you are being scanned

Would client-side scanning open new doors for government invasions of privacy?

It's 1890. Responding in part to the invention of "instantaneous" photography, Samuel Warren and Louis Brandeis write *The Right to Privacy*, urging legal recognition of "the right to be let alone," which they argue must evolve in parallel with technological development.[1] Their cause for concern is that the proliferation of "devices threaten[s] to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[2]

Over a century later, unease about privacy-invading technologies persists, and numerous companies now possess tremendous power to peer into people's personal lives. Take, for example, personal device scanning technology. A practice called "client-side scanning" allows private technology companies to search the contents of consumer devices, including cell phones. This new capability, and its potential for use in concert with law enforcement and without notice, consent, or accountability, raises a bevy of privacy concerns.

These concerns took on new complexity when Apple recently proposed to scan its users' phones for child sexual abuse materials (CSAM).[3] The purpose of the search was beyond reproach: Apple intended to alert the National Center for Missing and Exploited Children (NCMEC)[4] if any found images matched images the center maintains.[5] But the announcement unsettled many consumers, advocacy groups, cryptographers, and security and privacy experts who — despite supporting the ends of this type of search — found the means overly intrusive and warned that the same technology could be used for insidious purposes.[6] What would stop Apple, or other tech companies, from providing other kinds of images or content to law enforcement despite the absence of a warrant? Or keep authoritarian governments from exploiting this new technology to suppress dissent? Apple paused roll-out of the technology, scrubbed its website of references to the most controversial parts of its original plans,[7] and then abandoned its plans entirely.[8] But the questions of how, when, and whether to use this technology will undoubtedly resurface.

In Summer 2022, we asked two experts to discuss the legal and policy questions raised by Apple's proposal. **JOLYNN CHILDERS DELLINGER** teaches privacy law and policy at Duke Law School and is the Stephen and Janet Bear Visiting Lecturer and senior fellow at the Kenan Institute for Ethics at Duke University. **DAVID HOFFMAN** teaches cybersecurity policy at Duke Law and is the Steed Family Professor of the Practice of Cybersecurity Policy at Duke's Sanford School of Public Policy and the former associate counsel and global privacy officer for Intel Corporation. Their conversation follows.

– CONNOR LEYDECKER

Editor's note: In early December 2022, prior to this article's publication, Apple announced its decision to abandon its client-side scanning plan. Because the conversation that follows originally took place in Summer 2022, it does not reflect this decision by Apple.

▸

WHY WAS APPLE'S PROPOSAL TO SCAN PHONES FOR CHILD SEXUAL ABUSE MATERIALS SO CONTROVERSIAL?

DELLINGER: Of course, we should say up front: Finding and prosecuting people who exploit and abuse children sexually is incredibly important. No one is against that. But there are legitimate concerns about how we do it. The concerns about Apple's plan arose because Apple was not going to scan its *cloud* for these kind of images — but rather was planning to scan *people's actual devices* — their phones — for child sexual abuse material (CSAM). It's an important distinction because the cloud is usually considered part of Apple's territory, while the phone is traditionally thought to belong to the user.

The technology involved Apple pushing some code and a library of hashed images to people's phones that would then alert Apple if any images on a user's phone matched those in the library of images. This library of CSAM was sourced by the National Center for Missing and Exploited Children (NCMEC).[9] If the requisite number of matches occurred on a device, Apple would provide that information to NCMEC, NCMEC would provide that information to law enforcement, and then law enforcement could come back to Apple with a warrant to get further information.

HOFFMAN: It's also important to note that Apple's proposal was to implement this "client-side scanning" only for the photos that were designated to be uploaded to iCloud. It wasn't proposing to scan all the photos on the phone. But it raised concerns that eventually the scope might broaden to include more than just the photos that were going to be uploaded to the cloud. And it also raised concerns about whether people really understood their own phones' settings as to whether an image was designated to be uploaded to the cloud. This is a setting that most people usually have turned "on" or "off" for all of the images in their phone — and if it is set to "on," then all the images are designated to be uploaded to the cloud. It's not like a handful of photos at a time are flagged to be uploaded, so that users have individual image control over which images might get scanned. So there was a concern about transparency.

WHAT KIND OF PRIVACY CONCERNS DOES APPLE'S PROPOSAL IMPLICATE?

DELLINGER: Lots of tech companies scan material that is held on their own servers for many good reasons. But historically, when you're looking at privacy law, we have this public versus private dichotomy that has purportedly informed our expectations of privacy. There are significant problems with this dichotomy because there are plenty of cases in which it is perfectly reasonable to expect privacy even when we are in public. But the idea that we expect privacy in historically private places like the home, for example, is quite resilient. We certainly have this sense that what happens in our homes and the things that we have in our homes are protected from government intrusion. The Fourth Amendment, for example, protects our persons, houses, papers, and effects against unreasonable search and seizure. Those things are seen as intensely private. While the Fourth Amendment does not apply to Apple's conduct here, Apple's proposal calls our expectations of privacy into question.

Client-side scanning means the company is scanning material that is held on a private device. And, in *Riley v. California*, we have a Supreme Court case that recognizes the privacy of material on cell phones, limiting the scope of the "search incident to arrest" doctrine.[10] So I think it's just a break, a significant one, with what people understand as private to have a third party scanning a phone's content for illegal material.

HOFFMAN: I would say that it's a significant break from what people *misunderstand* as the current separation between private and public. The current public-private distinction for data held on phones and servers is different from what people may expect. We're not talking about, at least at the current point, what Apple's recommendation was.

HOW IS FOURTH AMENDMENT JURISPRUDENCE IMPLICATED BY THESE ISSUES?

HOFFMAN: Law enforcement is not requesting this information. This is Apple deciding to do the scanning themselves. So the Fourth Amendment arguably doesn't apply when the scanning is being done by Apple. You could say later that if law enforcement was going to make a demand for this information, then potentially the Fourth Amendment would apply. But we have lots of experiences where people own devices and the companies that operate those devices maintain access to information on those devices.

