EPISODE 09

[INTRODUCTION]

[0:00:00.7] JM: The internet is decreasing in privacy and increasing in utility. Under some conditions, this tradeoff makes sense. We publicize our profile photos so that people know what we look like. Under other conditions, this tradeoff does not make sense. We do not want to television that costs less to purchase because it is silently recording all of the conversations that takes place in the room and selling them to highest bidder.

The example of the TV that records everything you say just because it's cheaper, which is actually a real thing. This product actually exists. Samsung makes it. I have a link in the show notes, but this illustrates a tradeoff of the internet. The advertising industry pushes towards lower marginal costs for the products and services in exchange for less privacy.

Someday we will live in a world where it will be easy for consumers to control the dial on the tradeoff between privacy and the price of the services that they get from the internet. Until then, we have almost zero control over what information the advertising surveillance industrial complex knows about us.

Bill Budington is a security engineer with the Electronic Frontier Foundation. In today's episode, Bill describes some of the current techniques used by the advertising industry to track your activity through the web. Bill works on encryption tools as well as Panopticlick, a project that allows users to see what trackers they're vulnerable to.

Software Engineering Daily is having our third meet up, and I hope you're able to attend. It's Wednesday, May 3rd at Galvanize in San Francisco. The theme of this meet up is fraud and risk in software. We're going to have great food, we're going to have engaging speakers, and there is always a friendly intellectual atmosphere. To find out more, go to softwareengineeringdaily.com/meetup.

[SPONSOR MESSAGE]

[0:02:00.7] JM: Software engineers know that saving time means saving money. Save time on your accounting solution. Use FreshBooks Cloud Accounting Software. FreshBooks makes easy accounting software with a friendly UI that transforms how entrepreneurs and small business owners deal with a day-to-day paperwork. Get ready for the simplest way to be more productive and organized. Most importantly, get paid quickly.

FreshBooks is not only easy to use, it's also packed full of powerful features. From the visually appealing dashboard, you can see outstanding revenue, spending, reports, a notification center, and action items at a glance. Create and send invoices in less than 30 seconds. Set up online payments with just a couple of clicks. Your clients can pay by credit card straight from their invoice. If you send an invoice, you can see when the client has received and opened that invoice.

FreshBooks is also known for award-winning customer service and a real live person usually answers the phone in three rings or less. FreshBooks is offering a 30-day unrestricted free trial to Software Engineering Daily listeners. To claim it, just go to freshbooks.com/sed and enter Software Engineering Daily in the How Did You Hear About Us section. Again, that's freshbooks.com/sed.

Thanks to FreshBooks for being a sponsor of Software Engineering Daily.

[INTERVIEW]

[0:03:37.3] JM: Bill Budington is a security engineer with the Electronic Frontier Foundation. Bill, welcome to Software Engineering Daily.

[0:03:42.2] BB: Hi. Thanks for having me.

[0:03:43.3] JM: We had a pervious show about web tracking, and that was with someone from Ghostery. In that show we covered the basic engineering concepts of web tracking. In this episode, I'd like to explore web tracking more deeply and talk about some of the subjective decisions around tracking.

You work at the EFF, that means that your opinions will be less filtered than someone who works at a corporation. We will get into net neutrality, because that's been in the news lately and I'm sure you have some thoughts on it. Let's start with web tracking. What is wrong with the way that users are tracked on the web today?

[0:04:18.7] BB: If we go back to 1998, you have this situation where users were being tracked, but they were being tracked in a kind of transparent way via cookies. They can use the normal mechanisms within their browsers to actually just flush those cookies out and have a fresh start.

Ever since then, we've been seeing more and more pernicious and underhanded ways that trackers and advertisers have used technologies of the web to track users. One particularly pernicious thing that trackers are doing is they're using the fingerprint of your browser. This is a kind of a combination of web headers and JavaScript detected properties from your browser that you can use to kind of get a unique signature of what your browser looks like.

Other technologies have been used, such as evercookies. Evercookies are these way that you can have collusion between the cookies that are stored in your browser and those that are stored in something like Flash, or Silverlight, or Java plugins. What evercookies do is if you delete cookies in, say, Flash and Silverlight, then Java code can be used to propagate the cookies back to the Flash and Silverlight add-ons.

