If you look at the middle part of the graph, 2,000 of these apps, they are like, OK, I need this permission, but I also have a third-

We assured the users that-- I don't know if you can see it, but there is this library, which is present in these particular apps on your phone. Which decision would you like to make? Do you want to allow the location to this particular data, or deny it, or fake it?

We send them a reminder that you recently made this decision. Do you want to change it? And

While denying, the users mostly said that it's about, I don't really see a use case of my data. I don't really see why my data is being used. So they tended to block more. They wanted the libraries to earn their trust before they were willing to share their private data.

So overall, we introduced this app. We had organic users. And we support our system by crowdsourcing. So if only one user sees a particular app permission, we will know it. And we can display it to the other users in the form of the notification that this app is known to access your private data for this particular use.

So based on the results from 1,300 users, the number of decisions that you have to make reduces by 25%. And your protection increases by a similar number. So thank you.

[APPLAUSE]

MARK EICHORN: Thank you. Our third panelist is Ian Douglas. He's a colleague in the Office of the Privacy Commissioner of Canada.

IAN DOUGLAS: Afternoon. So we decided we would take a look at health and medical devices and try and come up with a scoring system for them as to how they dealt with and protected privacy. So our initiative was proactive in nature. It wasn't a result of any investigations. There was a GPEN sweep. And GPEN is a group of DPAs worldwide that, every year, do a sweep to see how privacy is going through the world.

And we basically picked a bunch of devices that they had. So it was kind of a random choice. And based on the groupings that we had, we added a few more devices. So we had three in each category.

We tried to do trend analysis. And there was absolutely no enforcement actions at all. This was an educate and guidance initiative. And when we found something of interest, we would talk to the manufacturers, and we would let them know what it was we were concerned about or found. And in most cases, they would immediately make a change.

So the prescto

being used, whether or not they were outdated and susceptible to attacks. And then pairing whether or not the device was always on, always listening, easy to connect to.

For consent, we basically took the total number of [INAUDIBLE] elements that were optional. We put them over all of the data elements that could be collected. And we used that ratio to come up with the number at the end of the day.

OK. My last line. OK. So we know the amount of data collected was quite varied. We had expected to find a lot of PI, but it wasn't. It was a lot of the developer SDKs were actually sending information back about the device.

So it would talk about the power the thing had left, how many times it had been used, stuff like that. And we realized that, OK, that shouldn't really be included in personal information.

The sharing was not as high as we expected. As I said earlier, we thought it was probably going to be something like 40 people that it would be shared with. And it wasn't. It was down around six, and a lot were only at two or three.

The established medical companies had much better safeguards than the newcomers to the game. They would make more errors, possibly in their selection of components. We had a weight scale that would turn on a access point, because the developers didn't realize that the component they had selected actually included an access point in it. And it also had a web server in it, which allowed for web configuration of the device.

It was password protected, but the password was very easily guessed. And we found another device that, when we updated the firmware on it, started sending out thousands of emails. And the email addresses were basically all of their users.

So we contacted them. They, three days later, put out a patch. It's fixed.

Scrubbing data was not always easy or possible. So we couldn't find instructions on how to do it in some cases. So if you wanted to get rid of it, you couldn't. The only way you could get rid of the data was to o 0 (w)2 (a>>BDC 0 -2.32 Td [(S de)4 ((r)3 (8(t)-2 (r)3 (i)-2 2Tc 0 Tw (cI 3PE -3.85 -)-6 (a v

All right. So we released our digital standard around this time last year. And our digital standard is a collaborative project that we completed with ranking digital rights, disconnect, and the Cyber Independent Testing Lab. The standard is designed to set expectations for manufacturers when they're developing connected products to make sure that they're keeping consumer privacy and security in mind, along with other digital rights, such as ownership and governance.

So as I said, this is the first time we have released testing results on our digital standard. And the goal of the standard and our testing under it is not only to educate consumers about the security and privacy options available to them but also to help incentivize or influence manufacturers when they're designing and producing these products themselves.