I think Professor Dellinger is absolutely right that this is out of line with people's expectations of their Fourth Amendment protections. But that's generally because their expectations are out of line with what the law actually is and because, generally, the law does not restrict companies from doing this type of scanning of private devices.

DELLINGER: Well, I think it's accurate to say that the Fourth Amendment doesn't prohibit a private company from deciding to scan a device. I do think it's an interesting situation, though, because Apple has chosen to do this on its own for the specific purpose of communicating any problematic images to NCMEC with the understanding that NCMEC provides those to law enforcement.[11] It's not a situation where law enforcement has asked Apple to do a certain thing that it's now doing. So Apple is not the "agent" of a law enforcement "principal" in this sense.

Actually, I think corporations proactively taking innovative steps to protect privacy and to help solve problems is good. Consider what Apple and Google did with contact tracing.[12] Those efforts can be very positive, but I do think that there are some issues like the private search doctrine that I worry about in general, not confined to the CSAM issue: the whole concept of creating the client-side scanning technology that allows this matching and searching.

This is a search on a person's device that is limited, right this minute, to CSAM, but that's a policy decision. They could search for anything they want. I know that we as consumers have choices, and we could say "Well, that doesn't sound like a good deal. I'm going to go buy an Android." There's competition, supposedly. But I'm not sure that this supposed alternative really answers all of our questions. We need to carefully look at relationships between law enforcement and companies. We should not restrict ourselves to just looking at Fourth Amendment issues but think more broadly about what behavior may circumvent the Fourth Amendment and accomplish the same things that the Fourth Amendment was meant to protect us against.

I THINK IT'S A BREAK, A SIGNIFICANT ONE, WITH WHAT PEOPLE UNDERSTAND AS PRIVATE TO HAVE A THIRD PARTY SCANNING A PHONE'S CONTENT FOR ILLEGAL MATERIAL.

I WOULD SAY THAT IT'S A SIGNIFICANT BREAK FROM WHAT PEOPLE *MISUNDERSTAND* AS THE CURRENT SEPARATION BETWEEN PRIVATE AND PUBLIC.

HOFFMAN: I don't disagree with that. I think that we should separate these issues into two categories. One category is implementation: What was Apple planning on doing, and was that a good plan to achieve the objective? And then the second category is policy. I think you could argue this is a search, though that may depend on implementation. But regardless, one thing that's very clear to me is that without some sort of government mandate it's not a constitutionally protected search. When we're outside of those boundaries, what privacy expectations should individuals have of the entities that are providing them with technology and digital services? This is an area where Professor Dellinger and I generally agree — we need further protections in law and an establishment of norms to determine what's appropriate.

Now, when we talk about data privacy, oftentimes we gravitate toward talking about what we call "collection limitations" — or the limits on what private information can be gathered. But that's only one aspect of data privacy. There are actually eight Fair Information Practice Principles (FIPPs), which are the traditional pillars for designing a system that can realize the objectives of using data while still protecting privacy. The most impactful set of FIPPs was developed by the Organization for Economic Cooperation and Development back in 1980. And "collection limitation" is just one of those eight principles.[13] The others are: data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.[14]

Those other FIPPs all apply here. Maybe we want to allow Apple to have access to this information, to do this kind of scanning, but one of the other FIPPs, "use limitation" — or how the gathered information is used — is an appropriate control to protect privacy here. So we might say exactly what Apple said: "We're only going to use this technology for this particular purpose. And this purpose is clearly something that most people in society agree with — to reduce sexually abusive materials that apply to children and to decrease the harm that's created from that."

YOU MENTIONED ACCOUNTABILITY AS ONE OF THE PRINCIPLES USED TO OPTIMIZE THE USE OF DATA WHILE PROTECTING PRIVACY. HOW DOES A DATA CONTROLLER'S RESPONSIBILITY TO DEMONSTRATE THAT IT IS ACTING RESPONSIBLY[15] FIGURE INTO APPLE'S ACTION HERE?

HOFFMAN: Apple can make that "use limitation" promise to us, but how does Apple demonstrate it is living up to that promise? How do we ensure that there's not a mission creep where Apple starts using the scanning tool for new uses? That's a critically important issue and one that Professor Dellinger and I have been exploring in our joint research on platform accountability with the Sanford School of Public ▸

Policy, the Law School, and the Keenan Institute of Ethics at Duke.[16]

DELLINGER: I think it's interesting to raise this issue of trust and accountability because, frankly, when you look around, Apple has built a reputation for trust in the privacy area. They have branded their products with privacy. They've taken three or four steps in the past year that try to offer consumers more privacy in terms of things like cross-device-tracking and app-tracking transparency.[17] But I think that we shouldn't need to rely on trust. As Professor Hoffman mentions, there should be laws in place that provide a base level of protection.

I also want to raise the issue of normalization of surveillance, mission creep, and function creep. A lot of the concerns around this type of technology ask: Once it's created, how will it be used? Many people don't object to finding and eliminating CSAM from the internet by client-side scanning of people's devices (which, incidentally would benefit the privacy of the people who were victimized in the process of the abuse). But, once the underlying scanning technology exists and is implemented, many questions about "use limitation" and "purpose specification" (another FIPP) arise. For example, a group of 14 security experts wrote a paper called *Bugs in Our Pockets: The Risks of Client-Side Scanning*, raising these types of concerns.[18] They say it would not be difficult to reconfigure the scanner to report any targeted content regardless of whether a user intended to upload it to the cloud.[19] They mentioned how, in the EU, authorities are already seeking to use this technology to look for terrorist information and other categories of information along with CSAM.[20] We also have a situation where Apple, a company about which I have many great things to say, acts a little differently in China and has made different concessions to continue to operate in China.[21] The *Bugs in Our Pocket* folks also discuss how client-side scanning could be used as a means of repression and political manipulation.[22]

CAN PRIVATE COMPANIES STOP FUTURE ABUSES OF THIS TECHNOLOGY?