Basically, it's very kind of underhanded. It's subverting the normal mechanisms that users are used to kind of deleting their cookies, or using private browsing mode. For finger printing, for instance, you can't do that. You can't actually be assured that you won't be tracked just because you're using private browsing mode.

[0:06:19.0] JM: There are a bunch of these companies who track me through the internet where I'm not aware of these companies. I'm not aware of giving them any sort of permission to track me. What does the law say about consent?

[0:06:35.6] BB: There is no real data protection regime for users within the U.S. There are laws on the books in Europe, but those don't apply here. When you are browsing the web, there's no

real way for you to be assured that you're not being tracked unless you install add-ons and employ technologies that make sure that you're protected.

For instance, one of the things that we developed here at EFF is an add-on called Privacy Badger. That will kind of give you a good indication of when you're being tracked. Unfortunately, there's no real way to know whether the remote site that you're accessing is just delivering that data to third parties behind the scenes via special deals or whatever relationship they might have with trackers.

Yeah, a lot of the companies are pretty sneaky about what they're doing and they're not sites that you might have heard of. You might have heard of AddThis, because they are added on a lot of websites to share different — To share articles on your social networks. Things like Ligatus, or SilverPush are companies that you don't necessarily know about. Behind the scenes, there are trackers that are gathering your data and using that to figure out what sites that you've been on and, more broadly, your browsing habits.

[0:08:21.7] JM: When people talk about tracking, I think they're usually thinking of it in terms of something has been put on their browser to track them form the browser's point of view and that browser information gets sent back to the company that's tracking them, but you also just described a type of tracking where if I log in to beefrecipes.com, beefrecipes.com is tracking that user session, or logging that user session, whatever terminology you want to use. Then, they might share that with some external broker, or somebody who wants to sell me ads directly. There are multiple types of web tracking that we could be talking about.

[0:09:08.2] BB: Yeah. By far, the most common form of web tracking is via third party inclusion of scripts, or fonts, or some kind of resource that's loaded on a webpage that isn't actually a part directly of the site that you're accessing.

In a recent study by the Center for Information Technologies Policy at Princeton, has found that the majority or, basically, the largest amount trackers are loaded on news sites. News sites are including a bunch of scripts from trackers that you don't — When you're going to newyorktimes.com, it's not New York Times tracking, it's the inclusion of third party scripts that are tracking you. That might be fonts, that might just be directly advertising.

Advertisers are a big, big way that third parties are included in news site. Often, they are keeping tabs on what kind of operation you're accessing. Additionally, it's one of the impediments to actually news sites adopting HTTPS, is that they can adopt HTTPS because ads are only loaded in secure sites and if they're dependent on ad revenue. Then, unless their ad servers are also supporting HTTPS, then the ads won't actually load, because of something called mixed content blocking.

Basically, you have this situation where even if new sites or sites that are including third party trackers want to move to HTTPS, they actually can't. The problem with tracking is kind of related to the problem of encryption in general.

[SPONSOR MESSAGE]

[0:11:18.7] JM: At Software Engineering Daily, we need to keep our metrics reliable. If a botnet started listening to all of our episodes and we had nothing to stop it, our statistics would be corrupted. We would have no way to know whether a listen came from a bot, or from a real user. That's why we use Encapsula to stop attackers and improve performance.

When a listener makes a request to play an episode of Software Engineering Daily, Encapsula checks that request before it reaches our servers and filters bot traffic preventing it from ever reaching us. Botnets and DDoS are not just a threat to podcasts. They can impact your application too. Encapsula can protect your API servers and your microservices from responding to unwanted requests.

To try Encapsula for yourself, got to encapsula.com/sedaily and get a month of Encapsula for free. Encapsula's API gives you control over the security and performance of your application. Whether you have a complex microservices architecture, or a WordPress site, like Software Engineering Daily.

Encapsula has a global network of over 30 data centers that optimize routing and cacher content. The same network of data centers that is filtering your content for attackers is operating

as a CDN and speeding up your application. To try Encapsula today, go to encapsula.com/sedaily and check it out. Thanks again Encapsula.

