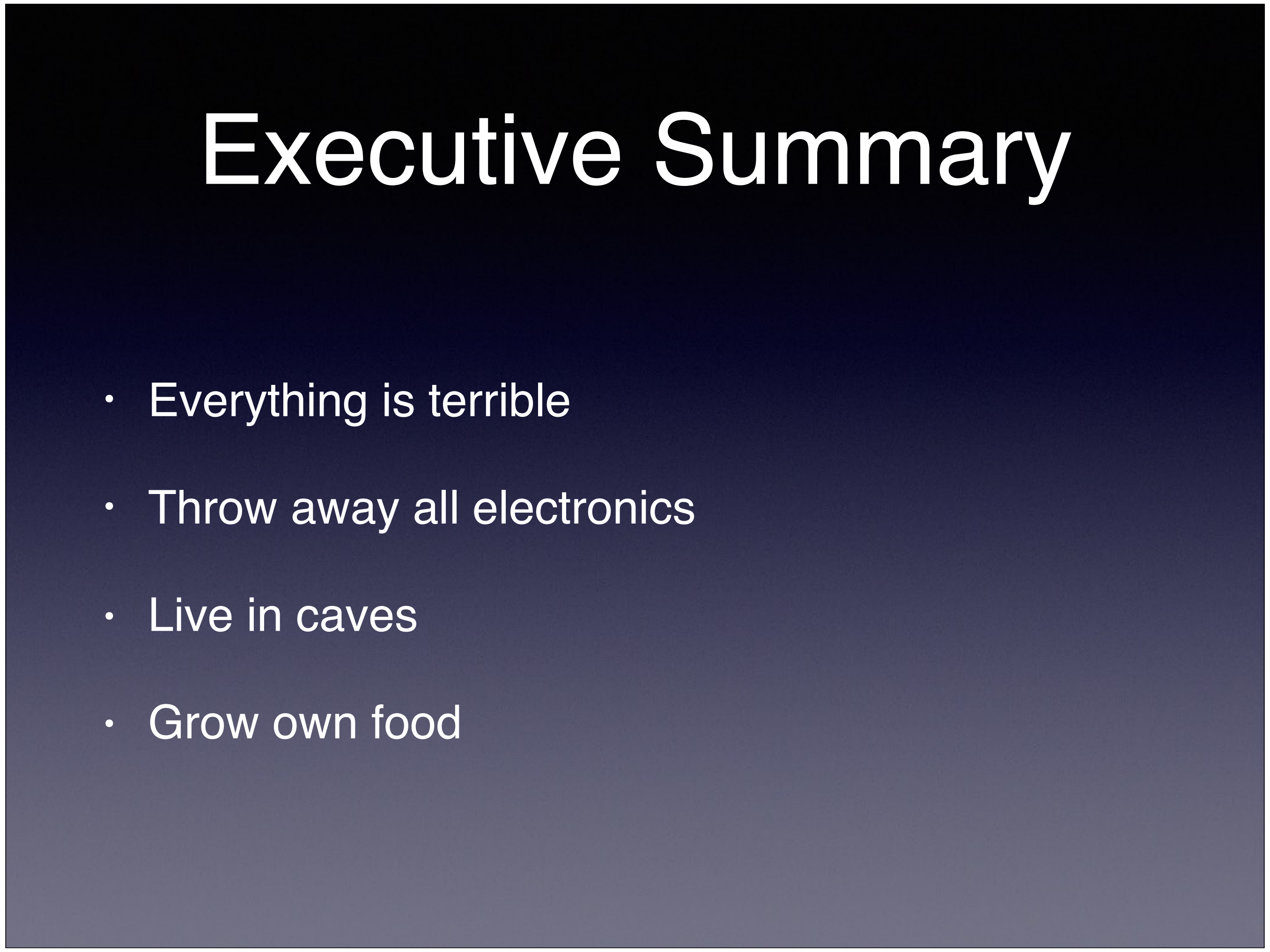
ars technica CONDÉ NAST

Taking Responsibility For Your Digital Life

Lee Hutchinson
Senior Technology Editor

@Lee_Ars
lee.hutchinson@arstechnica.com



Executive Summary

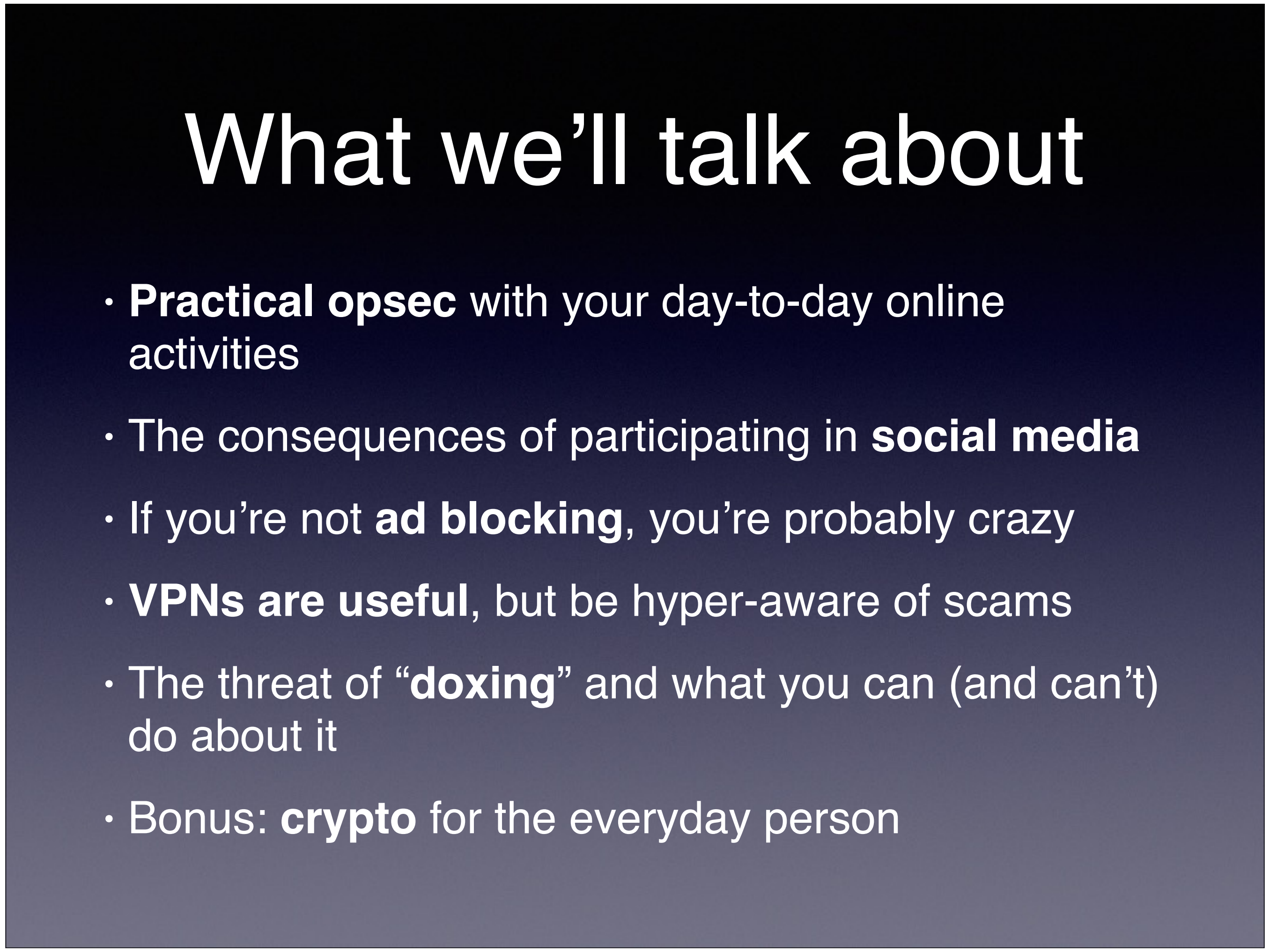
- Everything is terrible
- Throw away all electronics
- Live in caves
- Grow own food

I started putting this preso together and things quickly got really, really dark—after I did the outline and got into doing the slides, I realized that this presentation is going to have a lot of just profoundly negative stuff in it, and that there wasn’t a lot of solid, easily-explainable mitigation for the privacy problems described. The reality that everyone here has to face is that we live in a time when it’s incredibly easy to give away deeply personal details to total strangers, and some of those strangers are malicious. The good news is that there are some things you can do to be safer, but there are no silver bullets and there are no shortcuts.

It’s kind of one of those deals like how every industry has a public side and a dark side; I can tell you as someone with a decade in aerospace IT and five years covering technology news, the dark side of technology is, I mean, right there up on that slide. between invasive and unchecked data collection by internet providers and private companies, warrantless surveillance and data collection by state actors, and an incredibly varied and sophisticated set of tools being employed by black hat for-profit hackers….it’s not so much the wild west as it is Mad Max Fury Road, except we’re the normal people scrabbling around in the dirt trying to not get killed.

And while there are some things you can do to protect yourself and your privacy, some of the cures are worse than the disease.

So, apologies in advance for what will likely come across as a depressing, paranoid presentation—but seriously, folks, the overall state of personal security and anonymity online really, really is that bad.



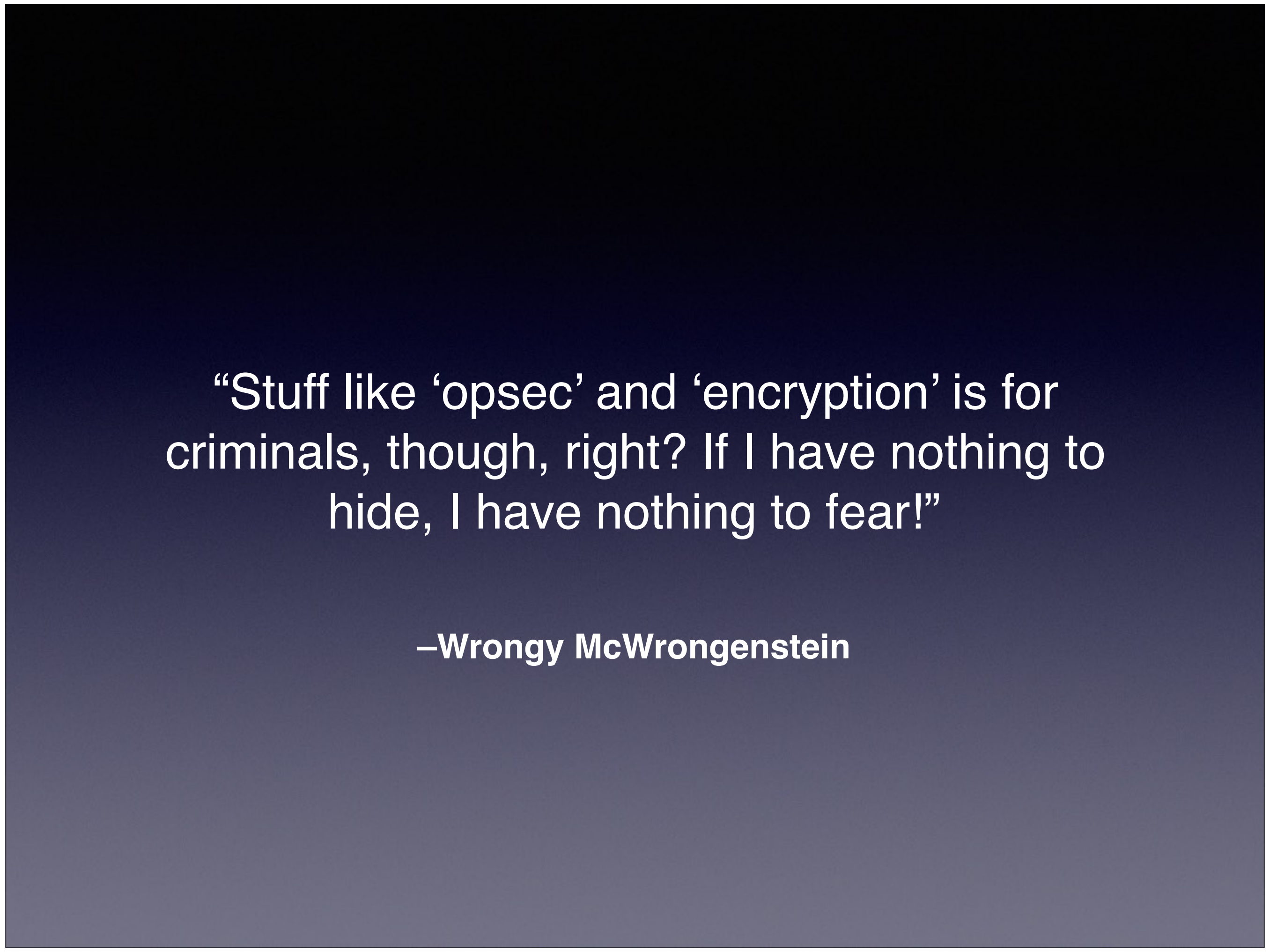
What we’ll talk about

- **Practical opsec** with your day-to-day online activities
- The consequences of participating in **social media**
- If you’re not **ad blocking**, you’re probably crazy
- **VPNs are useful**, but be hyper-aware of scams
- The threat of “**doxing**” and what you can (and can’t) do about it
- Bonus: **crypto** for the everyday person

There’s a lot to cover here and it’s going to be fast-paced, but please, interrupt at any time with questions and I’ll count on Phil & crew to stop me from running over.

OK, so—a lot of these topics are going to sound a little paranoid. In fact, a lot of these topics are going to sound _ultra_ paranoid, but the truth everyone has to recognize is that a lot of people still think of the internet as a sleepy neighborhood in the 50s where you can leave your doors unlocked at night, and that hasn’t been the case for years. the internet is a place where you leak info all the time, and both the government and advertisers have the ability to see and analyze everything you do if you’re not careful, and most things you do even if you ARE careful.

I can tell you why these things are problematic, but I can’t make you care—everybody’s own “why should I give a crap?” level on each of these things is going to be all over the map. But I can tell you why *I* care: my privacy is more important to me than anything else online, because as we’ve seen repeatedly over the past decade with various leaks and hacks, the majority of large internet companies and even the government act completely amorally and without regard to citizens’ privacy or really even safety. I can imagine all kinds of terrible nefarious things that might be done with my consumer profile or browsing data, but reality has in so many cases far exceeded what I could think of—what I’m scared of are the things that I’m not crazy enough to imagine, which reality has demonstrated time and time again to be the kinds of things that _do_ happen.



> “Stuff like ‘opsec’ and ‘encryption’ is for criminals, though, right? If I have nothing to hide, I have nothing to fear!”

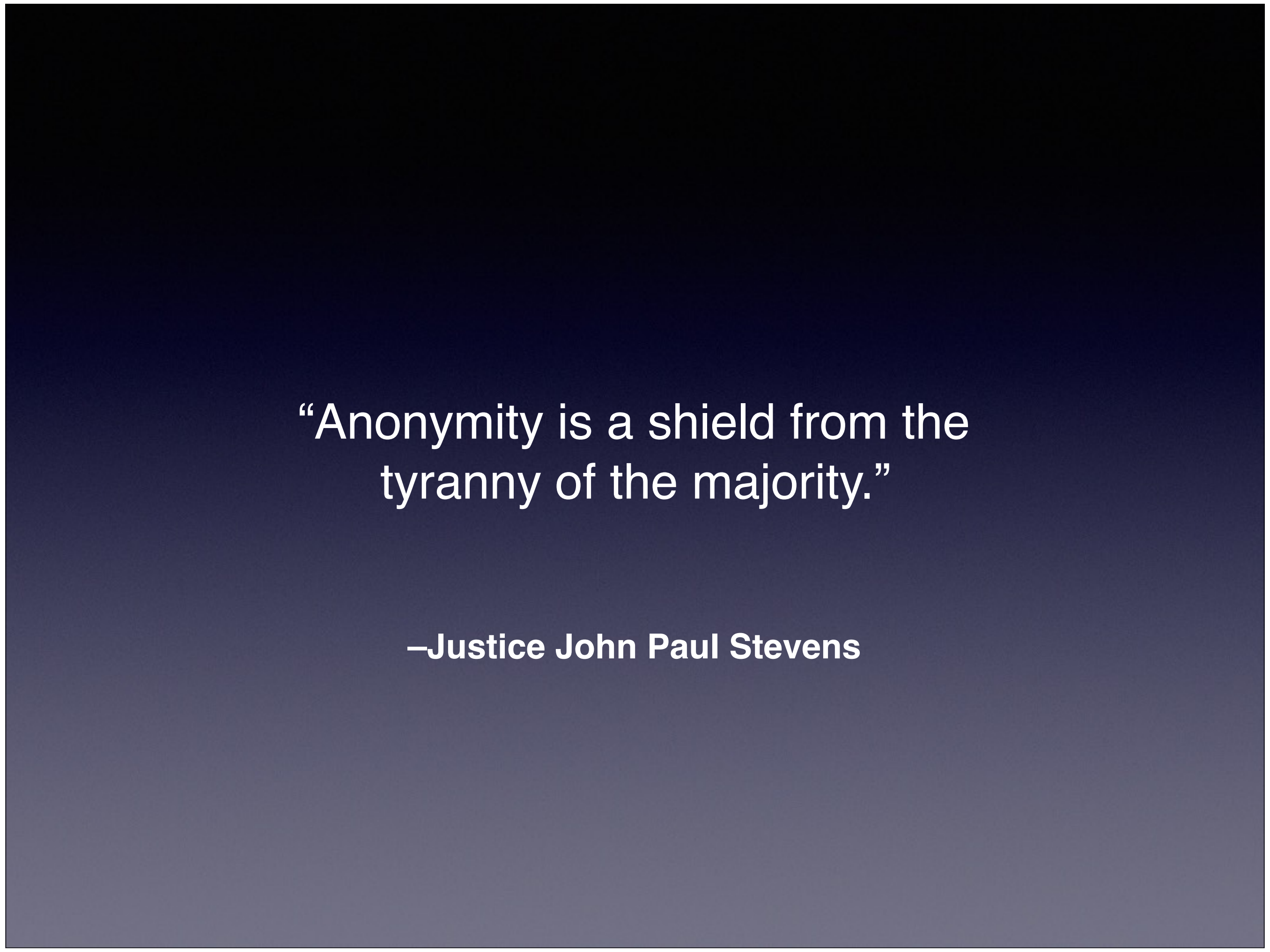
–Wrongy McWrongenstein

I’ve heard this from a lot of people. Hell, I’ve heard this from my parents.

It’s wrong. Wrong, wrong, wrong, wrong, wrong. Looking at just the US Code, there are over ten thousand possible offenses; Texas code adds thousands more. Everybody is guilty of multiple crimes of varying severity, and everyone _absolutely_ has stuff to hide, even if you’re not aware that you’re breaking the law (and remember, ignorance is not a defense). Stuff that is no big deal but that can be used against you if you’re ever potentially a person of interest in a criminal investigation or civil case; stuff that can be used against you by third parties if it’s exfiltrated.