DELLINGER: The question is: Once the technology exists, how will it be used? And further: How much power does Apple really have to tell our government "No, we won't do this," when the technology exists and has already been deployed on everyone's phones? I'm just not sure that people really trust that Apple can resist. If you look at the history of mission and function creep, whenever surveillance technology makes its appearance, it does not take long for that surveillance technology to be repurposed for different and more pervasive uses than those for which it was originally intended.[23]

As for normalizing surveillance, you can look at something as basic as the social security number or surveillance of employees or post-9/11 mass surveillance. We start data collection and it increases and increases. Often this happens without transparency and in a way that eludes public debate altogether. So, coming back to the idea of the relationship between the government and companies, I don't think we can just say "Well, this is just a company, and we can just trust the company." I think we also have to look at the interactions between companies and the government and consider what the government can ask the companies to do.

HOFFMAN: I agree with most of that, but where I potentially disagree is that I think we're already in that situation. Most technologies today, whether hardware or software, already have a mechanism where, if a company wants to do client-side scanning, it can be done. We can't operate internet-connected technologies without the ability to do software updates, which is another application of client-side scanning technology.

Companies push these updates remotely to users' devices, and the user has control to accept them or not but has little to no information regarding what that software update is doing. What is the software that's being installed? We trust these entities that we're working with — that they are using those software updates to provide us with more functionality, which they will describe to us, or to deliver security patches through this update process.

If you're using an Apple iPhone, then you are already trusting Apple not to install software that is doing something different from what Apple says it does. If you are using a laptop or a personal computer that has the Microsoft operating system on it, then you are trusting Microsoft not to push software to your system that is going to do certain things. If you are using a system that has an Intel microprocessor in it, then you are trusting that Intel is not going to send you software updates that create a backdoor for access to information stored in the memory of the device. If we are already trusting these companies to install this software on our devices, how much incremental risk is it to trust them that they are not going to misuse the client-side scanning functionality?

No matter what situation we're in, we need to trust the company that we are engaging with, or else we have very little protection. It's not clear to me how Apple's proposal here — that

basically says, "Trust us" — is any different from the kind of trust it has always asked us for. Apple delivers software code to users' machines all the time, and Apple expects that users trust them — and frankly, they have demonstrated that they deserve users' trust. Apple has shown that when governments have gone too far and asked for things, particularly here in the U.S. and particularly after the San Bernardino terrorist attack [when Apple refused to create the software needed to unlock an iPhone belonging to the accused attacker], it will push back on the government.[24] Apple has fought the government before and made that fight public.[25]

So, I wonder: If we can't trust Apple, who can we trust? And if we can't trust Apple or anybody else, maybe we should just throw all of these devices in the bathtub and turn on the water and stop using them. I don't want to do that, and instead I want to focus on mechanisms to evaluate whether companies are trustworthy. At some point, we've got to trust that they're going to set a policy around "use limitations" and, that if governments ask them to use scanning technology for other uses, that Apple will make that transparent to us. And if the government tells them to keep it secret or uses some law to hide it, then we are already in that situation. So it's difficult for me to see why, as policy, this CSAM proposal is worse than the status quo, even if I can understand why, as an implementation strategy, it might be worse. In the end, we already need a better system to evaluate when we can trust technology companies. There may be a role for third-party trust evaluators similar to accounting firms and requirements for companies to make certifications to regulators that they are following their policies. There are many ways we can create systems that aid in our ability to evaluate who we can trust.

WHENEVER SURVEILLANCE TECHNOLOGY MAKES ITS APPEARANCE, IT DOES NOT TAKE LONG FOR THAT SURVEILLANCE TECHNOLOGY TO BE REPURPOSED FOR DIFFERENT AND MORE PERVASIVE USES.

IF WE ARE ALREADY TRUSTING THESE COMPANIES TO INSTALL THIS SOFTWARE ON OUR DEVICES, HOW MUCH INCREMENTAL RISK IS IT TO TRUST THEM THAT THEY ARE NOT GOING TO MISUSE THE CLIENT-SIDE SCANNING FUNCTIONALITY?

DELLINGER: I think all of the cases that you mentioned involve companies doing something that is consistent with their business models to maximize profit for their shareholders and that would be ultimately beneficial to or appreciated by consumers. If users are pushed an update that makes their phones more secure, then that is something that benefits users and that they may want. This CSAM proposal switches those incentives around a little bit, because the client-side scanning that Apple proposed is not something that is for the benefit of individual consumers who have purchased Apple devices. It is something that, even though Apple is not acting as an agent of law enforcement, effectively surveils all Apple device users and is being undertaken with the specific purpose to provide potentially illegal materials to NCMEC, which in turn will provide them to law enforcement. So this use case is very different from pushing a software update to protect consumers.

Again, I'm not saying I don't trust Apple — I do trust Apple, particularly compared to a lot of the other choices that we have — but I don't think that trust is what we should be relying on, particularly when things are happening and, more importantly, could happen to the potential detriment of consumers and their legal rights. This scanning capability is also something that is going to be on the phone of every single person who owns an Apple device. What we're talking about is nonparticularized searching, which is mass surveillance. Again, it's not a Fourth Amendment search, but it's a search nonetheless — a search of the material on the phone of every single person who owns an Apple device.

We will all be subjected to this. We are not suspects. We are not targets. We are not all people who are believed to be using CSAM. But we are all going to be subject to this type of searching by this company. If it is Apple today, it will be a host of additional companies in the future. I just think trust isn't sufficient in this case, particularly given companies' association with the government and law enforcement.[26]

In the private search doctrine, if a private party conducts a search, law enforcement doesn't actually need a warrant to search that same stuff, whatever it is — whether it's a phone or a box or a computer.[27] How does this fit in with our Fourth Amendment jurisprudence at large — with our understanding of privacy, with what's private and what's not, with our feelings about what's okay and not okay for use of devices? And like Professor Hoffman says, yeah, we could all throw these devices in the bathtub. But it ▸

would be hard to get through work the next day, given the indispensable role that these types of devices have come to play in our lives.[28]

I think that it's not going to be just CSAM detection in the end. Going back to San Bernardino, I couldn't have been more thrilled about Apple's approach. I thought they were exactly right in what they did. And I know people disagree about that, but at that time the technology didn't exist. The FBI was asking them to actually create a technology. But, in this case, the technology does exist. It has been created. The question is: When is it going to be deployed — and to what ends? And that trust you're talking about: I don't have that trust that its use will be limited.