[INTERVIEW CONTINUED]

[0:13:03.1] JM: We had Brendan Eich on the show recently and he talked about the state of JavaScript, which he created, and he talked about his new browser that he's working on; Brave. One of the examples he gave of the brokenness of the advertising ecosystem is the New York Times having malware being delivered through their ad network. Basically, display ads that were served to users either caused malware directly or linked to malware. I think that's the extreme example. There's plenty of things in between malware and clean ad experience that are different shades of annoying, or threatening, or privacy encroaching.

It's no surprise that people are — That advertisers — I'm sorry. Brands, I should say, are moving to Facebook where it's more of a walled garden; Twitter, where it's kind of more of a walled garden. Moving more of their dollars to Google who may be, clearly from the recent YouTube advertisements on extremist videos, Google doesn't have a great handle on this, but they probably got a better handle on things than the average ad delivery service.

Talk about the incentives of the giant companies like Google, Facebook, Amazon and how they handle web tracking.

[0:14:39.4] BB: Yeah. Google acquired DoubleClick a little while ago, and I think this has incentivized them to care less about privacy than they obviously do about security. Google has a world-class security team, and because of that, the dangers of Google Ads, I presume, are decreased. If there's an ad network out there that's delivering malware with their ads, then I suspect that they have less protection than Google Ads than DoubleClick does.

There might idiosyncrasies in the business model that Google employs. By enlarge, Google takes that into consideration very well. One of the things that is lagging behind is privacy, and this is indicated by the fact that — This will kind of dovetail into talking about Panopticlick, where their browser is very unique, and so you can actually tell via these different properties that are

included in a Chrome browser exactly what that browser looks like and has very uniquely identifiable properties when users are using it.

Not to say that Firefox doesn't, but Firefox is moving in a direction that kind of precludes a lot of the worst tracking mechanisms. For instance, what Firefox started to do in their private browsing mode is employ tracking protection. Basically, it includes a list that has been cultivated by an add-on disconnect and uses that as a way to block malicious trackers. This is not something that is currently in Incognito mode for Chrome.

I think that we need to have Google do better in terms of privacy. They're already doing a world-class, spectacular job in terms of security, but privacy is something that they're unfortunately less and less concerned about. I think this is basically an example of, or a result of their business model becoming more and more reliant on advertising in general.

[0:17:18.4] JM: Your concerns with privacy had led you to working Panopticlick. Panopticlick lets a user diagnose how much non-consensual web tracking is occurring on their browser. Panopticlick is named after, as far as I know, the Panopticon, which is a building design that allows for all of the people in the building to be observed without knowing whether they are being watched. The Panopticon was originally designed for contained asylums, and prisons, and it evokes something chilling, because people who don't know whether they are being observed or not at any given time, there's a chilling effect that happens to their behavior, because they won't act as freely, generally. Human behaviors suggest that.

Why is Panopticlick named after The Panopticon? What is Panopticlick do?

[0:18:24.1] BB: Panopticlick measures these unique properties of your browser, and it's basically a volunteer-driven data project. We wanted to get an idea of how unique people's browsers were using fingerprinting techniques, using this kind of unique combination of browser headers and JavaScript detected properties.

When we launched Panopticlick, it was an effort not only to see how unique people's browsers were, but also to give them a good understanding of how unique their own browsers were. It does this by combining a bunch of different unique facts. For instance, we measure the user

agent that's delivered upon every request in combination with the language that the user is delivering in combination with the content types that your browser supports. In combination with the fonts that might be detected via fonts fingerprinting, or other more advanced techniques.

What happens is there are what's called in information theory bits of entropy, which you can gather via techniques that we employ on Panopticlick. Once we gather these unique bits of information, you can combine those to get a clearer picture of what the user's browser looks like. It's not just one property, but it's the combination of all these properties that you can use to get that unique picture.

We measure that, and we also provide a result of, "Hey, this was the only time that we've ever seen a browser with these properties," which is actually most of the time. The vast majority of the time, users' browsers are uniquely fingerprintable, or you have some protections against this, and we can give that result depending on how your browser measures up against other browsers that we've seen in the past.

[0:20:52.5] JM: We'll talk more about the engineering in a sec. I would like to know why is it called Panopticlick.