Although the digital standard is designed and can be used to analyze a large array of connected products or services, we thought smart TVs were a very convenient and obvious place to start. They are a hugely popular option for consumers. Many of the top TV models are also smart TVs. And we saw a huge number of connected TVs on the market in 2017, and that number is only expected to come up. In addition, smart TVs are able and are transmitting a huge amount of data about users and their viewing habits back to the manufacturers and the business partners.

So to conduct this test, we selected five TV models-- an LG, a Samsung, a Visio, a Sony, and a TCL Roku. Now, all of these models, except for the TCL, are recommended Consumer Reports models using our regular testing based on color clarity, ease of use, et cetera, but not assessing them on privacy and security.

The testing I'm presenting today was undergone with ranking digital rights and disconnect. In order to evaluate the TVs, we not only looked to the policies the consumer is presented with, but we also looked at the consent and data flows, along with security vulnerabilities.

So no surprise here. All the models that we tested want to watch what you're watching. So they do this using automatic content recognition, also known as ACR and other methods.

ACR works by taking little snippets of whatever you're watching, even if it's a kind of dumb product like a DVD or Blu-ray disc, in order to assess what you're watching. And then companies are collecting and using and processing this data not only to serve up targeted ads, which you may expect, but also to get at some of the more quiet companies, like Netflix, that have kept a lot of their viewing data in-house.

The TV policies that we also assessed stated that they could use the data from your viewing habits on these TVs in order to serve up ads to you on other devices that happened to be on your home network. We also found that consumers, although they can limit the data collection-- you're really undermining the functionality of the smart part of your TV. And we also found two models had concerning security vulnerabilities.

So ACR, not that new. But it has been around for a few years. It was a subject of an FTC action recently which led to a settlement with Visio for $1.5 million last year. Visio was collecting this viewing data from users, like we saw here in our TV models, but they were doing it without knowledge and consent of the user.

The FTC deemed that this was an unfair practice. And in her concurrence, Commissioner Ohlhausen said that viewing data is considered sensitive information. So you have to get consent from the user. But what does consent actually look like?

Here we have a screenshot of our Sony model that we tested. You can see that this is a consent prompt, and the user is asked to either say yes or no to a privacy policy. However, there's not a dedicated prompt letting the consumer know not only that ACR is happening but also the ability to opt in or out, although it is buried in this privacy policy.

So the question that is presented is whether or not this is effective notice and consent to the user. One good comparison to this example here is a Sears case of a few years back where the company buried the disclosure that they were using software to track users browsing data in a lengthy user license agreement. The FTC required the company to clearly and prominently disclose the types of data the software would monitor, record, or transmit.

So the question in here is, is this prominent disclosure? It's unclear. But we did find, via a reader poll that was conducted after we released our report on these findings, that 43% of respondents did not know that their smart TVs were transmitting data back to the TV manufacturers and their business partners.

In addition to this concern, many users may not realize that they can actually say no to these privacy policies. We've been conditioned, using our online services and apps, to see it as a take it or leave it situation where, if I'm going to use an app on my phone or go to a website, I have to agree to their terms of service and privacy policies in order to proceed or use their services.

That's not the case with these TVs. And for the models that we tested, users could actually say no. And yes, at some point, maybe they'd be undermining the functionality of their TV. But I don't think that users would necessarily know that they could say no to these policies and still proceed in the set up of their TV.

In fact, some of these pages even tell them that that's not possible. So here, we have the Samsung consent prompt. And as you can see, it's set up so that the user will say yes to all of these, despite the fact that the user does not have to. In addition, the screen tells the user that they have to say yes to these in order to proceed, despite the very tiny little skip button up there in the right-hand corner, which still lets them set up their TV without agreeing to these policies.

So as I mentioned, consumers can say no to some of these policies and, therefore, disagree and not allow some of this data collection. But then you're also losing, as I said, the functionality of the smart part of your new TV.