If you’re not being mindful of what kind of information you’re potentially leaking out, you’re potentially leaving a huge, rich trail of personally identifiable info all over the place. And you know the axiom about how you don’t need to be worried because you’re just one person in a sea of millions? “Big Data” trashes that, completely. The analytic ability available to anybody these days makes identifying and tracking needles in haystacks trivial.

Plus, what’s “legal” today might not be “legal” tomorrow, and once you’ve put something online, it’s there forever. The idea of allowing years of my uncaring, unthinking online activity to be constantly sifted and strained for new consumer-related insights and new ad profile opportunities is one thing; the idea of the government doing it to identify people who exhibit new “wrong” ways of thinking is a lot more terrifying.



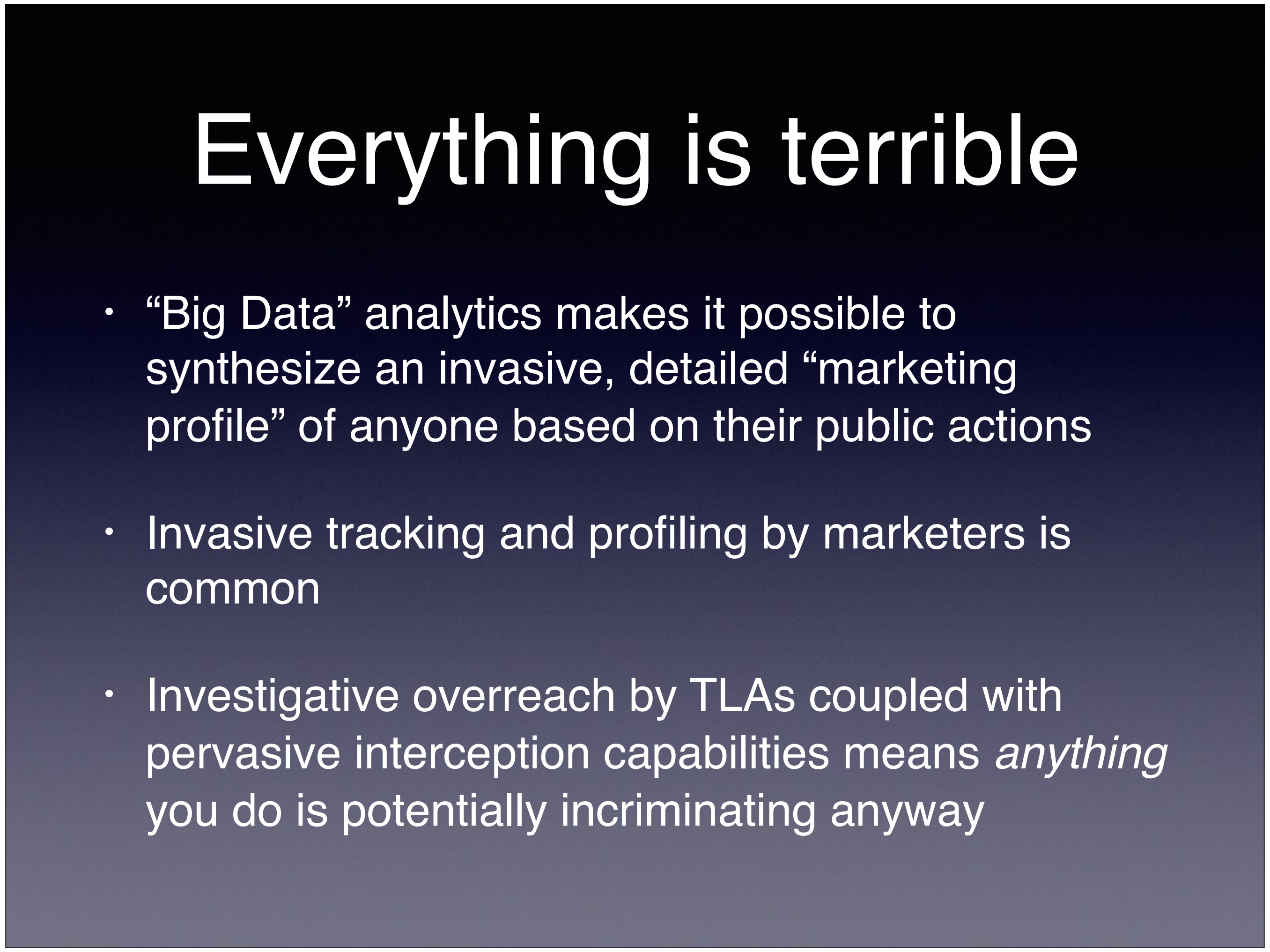
“Anonymity is a shield from the tyranny of the majority.”

–Justice John Paul Stevens

The ability for one person to speak to another person privately and non-publicly, without that private speech being automatically suspect, without the fear of reprisal for their words, (and, in the modern picture, without that speech being dissected for marketing purposes), is the centerpiece of freedom of speech. No company’s or government’s rights eclipse that. But it’s a right many people willingly give up for convenience or for the false illusion of increased security.

If you want a real-world example, there’s an ongoing action against Dreamhost, a large web hosting company, where the DoJ has demanded the names and addresses of not just the people running a specific political protest site hosted on Dreamhost, but the names and addresses of *all 1.3 million visitors to that site, too*. Think about that: it’s one set of legal issues to investigate the people running a protest site, but the demand for visitor records is terrifying. Merely by *visiting* the site—which you might have done even if you’re wildly opposed to the site’s ideas!—you’re potentially included in a DoJ list of names that could be used for literally any purpose. And, again, it’s not the stuff I can think of that’s really scary—it’s the stuff I can’t think of that really keeps me up at night.

https://www.dreamhost.com/blog/we-fight-for-the-users/

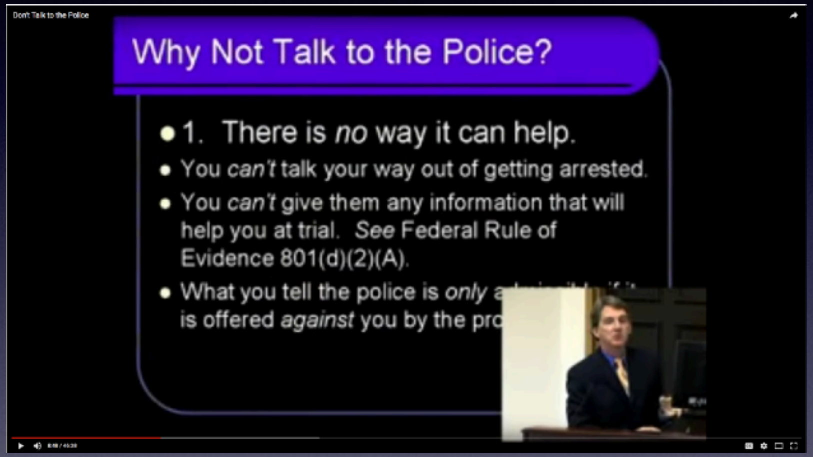


Everything is terrible

- “Big Data” analytics makes it possible to synthesize an invasive, detailed “marketing profile” of anyone based on their public actions
- Invasive tracking and profiling by marketers is common
- Investigative overreach by TLAs coupled with pervasive interception capabilities means *anything* you do is potentially incriminating anyway

I’m not going to comment one way or another about politics—it’s Saturday and who needs a fight on Saturday, right?!—but the Dreamhost incident is not isolated. It’s merely the latest. The DoJ as it’s constituted today is going on more and more detailed fishing expeditions to try to tease out potential “criminals” with the use of massively overreaching warrants—or sometimes without a warrant at all. And no matter WHO is in power, as Texans I think we can all agree that no government has the right to get into my business and preemptively ask what library books I’m reading and what web sites I’m visiting. And yet, they’re trying. It doesn’t matter whether I’ve done anything “wrong” or not—you are your only advocate and you are your only guardian. No one else—not the police, not the NSA, not the government, and sure as hell not Facebook or Google—are in your corner. You are alone and no one else is going to help you.

“Don’t Talk to the Police”



Why Not Talk to the Police?

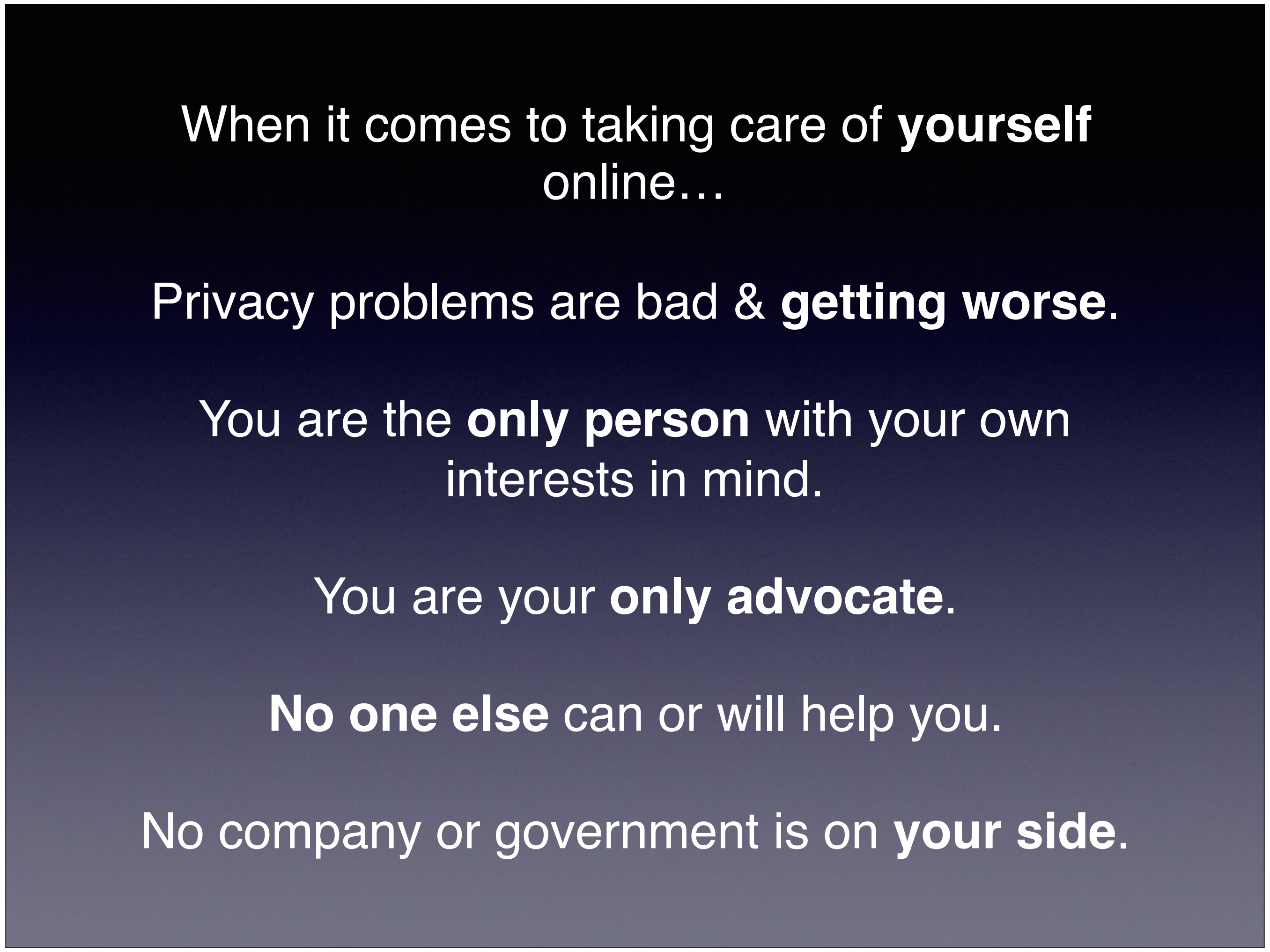
- 1. There is *no* way it can help.
- You *can't* talk your way out of getting arrested.
- You *can't* give them any information that will help you at trial. *See* Federal Rule of Evidence 801(d)(2)(A).
- What you tell the police is *only* a
  is offered *against* you by the pro

Remember this?
Summary: literally *anything* you say is potentially incriminating and harmful under the right circumstances.

And even if you still can’t see the problem with blindly allowing the government and companies access to your online life—even if you’re still clinging to the whole “if I have nothing to hide, then I have nothing to worry about” bit—this video does a great job encapsulating why even 100% “innocent” people should closely guard their personal info and activities and not talk about them to anyone. Whether it’s in the context of an interview with law enforcement or in freely allowing your life to be collected and catalogued online, literally NOTHING good can come from it. Ever.

(This is a great video that I’d highly recommend everyone watching—Regent University Law Professor James Duane talking to law students about the dangers of opening your mouth during a police interview and not doing the correct thing and letting your attorney talk for you.)

https://www.youtube.com/watch?v=d-7o9xYp7eE



When it comes to taking care of **yourself** online…

Privacy problems are bad & **getting worse**.

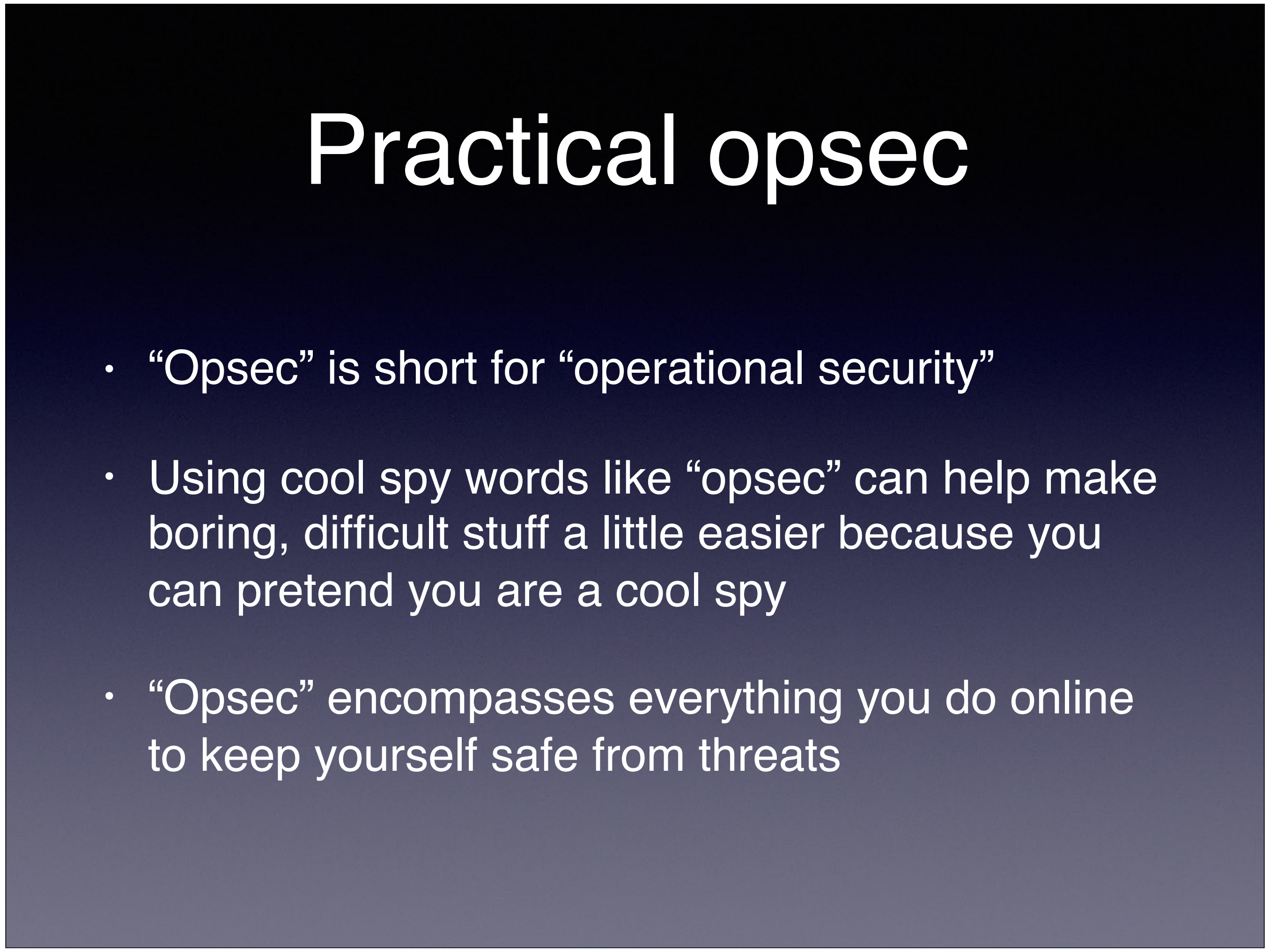
You are the **only person** with your own interests in mind.

You are your **only advocate**.

No one else can or will help you.

No company or government is on **your side**.

So, closing out the doom and gloom and moving on to the actual practical stuff! Here are the takeaways that you should keep in mind whenever you open a web browser or check your email or type personal information into a form. No one else has your back. No one will help you. You have to take care of yourself.