I don't have the trust that our government and law enforcement will not end up using this in a way that Apple was not anticipating. And even if it's not our country, I think in other countries you have more serious concerns about dissent, dissenting opinions, and government. But we do have a history of the FBI tracking leaders of the civil rights movement[29] and the Black Lives Matter movement.[30] These things do happen, and I just find it highly concerning. And I don't think we have seen the end of it. In the wake of *Dobbs*,[31] which has effectively eviscerated women's decisional, physical, and informational privacy, we have to consider that future administrations could attempt to enact federal laws declaring fetuses to be "persons" or criminalizing abortion; people need to understand what surveillance could look like in that world and how the content on their devices may be used against them.[32] This technology is there and, once the technology is in use, decisions about how it can be used are very different than a situation where the government is saying "You must create a technology which doesn't currently exist." So I think that leaves us open to more problems.

HOFFMAN: To Professor Dellinger's first point about trust and accountability, I don't disagree that it would be great to have something more than trust; that it would be great to have a way to verify that these technology companies are acting in a responsible and accountable way. That's a large part of the research that we're doing in exploring different governance models. All I'm trying to say is that's where we are now. This situation does not cause a greater need for trust. It highlights the fact that we're in a situation where we don't have devices that we can use without having to trust companies. And I don't disagree that there have been companies that have made big mistakes.

However, I don't think we can point to Apple as having been one of those companies. And that's what I find interesting: If there is any company, or maybe two companies in the tech space that have stood for the principle that their users should be able to trust them, they are the one that I used to work for, Intel Corporation, and Apple.

Intel has had a policy, about which it has been very vocal, that it would never install technologies into the devices to weaken the security of those devices, and that it would not create back doors. And Apple has gone to great lengths to make privacy and cybersecurity a core part of its product offering and its competitive advantage. So I think this is what took the Apple folks by surprise. I think Apple thought, "People trust us, and when we tell them we're only going to scan these devices to stop this horrible social harm, people will trust us." Privacy is not just about collection limitation, and Apple likely thought folks would be able to trust it to enforce a policy of "use limitation" and "accountability." I probably come down on the side saying "That's pretty good, but can you build in some additional mechanisms to demonstrate that you are living up to your promises?"

When you install cybersecurity software on your machine, it scans your machine. And in many instances, it transmits information about what's on your machine back to the cybersecurity company so that it can understand, communicate about, and react to threats and vulnerabilities. We have a huge cybersecurity issue, and client-side scanning (or, as people refer to it, "end-point threat detection") can help address it. But we have to then trust that that's all that they're looking for and that the information sent back isn't going to be used in a way to harm me as an individual. I think that's a really important legal policy and societal conversation that we need to have: What are the reasonable limits of that trust? And what are the right accountability mechanisms to make sure that these companies can demonstrate that they're behaving responsibly?

And to Professor Dellinger's later points about the private search doctrine, I would agree. I actually think we do need to be careful here about bad facts creating bad law or really good facts for Apple creating bad law when we try to apply it to everybody else. Like I said, I think Apple is one of the most trustworthy companies and has invested a lot in demonstrating that. The question is how do we set up the right structures to hold other organizations accountable so that we have some degree of understanding that they're worthy of that trust.

I agree with Professor Dellinger that there's some really interesting analysis that needs to be done on the

PEOPLE NEED TO UNDERSTAND WHAT SURVEILLANCE COULD LOOK LIKE AND HOW THE CONTENT ON THEIR DEVICES MAY BE USED AGAINST THEM.

I THINK THAT'S A REALLY IMPORTANT LEGAL POLICY AND SOCIETAL CONVERSATION THAT WE NEED TO HAVE: WHAT ARE THE REASONABLE LIMITS OF THAT TRUST?

private search doctrine, and my limited understanding is that the law is not completely clear because it's very fact-specific and based on the context of the relationship between the government and the private actor who's doing the search. It's got to be more than just knowledge and acquiescence by the government. But, generally, a lot of the cases, I think, point to the level at which the government is directing the search. What does that mean in this context? What does it mean when the government may have had many conversations with Apple about what they would like to see — when the government is not directing a particular search, but it *is* directing the overall idea that searches should happen?

ENCRYPTION ENABLES PEOPLE TO PREVENT OTHERS FROM GAINING ACCESS TO THEIR DEVICES. PRIVACY AND CIVIL LIBERTY ADVOCATES CLAIM ENCRYPTION IS NEEDED TO PROTECT AGAINST ENCROACHING SURVEILLANCE OF PERSONAL INFORMATION. LAW ENFORCEMENT AND NATIONAL SECURITY ADVOCATES ASSERT THE NEED TO ACCESS THE DEVICES OF THOSE SUSPECTED OF CRIMES TO PROPERLY INVESTIGATE AND KEEP PEOPLE SAFE. WHERE DOES THIS TECHNOLOGY FIT INTO THIS DEBATE?

DELLINGER: There's a huge, ongoing, seemingly never-ending debate about encryption. In the encryption debates, law enforcement has argued that encryption hampers their ability to do their job because they can't get access to the data that they need to solve crimes. On the other hand, people will say "Well, no, we need encryption. Encryption protects the privacy of our devices and our communications. And if we don't have encryption, that's actually a security threat because a back door is a back door. It's a back door for everyone, including malicious actors, hackers, and even our enemies." This is the ongoing debate.

This encryption debate applies here because encryption could protect our communications when we create content on our devices, when we back up our devices to the cloud, and when we send messages, photos, or other content to one another. One can imagine a policy for using encryption based on where data is stored (in the cloud versus in local device storage). Hypothetically, if a company did want to encrypt its cloud, that could provide even more privacy protection to people. But Apple has not said yet (and may never say) that it's trying to or wants to encrypt its cloud.