This is another consent page that we are presented with. This is the LG model. And in contrast to some of the other TVs that we tested, this is a more granular consent regime. So not only do you have here on the left hand side-- they're telling you what you're agreeing to in simple title language. But you also can turn off and on the functions as you see fit.

So this viewing data is collected for two primary reasons. One, for advertising. And then, two, to also recommend that, since you watched Game of Thrones, you may also like x, y, and z show.

One is clearly helpful to the user, and LG, here, lets you use your viewing data in order to have the smart TV recommendations that you may like this other show while also saying that you

And while that's upsetting, I do want to emphasize that the concern here is the fact that you can actually use the data from these TVs to correlate with activity on other devices and serve more targeted ads. And I don't think that many people are buying smart TVs with that understanding.

In the future, we plan to publish more detailed findings from our smart TV test. We also plan to use the digital standard that I spoke of earlier to do assessments of other similar products and services. We also plan to look at criteria that we didn't get to look at in this test, such as interoperability and repairability.

And as a final note, thank you for letting me talk to you about our test results today. And I encourage you to go to TheDigitalStandard.org and contribute to our digital standard, which is an open source project, and give us any input you might see through our GitHub. Thank you.

MARK EICHORN: Thank you, Katie.

[APPLAUSE]

Norman Sadeh is a professor in the School of Computer Science at Carnegie Mellon University.

NORMAN SADEH: Thank you. So I'd like to talk today about a paper that was presented back in July at the Computer Vision workshop on privacy and security. The first author on this paper appears first. Unfortunately, he's not available to present, and so it's fallen upon me to try to do my very best here. The first author is Anupam Das, and there are a number of other people who've contributed to this paper, as well.

As I think we all realize to some extent, there are lots of cameras out there. Cameras have been deployed on a very broad scale. You might have come across a number of different statistics. Some people have said that on a typical day, we tend to come in front of something like 70 or more cameras, and that's probably not mentioning all the cameras that we have in our pocket.

And so as this happens, the question is to what extent people

And so what sorts of applications are behind these cameras? As I said, it could be monitoring and surveillance. But it's also lots of marketing types of scenarios that are being pursued, so scenarios where you walk in front of a store window and you've got cameras observing you, trying to look at how you're responding to different kinds of products, what products you're spending more time looking at, but actually also adjusting advertising offers that are being shown to you based on demographic information, based on your gender.

And in fact, even people experimenting today with customized ads where they're going to recognize you as a customer specifically and start offering you specials that are in the menu based on what they've identified as potentially being your preferences. So clearly, lots of different scenarios are being experimented with. I could go on with a very long list here of applications.

I'm sure that many of you are familiar with Facebook Moments. The display here shows you a few other types of scenarios, the specialized recommendations based on who you are at the restaurant. I'm sure many of us have heard about the Amazon Go store that's trying to figure out what you've been purchasing and charging you as you exit the store without requiring any interaction on your part. So many, many different kinds of scenarios, clearly.

And obviously, all this data can be mined, also, and that can lead to yet a number of additional inferences about your preferences, who you tend to go out with, what your health situation might be, and all sorts of other things that are fairly easy to identify as potentially sensitive for a variety of different people. And so when it comes to regulation in this space here in the US, as I think we all realize, we certainly don't have any regulation that cuts across the board and addresses the collection of this data.

There are a few states that have regulations when it comes to identifiable biometric identifiers. The ones that I'm aware of are Texas and Illinois. So in those states, only according to law, you have to disclose the collection of this type of data, which covers data being collected by cameras. It requires even some form of consent.

Obviously, in Europe, they've taken a different approach. In other places, they've taken different approaches. So certainly, if you're looking at GDPR, there's an expectation that these things will be disclosed and that you're going to be obtaining what is referred to as "affirmative consent," whatever that means. They're still in a process of trying to define at this stage how that's going to be interpreted. We can expect these things to evolve over time.