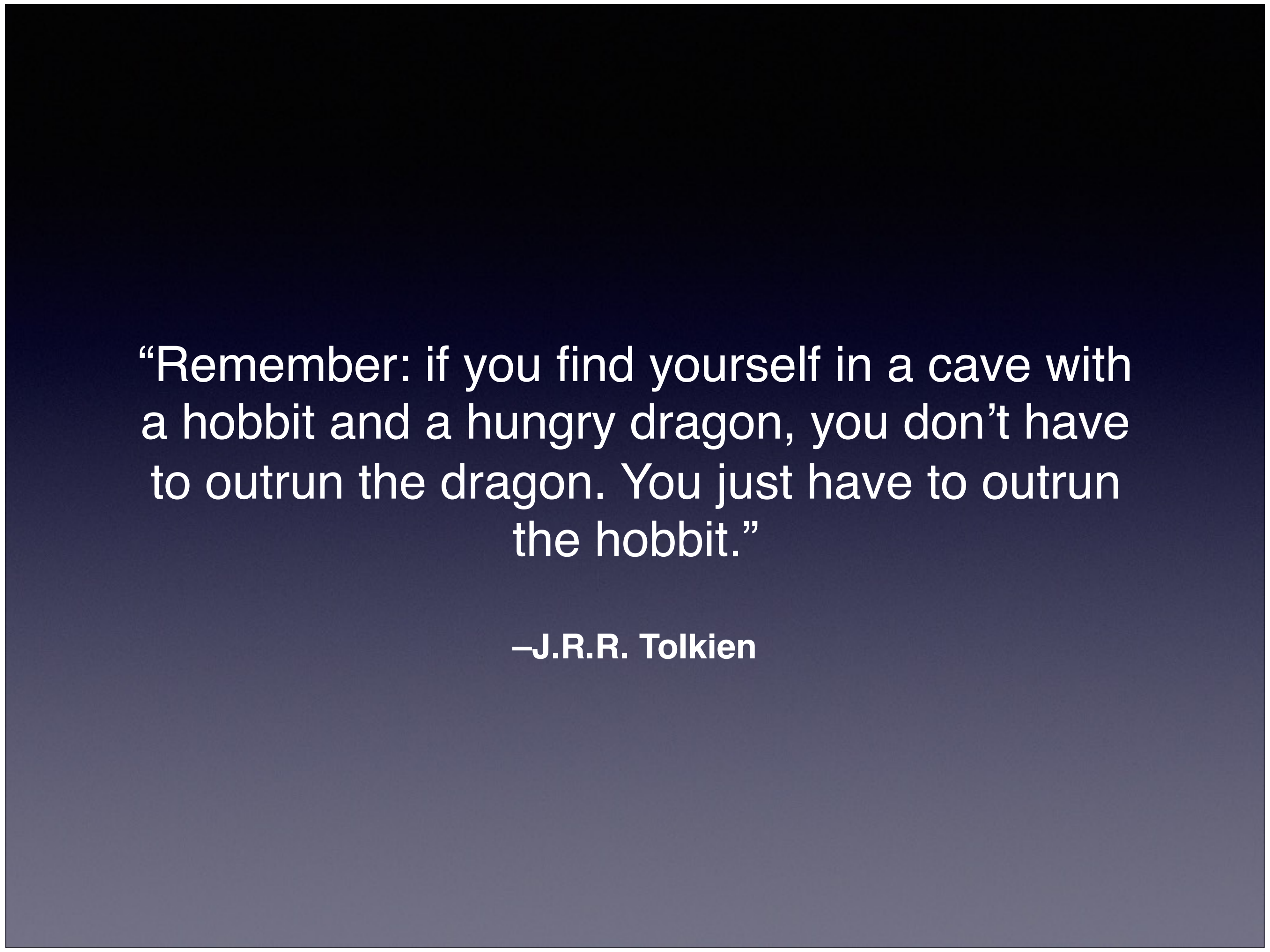
Practical opsec

- “Opsec” is short for “operational security”
- Using cool spy words like “opsec” can help make boring, difficult stuff a little easier because you can pretend you are a cool spy
- “Opsec” encompasses everything you do online to keep yourself safe from threats

So let’s move onto item 1 - “Practical Opsec”

“Opsec” is the fancy cool way of referring to your general approach to keeping yourself secure and your privacy intact. It refers to the whole suite of behaviors you engage in—how you store passwords, how you respond to online surveys, when you do and don’t use a VPN, when you do and don’t use encryption, what you do and don’t say in emails, when to lie online (most of the time) and when to tell the truth (rarely).

Trying to get your hands around EVERYTHING you do online is a little daunting, but remember:



“Remember: if you find yourself in a cave with a hobbit and a hungry dragon, you don’t have to outrun the dragon. You just have to outrun the hobbit.”

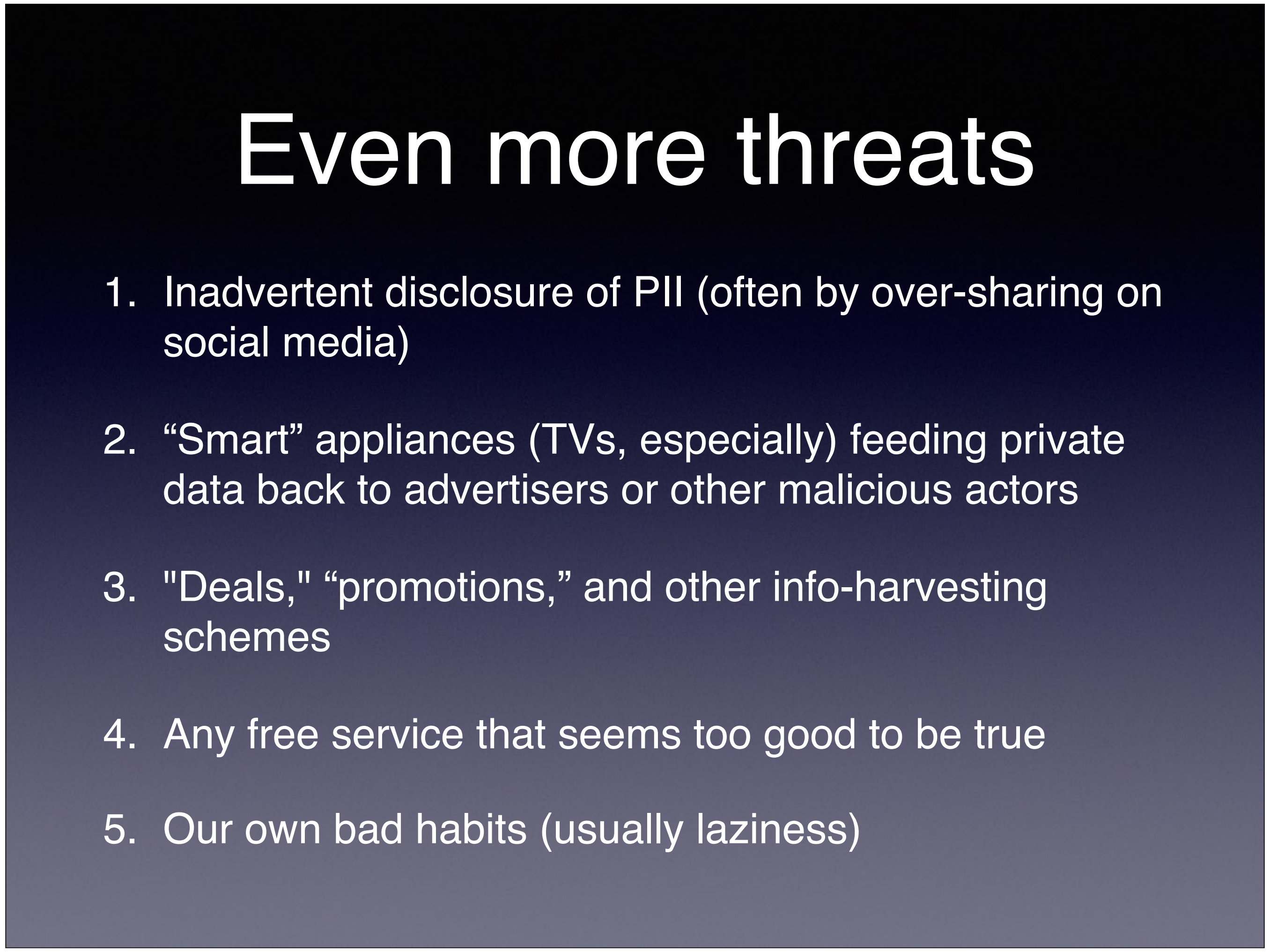
–J.R.R. Tolkien

OK, JRR Tolkien might not actually have said this, but it holds true and it’s kind of like cleaning your house. You generally don’t have to make yourself 100% secure immediately—you should instead focus on big stuff first and try to make yourself less of a potential target than the next guy, because a lot of the threats to privacy and security you’ll encounter are opportunistic—they’ll ignore harder targets because there’s a wealth of easy ones. Just like how if you try to clean your whole house at once you’ll generally give up before you’re done, online security works the same way. It’s a constant process, not a done-in-one thing.

Threats?!

1. Malicious applications (spyware, malware, ransomware, etc)
2. Phishing in all its guises
3. Fraud (419 scammers, tech support scammers, etc)

So what, EXACTLY, are we talking about? There's all kinds of stuff you need to be on guard against—there are "active" threats, like on this slide. Malware, viruses, scams, phishing attempts—everybody knows what phishing with a ph means, right? (definition if not)—and other kinds of fraud. These are actual "attacks" that happen—a virus tries to install itself when you visit a compromised web site, or someone calls you on the phone from "Microsoft" and tries to get you to tell them your credit card number. Many of these are obvious, and you protect yourself from them by not engaging.



Even more threats

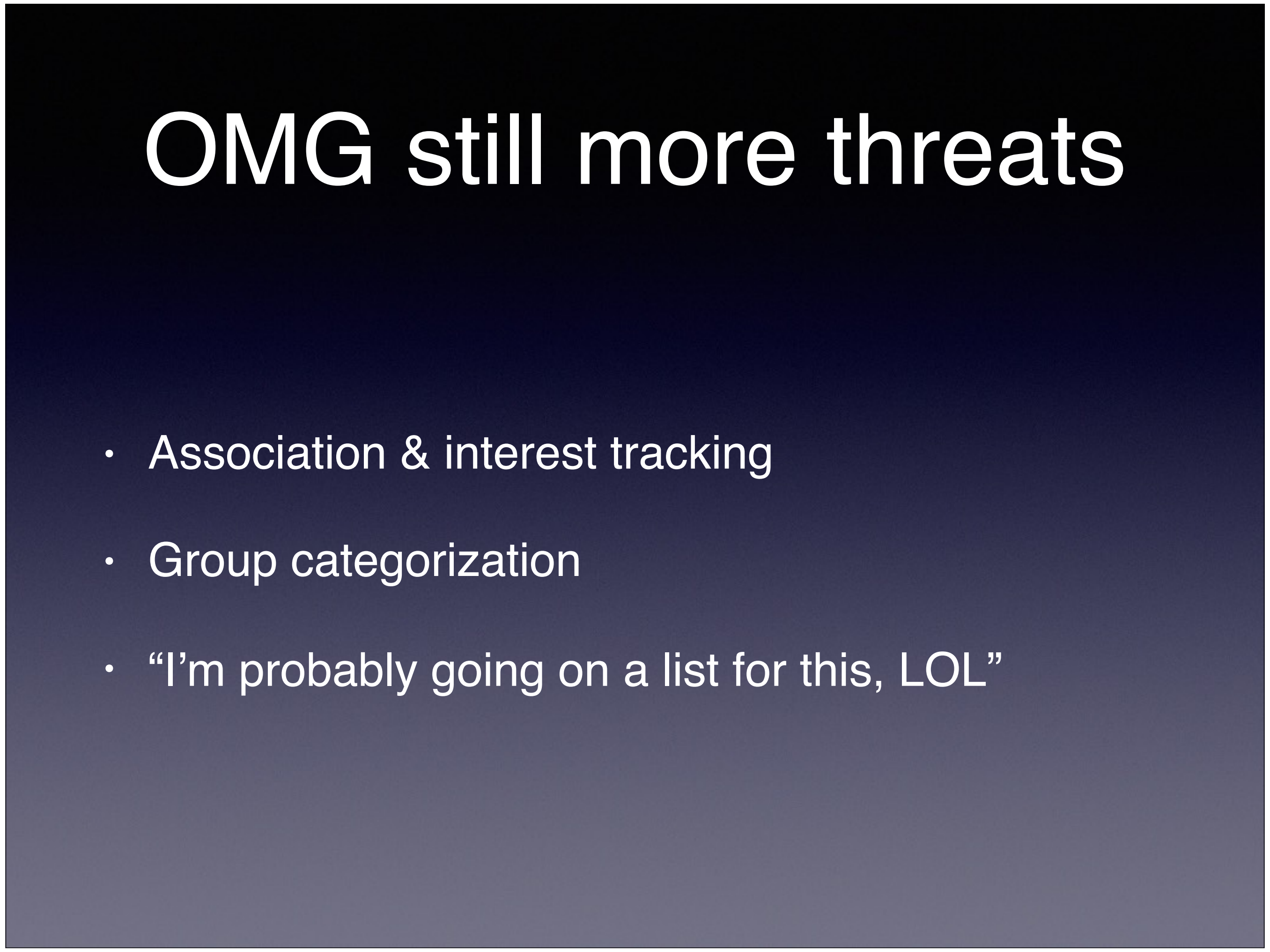
1. Inadvertent disclosure of PII (often by over-sharing on social media)
2. “Smart” appliances (TVs, especially) feeding private data back to advertisers or other malicious actors
3. "Deals," “promotions,” and other info-harvesting schemes
4. Any free service that seems too good to be true
5. Our own bad habits (usually laziness)

But threats can be insidious—these are all more “passive” threats rather than active. Oversharing on social media is a huge problem and we’ll get to that; but also be aware of coupon sites, deals or promotions, or places like facebook that offer complex services for free. You know the saying: “if you can’t see the price tag on a service, it’s because you’re actually the product the service sells.” Using FB as an example—Facebook doesn’t exist to connect you to your friends and family. Facebook exists to build rich, complex consumer profiles and then to monetize those profiles by either serving targeted advertisements or by selling your consumer profiles to other companies so that they can serve you up targeted advertisements.

And we’re also social creatures—sometimes we leak data ourselves because we’re talking to someone who seems trustworthy. Confidence scams are as old as the hills, and the internet has been a goldmine for scammers. You might have heard the term “social engineering”—that’s a fancy phrase that essentially means “bluffing and conning info out of someone.”

Smart TVs, Smart fridges, or anything else “smart”—throw that shit in the trash. They’re invariably insecure and more to the point they represent a threat you CAN’T do anything about. Vizio and Samsung both have been caught just flat-out spying on customers—with Samsung, it was the voice command mics on their “smart TVs” were always on and always recording, and while Samsung said that the data being collected was anonymized, security researches dissected the network traffic from one of the TVs and found that the TV was transmitting tremendous amounts of PII back along with the voice recordings. Vizio was flat-out sending advertisers poorly-anonymized viewing data—basically saying this household watches these shows.

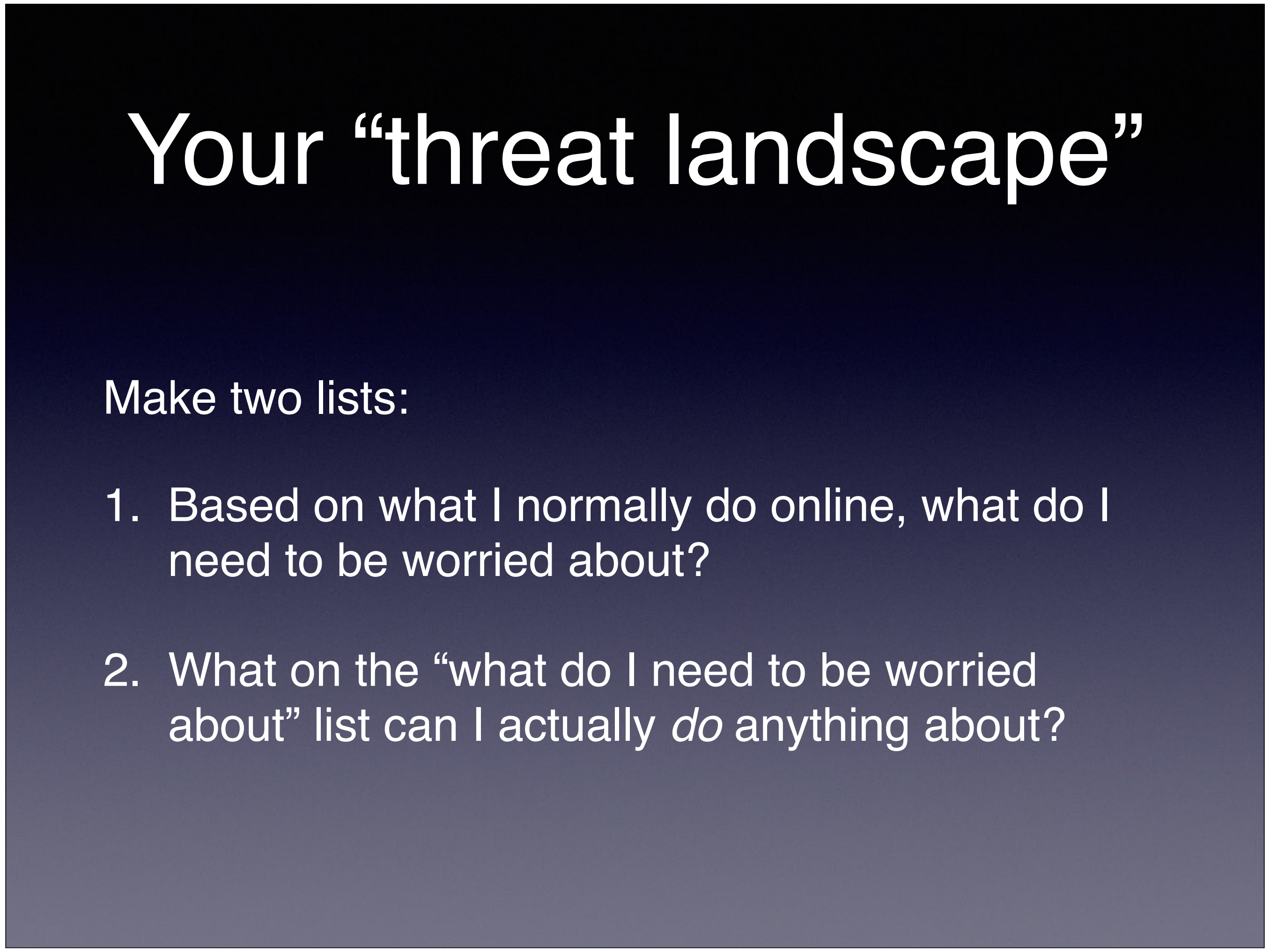
Plus, this goes a step further—if you’ve got what’s effectively a computer listening to you and reporting back everything that you do when it’s working normally, how much worse is it when a SmartTV or smart fridge catches malware? it’s becoming more and more common—and at that point it’s not just advertisers listening to your private conversations, but also potentially foreign hackers or even foreign governments.



OMG still more threats

- Association & interest tracking
- Group categorization
- “I’m probably going on a list for this, LOL”

And finally, there’s the threat posed by broad and uncontrolled data collection by state actors, foreign and domestic. These are the really scary things—the things that sound like conspiracy theory craziness until you realize that these and so many other absurd-sounding things have been multiply corroborated. These are the broad categorizations and assignations made by government agencies—profile data that gets used in determining your potential likeliness for being included on no-fly lists, or that might cause you to fail a security clearance investigation for a job. While there are typically methods for you to force marketers to show you the profile info they have on you, there’s not a lot you can do about any of these other than to be extremely cognizant of EVERY online interaction you have and the potential implications.



