent of cyber attacks.

So that's what our PSA campaign is all about, our Cybersecurity Public Service Awareness campaign, called Secure Our World. We launched it last year, and its a multi-year effort, and we have it all up on our website with little animated videos.

RAFFI VO: By the way, those videos are no joke.

> **CLIP [CISA PSA 0:03-0:11]:** *I’m Joan the phone, here to show you four easy ways to stay safe online.*

RAFFI VO: They go pretty hard.

> **CLIP [CISA PSA 0:47-0:59]** *We can secure our world, install updates, make better passwords, think before you click, use multiple factors. That’s how we can secure our world.*

JEN EASTERLY: You know, a lot of this is about empowering the digital citizen. This is something we can all do, but, but we need to be very deliberate, very conscious about it, and we need to take those basic steps.

RAFFI VO RT: Okay, but that’s a lot of responsibility to put on individuals, right? Like, don’t we also want to hold the tech companies accountable?

JEN EASTERLY: Well, we do, and, and you know, a lot of this comes down to how to construct a sustainable approach to cybersecurity and the most important element of this is what we call secure by design technology.

I mean, go back just 40 years, Raffi, think about the TCP IP protocol that was implemented to allow computers to talk to each other. You know, since that period of time when the internet was putatively born, security has never been a priority. Never. Software was never created to be secure.

Security was really something that became a bolt on. And that's why we have a multi-billion dollar cybersecurity industry because it was all about, well, let's get this to market and let's, you know, innovate, but it wasn't responsible innovation.

And when you bolt things on, you're going to have a lot of imperfect integration, and so there are those holes that allow the bad actors to weasel their way in. And how do we fix it? Well, frankly, we have the technology manufacturers who arguably got us deep into this mess, make sure that the products that they are getting out to market are developed in a way that dramatically reduces the number of exploitable flaws. And that's the Secure by Design Revolution. We linked arms with industry over the past year and are really driving forward ways to enable technology to be more safe, more secure, so the burden is not placed on them, who often, you know, don't understand the threats that well and don't know what they need to do to protect themselves.

RAFFI VO: As part of this initiative, software manufacturers can choose to take the Secure By Design pledge, where they promise to make a good faith effort towards goals around security and transparency. Things like implementing multi-factor authentication, increasing security patching, publicizing evidence of cybersecurity breaches, and some others.

As of May 2024, Microsoft, Amazon Web Services, and Google are all signatories, and they're joined by more than 50 other companies.

But there's a difference between unsafe design, and surveillant design. Yes, security flaws and vulnerabilities can leave data exposed to hacks, breaches, or leaks. But then there's software that's been *designed* to plunder your information…on purpose.

Like, for example…what's up with the software in your car?

> **CLIP [(CNN 0:00-0:11) Smerconish]:** *Is your car spying on you? And upping the cost of your insurance? Turns out that's a growing problem, thanks to today's internet-equipped vehicles. It can occur without the driver's knowledge or permission. . .*

RAFFI VO: This has been a subject of recent reporting by none other than Kashmir Hill of the New York Times, who we heard from earlier.

> **CLIP [Kashmir Hill on CNN, 4:19-4:33; 4:38-4:46]:** *What is happening right now is that cars are becoming smartphones on wheels. They are massive data collectors. They have hundreds of cameras and sensors in the car. And I think the automakers have realized that they can do what Silicon Valley has done, what Google and Facebook has done, you know, find a way to monetize this data.*

RAFFI VO: This is not a case of "secure by design." But it's not a case of *flawed* design, either, exactly. So what do we do about products like this? In this in-between area? I put that exact question to Director Easterly.

How should we be thinking about these cars capturing so much of our data?

JEN EASTERLY: I mean, I don't love it at all. To be, to be totally frank with you. For somebody who's spent so much of my life immersed in technology, there's like a little Luddite in there that just wants to, you know, do the…

RAFFI: Return to a simpler time?

JEN EASTERLY: [LAFF] Right?

So, you know, in a world where everything is underpinned by a technology backbone we all need to be much more intentional and conscious about how the technology that we use every day may ultimately impact the risk that we take on. I realize some of the things that I'm saying, Raffi, these are not things that are turnkey, this is not going to happen next year.