But what we wanted to do in our research is we wanted to better understand how people feel about these scenarios. And obviously, there are potentially different views. You might say, well, at this point, everybody knows there are cameras everywhere. So chances are they're already expecting this, and maybe we don't necessarily need to go overboard here in terms of notifying them and potentially allowing them to explicitly or requiring them to explicitly opt in or allowing them to opt out, depending on which particular approach you want to take.

And so we've done these studies in particular. In fact, one of our colleagues [INAUDIBLE] presented a paper earlier today on research that we've done across a number of IoT scenarios.

That study that you presented earlier today, in fact, included a number of scenarios that were centered around the use of cameras and facial recognition.

And so they could be deeper as far as that study is concerned, the kinds of results that you get when you ask people how they feel about many of these scenarios. And for those of you who, perhaps, were not there when this was presented, this is a vignette study where we asked a number of people to think about a variety of different IoT scenarios, including scenarios where facial recognition would be used, placing people in as realistic as scenarios we can through these vignette studies, requiring them to tell us how comfortable or uncomfortable they are with the scenarios, as well as tell a varn(a)-10 (r)-1 (i)-6.1 (o)-3.9 ,

And so work has revolved around trying to see to what extent we could actually develop an infrastructure that would support notice and choice in the presence of cameras and, more generally, in the context of other types of IoT scenarios. So this research is being conducted in the context of a larger project that's called the Personalized Privacy Assistant Project. And today, I'm talking specifically about camera notice and choice within that context, which, in its own right, is actually very rich and for which we're planning to make an infrastructure available within roughly a couple of months.

And so how does this work? Well, the basic idea, if you think about it, is not terribly, terribly complex. The basic idea is that there should be, in fact, a mechanism whereby we might be able to discover the presence of these cameras and whereby we could use this to notify users about what these cameras are doing.

Are they just capturing footage? Are they retaining that footage for a minute? Are they retaining it for the rest of times? Are they mining it to death? Wd ohituringcomg timeg it to cta(e)-14 (y)22 (min)2 d2 (ta)
tmsshts(der4 (s)-5 (t)-6 co)-6 (ver4 (er)-2 (ha)62 (er4(b(t)-6 ,)-4 ((-a)4 d)-4 ((f-a4 -9 (af)-5 (c t)--1 (,ers)-5 (o)

of the mobile apps. We've shown we can learn people's privacy preferences. And so we're hoping that, through the same type of learning, we might be able to help people configure security settings semi-automatically, occasionally verifying with them that what we're doing is consistent with their expectations.

So we've also done some real-time denaturing of camera footage. I don't have the time to show you that. But at the end of the slide, there is an SQR code. And so if you want to see a demo of how that would work in real time, whether you want to opt in or opt out of some of these

According to the National Center for Victims of Crime, 7 and 1/2 million people were stalked in one year in the US. 61% percent of female victims and 44% of male victims were stalked by a current or former intimate partner. An estimated 15% of women and 6% of men have been a victim of stalking during their lifetimes.

And then as far as the role of technology in all this, a little bit less research has been done about that. But in your paper, you cite interviews with victims of domestic violence, intimate partner violence. And basically, three of 15 people interviewed said that tracking software seemed to play some role in that. So that's 20%. That's a pretty significant sign that this is going on.

But I guess my question, Peri-- and it's sort of a question for everyone, as well, because one potential fix to the problem that you raise is this fact that something could be on my phone and I don't know about it and that the platforms have rules about icons being visible. So those could be better enforced.

But it raises some interesting questions about the role of platforms, in part because, as you mentioned in the paper, there's also stores that are not the official store provided by the platform that provide this software. And so even if the app store policed its apps better, they might not be able to completely solve the problem. But do you have any thoughts on that?

PERIWINKLE DOERFLER: Yeah. And that's an important point that I don't think I highlighted as well in my presentation as I could have for lack of time. We focused mostly on Android apps in the study, but iPhone apps also exist. And on both Android and iPhone, there's an official app store. And for Android more so than iPhone, you have the ability to download apps that are not on that store. Those are some of the more malicious ones.