Your “threat landscape”

Make two lists:

1. Based on what I normally do online, what do I need to be worried about?

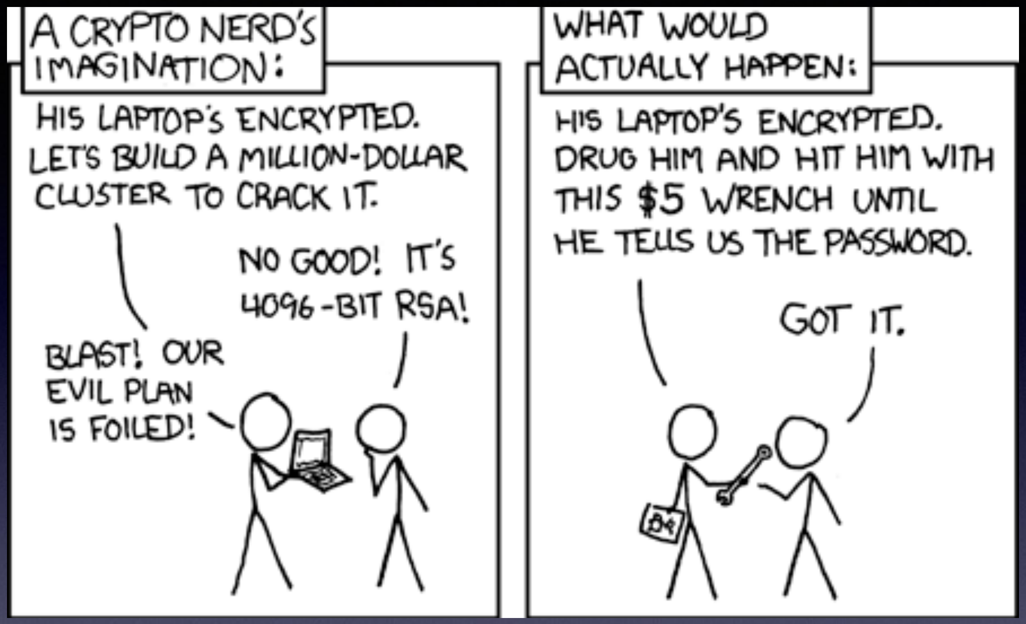
2. What on the “what do I need to be worried about” list can I actually *do* anything about?

So—what the hell do we DO about any of this?

First you gotta figure out your own personal “threat landscape.” Think of this as an assessment of what you regularly do online every day. What sites do you visit? What kind of information do you usually post? Who are you emailing? Do you pay attention to whether or not the sites you’re visiting are using HTTPS encryption? Are you using your real name, address, birthdate, SSN, or phone number anywhere where it’s not 100% necessary? What about your spouse, kids, and other family? Are you using THEIR real info anywhere? Do you buy lots of stuff online? Are you using encryption on your own devices? Do you have passcodes in place? Are you doing backups? Need to do a complete assessment, front to back, of essentially anything electronic.

then, throw away the threats you can’t do anything else about—because that’s going to be a lot of things. it’s kinda like doing a burglar-proofing assessment on your house—no deadbolt, alarm, anti-kick door frame reinforcement, or shatterproof window will stop a sufficiently motivated attacker, and there are certain classes of online attacker you can’t really protect yourself against. State actors, for example—if the NSA has decided you’re a person of interest for some reason, they’re going to get what they want out of you and you can’t stop them. Same if you’ve somehow managed to piss off some Russian hackers. Some threats are overwhelming.

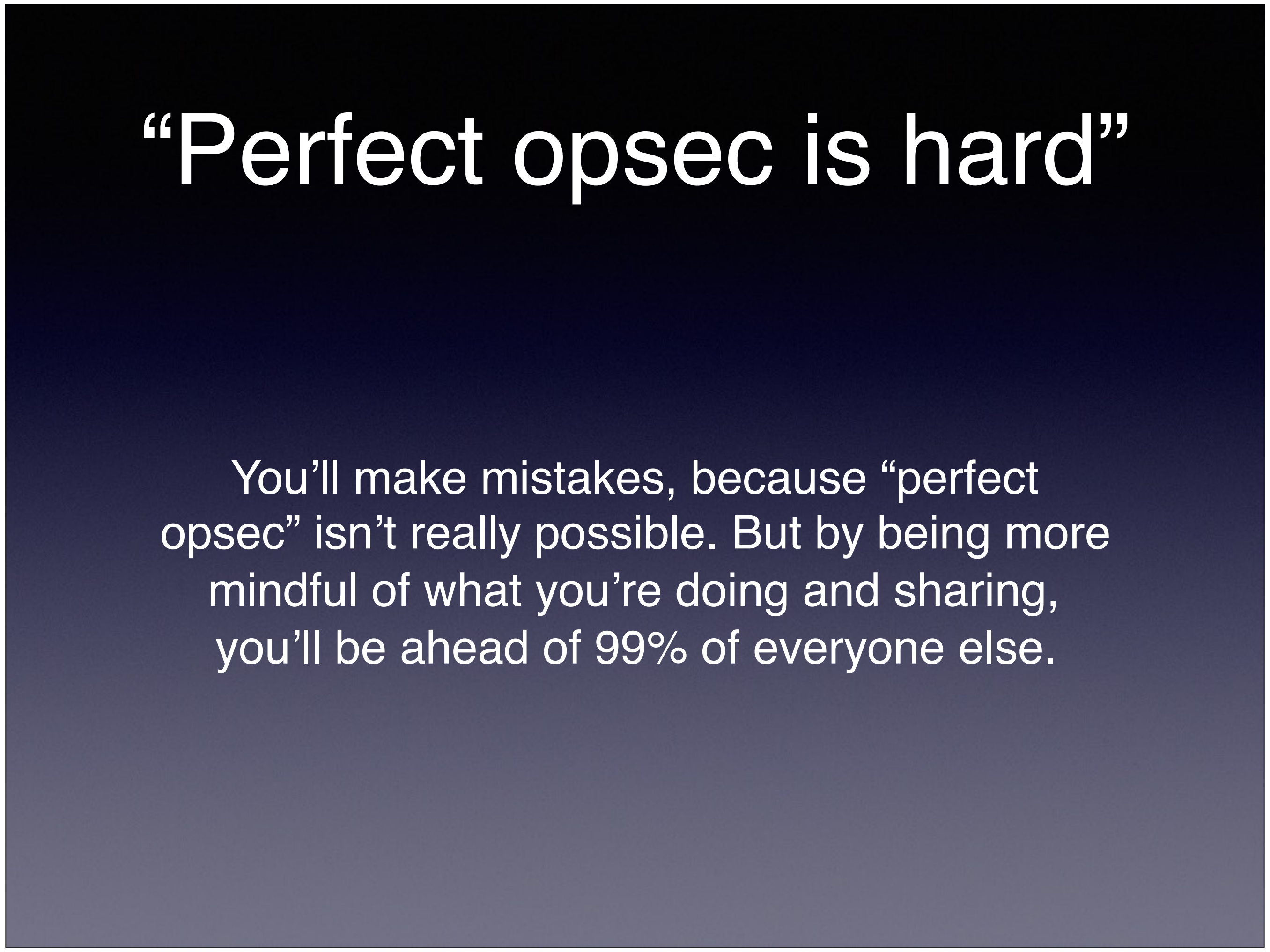
But most aren’t—and most can be identified and mitigated.


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Expectation vs. reality

“Percussive codebreaking” is impossible to defeat.

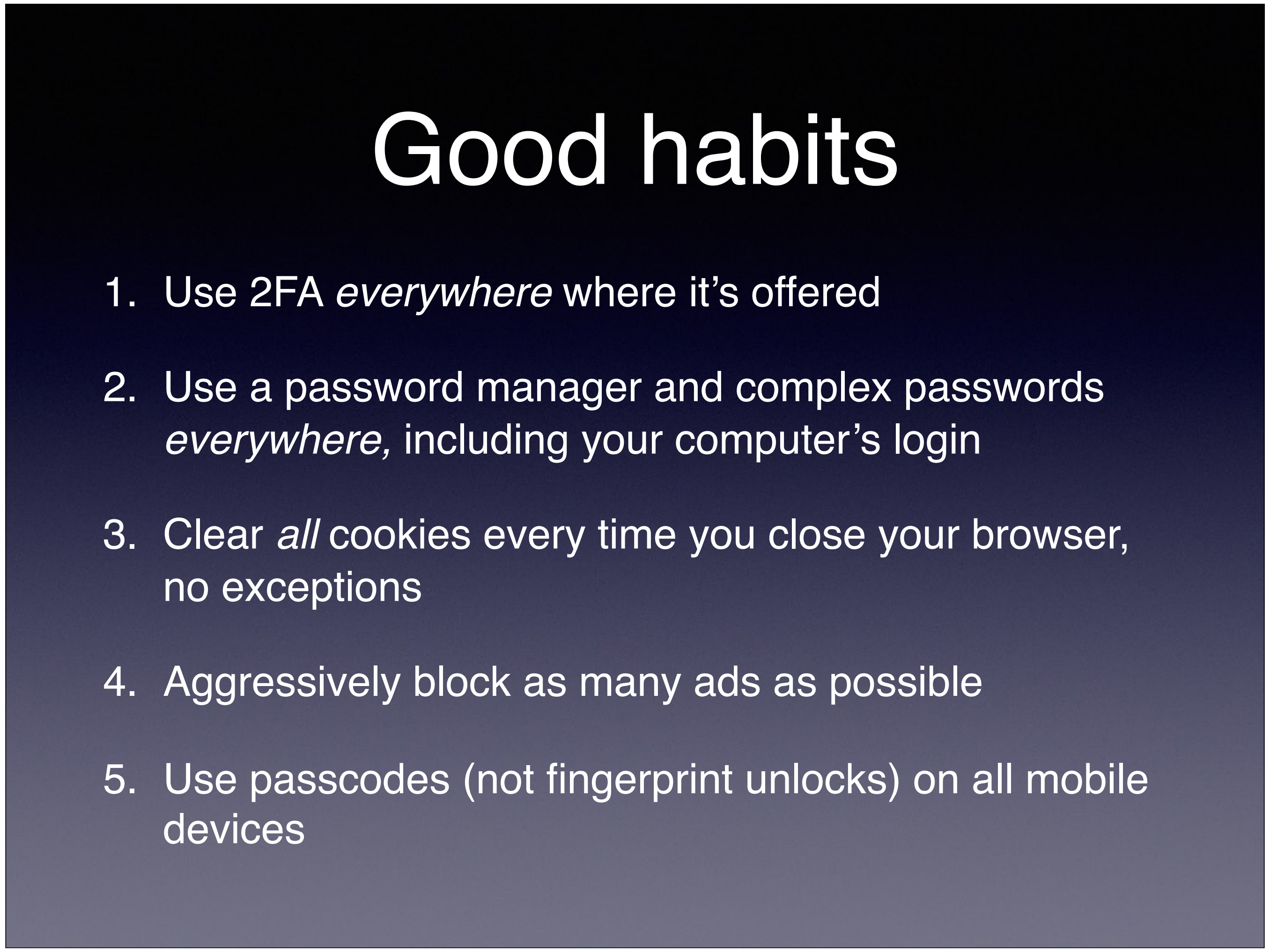
Don’t fall into the trap of thinking “Oh, whatever, if I have something sensitive i’ll just encrypt it and then it’s safe!” As noted, no encryption is no match against a sufficiently motivated threat. This includes state-level actors (three-letter agencies) and organized crime. If you’ve done something to piss off either of those, ain’t nothing I can tell you that will help you.



“Perfect opsec is hard”

You’ll make mistakes, because “perfect opsec” isn’t really possible. But by being more mindful of what you’re doing and sharing, you’ll be ahead of 99% of everyone else.

That being said, this isn’t a “can’t win, don’t try” scenario. Remember the hobbit and the dragon—protect yourself against everyday realistic stuff and you’ll still be doing better than most other folks. Just don’t get it in your head that you can outwit and out-encrypt either the cops or the mob. A ton of very, very smart people have tried and failed.



Good habits

1. Use 2FA *everywhere* where it’s offered
2. Use a password manager and complex passwords *everywhere,* including your computer’s login
3. Clear *all* cookies every time you close your browser, no exceptions
4. Aggressively block as many ads as possible
5. Use passcodes (not fingerprint unlocks) on all mobile devices

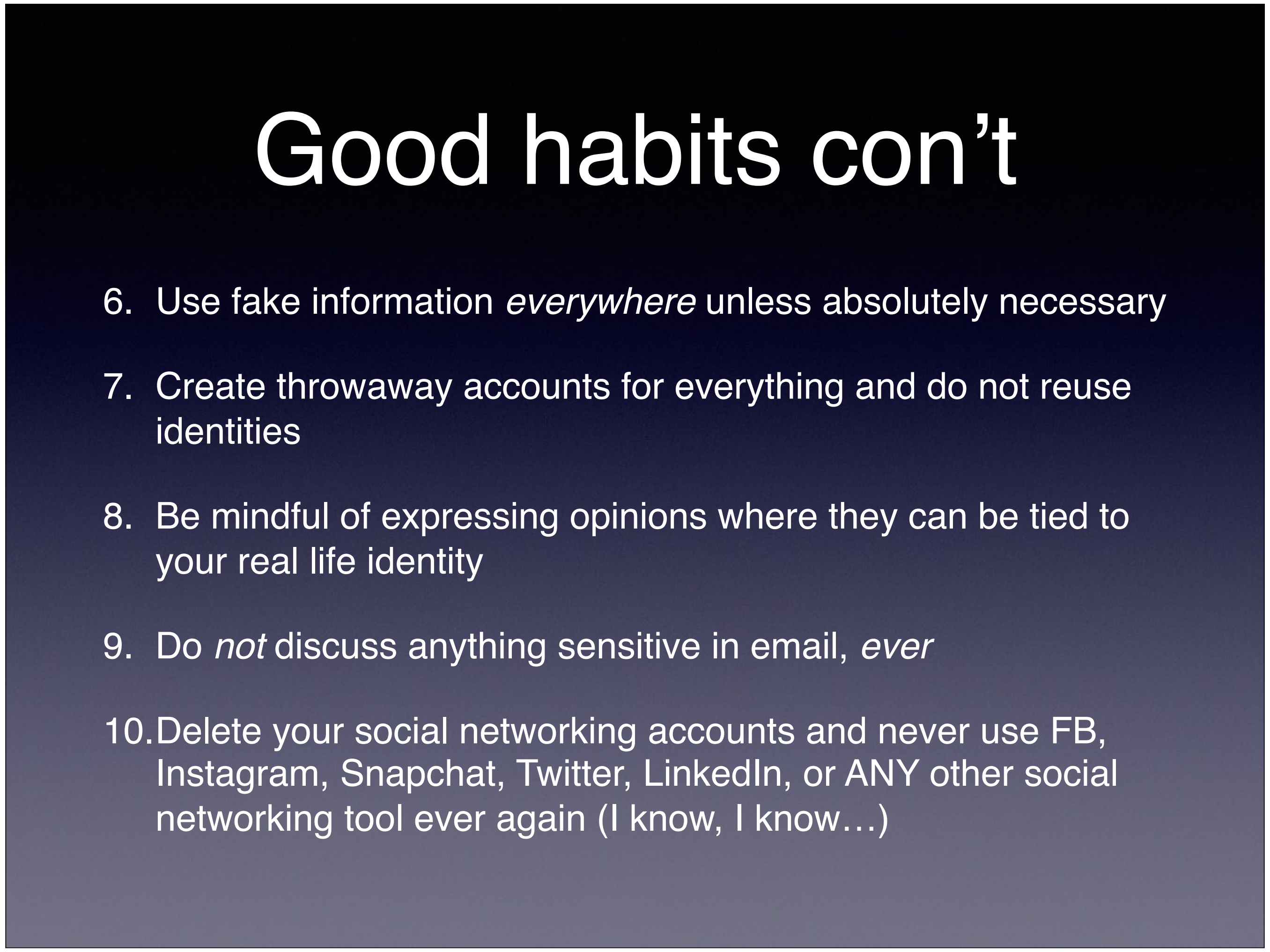
Here are some quick tips—and we’ll touch on #4 a bit in its own section.

#3 is one that a lot of people object to because of the inconvenience, but it’s just honestly a necessity. You can configure your browser to do this automatically and you should. the last thing you want are years worth of tracking cookies giving sites a data-rich view of your browsing and shopping habits.

Let’s look at this last one real quick, too - why passcodes and not fingerprint unlocks? Because in multiple unrelated cases over the past two years, courts at all levels have ruled that you can be legally compelled to unlock your phone if it’s locked with biometric data—fingerprint, retina, facial recognition. However, you can NOT be compelled to unlock your phone if it’s got a simple passcode. The reasoning is that under the 5th Amendment, a person cannot be compelled to provide self-incriminating testimony and established caselaw is that because combinations, codes, and passwords are things that you know, they also receive 5th amendment protection. Biometrics, being something that you inherently ARE rather than a piece of knowledge, do not enjoy that same protection—you casually leave fingerprints on everything you touch, after all, and so you have no expectation that your fingerprints are private.