This leads some people to wonder why Apple doesn't just limit its scanning to the cloud, rather than reaching out further to scan at the local device level, as it initially proposed. This is what other companies are doing, just scanning data stored in the cloud.[33] Apple certainly does scan data stored in the cloud but has sent fewer reports to NCMEC as a result — certainly fewer than Facebook has, for example.[34]

I imagine that if Apple did encrypt the cloud, they would get more pushback because the encryption creates an obstacle for law enforcement to access information that it may need. From the perspective of that potential future, doing this very limited client-side scanning on a phone may be acceptable to some people *if* it enabled encryption of the cloud. Of course, this wasn't how Apple's proposal was presented — this is completely hypothetical. There may still be too many privacy and security issues raised by the client-side scanning technology to buy that argument. But I'm wondering if something like that might be in the offing because Apple is a pretty privacy-forward company. Ultimately, though, even that would be a compromise of the privacy of the device itself, which could reasonably be thought of like the privacy of a person's home.

Another wrinkle to this debate is the risk of false positives created by automated client-side scanning, especially when companies do not implement adequate human review into the process. Take, for example, a father who sent photos of his son's groin to a doctor to help assist in diagnosis and whose Google account was disabled because Google flagged the father as violating its terms of service regarding distribution of CSAM.[35] The father appealed the decision to Google, but Google rejected the appeal without further explanation and notified the father that he was already under investigation by the police.[36] Even if the threat of criminal charges was unlikely, the father suffered significant harm due to "the domino effect of Google's rejection."[37] He lost emails, contact information, memories of his son's first year, and his phone number, and, "[w]ithout access to his old phone number and email address, he couldn't get the security codes he needed to sign in to other internet accounts, locking him out of much of his digital life."[38]

▸

As you mention, David, we have come to depend on these companies for so many facets of our lives, yet there is little recourse for someone involved in a situation like the one where this man found himself.

I bring up this example to make a few points. First, I want to highlight this difference in approach between Google and Apple in scanning for CSAM. Google's approach involves using technology to identify new examples of CSAM. By contrast, Apple's proposal only involved looking only for hashed images that were already on file with NCMEC. If Google had been using Apple's client-side scanning method, this situation would likely not have happened to this father and others like him. Second, the use of Google's image identification technology and occasionally flawed process in identifying CSAM is another type of technology that is subject to mission creep. Because this technology already exists, there is no reason to think that it could not be incorporated into client-side scanning. And, of course, the current goal is to protect kids, but that is a policy choice that could easily change. Last, this example shows that there are still significant dangers to privacy and civil liberty for scanning "just" the photos that have been uploaded to the cloud. So, regardless of where the scanning is taking place — on a personal device or in the cloud — there are risks involved with scanning.

HOFFMAN: Well, I find this overall topic interesting because I think there are some big implementation issues that are perplexing, frankly. A lot of people wonder why Apple did not look to some of the newer technologies that potentially would allow it to continue to just do the scanning in the cloud, even if the information remains encrypted. Generally, that approach is what they call "homomorphic encryption," which allows for observations to be drawn from encrypted data. You'll only get a yes or no answer out of that analysis. You wouldn't be able to access the image, the technology would just report out: This was a match. And then they could potentially report that information to law enforcement.

Those types of implementations are complicated. There are issues around speed, but a lot of advances have been made. There are real questions about whether this is trying to get us used to scanning images on the phone because maybe in the future, this is going to be just about scanning all images, not just those uploaded to the cloud. That raises some interesting policy questions. This is one where Professor Dellinger and I probably disagree. I'm open to that conversation about whether this proposal should have been just limited to photos that are being uploaded to or stored in the cloud. I'm not sure that this limit makes sense, given Apple's articulated goals.

If we get to the point where we're comfortable that there aren't going to be a lot of false positives, and if we're comfortable with the fact that we're really just talking about child sexual abuse materials, then is it reasonable for Apple to say "Look, we put a lot of time and energy and resources into making this device. We're not interested in our device being used to harm children. If you want to do that, buy somebody else's device. And we're going to scan for that." This is why I was puzzled by the decision to restrict scanning to images that are going to be stored in the cloud. So you're only going to catch the dumb people who abuse children? The ones who are smart and know not to upload to iCloud but figure out another way to share images aren't going to be caught? That never really made much sense to me.

YOU HAVE BOTH RESEARCHED DIFFERENT GOVERNANCE MODELS THAT MAY ADDRESS SOME OF THESE ISSUES. CAN YOU TELL US MORE ABOUT THAT RESEARCH?

HOFFMAN: The Platform Accountability Project has a research team at the Keenan Institute of Ethics and the Sanford School of Public Policy. What we've been doing is looking at how the technology platforms are generally regulated under what we would call mostly an enforcement model: We wait for bad things to happen that violate the law. Then a small group of lawyers does investigations and regulatory enforcement actions or litigation to hold them accountable. That's not the way things operate in many other industry sectors. We've been looking at environmental regulations, oil and gas, and offshore exploration. We've been looking at the financial sector and asking the question "How do these sectors hold companies accountable?"[39]

It tends to be a mix of enforcement and much more of a focus on what we would call supervision and monitoring. This idea entails either regulators or independent private parties overseen by the regulators who advise businesses on what they need to do to be in compliance and work with them to get in compliance.

Each of these industry sectors has different approaches to implement both the enforcement side and the supervision and monitoring side. We've been playing around with what those would look like with respect to technology platforms, to have a system that would be more likely to hold them accountable.

We address some of these issues in a special three-episode series on the

"Ways and Means" podcast from the Sanford School of Public Policy.[40]

WHAT SHOULD JUDGES KNOW WHEN IT COMES TO THIS AREA OF DEVICE PRIVACY?

HOFFMAN: I think it will be important for judges to understand that these issues are going to continue to come up in the context of these technologies. How far would they allow the relationship between the government and the private sector to go before it would be deemed a search under the Fourth Amendment? That's an absolutely fascinating question.