But the one I demoed, for example, is freely available on the app store. And when you've got that paid version on the phone that was passed around, you couldn't find an icon for that app. There's no notice that it's recording. There's no notice that it's tracking. It's nothing at all. If you were the person that owned that phone, you really wouldn't know it's there.

And that's directly in violation of a lot of Google's policies that developers have to agree to when they sign up and put their apps on the app store. But the issue is that those policies aren't enforced.

In contrast, the same app exists in the Apple ecosystem, and those capabilities aren't there. In fact, you see would-be abusers get very upset in TrackView's customer support forums, because they can't find a way to hide the app icon if their victim has an iPhone. And that's because it's not possible, because iOS, as an operating system, does not allow that, whereas Android says you can't do that but then, as an operating system, doesn't enforce it.

So I think in that particular case, there's a pretty good reasoning that it can be done on an operating system level, and maybe it should. That's certainly not a universal answer. But I think there are some places where we could see operating systems make some changes. But with some things that are more nuanced, it's a little more difficult.

Or you talked about various tradeoffs between how many parties it's going to and the type of information and so forth.

Is privacy too context dependent to really sort of scale this up so that you have one type of test where it would work for both smart TVs and other types of products? And maybe, Katie, you can start on that, since you guys have been developing the digital standard. And I know it's to be applied in a lot of different contexts.

KATIE MCINNIS: Yeah, so one thing that we've been working through with the digital standard

For now, we're trying to do a high, low, medium type model at the end of the day. But it's still hard to say, OK, how many is too many? And that's where it gets difficult.

MARK EICHORN: Great. OK. All right, for Peri, here's a question from the audience. Will a factory reset get rid of a hidden tracking app on a phone?

PERIWINKLE DOERFLER: That's a great question. "Sometimes" is the answer there. It depends on the nature of the application, how it's installed, whether the phone is rooted or jailbroken.

Anything that's come directly off the Android or Apple Store, probably yes. Most things that have come off of the open web, that depends on whether the phone has been, in the case of an iPhone, jailbroken, in the case of an Android, rooted. If it has been, then no, probably not.

The other category of apps that we looked at a lot that we talk about in the paper are things like Verizon Family Tracker, which come prepackaged with your OS if you buy a phone directly at the Verizon store, which you cannot get rid of, no matter what you do. So yes and no. The answer is sometimes.

MARK EICHORN: And are there any phones that you cannot put this tracking software on? I know there are phones where you can't get it off.

PERIWINKLE DOERFLER: Yeah, so it's specifically the apps that are packaged with the OS. So if you buy a new iPhone, Find My Friends is installed, and you can't uninstall it. Similarly, if you buy a new Android, Gmail. You cannot uninstall Gmail no matter what you do.

It's the same thing where there's some of this stuff layered on top of the OS that you can't get rid of. The two major operating systems are Android and iOS, and those are the ones that we've looked at, Android more so than iOS.

I don't know about Windows phones. I mean, it's possible that there's different things there. I, myself, have a BlackBerry. But BlackBerrys are Androids these days, so I can't tell you about when BlackBerry had its own operating system. Yeah.

MARK EICHORN: A question from Twitter for Norm. I guess, do tools to help users opt out include opting out from surveillance for law enforcement purposes? For example, in public streets or possibly secret operations. If so, have you considered those interests? So I guess this is considering that this will be rolled out in the future and will be pretty ubiquitous.

NORMAN SADEH: So realistically, we believe that the first step in terms of making this technology useful will be to focus on notification, right? And obviously, opting out in terms of government surveillance, I think that's an illusion. It's probably even an illusion in terms of notification in some regard, I think.

So the focus, however, is, number one, on making people aware of what's being recorded about them. So I think, under some regulatory regime, there is actually pressure to do that. In other

places, we're hoping that people will just find it's a good idea. You certainly find many places these days where people have a sign saying this room is under video surveillance, except that the sign is very tiny, and 90% of people in the room will never see it. So we'd like to, obviously, overcome that.