In January of this year, a Minnesota appellate court wrote: “Instead, the task that Diamond (the suspect’s name) was compelled to perform—to provide his fingerprint—is no more testimonial than furnishing a blood sample, providing handwriting or voice exemplars, standing in a lineup, or wearing particular clothing.” the laws vary by state, but in many states including TX, police only need “reasonable suspicion” to attempt to search your device during an otherwise unrelated interaction, and if you don’t have a passcode, you have to let them or risk jail.

https://arstechnica.com/tech-policy/2017/01/court-rules-against-man-who-was-forced-to-fingerprint-unlock-his-phone/



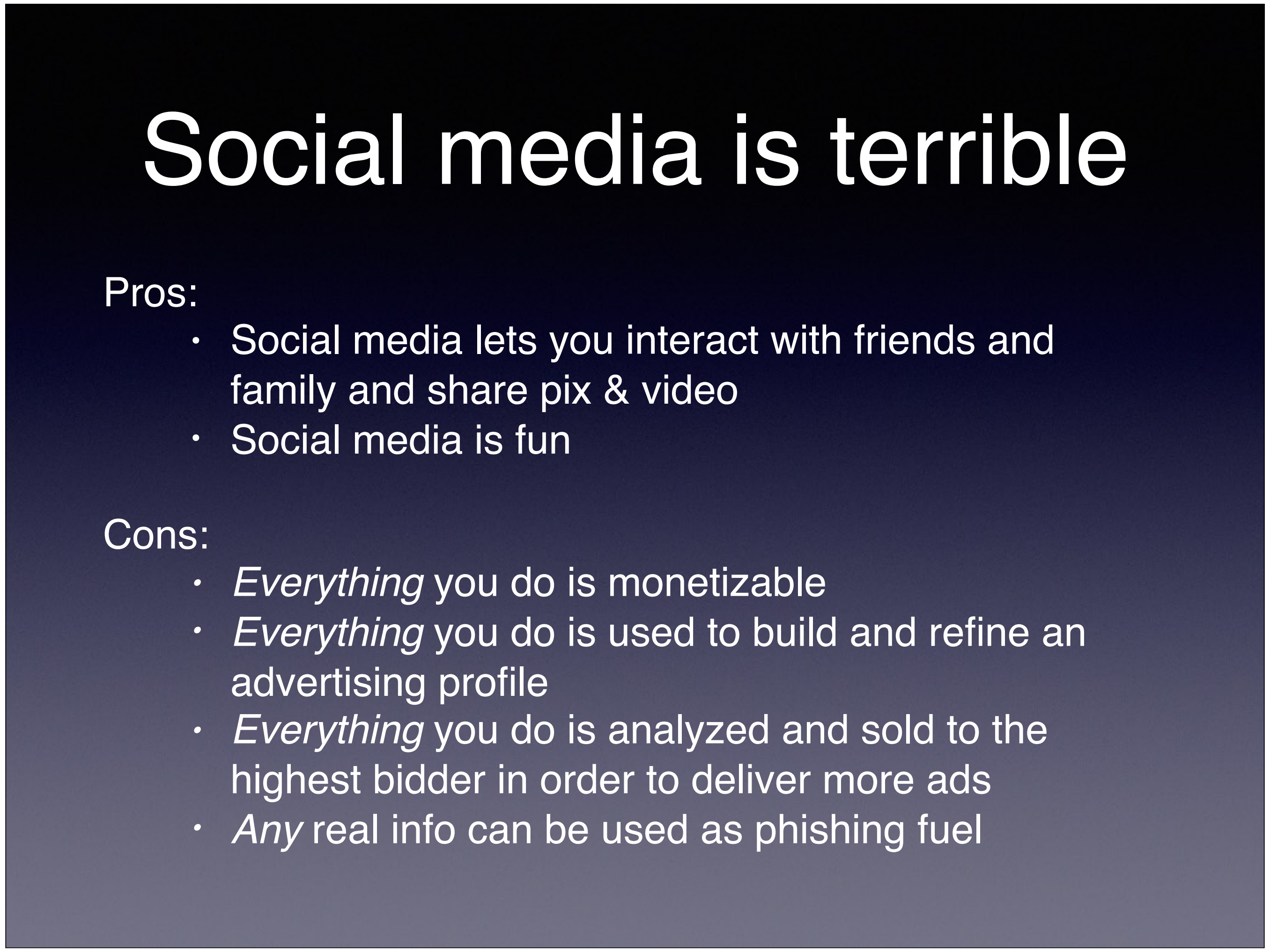
Good habits con’t

6. Use fake information *everywhere* unless absolutely necessary
7. Create throwaway accounts for everything and do not reuse identities
8. Be mindful of expressing opinions where they can be tied to your real life identity
9. Do *not* discuss anything sensitive in email, *ever*
10. Delete your social networking accounts and never use FB, Instagram, Snapchat, Twitter, LinkedIn, or ANY other social networking tool ever again (I know, I know…)

number 6 - weirdly, i’ve heard a lot of people object to #6 when i’ve insisted on it in the past, and that really bothers me. unless you’re engaging in commerce with a site—like an online vendor–why on God’s green earth would you give your real info out?! Why does a newsletter or a forum or a coupon web site need to know your real name and birthdate?

re number 9) What’s the difference between the post office and google? Well, google’s faster and google also reads your mail. though google’s actually stopped scanning email text in order to do ad placement, what they DO have is the ability to respond to a subpoena with the entire contents of your mailbox. ALL OF IT. And that comes back to the whole “don’t talk to the police" thing—what do you think a motivated prosecuting attorney could do with your inbox’s contents, stripped of all context? Based on the shit I’ve joked about with friends and family before, there’s probably no crime I COULDN’T be accused of.

which leads us to…



Social media is terrible

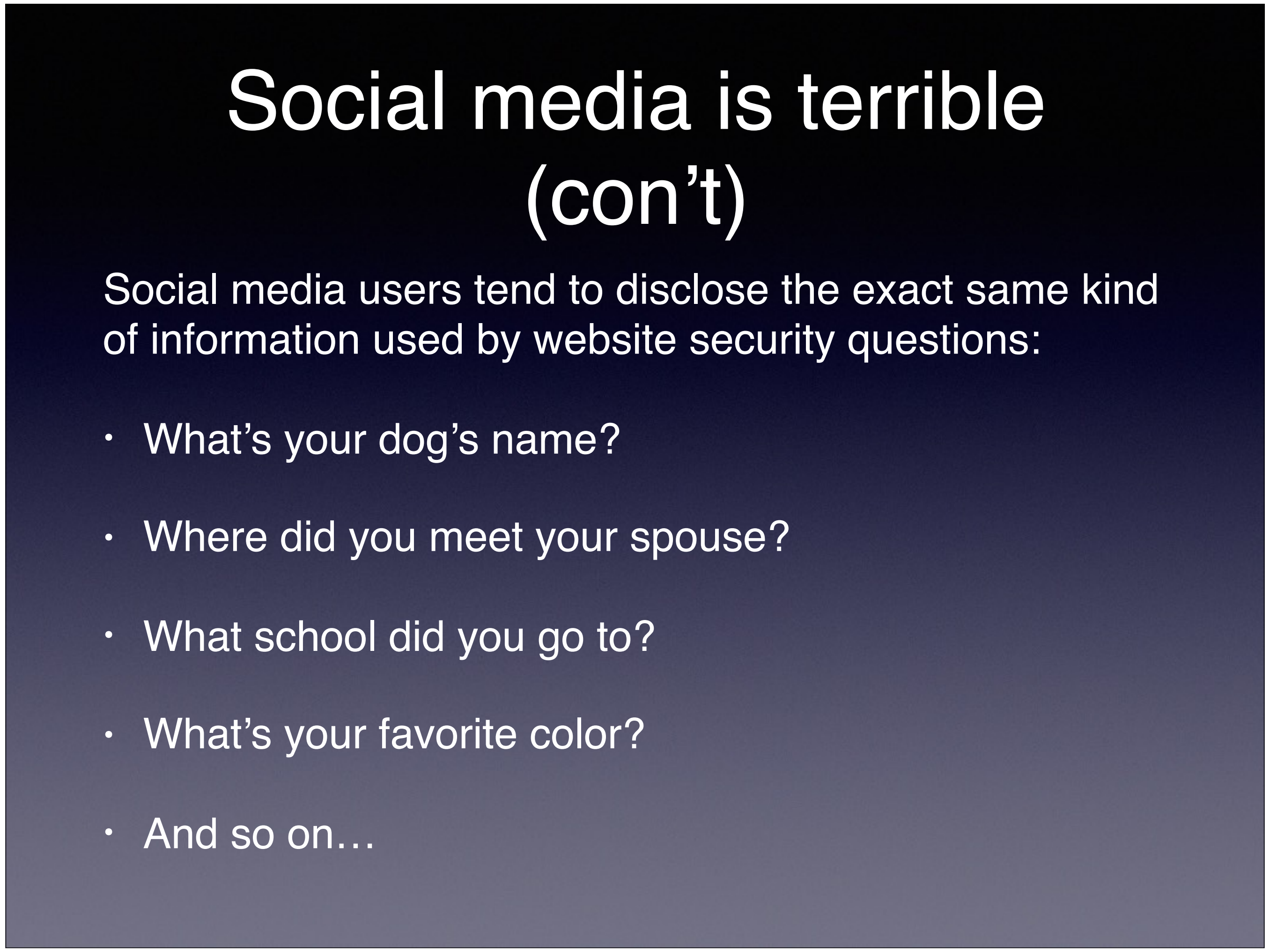
Pros:

- Social media lets you interact with friends and family and share pix & video
- Social media is fun

Cons:

- *Everything* you do is monetizable
- *Everything* you do is used to build and refine an advertising profile
- *Everything* you do is analyzed and sold to the highest bidder in order to deliver more ads
- *Any* real info can be used as phishing fuel

Social media. Everybody uses it in all its forms. By show of hands, how many of you folks check facebook at least once a day? How many of you folks have checked facebook at least once since you got here today? Not gonna lie, social media is a hugely important part of just how we live life right now, but it’s also a huge privacy and security problem, in aggregate and also for each individual social media company.



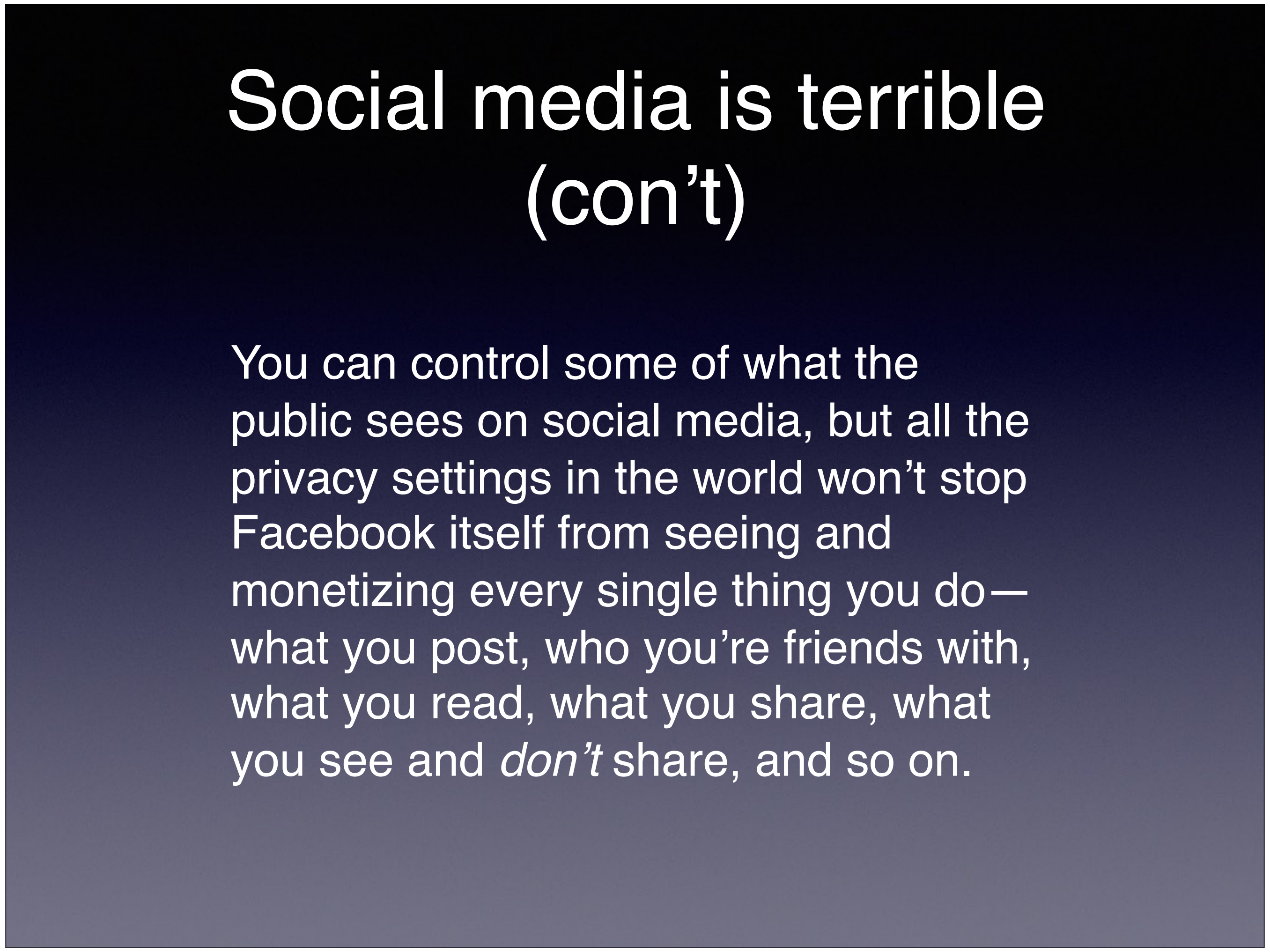
Social media is terrible (con’t)

Social media users tend to disclose the exact same kind of information used by website security questions:

- What’s your dog’s name?
- Where did you meet your spouse?
- What school did you go to?
- What’s your favorite color?
- And so on…

Worst of all, for the overwhelming majority of people, they kneecap themselves by posting on social media the EXACT stuff that typically gets used by other companies as security questions. This is why any kind of hacking or social engineering attempts _ALWAYS_ start with an assay of the potential victim’s social media—it’s the fastest and most efficient way to get details on possible answers for security questions or even hints about what a person's password would be.

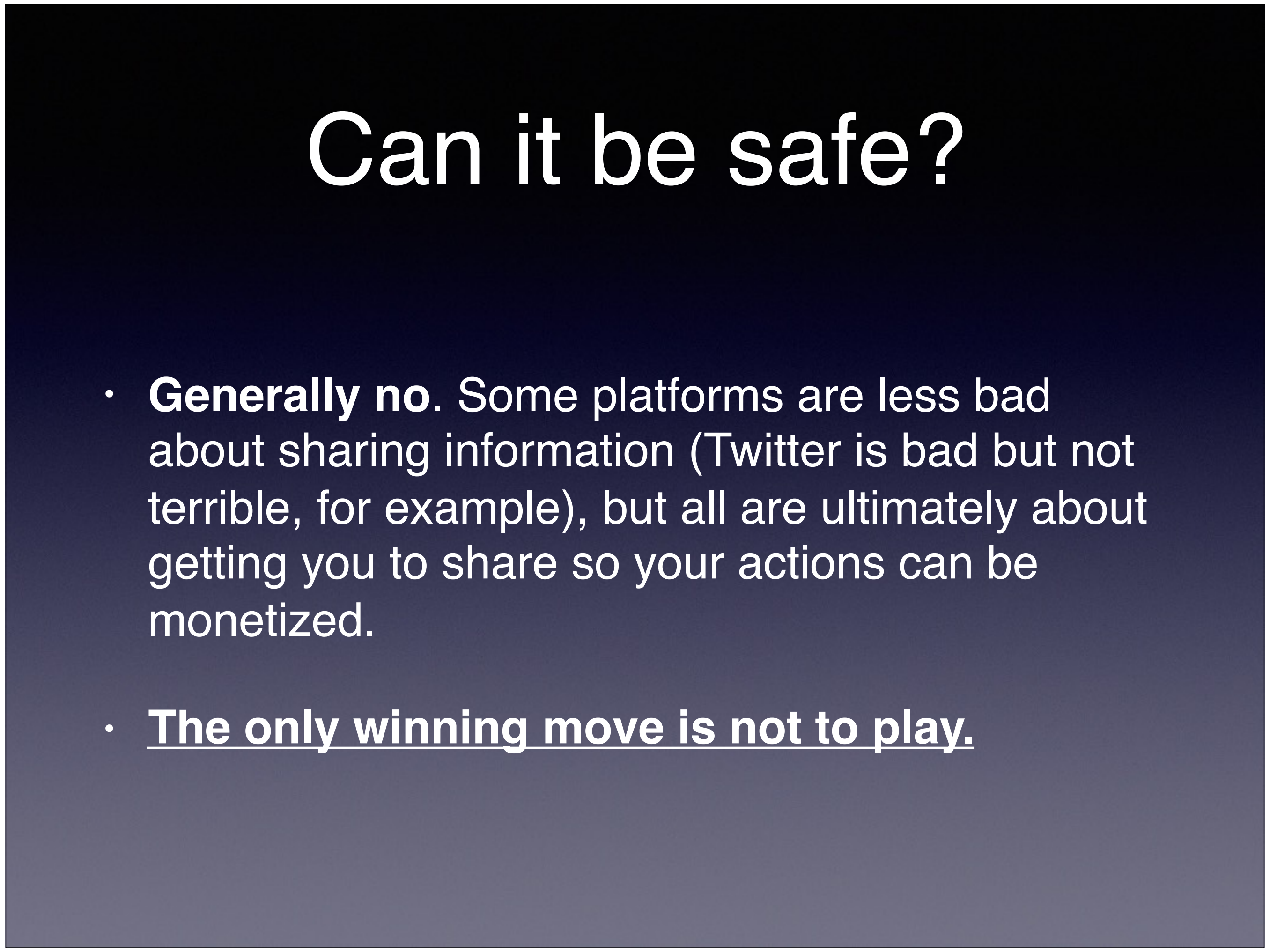
(one way to combat this is to make sure that your security questions everywhere are always nonsense random characters—as far as Bank of America is concerned, for example, your dog’s name should be a 64-character random collection of letters, numbers, and special characters stored in a password manager)



Social media is terrible (con’t)

You can control some of what the public sees on social media, but all the privacy settings in the world won’t stop Facebook itself from seeing and monetizing every single thing you do—what you post, who you’re friends with, what you read, what you share, what you see and *don’t* share, and so on.

Ultimately, you need to be aware that every single mouse movement you make on a social media site is tracked, analyzed, catalogued, and filed as part of a very valuable, very sellable marketing profile.

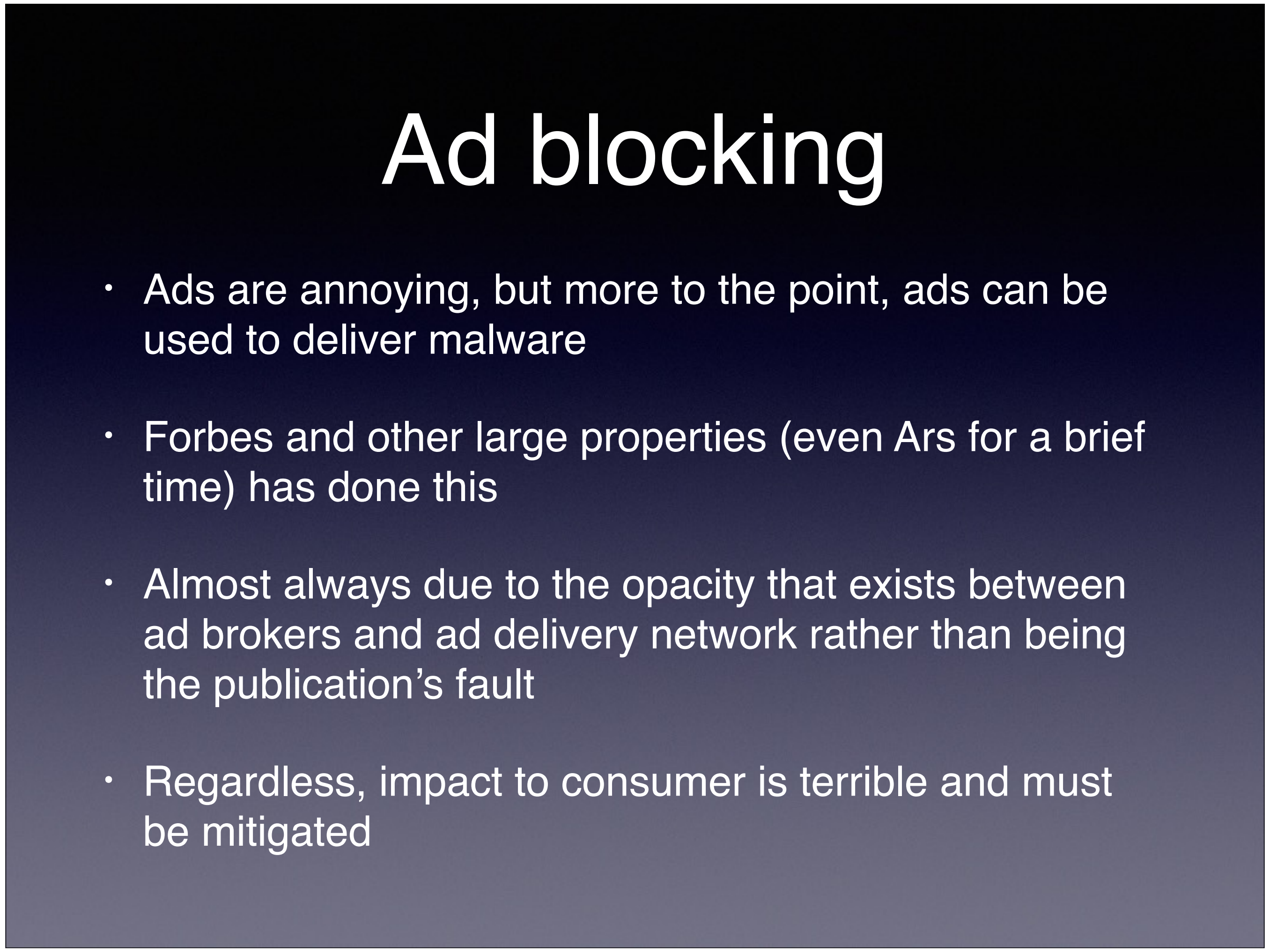


Can it be safe?