[0:20:57.3] BB: It's just a way to basically — We thought it was a good analogy to the original Panopticon developed by Jeremy Bentham. This was something that was meant to observe the movements of prisoners and their behaviors as they went about their daily business in the prison. We thought this was a great analogy for trackers are attempting to do to see user's browsing habits, see what they're looking, how they behave as they traverse the web.

The scary part about it is the totality of the observation of these different — In the case of the Panopticon, it was the prisoners. The ubiquity and presence of trackers on the web has really, really increased. In the late 90s, it was only 5% of webpages that included trackers. Now, it's the vast majority. I think it's about 85% or so. I didn't get that figure for you. We can add that.

[0:22:20.8] JM: You don't have to convince me of the totality, because the Panopticon model where you have this building that is structured such that there are little observation panels into every room, that would seem innocent compared to what we have today, or the future of the

way you're asymptoting towards where you have smart TVs that you can't even tell if they're on. You have Google Home sitting on your desk. I don't know if you have one or if you've used one, but it is such an effective utility. I probably use it 40 times a day, 30 times a day. I don't want to start to cast aspersions, because I know that Google would dispute me on this. I swear there are — It could just be my phone doing this, but I swear there are times where I say something and minutes later I get served an ad, and there should be no way for the internet to know that I want that thing other than if they were recording what I said. Has that ever happened to you?

[0:23:32.2] BB: I haven't had that experience myself. I don't use Google Home. The problem with these technologies is that it's really opaque what they're doing. When you say — I won't say what the keyword is because maybe your listeners will have that ordered for them. Get a dollhouse, which was actually said on a program in San Diego, and everyone's home assistant actually ordered them a dollhouse, because it was said on the program.

When you say that kind of thing, you don't know where that data is going, what's being done with it? It's not transparent. We have no idea what they're doing with our data once it's actually delivered through remote servers. We do know that it's not being processed on our local devices. We know that it's being delivered to the cloud. We can be pretty well-assured that they are doing something in delving advertising with that data, because these are big data-driven advertising driven companies. That's how they get their revenue.

We can actually know what's happening behind the scenes. That's very scary. We have this kind of situation where our data is leaking all the time. Most people kind of think that this is just to give us better advertising.

One recent NPR story talked of a woman who was looking up alcohol abuse counseling online, and minutes later she had the local liquor store being advertised to her. Is that a form of better advertising? Maybe it is from the perspective of the liquor store. That does get them more business, because this is someone who is more likely to buy alcohol because they're addicted to it. This isn't like a side effect, it's the intended purpose of these advertising.

Another very pernicious example of this is described in a recent book by Cathy O'Neil, which is called *Weapons of Math Destruction,* talks about these diploma mills and how those that are

kind of lumped into a category of low income users on the web because of their browsing habits are advertised universities that the diploma which you get from them isn't really worth the paper that it's printed on. The people that are getting advertised these diploma mills don't have the level of social access to know that this is going to not help them in life.

These algorithms aren't just providing me better advertising, they're actually providing a social ill. That's something that I think is lost on a lot of people, that they don't know that it's just — They think it's just better advertising for me so that I'll get products that I want. It's becoming more and more reaching into more deeply entrenched position in our society. It's actually kind of becoming part of the social fabric in a lot of ways.

[0:27:25.6] JM: When I go to the Panopticlick website, I run these tests against my browser. Describe more what is going on when I'm running those tests.

[0:27:37.5] BB: Sure. In a classical Panopticlick, what we had happened was basically every time your browser accesses a website, it delivers theses little text fields called headers. Those happen no matter if you have JavaScript turned off, or turned on, or whatever. There is always going to be web headers that are delivered to a website that you accessed by your browser.

In addition, we read — If you had the JavaScript turned on, we employed techniques that would basically figure out certain things about your browser in a more unique way, or intimate way. We would try to enumerate the fonts that you have installed, try to see what plugins you had installed, if any. Now, we have the number of touch points that your device is advertising. There are a bunch of different JavaScript detected properties that you can actually determine based on a user's browser.

We kind of look at those and see how many — For each of these, how many other users have had the same result. We use a formula that is derived from basic information theory to give you a quantified results of exactly how much bits of entropy or uniqueness that you have for any one of these categories. Also, we provide a summation of all of these combined, how unique you are.