In terms of opting into different practices, again, I think, in some jurisdictions, there will be a need to obtain a form of consent. In others, that might take a bit longer. And so we're going to have to see how things evolve.

We're also hoping that people will-- so our registry can be managed, also, by activists. So we're hoping that some of these registries will just be populated by activists who will say, well, I've spotted these cameras. And whether or not the people who actually own these cameras are willing to admit that these cameras are there, we would like to see some people indicate that these cameras are there, potentially even speculate as to what these cameras might be doing.

And we would like these registries to acknowledge that some of the things in these registries are more credible than others. And so if the registry is managed by a building and the building says that it has a camera that does x, there's a good chance that, in fact, it does x. On the other hand, if it's a registry that's managed by activists, the manager will be speculating. So we'll try to also support differentiating between these different scenarios.

sctnarilacis a camferi |OMARK EICHORN-11 (. Aha)4 (S-5 (eava)4 (i)-2 h(c)4 (a)4 ,(.)-2 ( )2-10 i)-2 (

MARK EICHORN: I had a question for you as well about, have you thought about different scenarios for this? Because it seems like the same kind of idea could be used for other types of tracking, like mall tracking, where I don't normally have a lot of insiMalsR32sR31 (i)-2 \ÓMalRHOMRMN (O)

So that's one way, but I don't see it happening in the near future. So the alternate would be limiting the data which is sent out from your device. So if people actually want to block a lot of it, you obviously can't break the entire third-party library model.

So you would want to limit what flows you would want to inform the user that, OK, this is happening. And you would want to have an option to opt out. Like right now, it's all or nothing. Either you give your data to the third-party libraries or not.

So I'd like to see a ecosystem where the users have more control over their data. The users should be like, OK, I want to block my data for this particular library. And then you can sort of limit it that, OK, you can block for this particular thing but not for every particular thing. As long as users know about it and users have control over it, that would be an ideal place.

MARK EICHORN: OK. All right. Let's see. I guess one final question, then we'll roll into Neil's presentation. But Katie, this is a question for you. Do you view the FTC's Visio decision as setting an industry standard requiring opt-in consent from consumers for ACR features? And I guess I'll take the opportunity with this question to note that our colleagues in New Jersey worked with us on that matter, and some of them are here today.

KATIE MCINNIS: That's right. I should have mentioned New Jersey in that decision. But 10 minutes, what a tight time.

Yeah, so I think that's up to, obviously, to some extent, the FTC. But we've seen that the companies-- a lot of their privacy policies were updated after the FTC decision, which also was around the start of the year. So maybe they were just refreshing everything. But I do see that these TVs have obviously tried to be in compliance with that. So maybe it is setting an industry standard.

In any case, I think, anytime your data is being collected, you should have some kind of notice. So the Visio decision is only effecting one company. But definitely, I think the other companies have tried to disclose and let consumers know what's going on.

And to some extent, consumers are benefiting from this practice. I definitely want some TV recommendations, and so I would benefit from the practice. I may not want it to be used for advertising, however. So it's good to know what's going on, I think, with your devices and what they're transmitting.

MARK EICHORN: With that, let's give the panel a hand. And our chief technologist is coming up to speak.

[APPLAUSE]

Thank you all.

NEIL CHILSON: Thanks, Mark. And thanks to the panelists. And thanks to all of you for being here today. Quite a day, huh? We started with Commissioner Chairman Ohlhausen's remarks this

morning. We had 20 fascinating, very detailed presentations, four panel discussions, a lunchtime poster session. And I'm sure, somewhere in there, you all squeezed in a quick read of our mobile data security update report. So great job.

So I just want to share three things with you really quickly. First, I'll offer quick thoughts. Basically, one thought per session of my takeaways of today. Then I'll give a really high-level picture of how maybe policymakers and engineers should think about solving some of the problems that we heard about today or generally in the technology space. And then I'll end with some quick thank yous.