- **Generally no**. Some platforms are less bad about sharing information (Twitter is bad but not terrible, for example), but all are ultimately about getting you to share so your actions can be monetized.
- **<u>The only winning move is not to play.</u>**

Can I safely use social media without leaking any personal information that would be valuable to companies or bad actors?

No.



Ad blocking

- Ads are annoying, but more to the point, ads can be used to deliver malware
- Forbes and other large properties (even Ars for a brief time) has done this
- Almost always due to the opacity that exists between ad brokers and ad delivery network rather than being the publication’s fault
- Regardless, impact to consumer is terrible and must be mitigated

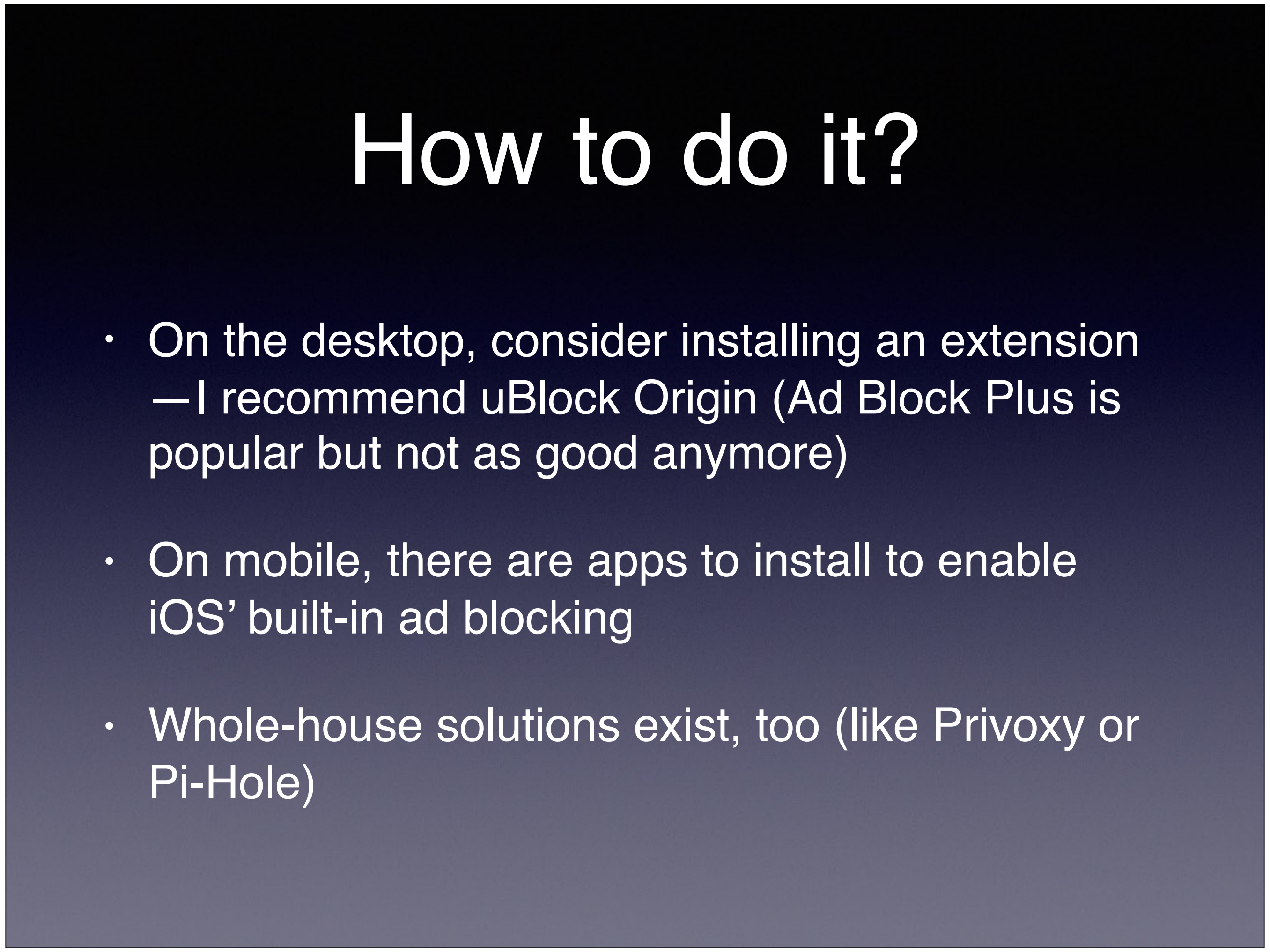
Ahh, ad blocking. As an informal poll, how many of you folks are using some kind of ad blocking, either on desktop or on mobile? (more, less than expected?)

I’m going to betray my entire ad-supported profession and tell you that while work-lee wishes you wouldn’t because he likes getting paid, private citizen lee says that if you’re not ad blocking, you’re INSANE. The ad situation online is completely out of control and completely untameable. Companies deal with ad brokers and ad networks which in turn source ads from all kinds of places; it’s essentially impossible even for the biggest players (like my employer Conde Nast, which is a multi-billion dollar publisher that owns most of the magazines you’ve ever heard of) to police their ads fully.

(Why? Because there are a lot of layers in the cake, and generally the layers generating and serving the ads are separated by multiple layers of middle bureaucracy without a lot of accountability. There’s so much money changing hands that a lot of it leaks.)

But…

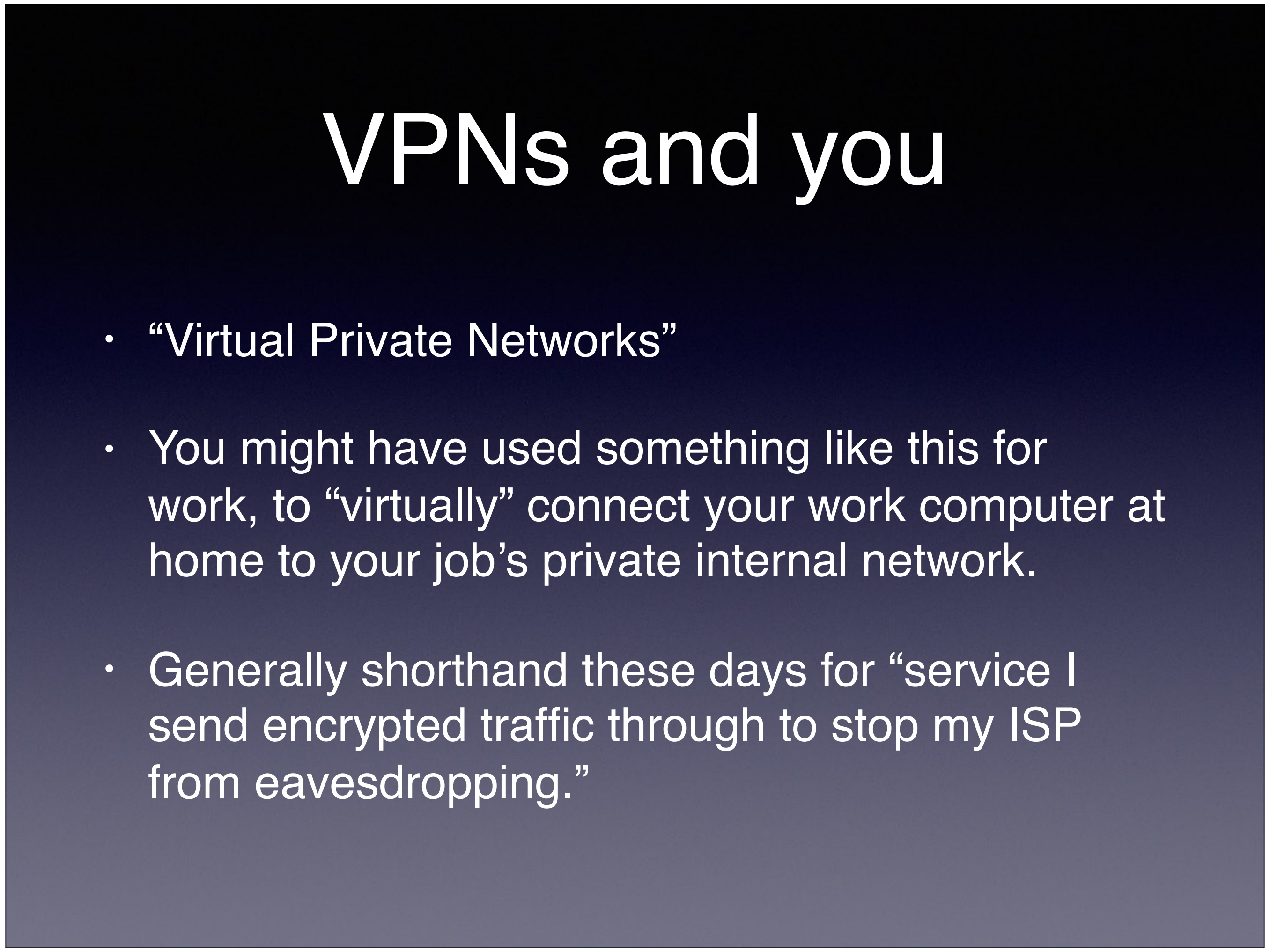
- Ad blocking presents moral and ethical issues for both consumers and publishers—is it theft, and is theft okay under the circumstances?
- Ad blocking directly deprives companies like my employer of revenue and makes it harder to hire quality employees
- Although publishers brought this on themselves, the potential effect on news, entertainment, and any other traditionally ad-sponsored business model is devastating
- Personal decision: to block or not to block?
- Consider supporting sites you love with donations, subscriptions, or whitelisting



How to do it?

- On the desktop, consider installing an extension—I recommend uBlock Origin (Ad Block Plus is popular but not as good anymore)
- On mobile, there are apps to install to enable iOS' built-in ad blocking
- Whole-house solutions exist, too (like Privoxy or Pi-Hole)

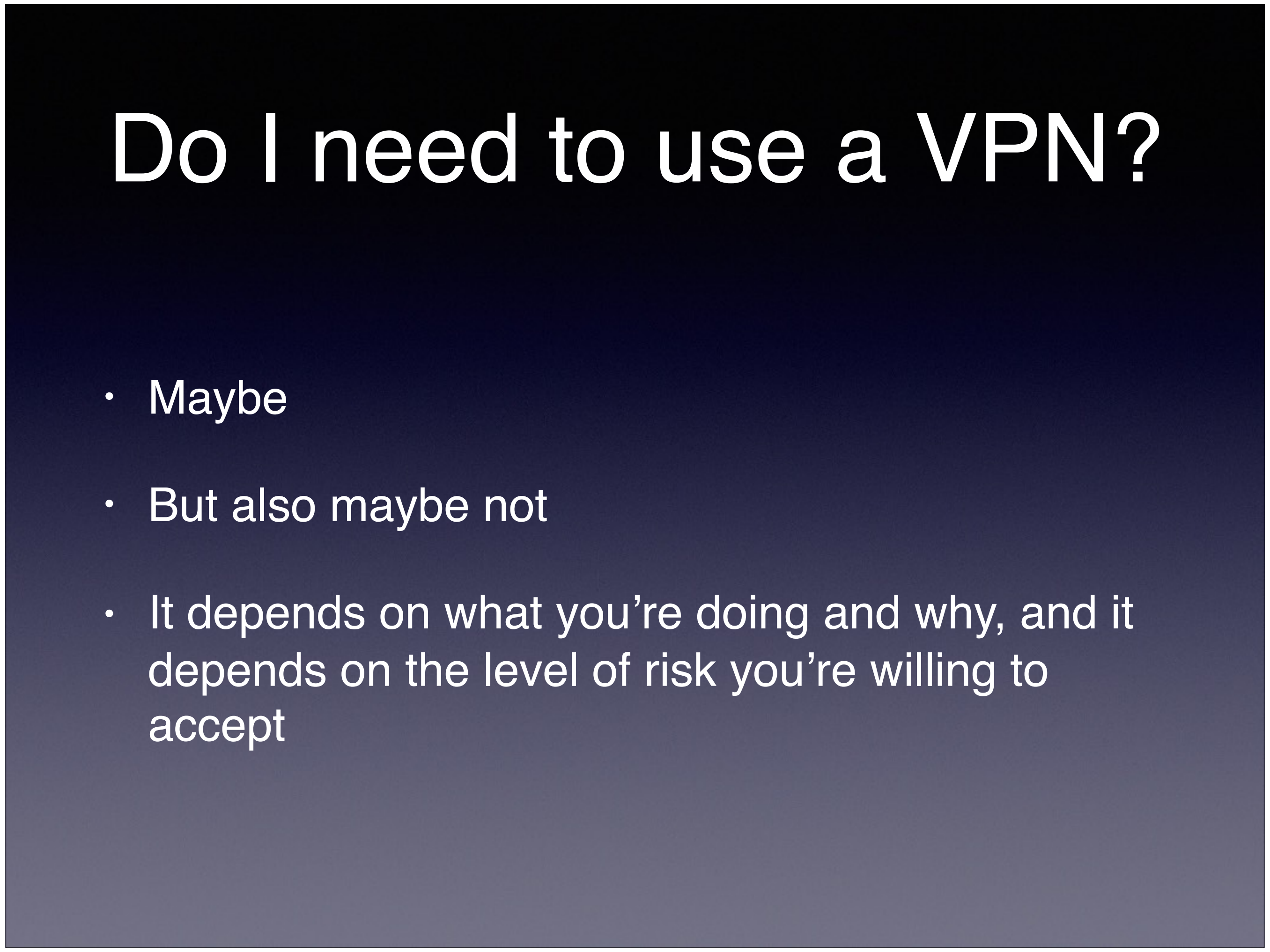
Downsides of adblocking—sometimes ad blocking breaks sites. Sometimes sites have “anti-adblocking” measures, which can be defeated with different adblocking filters and it’s a constant arms race between sides. Adblocking is GENERALLY set-it-and-forget-it to catch most stuff, but requires tweaking and custom filters to catch EVERYTHING. it’s something you should be doing, but requires configuration and effort to do properly. ain’t no such thing as a free lunch.



VPNs and you

- “Virtual Private Networks”
- You might have used something like this for work, to “virtually” connect your work computer at home to your job’s private internal network.
- Generally shorthand these days for “service I send encrypted traffic through to stop my ISP from eavesdropping.”

A VPN creates an ostensibly secure “tunnel” between the computer you’re on—and “computer” here can mean both your desktop and your mobile—and another computer somewhere else. It effectively changes _where_ you connect to the internet, and can foil attempts by your internet provider to snoop. More to the point, if you’re out at like a Starbucks or other public place using public wifi, a VPN can keep you safe from being spied on by the network operator, since it effectively encapsulates all your activity into an encrypted tunnel between you and the VPN provider. All the Starbucks operator sees is encrypted data.



Do I need to use a VPN?

- Maybe
- But also maybe not
- It depends on what you’re doing and why, and it depends on the level of risk you’re willing to accept

Maybe, maybe not.

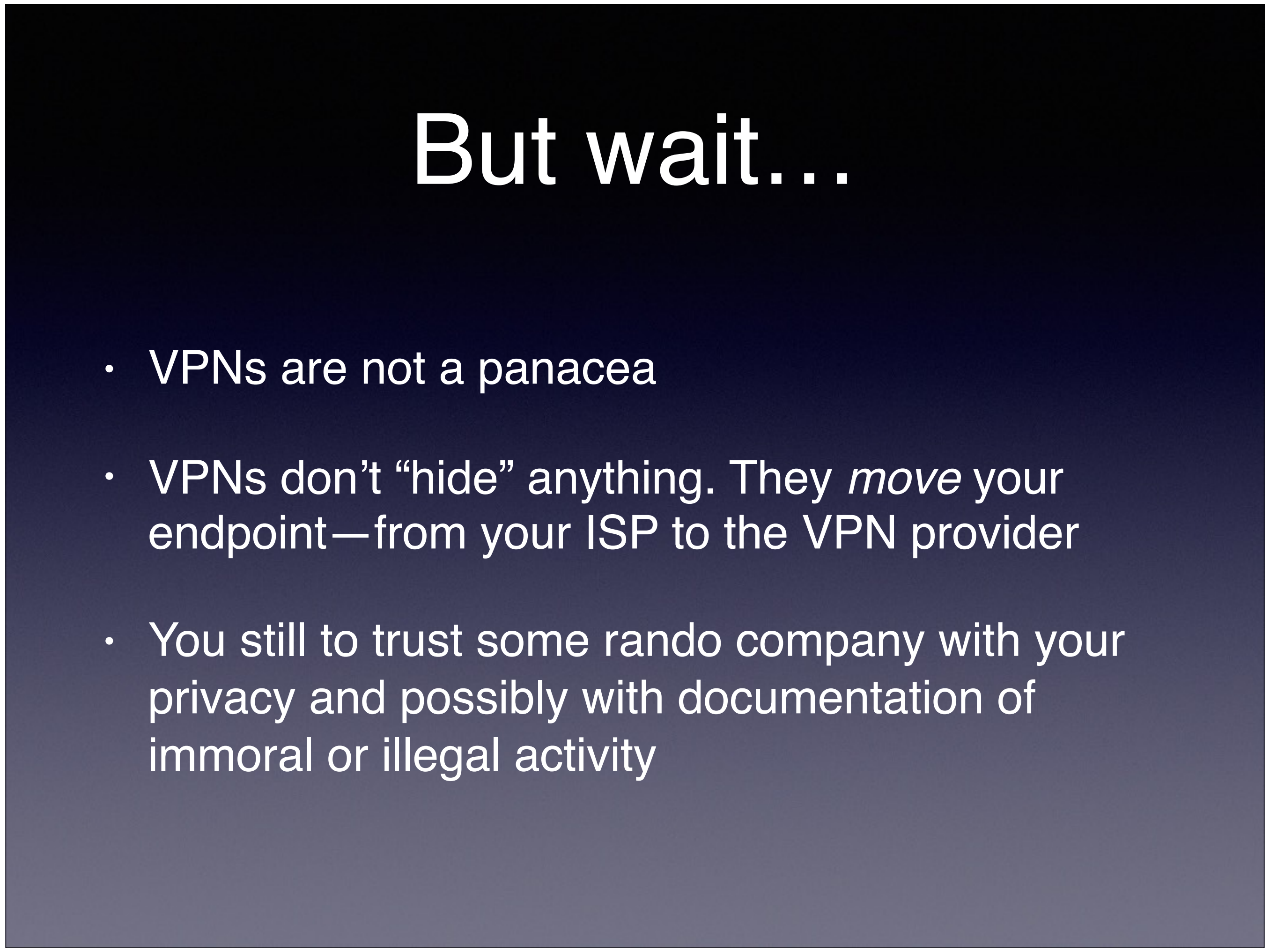
You’ll run into people who tell you you absolutely have to use a VPN for everything all the time. They’re not necessarily wrong—that might be advantageous. But they’re not necessarily right, either, since “always use a VPN everywhere” complicates your opsec greatly and can be a pain in the ass. (how do i know?! is next)

How do I know?!