You know, I, I say tongue in cheek, we call technology like unsafe at any CPU speed, because you, of course, remember the 1965 book by Ralph Nader, Unsafe at Any Speed, and that was back then when, when people thought car crashes were the fault of bad drivers, right? You know, people want to blame data breaches on consumers or small businesses, as opposed to asking the question: Well, you know, why was there so much vulnerability in that software?

So, it may take a while, like it took until 1983 to get seat belt legislation. But again, this is the most important thing that we can do is to ensure that the technology that we rely upon every hour of every day is as safe and secure and resilient and defensible as possible.

You know, this podcast is called Technically…Optimistic.

RAFFI: Optimistic. Mmm-hmm.

JEN EASTERLY: I would say I'm an optimist, I think so, but I've become much more of a tech realist. You know, there's a lot of tech catastrophists out there, like this is going to end the world. I'm not there. I just think we have to be really, really realistic about how tech has failed us.

You know, I see this and live this and breathe this every day. And before these generative AI capabilities get, you know, embedded in everything, and they are. It's happening now. We have to put the right structures and guardrails in place to prevent them from being used easily by terrorists, by cybercriminals, by rogue nations to create enormous risk.

REP. TED LIEU: I'll give you my, uh, perspective.

RAFFI VO: That's Congressman Ted Lieu, from California's 36th district. He's a co-leader on the House Bipartisan Task Force on AI, and he thinks a lot about data privacy, security, and the risks posed by emerging technology.

REP. TED LIEU: I think about three buckets. Basically, the first bucket is things that can destroy the world. The second bucket would be things that can't destroy the world, but could kill you individually.

Turns out there's a lot of AI in moving objects. Planes, trains, automobiles . . . And last bucket is the hardest, which is, AI that isn't going to kill you, but has harm that we believe is bad for society.

So we wouldn't want, for example, loans to be determined by an AI algorithm that's biased towards gender or race or another protected class. We wouldn't want a company who hires people using AI algorithm for that algorithm to be biased. We wouldn't want biases in many places, such as, for example, facial recognition.

Many of the products are amazing at recognizing faces, but many of those products also are worse for people with darker skin. So my view is we deploy this nationwide law enforcement agencies, then it's a massive equal protection violation. And I've introduced legislation to put guardrails around that use case.

RAFFI VO: Congressman Lieu introduced the Facial Recognition Act in October 2023. This would place federal limits on how law enforcement could use facial recognition technology, or FRT. For instance, under the law, police could never use FRT as the *sole* basis for arrest. It would prohibit FRT from being used against protestors, or to enforce immigration laws. And it would ban the use of facial recognition databases that contain illegitimately obtained images.

But, as of this recording, the bill hasn't even left committee.

REP. TED LIEU: Just on a purely political analysis, it's not going to move while the Republicans control the House. If Democrats flip the House, then I do hope to get that bill moving. It does have guardrails in there that will make it harder for law enforcement agencies to use facial recognition. I also think those guardrails are important because it prevents discrimination against people with darker skin.

RAFFI VO: I wanted to ask Congressman Lieu the same thing I asked Director Easterly: How should we think about the tradeoffs between privacy and national security? Are there limits on what information the government has a national security interest in collecting?

REP. TED LIEU: So the floor is absolutely the Constitution of the United States, right? Every intelligence agency has to comply with the Fourth Amendment, including the FBI. Now, when it comes to the private sector, the Constitution doesn't apply to them. However, I think it would be

great policy if they acted as if it did. And so, my view is tech companies, I think, should pay a lot more attention to privacy. That is my general view.

Now I just voted for a bill, by the way, uh, that is called the Fourth Amendment Is Not For Sale Act. It basically says, look, our government and law enforcement agencies can't just buy this data on you from data brokers when they couldn't have gotten it in the first place without violating the fourth amendment.

RAFFI VO: It would also prohibit any government agency from sharing any data they *already* obtained with law enforcement or intelligence agencies.

The bill passed the House in April.