So first, some observations. I learned so much today. I'm going to limit myself to one per session. On the first session about collection, exfiltration, and the leakage of private information, each of the panelists set out quite concerning scenarios involving a wide range of technologies-- IFTTT recipes, browser extensions, session replay scripts.

I was heartened to hear, at least from three of the panelists, that, upon publishing their research, companies took action to address some of the problems, at least in part. That, to me, must be really gratifying as a privacy researcher, and I think it shows the great value of this sort of research. So that was kind of my takeaway from session 1.

Session 2 on consumer preferences, expectations, and behaviors-- I think one thing that I took away is that there's a lot of unease by consumers when they encounter new technologies, whether that be connected toys or the mTurk system, and that even in cases such as the mTurk system, where it was pretty clear the user had full knowledge-- I mean, they participated in the system, and they didn't always know what the information was being used for, but they knew a lot about what information they were giving. And they knew something, at least, about that they were getting paid for it.

Even after they had done that, they felt some regret in many cases. And I thought that was interesting. Even when they had considered tradeoffs, they still felt unease about the use of their data.

And that actually rolled into my takeaway from panel 3. I mean, the idea there, I thought, that came through to me the most was the real need to look at real choices that consumers make when they're faced with two different options or when they're faced with tradeoffs. And how do they make that?

And I thought there was a lot of consistency, actually, in the reports, the studies, especially the two who are on the far end, between what they took away from the data, essentially, that consumers didn't seem to value this that much or that they seem to have a real disparity between what they said they cared about and then how they acted. Now, I think they had kind of different takes on what that meant. And I think that comes down to whether or not you think that the expressed preference is the real preference and that consumers are subsequently being sort of tricked into sharing their data when they don't really want to, because they said they didn't, or if you think the stated preference is sort of their tradeoff-free version of how they would make

decisions and that the revealed preference when they're actually faced with choices is the real one.

way is so good. It's so orderly. And in fact, he imposes those designs on everybody in Legoland, or he tries to. Both through force and also through, essentially, propaganda-like advertising.

But there is this team of rebels in this movie. And there's a boring guy named Emmet, who's kind of an every man. And these rebels, some of them are expert builders. They're really good at crafting things on the go, on the fly, with the materials that are near them, to solve the specific problems that they face.

And Emmet is not an expert. He's actually really bad at this. And his designs get mocked by his fellow rebels all the time. But ultimately, they actually turn out to be useful, even if they're really ugly and weird.

And the main thing is that Emmet and his rebel friends, unlike President Business, they're really just trying to solve the problem that they're faced with the materials that they have at hand. And they apply their sort of local knowledge and their own creativity to solve those problems.

And so needless to say, President Business doesn't like these guys. They really mess up his plans, even more so than the regular residents of Legoland. And so he gets really tired of this, and he ultimately decides he's going to just superglue his designs everywhere. That's a spoiler, by the way. Sorry.

He's going to superglue everything into place so nobody can mess up his plans. And obviously, a fight ensues, and the heroes win, largely because they convince everyday Lego people that it's OK to make your own designs and try to solve your own problems with the tools that you have.

So what's this have to do with tech policy? Maybe the parallel is obvious. I mean, it is to me. But I'll walk through it a little bit.

I'm an engineer. I'm often asked to help solve policy problems. And there's a real temptation as an engineer to come up with the solution.

Surely we can do legal code the same way we do computer code, where we consider every possibility, and we account for it. But the real problem is that humans aren't bits. They're not billiard balls or Legos.

And so as individual humans interact, they create a sort of dynamic, non-linear, nondeterministic system that we call society. And it's not total chaos. There's lots of patterns-- social and ethical norms, markets, institutions, political structures. These are all patterns in society.

But these patterns are le cal prolut2 (of)3 (d)-20 (yd(a)6 (ll p)2)]TJ 0.01 2.