Since the version two of Panopticlick, which was launched in December of 2015, we've also included a number of other tests. These tests aren't about fingerprinting, they're about how well you're protected from third party trackers. We employ a tracker blocker detection test. The way that we do this is kind of interesting. There are trackers blockers that block trackers in any number of ways.

The three most common are based on URL fragments. If a URL path looks like it's a tracking beacon, say, it has something like ad_server= in the URL, then that looks like an advertiser, or tracker_ID=, then that looks like a tracker. Most of them aren't that obvious. Those are using URL fragments. Other blockers use blacklists to determine which servers are actually requesting tracking information from your browser. For privacy badger, for instance, we employ a heuristic approach. We determine what third parties are setting cookies and which of them look like trackers based on their behavior.

For each three of these categories, Panopticlick mimics trackers and we have a number of domains that we've set up that look alike like trackers. If your tracking blocking is working properly, then those domains will actually be blocked after we've finished the tests. If it's not configured correctly, or it's turned off, then those domains won't be blocked.

Across three of these third party domains, we kind of can get a good sense of how well your tracker blocker is working. Then, we display a result based on that. We also have results that indicate whether your browser is complying with our do not track policy, which I can get into. Basically, there is this initiative at EFF to have trackers promise not to and actually provide a privacy policy, which is actionable not to track users.

If an ad company, an ad tech company is not tracking users, then they can actually post this very well-defined document that stipulates the ways in which they are not tracking users behind some well-known location in their domain, behind their web group, basically. This means that once you are accessing ads from that site, then you can be assured that they're not actually tracking you in some deep way or some unknown way, that they're just providing those ads. We don't want to block them. Once they provide this policy and post this on their site, this is an indication that we can actually serve their content with a privacy badger.

The second test is to basically tell whether your — I'm sorry. This is a third test. Is to tell whether your browser is allowing those resources, because we know that they're not tracking you.

[0:33:54.8] JM: Yes, and I executed this test on myself, and I only got a green check mark for the one that I was running an ad blocker. I guess I have some work to do. I recommend everybody else who's listening to check out Panopticlick and try it out for them self to get a better understanding of what is going on in terms of tracking through their browser.

I want to talk about net neutrality. I want to talk about EFFs position on Net Neutrality and your personal position. I would love to talk more about Panopticlick too, but I wanted to get into these other topics, because it's fairly topical right now.

The FCC has changed its standards on net neutrality in the last couple of days. Explain what these changes mean for corporations and for users.

[0:34:50.2] BB: The stipulations on the FCC that basically say that broadband providers can't just fork over your data to the highest bidder or that they can't, for instance, modify traffic in real time. There's pretty good regulations that have been enacted — They were enacted last year. Under the new FCC chairman, this is really kind of being revoked in a very, very alarming way.

What we see is we've seen a big push by the broadband providers to actually make sure that they can advertise you for tracking beacons in your traffic and do all sorts of things that they had been doing. They don't have a very good track record of protecting users' privacy, unfortunately, but that they have been doing and were told to stop.

Usually, this comes in the form of un-encrypted traffic being able to be picked up and they can insert ads, they can use their privileged position on your network path to see exactly what your accessing and to provide targeted advertising, or monetize your user data. That's something that we've been very vociferously fighting against in the last few weeks.

Yeah, that's pretty much the kind of long and short of what has been going on. As far as I understand, the latest — And I'm not sure if this will change by the time you broadcast. The latest is that this has passed both houses of congress and it is going to sit before our President

Trump's desk. Hopefully, the very privacy-centric and anti-big business, drain the swamp crowd, can come out in full force and say, "Hey, look. If you want to drain the swamp, then there's a way to do it, and it's not sign this into law." To actually stand up for Americans and make sure that this isn't just a selloff of users' data. Actually, put something into law that makes sense so that their rights are protected rather than rescinded.

[0:37:42.6] JM: It sounds like what you're saying is that regardless of where this legislation went, we would pretty much be in the same situation regardless, because these policies are pretty hard to enforce. Obviously, we would rather have policies that were navigating us towards a world that enforces consumer privacy, but it sounds like what you're saying is that, in effect, these policies were not being policed.

[0:38:15.2] BB: The FCC often lacks the enforcement mechanism to make it so that companies will actually have real protections. This isn't always the case.