1. Do you want to view geo-locked content that isn't available where you are?
2. Are you viewing sites you're not comfortable others knowing about? Porn, piracy, politics, pharmaceuticals?
3. Are you okay with the idea of your ISP tracking everything you do and selling your data to advertisers?

First look at the "why"—why use one? There are obvious privacy reasons, but remember that a VPN effectively changes where your "endpoint" is—it changes where all the sites on the internet think you're connecting from, since the remote computer you VPN to effectively becomes the place where "you" are. So in addition to being used for privacy, VPNs can be used to circumvent geographical restrictions on content—like, want to watch Canadian Netflix, which has a bunch of shows on it that were pulled from US Netflix because of stupid licensing deals? Fire up a VPN that offers a Canadian endpoint and then connect to Netflix. Or, inversely, are you traveling in Canada and want to watch US Netflix? Fire up a VPN with a US endpoint. Want to watch a bunch of awesome Top Gear reruns on Youtube—or even better, on the BBC directly? It's all blocked in the US, but if you fire up a VPN with a UK endpoint, boom, instant access because suddenly youtube and bbc.com think you're in the UK.

There are also the four Ps—everything you do is visible to your ISP, and you need to assess what you're comfortable with them knowing.



But wait…

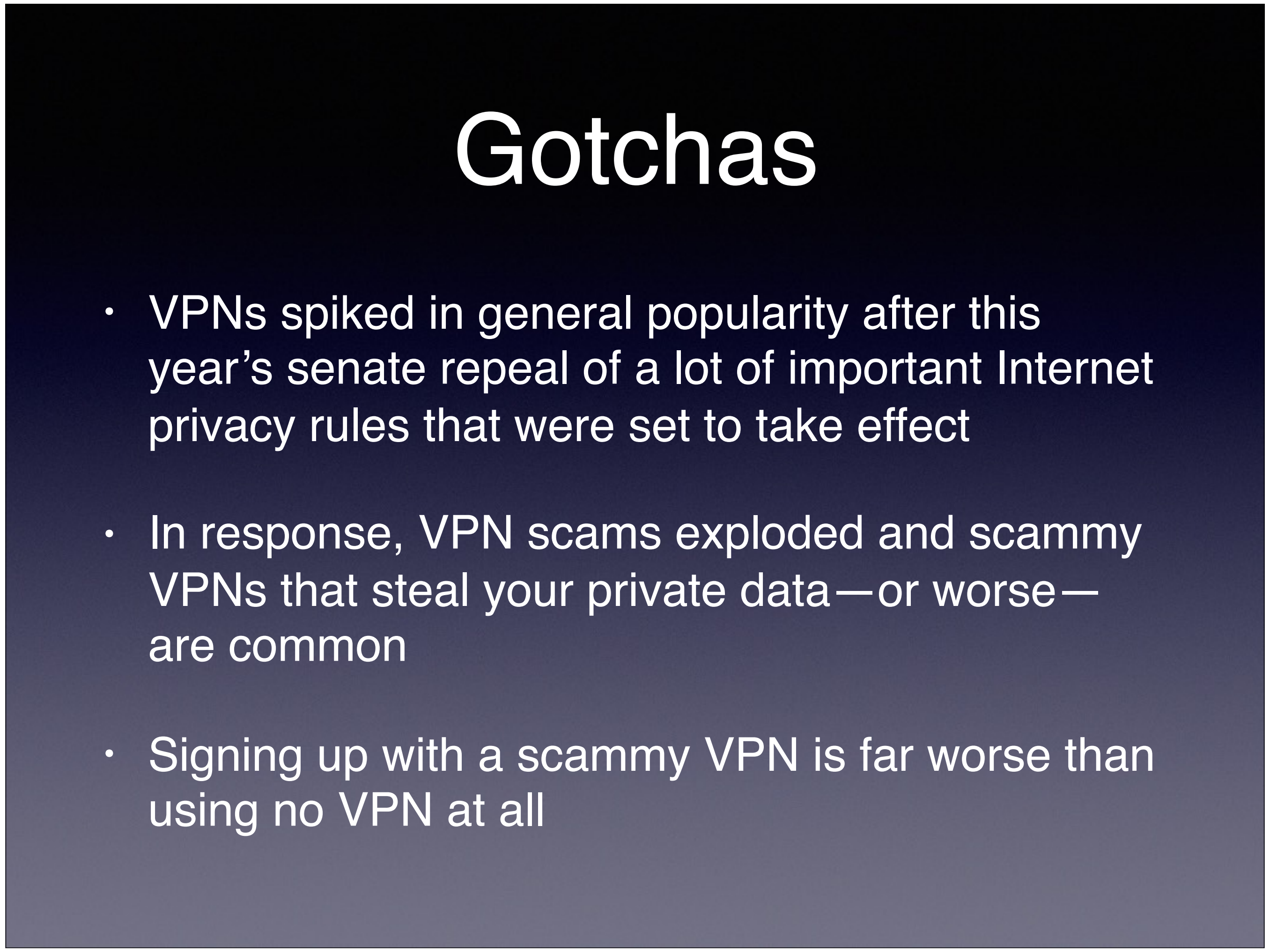
- VPNs are not a panacea
- VPNs don't "hide" anything. They *move* your endpoint—from your ISP to the VPN provider
- You still to trust some rando company with your privacy and possibly with documentation of immoral or illegal activity

There's always a but. Be aware of the downsides of VPNs, too.

"VPNs are not a panacea"—VPNs protect you against and provide certain things. They protect you against eavesdropping or snooping on your connection under most circumstances. They allow you to circumvent geographical restrictions under most circumstances. And that is all. They don't magically make it okay to do anything illegal, and they don't magically make you immune from a dedicated threat, like if you've pissed off a motivated white supremacist hacker or something.

More mundanely—and more worryingly—VPNs put you in a position of having to totally trust the VPN provider to do what they say. Yeah, it might sound cool to sign up for a cheap VPN provider based in Croatia that says they don't keep any logs of your activity, but what guarantee do you have that that Croatian company won't immediately acquiesce to a request by the Croatian government or law enforcement to hand over your information and identify you? I mean, sure, their privacy policy may say they won't…but that's just words. What proof do you have? Absolutely none.

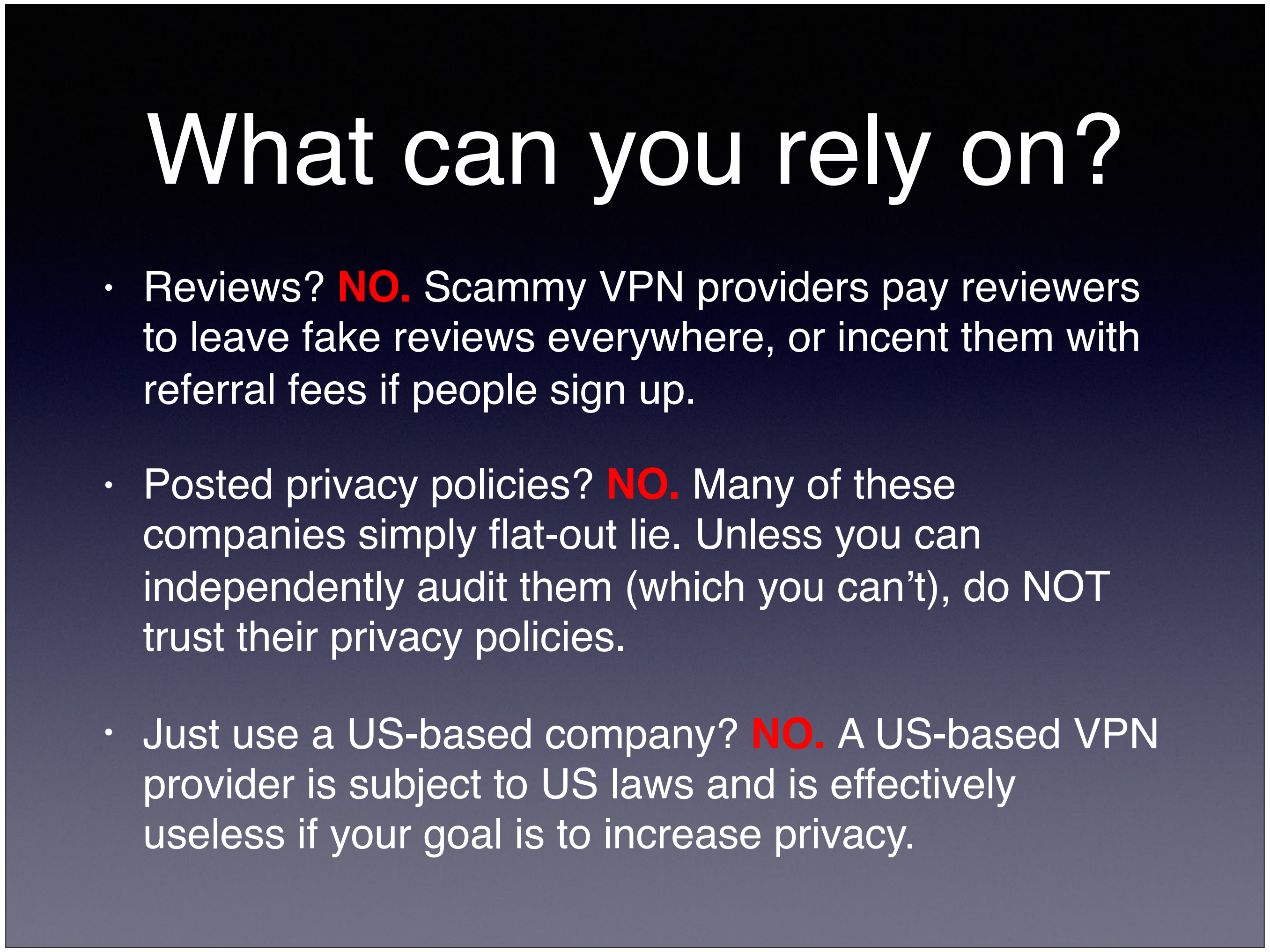
The fact is that picking a VPN provider that won't screw you over is hard.



Gotchas

- VPNs spiked in general popularity after this year's senate repeal of a lot of important Internet privacy rules that were set to take effect
- In response, VPN scams exploded and scammy VPNs that steal your private data—or worse—are common
- Signing up with a scammy VPN is far worse than using no VPN at all

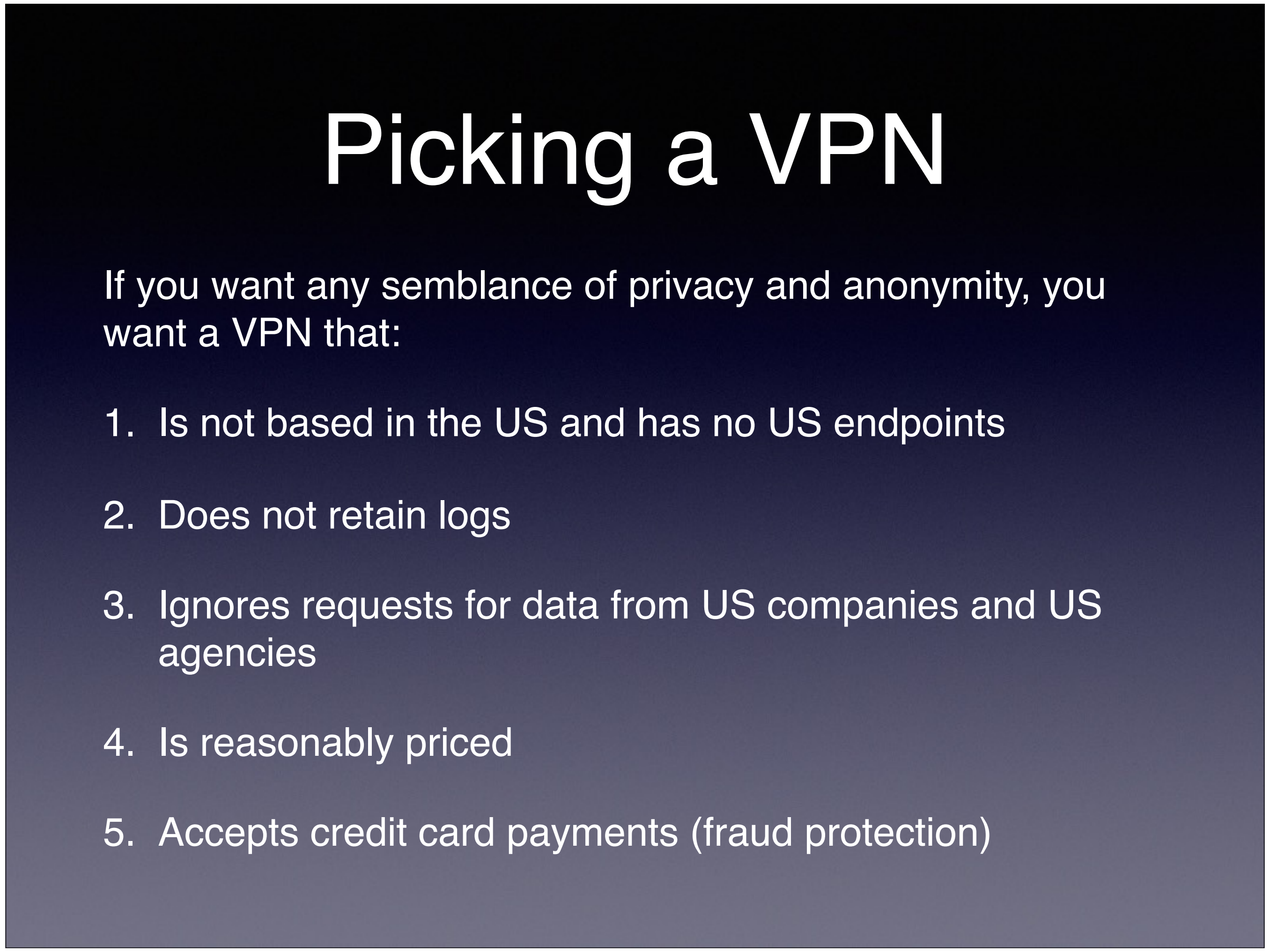
You hear a lot more about VPNs today because of the increased privacy threat, and shady companies take advantage of the popularity of the "i have to have a VPN!" craze. there are scams everywhere, and signing up with a scammy VPN provider—which might do anything, from sell your private data to purposefully alerting law enforcement that you're trying to hide something, even if your intent is simply privacy—is worse than not having a VPN at all.



What can you rely on?

- Reviews? **NO.** Scammy VPN providers pay reviewers to leave fake reviews everywhere, or incent them with referral fees if people sign up.
- Posted privacy policies? **NO.** Many of these companies simply flat-out lie. Unless you can independently audit them (which you can't), do NOT trust their privacy policies.
- Just use a US-based company? **NO.** A US-based VPN provider is subject to US laws and is effectively useless if your goal is to increase privacy.

How can you pick a VPN provider? It's hard. You can't rely on a lot of normal indicators because they've been subverted.



Picking a VPN

If you want any semblance of privacy and anonymity, you want a VPN that:

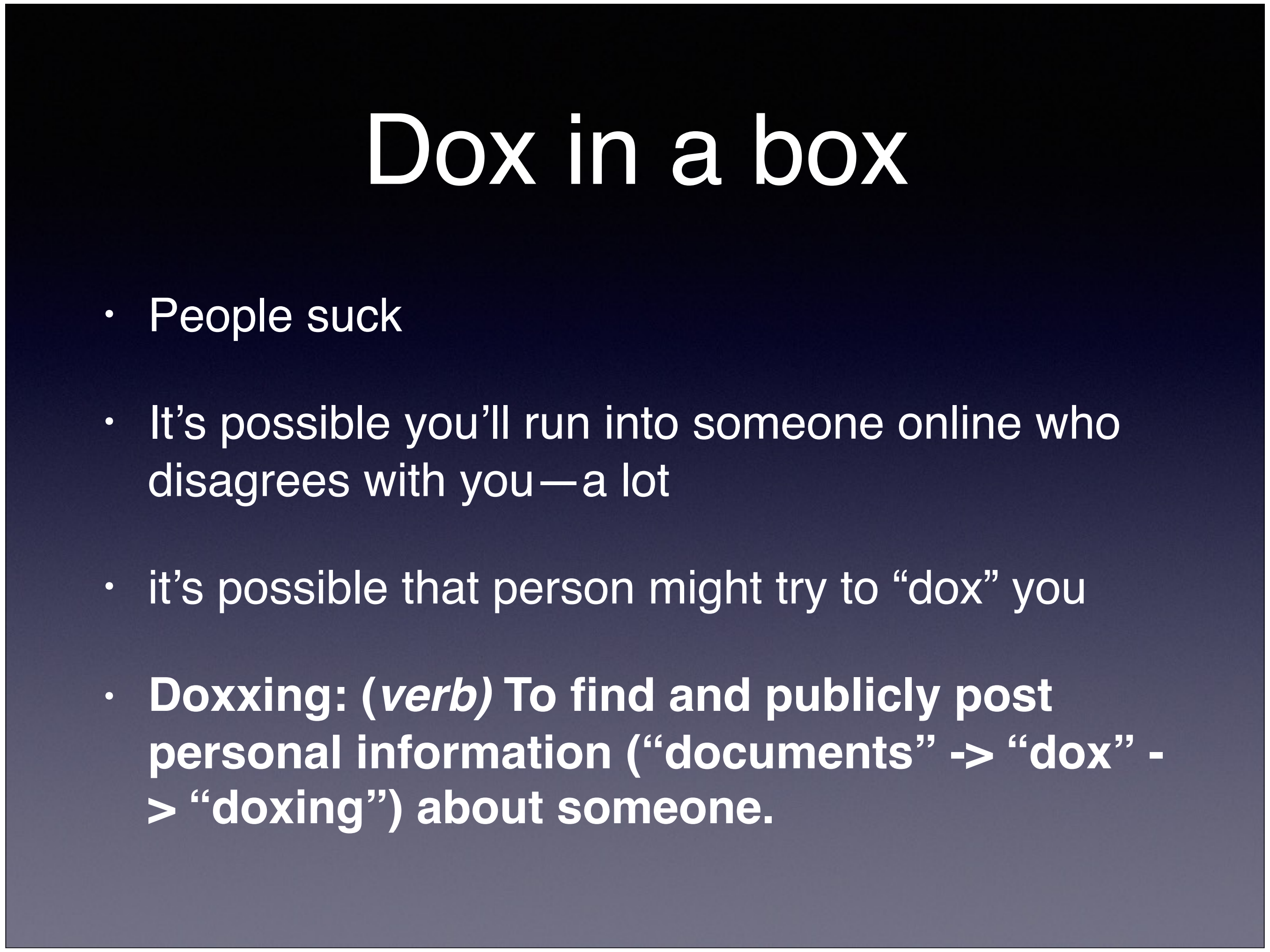
1. Is not based in the US and has no US endpoints
2. Does not retain logs
3. Ignores requests for data from US companies and US agencies
4. Is reasonably priced
5. Accepts credit card payments (fraud protection)

Your best bet, annoyingly enough, is anecdotal based on what security researchers (not me, actual researchers) recommend. I have some recommendations if you guys want after the talk.