I think the other thing that would be interesting for judges to be thinking about is what role should there be moving forward for individuals to be able to hold technology companies accountable by filing their own claims. One of the things that our research team has been looking into is the potential applicability of two different laws that allow for such actions to be brought: the False Statements Accountability Act and the False Claims Act. The False Statements Accountability Act criminalizes knowingly and willfully making a materially false statement to the government.[41] However, enforcement of the law requires that the Department of Justice bring an action against the party making false statements.

The False Claims Act is even more interesting to me. Currently, it only applies to claims that are made to the government for money or property,[42] and it allows for *qui tam* lawsuits, so that individual employee whistleblowers can bring a claim stating that the representation is false.[43] But if it were modified and extended to apply in this situation, it would allow for more private enforcement. So you could imagine a situation where we would say "Okay, Apple, you're making all of these promises, we actually want you to make those in writing in a government filing and to renew that every year and make sure that you've done a full analysis that your implementation continues to comply with all of the processes that you've put in place."

And if *qui tam* lawsuits applied, so that a corporate employee wants to be a whistleblower and could challenge that claim on False Claims Act grounds, then that whistleblower would be allowed to keep a substantial amount of the recovery. That is a great incentive for whistleblowers to come forward, even if they know that their career could be substantially impacted. For example, in a 2019 case involving a software development company, the employee whistleblower recovered $4 million as part of the incentive.[44] These are the types of governance and accountability models we need to look at from a policy perspective. It would be interesting for judges to think about, if cases like that came in front of them, how they would receive them.

DELLINGER: Another thing that I would throw in for judges to consider, going back to an earlier point, is to ask when these types of searches would require a warrant when conducted by or at the direction of law enforcement? After *Carpenter v. United States*, police need a warrant to obtain more than seven days' worth of cell-site location information from a phone company.[45] But we also have some recent reporting about law enforcement just buying location data from data brokers or companies.[46] That would seem to be kind of an end run around a Fourth Amendment protection. If you would require a warrant for the government to get a week of that information directly from a phone company or an internet service provider, then why would it be okay to buy a month's worth of location data from a data broker who purchased that data from one of those companies? What really is a search? And I can answer that question for my Privacy Law class from the traditional Fourth Amendment perspective, but I'm wondering if it is changing. I'm wondering if there should be more of an eye out for what the relationship is between government and private companies. And when we're going to have these purchases of information that can be used against people and against their best interests or personal interests, then shouldn't that mean that we have a different view of companies collecting this information and to whom it is sent?

A lot of the concern is not having visibility into what happens because so many times something that might be dissent — speaking out against the government or engaging in some kind of critical activity — can be branded ▸

IF YOU WOULD REQUIRE A WARRANT FOR THE GOVERNMENT TO GET A WEEK OF THAT INFORMATION DIRECTLY FROM A PHONE COMPANY OR AN INTERNET SERVICE PROVIDER, THEN WHY WOULD IT BE OKAY TO BUY A MONTH'S WORTH OF LOCATION DATA FROM A DATA BROKER?

HOW FAR WOULD [JUDGES] ALLOW THE RELATIONSHIP BETWEEN THE GOVERNMENT AND THE PRIVATE SECTOR TO GO BEFORE IT WOULD BE DEEMED A SEARCH UNDER THE FOURTH AMENDMENT?

as a security threat. Then whatever is happening behind the scenes from an intelligence perspective may not be visible to the public for a variety of reasons that are understandable from the intelligence community's standpoint. But it's dissent, and dissent is incredibly valuable to a democracy. Now, all of a sudden, we can't see what's happening. My concern is about how searches are changing when the government has been told by the Supreme Court "Here's the rule," but then they can just go do it this other way and accomplish the same end.

HOFFMAN: I want to echo that this is a really important point for judges to start thinking about: When we do the Fourth Amendment analysis, and we think about the traditional reasonable expectations of privacy question, we get hung up on the fact that data already has been provided by the individual to someone. It gets captured under what we call the "third-party doctrine," and then is not thought to have any privacy protection anymore.[47]

Additionally, we need to start thinking more about the advanced data analytics that these data brokers operate on much of this data, whether it's data that comes from a company that's collected it from an individual or even aggregations of publicly available data and government records. This is concerning because when the government uses those insights, particularly for a law enforcement function, they can learn more than people would ever reasonably expect. People may know that they have to provide this data, but they do not expect that by examining a credit card bill someone could determine whether or not they are paying their child support, for example. Advanced data analytics and the data broker ecosystem are increasingly creating these kinds of Fourth Amendment questions.

We really need to move toward an understanding that much of this is well beyond the public's reasonable expectations of privacy.

---

1 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890) (quotations omitted).

2 *Id.* (quotations omitted).

3 In August 2021, Apple announced two new features designed to detect and thus enable protection against dissemination of child sexual abuse material (CSAM). *See* Jon Brodkin, *Apple explains how iPhones will scan photos for child-sexual-abuse images*, Ars Technica, https://arstechnica.com/tech-policy/2021/08/apple-explains-how-iphones-will-scan-photos-for-child-sexual-abuse-images/ (Aug. 5, 2021); *Expanded Protections for Children*, Apple, https://www.apple.com/child-safety/ (last visited on Jan. 15, 2022). The first feature would provide tools for messaging to prevent receipt of sexually explicit images to minors and report messages containing them to their parents, and the second feature would use a new technology to scan for CSAM images on Apple devices "as part of the process for storing images in iCloud Photos." *Expanded Protections for Children: Frequently Asked Questions*, Apple, 1, 2, 5 (Aug. 2021), https://www.apple.com/child-safety/pdf/Expanded_Protections_for_Children_Frequently_Asked_Questions.pdf. For more background on Apple's proposal, *see* Paul Rosenzweig, *The Apple Client-Side Scanning System*, Lawfare (Aug. 24, 2021), https://www.lawfareblog.com/apple-client-side-scanning-system.