In very particular circumstances, federal regulators have stepped in and made sure that advertising companies can't do the worst abuses of the past that they've been found to be doing. Not the FCC, but the FTC, was issuing letters to applications which included this SilverPush SDK. SilverPush is a company that basically does inaudible tracking beacons emitted from your TV to link your devices up. It's a technology called Cross Device Tracking.

Last year, the FTC — Basically, if an app has the SilverPush SDK installed and it's installed on your phone, or on your tablet, or whatever, and it's in the same room as an advertisement which is played from your TV which has an audio beacon that isn't audible, that's basically too high of a pitch for the human ear to pick up, but your device can still listen to that.

SilverPush is a company that was basically providing this technology to advertisers to give link your devices in that room and make sure that there's a picture of who you are based on numerous of your devices, not just your TV.

The FTC, last year, actually bid them and apps that had a SilverPush SDK included in their code were given a harsh warning. We don't know which apps they were, because the letter didn't

indicate which apps were actually doing this, but they were given a harsh warning about, “Hey, you might be in violation of the law if you continue to do this type of tracking.”

This is one of the kind of things which is on the bleeding edge of what tracking means. This is something — Linking your devices up between them and using behavioral fingerprinting to tell when a user has switched browsers based on their unique typing patterns. Things like that are used to be the world of science fiction. Increasingly, it’s becoming a reality as trackers become smarter and smarter. Unfortunately, there’s not a good data protection regime in the U.S. to protect users against the worst of these abuses.

In the last few weeks, we’ve seen that the carriers and the broadband providers are given more license to track users and to insert targeted advertising in the traffic stream. There are technologies — And the only way for users to protect themselves is to use technologies that we can provide to prevent these abuses from happening.

At EFF, we fight for the best in the legislative world so that we fight against the worst kind of abuses happening. We fought against the repeal of the FCC protections and we’ll continue to do so. One of the big things that users can do is to install software such as privacy badger, such as HTTPS Everywhere, which is a software project that I maintain and we’ve developed here at EFF, such as downloading the Tor Browser as well.

One of the great things about the Tor Browser is that it has — The Tor Browser and the folks that are developing it have put a lot of effort into making sure that your anonymous when you use it. When you use Panopticlick with Tor Browser, it gives you a very, very good result in terms of fingerprintability , because the Tor Browser puts you in a pool of users that pretty much all look the same. Everyone using the Tor Browser looks very, very similar, if not the same.

There are good protection mechanisms that users can, themselves, install on their machines to make sure that they’re not suffering the worst abuses of trackers.

[SPONSOR MESSAGE]

[0:43:49.7] JM: Spring is a season of growth and change. Have you been thinking you'd be happier at a new job? If you're dreaming about a new job and have been waiting for the right time to make a move, go to hire.com/sedaily today. Hired makes finding work enjoyable. Hired uses an algorithmic job-matching tool in combination with a talent advocate who will walk you through the process of finding a better job.

Maybe you want more flexible hours, or more money, or remote work. Maybe you work at Zillow, or Squarespace, or Postmates, or some of the other top technology companies that are desperately looking for engineers on Hired. You and your skills are in high demand. You listen to a software engineering podcast in your spare time, so you're clearly passionate about technology.

Check out hired.com/sedaily to get a special offer for Software Engineering Daily listeners. A $600 signing bonus from Hired when you find that great job that gives you the respect and the salary that you deserve as a talented engineer. I love Hired because it puts you in charge. Go to hired.com/sedaily, and thanks to Hired for being a continued long-running sponsor of Software Engineering Daily.

[INTERVIEW CONTINUED]

[0:45:14.8] JM: It seems inevitable that our meet space world is colliding with this violent and widespread use of tracking, and retargeting, and poorly designed advertising experiences. It seems like this collision is occurring faster than the advertising ecosystem is improving. You're starting to see information come out into the public eye about ad fraud and advertising malware. I've been doing so many shows about it, so maybe I'm biased.

In any case, it seems like this intersection is happening too fast for, certainly, any kind of government regulation that I can imagine in the near future inhibiting it. To the contrary, government seems to prefer to piggyback on it and use it as a tool for surveillance, "Okay. We're already surveilling you because — We're already incentivized to — Google, or name your sketch ad tech company is incentivized to track you." NASA says, "That's convenient for us. We'll just piggyback on that and track you to make sure that you're not a terrorist."