It doesn't do anything to prevent these data brokers from buying or selling your data. It just stops government officials from transacting with them. So it kinda seems like the real problem is that those data brokers have access in the first place. And this bill doesn't do anything to stop them, but…I digress.

REP. TED LIEU: China doesn't have the fourth amendment. Now, I'm not willing to go and become more of a surveillance state just so we can compete with China. And so we're just simply going to not be able to compete with China in certain areas because we are a free, open, democratic society. That is a trade off of being a democracy.

RAFFI VO: That's an important tradeoff. Do we wanna live in a surveillance state, where government officials have total access to facial recognition technology? Or do we want to live in a democracy, where sometimes police don't have all the tools *they* might want in order to solve crimes?

Kashmir Hill of the New York TImes has been thinking a lot about this, and about the broader issue of accountability. Who's responsible for cases when facial recognition gets it wrong?

KASHMIR HILL: You know, when it does go wrong, they kind of absolve themselves of blame because they, like the Detroit police chief, say this is human error.

> **CLIP [(CNN 1:09-1:15) Anchor]:** *Defending the technology, Detroit's police chief blamed his officers for the error.*
> **[Police chief]:** . . . *that the investigator did shoddy investigative work.*

KASHMIR HILL: You know, we're not telling you who this person is. There's a human being that goes through and decides which, you know, photo looks like the best match. And so they say, ultimately, it's the police making a decision about who to arrest, not our app.

RAFFI: Mm-hmm.

KASHMIR HILL: And some cities have banned or temporarily banned police access to facial recognition technology until we kind of work out the answers to some of these questions.

RAFFI VO: In the absence of a federal ban, cities like San Francisco, Boston, New Orleans, Portland, Maine, and Portland, Oregon have taken it on themselves to vote in local bans on the use of facial recognition by law enforcement. Other cities have passed laws limiting its use, like Detroit.

These local bans acknowledge that at the time that many police departments got access to Clearview AI, its algorithm was unregulated, and untested. That has changed now.

KASHMIR HILL: And it wasn't until a few years later, after it already started being used by police, that Clearview submitted it to the National Institute of Standards and Technologies, this federal lab that tests facial recognition algorithms. And when it was tested, it actually performed incredibly well. It was, in that first test, the most accurate algorithm in the United States.

RAFFI: So wait, are you saying that they did have a technological breakthrough in making this or is this purely because their data set is amazing?

KASHMIR HILL:I think the data set is really helpful. It's also just that facial recognition in general has just gotten very powerful. Um, the algorithms have come a long way. You know, some people online just talk about facial recognition as a solved problem. I wouldn't say it's completely solved.

RAFFI VO: And I wouldn't either. Because the evaluation that was done by NIST falls short of examining how it performs in real-world situations. This was highlighted in a hearing this past March, held by the US Commission on Civil Rights.

> **CLIP [(USCCR 4:39:53-4:40:28 Mondaire Jones]:** *Although NIST testing provides an important benchmark of algorithms' technical capabilities, NIST doesn't test these algorithms on the actual low-quality images used by law enforcement.*

KASHMIR HILL: I mean, I spent a lot of time talking to Hoan Ton-That and I mean, I think he sees himself very much as the representative for this technology. And he is trying to convince the world that it's good for the world, you know, that this is going to help solve crimes. Some of the other people attached to the company, investors, they all had this kind of line that facial recognition technology is going to make our world more accountable. I mean, I get it. If it's always possible to tell who everyone is all the time, it might make people be better behaved because they're terrified of having every little thing tied back to them. But I also find that really chilling.

It means that a woman coming out of a Planned Parenthood could have her photo taken by protesters that are outside. We've seen a lot of calls for identifying people that are involved in protests right now. Just this idea that anything you do in public can be tied back to you by somebody who takes your photo. Yeah, I just think that we would really miss that anonymity.

RAFFI: Yeah.

KASHMIR HILL: But yeah, I mean, once these technologies are out there and shared, you really can't control how they are ultimately used.

RAFFI VO: So, now that this technology *is* out there, how do we go forward as a democracy?

We could rethink the whole relationship we have to our data — from a legal perspective. If individuals had to decisively opt-in to images of their faces being used in things like Clearview's database… it could prevent the next Clearview from even popping up.