4 The NCMEC, a private, not-for-profit corporation, has served as the national clearinghouse for issues relating to missing children and child exploitation since 1984. Nat'l Ctr. Missing & Exploited Child (last visited May 31, 2022), https://www.missingkids.org/footer/about. Congress provides most of the NCMEC's funding and has authorized the NCMEC to administer programs on behalf of the U.S. government. Thought the NCMEC is not itself a part of the federal government, it functions in close partnership with federal agencies and law enforcement throughout the country. Adrienne L. Fernandes-Alcantara & Emily J. Hanson, Cong. Research Serv., RL34050, Missing and Exploited Children: Background, Policies, and Issues 12.

5 Nat'l Ctr. Missing & Exploited Child (last visited Mar. 21, 2022), https://www.missingkids.org/home. *See also* Nat'l Ctr. Missing & Exploited Child (last visited May 11, 2022), https://www.missingkids.org/ theissues/csam ("U.S. federal law requires that U.S.-based [Electronic Service Providers] report instances of apparent child pornography that they become aware of on their systems to NCMEC's CyberTipline. NCMEC works closely with ESPs on voluntary initiatives that many companies choose to engage in to deter and prevent the proliferation of online child sexual exploitation images. To date, over 1,400 companies are registered to make reports to NCMEC's CyberTipline and, in addition to making reports, these companies also receive notices from NCMEC about suspected CSAM on their servers.").

6 In response to its announcement, Apple received backlash from groups ranging from civil rights organizations to privacy experts. *See, e.g.*, Jon Brodkin, *Apple photo-scanning plan faces global backlash from 90 rights groups*, Ars Technica, https://arstechnica.com/tech-policy/2021/08/apple-photo-scanning-plan-faces-global-backlash-from-90-rights-groups/ (Aug. 19, 2021); *An Open Letter Against Apple's Privacy-Invasive Content Scanning Technology*, Apple Privacy Letter, https://appleprivacyletter.com/ (Aug. 6, 2021).

7 Jon Porter, *Apple scrubs controversial CSAM detection feature from webpage but says plans haven't changed*, The Verge, https://www.theverge.com/2021/12/15/22837631/apple-csam-detection-child-safety-feature-webpage-removal-delay (Dec. 15, 2021). Following broad criticism and confusion, Apple withdrew its proposal. For more context, *see* Paul Rosenzweig, *Apple Client-Side Scanning Takes A Pause*, Lawfare (Sept. 4, 2021), https://www.lawfareblog.com/apple-client-side-scanning-takes-pause.

8 Lily Hay Newman, *Apple Kills Its Plan to Scan Your Photos for CSAM. Here's What's Next*, Wired (Dec. 7, 2022), https://www.wired.com/story/apple-photo-scanning-csam-communication-safety-messages/.

9 Nat'l Ctr. Missing & Exploited Child (last visited Mar. 21, 2022), https://www.missingkids.org/home.

10 *Riley v. California*, 573 U.S. 373 (2014).

11 *See About Us*, Nat'l Ctr. Missing & Exploited Child. (last visited Mar. 21, 2022), https://www.missingkids.org/footer/about ("NCMEC works with families, victims, private industry, law enforcement, and the public to assist with preventing child abductions, recovering missing children, and providing services to deter and combat child sexual exploitation.").

12 *See* Asmae Fahmy, *Google and Apple Join Forces to Bolster Contact Tracing*, VerywellHealth (last updated Dec. 21, 2020) (outlining the companies' efforts to enhance exposure notification during the COVID-19 pandemic using widespread Bluetooth technology).

13 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (last visited on Mar. 21, 2022), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Collection Limitation is the principle that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."). *See also 50 years and still kicking: An examination of FIPPs in modern regulation*, Int'l Ass'n Privacy Pros. (May 25, 2021), https://iapp.org/news/a/50-years-and-still-kicking-an-examination-of-fipps-in-modern-regulation/.

14 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (last visited on May 11, 2022), https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

15 *Id.*

16 *See, e.g.*, Carol Jackson, *New Series: Defending Democracy (and Us!) From Big Tech*, Duke Sanford Sch. Pub. Pol'y (Mar. 1, 2022), https://waysandmeansshow.org/2022/03/01/new-series-defending-democracy-and-us-from-big-tech/.

17 *See, e.g.*, Press Release, *Apple advances its privacy leadership with iOS 15, iPadOS 15, macOS Monterey, and watchOS 8*, Apple (June 7, 2021), https://www.apple.com/jo/newsroom/2021/06/apple-advances-its-privacy-leadership-with-ios-15-ipados-15-macos-monterey-and-watchos-8/.

18 Hal Abelson et al., *Bugs in our Pockets: The Risks of Client-Side Scanning* (Oct. 15, 2021), https://arxiv.org/pdf/2110.07450.pdf.

19 *Id.* at 18.

20 *Id.* at 5, 11–12, 38.

21 *See* Jack Nicas, Raymond Zhong and Daisuke Wakabayashi, *Censorship, Surveillance and Profits: A Hard Bargain for Apple in China*, N.Y. Times (last updated June 17, 2021) (noting Apple's privacy concessions in China). *See also Bugs in Our Pockets, supra* note 18, at 36.

22 *Id.* at 13.

23 *See, e.g.*, Andrew Guthrie Ferguson, *Surveillance and the Tyrant Test*, 110 Geo. L.J. 205 (2021); Ali Watkins, *How the N.Y.P.D. Is Using Post-9/11 Tools on Everyday New Yorkers*, N.Y. Times (Sep. 8, 2021).

24 *See* Amy Davidson Sorkin, *The Dangerous All Writs Act Precedent in the Apple Encryption Case*, New Yorker (Feb. 19, 2016) (explaining the FBI's unusual attempt to use the All Writs Act to force Apple to build something new to unlock the San Bernardino shooter's iPhone) (mentioning the All Writs Act, 28 U.S.C. § 1651, which authorizes the federal government the power to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law").