At this point, I have kind of personally made my piece with this world that we're moving towards. I hope there are different shades of privacy depending on where in meet space I am. Maybe I have to have a part of my house that has no computers in it and its got walls that are insulated in certain ways to prevent electronic stuff from — Maybe that's my bedroom.

Philosophically, what are the social norms that we need to deal with this new world given that the Panopticon is going to be everywhere it's increasingly feeling inevitable?

[0:47:31.7] BB: I think that you touched on a really interesting point which is that this isn't black or white. There are gradations and you can have some privacy without having total privacy all the time. For instance, you can envision having a browser that you have a slider on it, and you basically — If you want total protection, then that comes at a cost of functionality of the web.

If I want to play video games in my browser and have real time chats over the web, then that is enabling functionality that alternatively can be used to track me. That doesn't mean that I have to enable that on every single site that I visit. We can envision a world there are different gradations of, "Okay. I want this site to be able to enable these feature-rich web technologies, but this site over here is just news. I don't necessarily need everything that can be used to track me enabled on my browser."

I think that this is mostly a problem of user education. When users aren't aware of the fact that they can be tracked in every single aspect of their lives, then they don't get angry about it. They don't have any incentive to think of anything better.

One of the big things that we try to do at EFF is to have user education happen. We give these training sessions on how to better protect yourself, but also to have users be aware of the risks. I think that there are things that you can do and kind of build into your common habits that are maybe a step in the right direction.

If you have an Amazon Echo, for instance, you don't need that device listening all the time. There's a mute button that you can have — There's a mute button on the device that you can press and it won't listen all the time. Yeah, maybe that's a sacrifice for usability, but it also comes with the assurance that your every word isn't being uploaded to the cloud, or that a

hacker can't come along and find a vulnerability and it's on Echo and use it as a remote listening device.

That's something that users can do, and that only comes with user education when users know that the Echo is listening for that trigger word. That means that it's listening all the time for that trigger word. I think that that's something that can be done on an everyday level for users. What is something requires more engineering is for us to be assured that our products have some kind of a hardware switch that they can't listen to us if we flip this hardware switch.

If the Amazon Echo, for instance, had disconnected the circuit to the microphone, if I had a button that actually does that that disconnects that circuit. These are things that are hardware requirements that we should demand on companies actually build into products in order to give good privacy guarantees. I think that that's not going to happen unless users know the risks. That's the first step; to get users aware of what the risks are so that they can better protect themselves in the short term and demand better privacy in the hardware controls and in the privacy policies and in the way that these companies behave in the long term.

[0:51:41.9] JM: Okay, Bill. Thanks for coming on Software Engineering Daily. It's been great talking to you. It's always nice to talk to the EFF folks. We've already done a couple of shows with different EFF people, and it's always a pleasant conversation, because you guys are removed — Or I shouldn't say you guys. Your team is removed from the censorious trappings of corporations or governments.

[0:52:09.3] BB: Yeah, I mean we work them too. They're concerned about how they are perceived in the world. They want their users to be protected and they don't want bad media. We often consult with these corporations and try to make their products better and try to advise them on how they can better. Sometimes it's a matter of them actually being pernicious, or them not wanting to take user considerations into their worldview.

More often, it's just that they don't know what their devices are capable of. They kind of want to develop a product and have it be cool and put it out to the world. Sometimes that does ill to the world if it actually can cause problems and actually impacts people's security or privacy. It's not always the fault of the companies that they want to create a cool thing and have it delivered to

the users. Sometimes they just kind of need that reminder that some of the stuff that they're developing could be used for harm.

[0:53:30.4] JM: Bill, thank you so much.

[0:53:31.1] BB: Thank you, Jeff.

[END OF INTERVIEW]

[0:53:34.0] JM: Thanks to Symphono for sponsoring Software Engineering Daily. Symphono is a custom engineering shop where senior engineers tackle big tech challenges while learning from each other. Check it out at symphono.com/sedaily. Thanks again Symphono for being a sponsor of Software Engineering Daily for almost a year now. Your continued support allows us to deliver this content to the listeners on a regular basis.

[END]