But, as Jennifer Lynch of the EFF explains, an opt-in structure gets confusing in a hurry.

JENNIFER LYNCH: Really the question is, well, what does that opt-in consent mean? Is it just that screen that somebody clicks through to try and get to the shopping website that they want to get to? Or the app they want to download onto their phone. Or is it something that's more meaningful than that? And I think we're sort of struggling with that as a society right now.

What is necessary for opt in consent? Can it just be, I mean in the physical world, can it just be a sign when you go into Rite Aid that says we use facial recognition? And then by going into the store you've opted in? Or is that insufficient? Or is there a situation where we decide that a technology or a surveillance is so invasive or so harmful that we're just going to ban it outright?

RAFFI VO: What about a model where we don't just have to opt in, but where we actually *own* our digital data, even stuff we upload to third parties? Turns out, that might not be the right way forward, either.

JENNIFER LYNCH: Some people have said, well, the real way to protect our data and our privacy is to say that we own our data. And I think that the problem with that scenario is a problem with any kind of ownership situation, which is that it's very easy for somebody to convince me to give up my ownership of that data.

So for example, if I'm providing, um, a review to a cosmetics company in exchange for the chance to get a sweepstakes entry? Does the cosmetics company then own my data? And if I click agree, yes, that's fine. It might be because I'm thinking, well, that's just a small amount of data and it doesn't really matter that I've said that I have some, you know, skincare problem.

But the cosmetics company could then sell that data and it could be combined with lots of other data to create a picture of me, but I won't see that and I won't be able to calculate what it means to sell or get rid of my data or give somebody a right to my data. So I think that that's a challenge with creating this sort of ownership model of data. It's too easy to alienate our data to give up our rights to our property rights to that data.

RAFFI VO: Okay so…neither of those work. Both the opt-in model and the ownership model have some issues. There might be another way to frame this, though. And that is to think about our right to our data as a *civil right.*

JENNIFER LYNCH: Civil rights are inalienable rights. They're rights that exist outside of ownership. I don't have to show that I have a property interest in protected speech, for example, I don't have to show that I own my speech, it is just protected. And so if we think about privacy from that perspective, it's not, under that kind of a model, a civil rights model, it's not possible to alienate or to sell off your right to privacy because it's just protected from the beginning.

RAFFI VO: Here's Kashmir Hill again, with a hopeful reminder.

KASHMIR HILL: Some people say, okay, the technology is powerful. There's companies out there selling it. I think we're doomed. This is the world we're going to live in. You're just going to scan someone's face and know who they are. Privacy is lost. But there have been moments before where we had new invasive technologies. And we did rein them in. And a great example is bugs in wiretapping devices. There was this time in the last century where people thought conversational privacy is over. It's just too easy to record you. Your words are going to haunt you forever. And we passed laws that made it illegal to kind of secretly record people. And it's a reason why the surveillance cameras that are all over the country, you know, you pass so many every day. They're only recording your image and not audio, not recording your conversations. We decided that kind of privacy was important.

RAFFI VO: We decided that kind of privacy was important. It seems to me, we could make that same kind of decision again.

Next week on Technically Optimistic…

We're talking about a group of people whose data we are especially interested in protecting: children.

How can we safeguard our kids' data from the harms of social media?

And I'm joined by Senator Richard Blumenthal to talk about the bill he's co-sponsored to try and solve some of these problems.

That's next time…on Technically Optimistic.

[CREDITS]

Technically Optimistic is produced by Emerson Collective, with original music by Mattie Safer. Production assistance from Christine Muhlke. Our senior producer is Erikk Geannikis.

If you've enjoyed the podcast, please rate and review us – and subscribe on Apple, Spotify, or wherever you get your podcasts. Follow along on social, @emersoncollective.

And sign up for the Technically Optimistic newsletter! You'll get my thoughts about the week in tech, with lots of big questions, interesting links. And, you know, tons of ways to get in on the conversation. Subscribe for free at technically optimistic.substack.com.

I'm Raffi Krikorian. Thanks for listening. See you next time.