25 Tim Cook, *A Message to Our Customers*, Apple (Feb. 16, 2016) ("[W]hile the government may argue that [a backdoor's] use would be limited to this case, there is no way to guarantee such control.").

26 For more information about law enforcement requests to Apple and Google, *see Account Requests*, Apple (last accessed July 2, 2022), https://www.apple.com/legal/transparency/account.html; *Global requests for user information*, Google (last accessed July 2, 2022), https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period.

27 *See* Jeff Kosseff, *Online Service Providers and the Fight Against Child Exploitation: The Fourth Amendment Agency Dilemma*, Lawfare, 1, 2 (Jan. 2021); Jake Holland, *Facebook Data Releases to Cops Evades Fourth Amendment Limits*, Bloomberg Law, (Apr. 29, 2022), https://news.bloomberglaw.com/privacy-and-data-security/facebook-data-release-to-cops-evades-fourth-amendment-limits.

28 *See* Kashmir Hill, *I Cut the 'Big Five' Tech Giants From My Life. It Was Hell*, Gizmodo (Feb. 7, 2019), https://gizmodo.com/i-cut-the-big-five-tech-giants-from-my-life-it-was-hel-1831304194.

29 *See* Alvaro Bedoya, *Privacy as Civil Right*, 50 N.M. L. Rev. 301 (2020).

30 *See* George Joseph & Murtaza Hussain, *FBI Tracked an Activist Involved with Black Lives Matter as They Traveled Across the U.S., Documents Show*, The Intercept (Mar. 19, 2018), https://theintercept.com/2018/03/19/black-lives-matter-fbi-surveillance/.

31 *Dobbs v. Jackson Women's Health Organization*, 597 U.S. ___ (2022).

32 *See, e.g.*, Gideon Lichfield, *How Might Your Data May Be Used to Pin Charges on You?*, Wired (July 12, 2022), https://www.wired.com/story/how-might-your-data-be-used-against-you/.

33 *See, e.g.*, Ernesto Van Der Sar, *Google Drive Uses Hash Matching to Detect Pirated Content*, TorrentFreak (Feb. 11, 2017).

34 Tom Porter, *Facebook reported more than 20 million child sexual abuse images in 2020, more than any other company*, Business Insider (Feb. 26, 2021), https://www.businessinsider.com/facebook-instagram-report-20-million-child-sexual-abuse-images-2021-2. *See also* Alex Hern, *Sites reported record 29.3m child abuse images in 2021*, The Guardian (Mar. 24, 2022), https://www.theguardian.com/technology/2022/mar/24/sites-reported-record-293m-child-abuse-images-in-2021.

35 Kashmir Hill, *"A Dad Took Photos of His Naked Toddler for the Doctor. Google Flagged Him as a Criminal,"* N.Y. Times (Aug. 21, 2022), https://www.nytimes.com/2022/08/21/technology/google-surveillance-toddler-photo.html.

36 *Id*.

37 *Id*.

38 *Id*.

39 *See* Podcast, *Defending Democracy (and Us!) From Big Tech*, Duke Sanford Sch. Pub. Pol'y, (Mar. 1, 2022), https://waysandmeansshow.org/2022/03/01/new-series-defending-democracy-and-us-from-big-tech/ (This three-episode series describes the results of the professors' research on Platform Accountability). *See also infra*, notes 33–36 and accompanying text for a podcast in which the authors' discuss their research in this area and examples of different regulatory models used in these types of industries.

40 *Id.*

41 *See* 18 U.S.C. § 1001 (prohibiting the knowing submission of "any materially false, fictitious, or fraudulent statement or representation" to the government).

42 31 U.S.C. §§ 3729–3733. *See The False Claims Act*, U.S. Dep't Just. (last updated Feb. 2, 2022), https://www.justice.gov/civil/false-claims-act ("The FCA provided that any person who knowingly submitted false claims to the government was liable for double the government's damages plus a penalty of $2,000 for each false claim. The FCA has been amended several times and now provides that violators are liable for treble damages plus a penalty that is linked to inflation. In addition to allowing the United States to pursue perpetrators of fraud on its own, the FCA allows private citizens to file suits on behalf of the government (called 'qui tam' suits) against those who have defrauded the government. Private citizens who successfully bring qui tam actions may receive a portion of the government's recovery.").

43 *See Provisions for the handling of qui tam suits under the False Claims Act*, U.S. Dep't Just. (last updated Jan. 21, 2020), https://www.justice.gov/archives/jm/criminal-resource-manual-932-provisions-handling-qui-tam-suits-filed-under-false-claims-act ("One of Congress's objectives in modifying the Act was to encourage the use of qui tam actions in which citizens are authorized to bring, as 'private Attorneys General,' lawsuits on behalf of the United States alleging frauds upon the government.").

44 *See* Press Release, *Informatica Agrees to Pay $21.57 Million for Alleged False Claims Caused by Its Commercial Pricing Disclosures*, U.S. Dep't Just. (last updated May 13, 2019) ("The whistleblower, who is a former employee of Informatica, will receive $4,314,000.").

45 *Carpenter v. United States*, 138 S.Ct. 2206 (2018) (holding that the government's warrantless acquisition of about a week of cell-site location data showing Carpenter's movements violated the Fourth Amendment and declining to extend the "third-party doctrine" where data disclosed to a third party carries no reasonable expectation of privacy).

46 *See, e.g.*, Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, Brennan Ctr. Just. (Apr. 16, 2021) ("The IRS is not alone in circumventing the warrant requirement by simply buying location data. The FBI, Department of Homeland Security, and Department of Defense have all been caught secretly purchasing cell phone location information, as well as other sensitive consumer data.").

47 The doctrine arose from *Smith v. Maryland*, 442 U.S. 735 (1979) ("This Court has consistently held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). A growing number of scholars are calling for it to be overturned now that consumers must increasingly rely on third parties to use devices that are themselves increasingly necessary to participate in basic functions of society. *Compare* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561 (2009), *with* Erin Murphy, *The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 Berkeley Tech. L.J. 1239 (2009).