Now, the last point goes against a lot of conventional wisdom online that says you should only pay for your privacy-enhancing VPN with bitcoin or some other pseudo-anonymous method to keep your identity hidden even from the VPN provider. that's valid logic, and if you feel like your personal threat landscape is complex enough, maybe that's a viable strategy for you, but for most folks you do eventually have to balance convenience and reality with the desire for security—recognizing, again, that if you're the target of a state level actor you're basically screwed and none of this will help you.

FYI, personally, I have used and had success with:
https://www.mullvad.net/

Or, for a little easier setup with their own app:
https://www.ivpn.net/

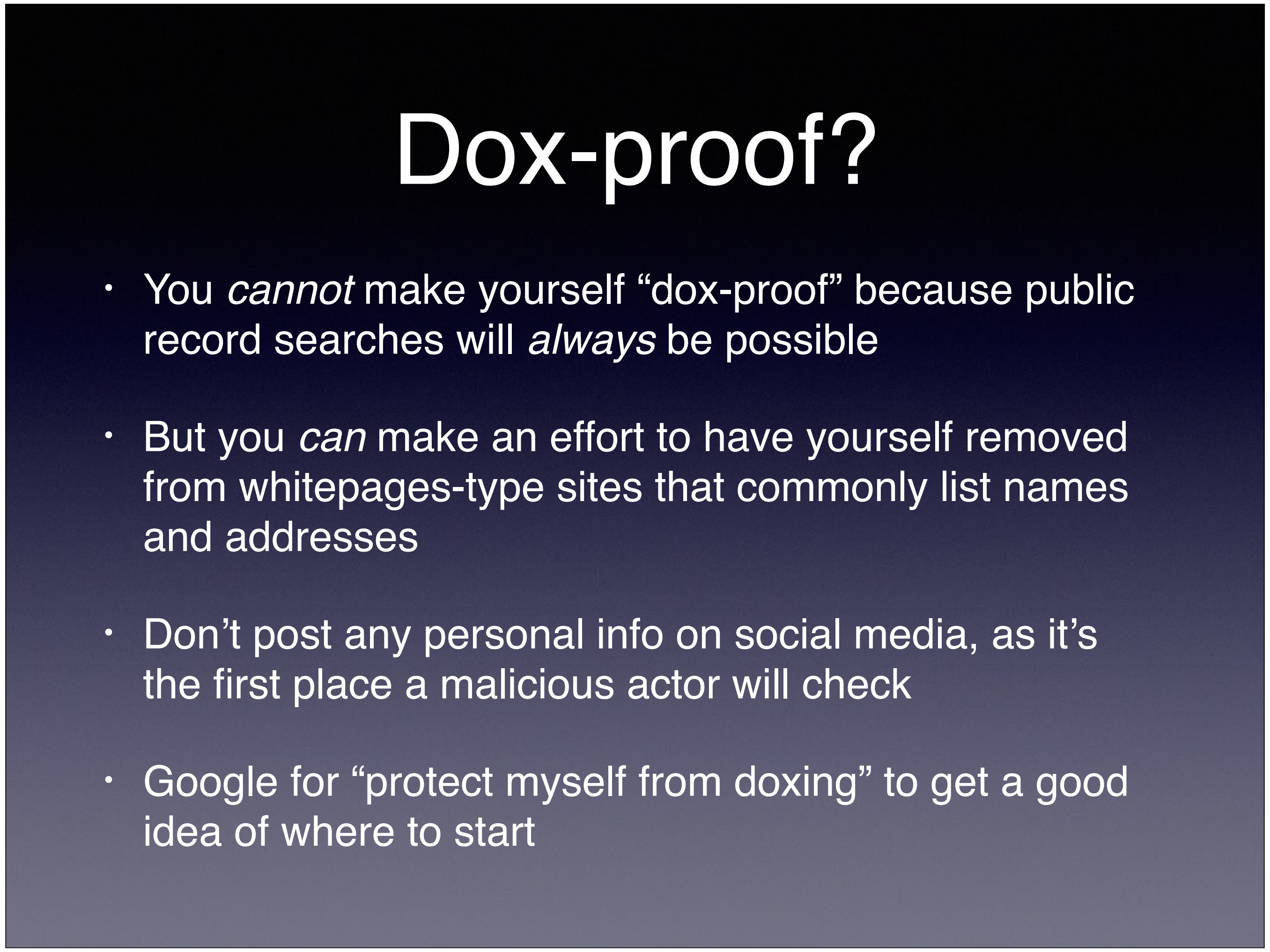


Dox in a box

- People suck
- It’s possible you’ll run into someone online who disagrees with you—a lot
- it’s possible that person might try to “dox” you
- **Doxxing: (*verb)* To find and publicly post personal information (“documents” -> “dox” -> “doxing”) about someone.**

The internet being what it is, it’s possible that you’ll encounter at some point online someone with whom you disagree and with whom maybe you get into an argument. Maybe it’s a bitter argument. And maybe you demonstrate awesome rhetorical abilities and totally crush that person’s argument. And maybe…they don’t like having their arguments deconstructed. Maybe they want to get back at you. Maybe they dig up your address and pictures of your kids or grandkids and post those with a note saying “I’m coming for you.”

While I haven’t yet had the personal pleasure of being doxxed, as a journalist I’ve had it happen to many of my coworkers. and it’s not fun—we wrote up a big piece on a group of far-right extremist crazies last year, and the crazies responded by digging up the author’s home address and sending him thousands of copies of the qur’an, hundreds of pizzas, obscene photographs, pictures of guns and knives, and even explicit and threatening notes describing the harm they were going to do to the guy and his family. Now, unless you run around pissing off neo-nazis you probably won’t have THAT happen to you, but pissing someone off online and having them respond by trying to dig up your personal info is a relatively common thing.



Dox-proof?

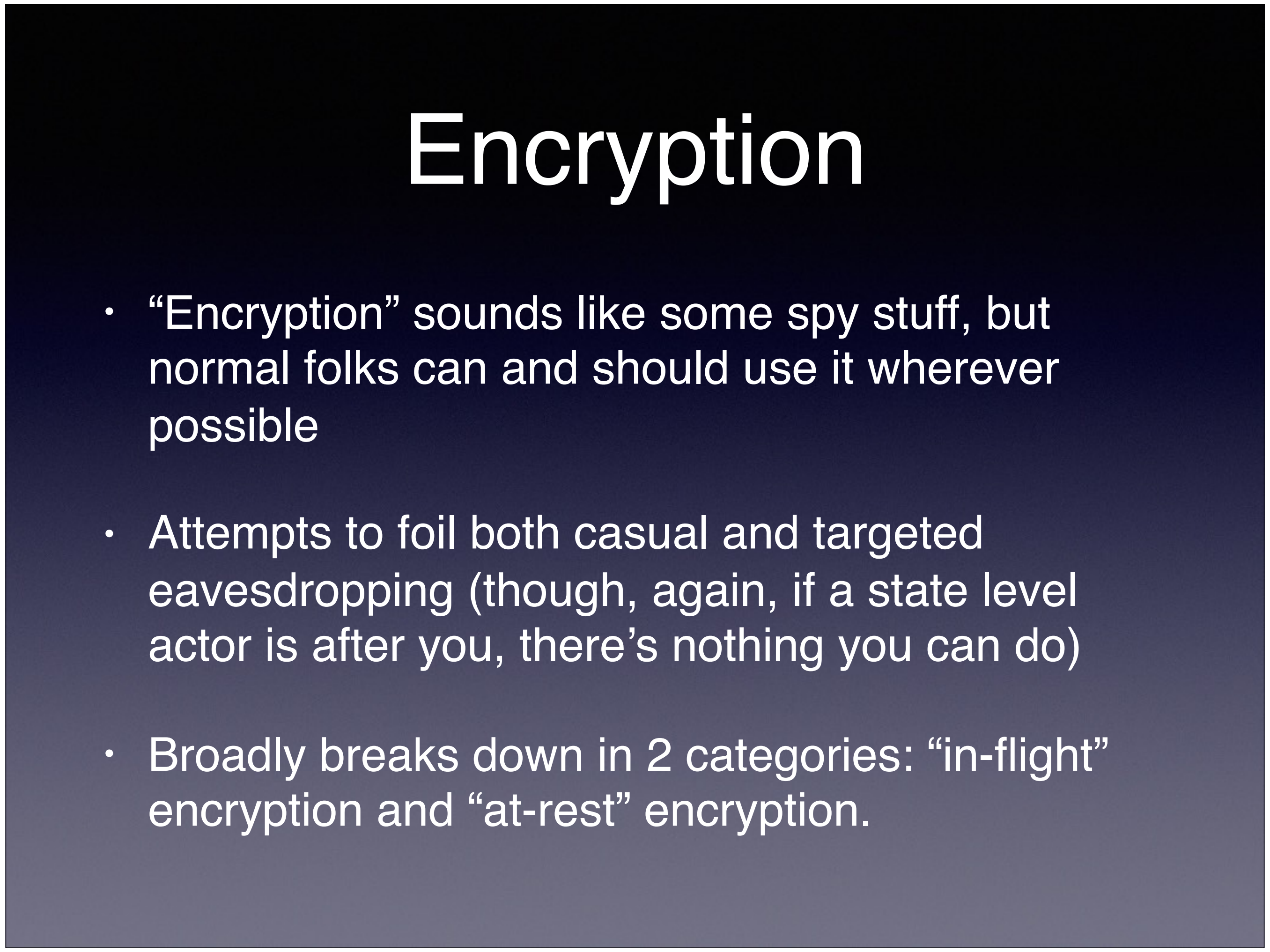
- You *cannot* make yourself “dox-proof” because public record searches will *always* be possible
- But you *can* make an effort to have yourself removed from whitepages-type sites that commonly list names and addresses
- Don’t post any personal info on social media, as it’s the first place a malicious actor will check
- Google for “protect myself from doxing” to get a good idea of where to start

As in all things, the best medicine is preventative—don’t get into arguments online with people likely to post your info—but you can also help yourself a bit by not having any personally identifiable information—like a picture of your house with an address visible, for example—available on facebook or linkedin or whatever. seriously, social media is an absolute goldmine for anyone looking to attack you.

You can also start aggressively removing your personal information from public sites like spokeo, pipl, peoplesmart, and the rest of the hundreds of sites that aggregate personal info. And do the same thing for your spouse and kids and anyone else who lives in your home—doesn’t do you any good to remove all of your info, only to have an attacker just look up your spouse and use their info instead. There’s a long list of sites to request removal from—Google can get you started, and it’s a constant process.

If there’s a practical takeaway from this section, it’s that information about you is out there and easy to find. if you really piss someone off, they might go to the county with public records requests—though if you’re pissing people off enough that they’re willing to spend money to get back at you, you might want to reevaluate your regular communications style.

Removing personal information:
http://www.crashoverridenetwork.com/preventingdoxing.html



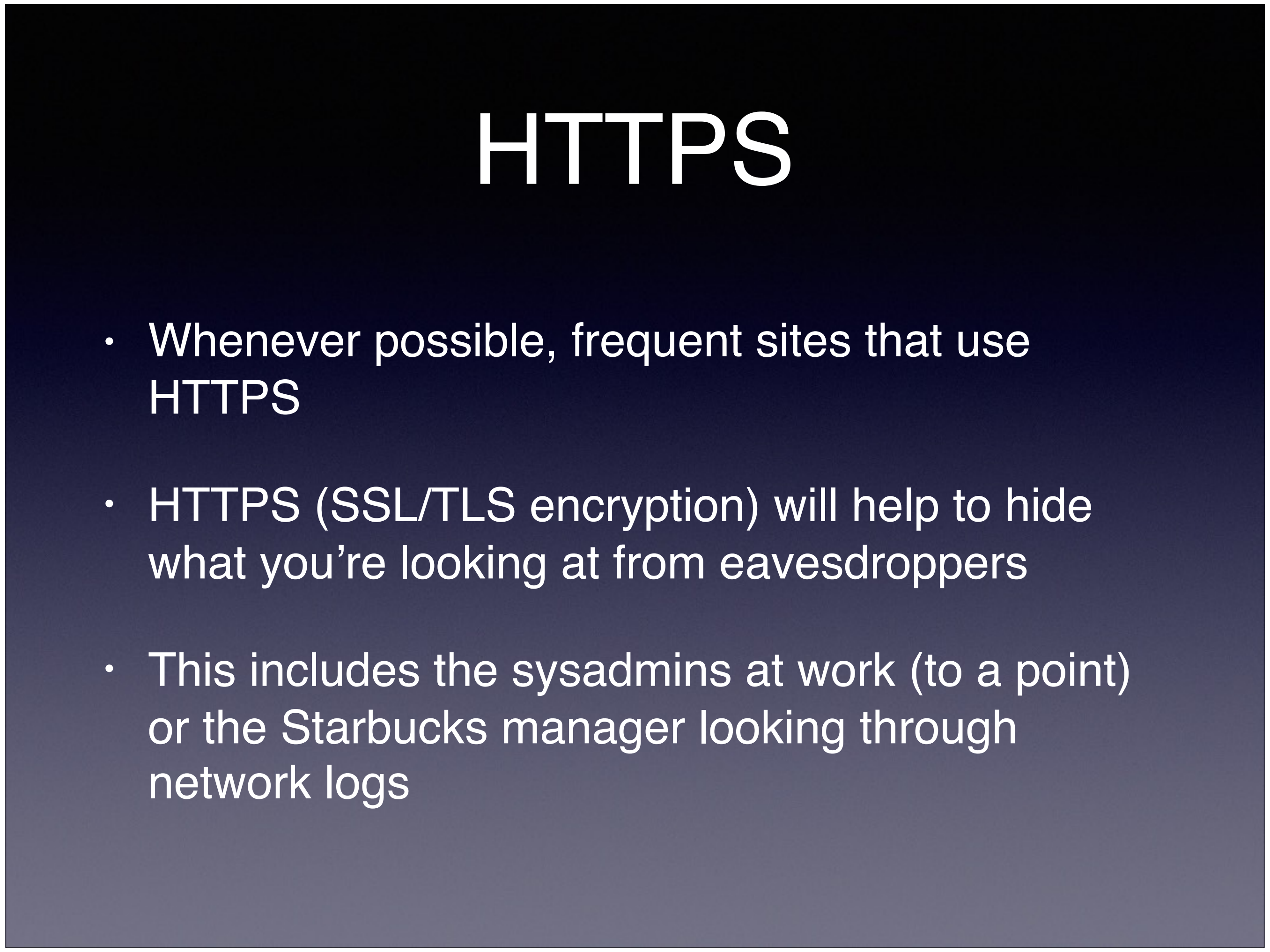
Encryption

- “Encryption” sounds like some spy stuff, but normal folks can and should use it wherever possible
- Attempts to foil both casual and targeted eavesdropping (though, again, if a state level actor is after you, there’s nothing you can do)
- Broadly breaks down in 2 categories: “in-flight” encryption and “at-rest” encryption.

Encryption! “Encryption” sounds like spy stuff, right? like you’re going to encrypt the documents and put them on the self-destructing USB stick and leave it in the dead drop under the oak tree. But encryption is useful and valuable to regular folks and has a place in anybody’s toolkit.

“At rest” encryption:
Encrypted file -> Unencryted transit -> Encrypted file

“In flight” encryption:
Plaintext file -> Encrypted transit -> Plaintext file



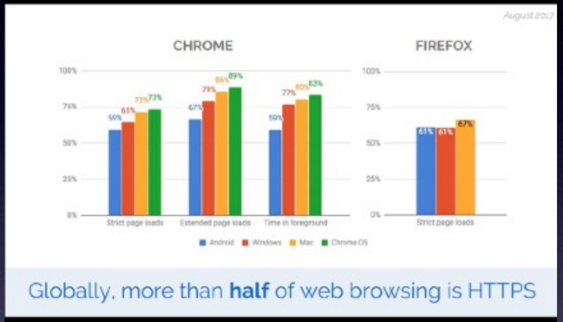
HTTPS

- Whenever possible, frequent sites that use HTTPS
- HTTPS (SSL/TLS encryption) will help to hide what you’re looking at from eavesdroppers
- This includes the sysadmins at work (to a point) or the Starbucks manager looking through network logs

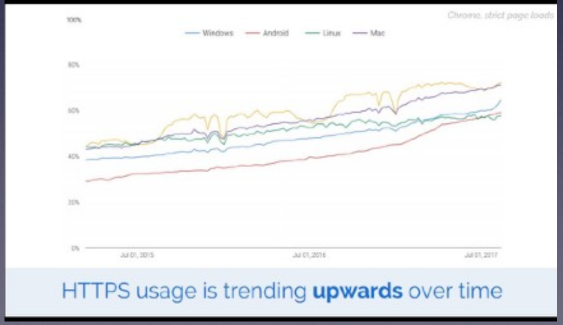
I bring up encryption as a way of leading into HTTPS—browsing sites that offer SSL/TLS encryption. In general, you want to make sure that you’re browsing mainly to sites that offer HTTPS, because it’s the easiest and also one of the most effective ways to ensure that what you’re reading and looking at online isn’t being monitored (though nothing is fool proof against attackers).

HTTPS on the rise

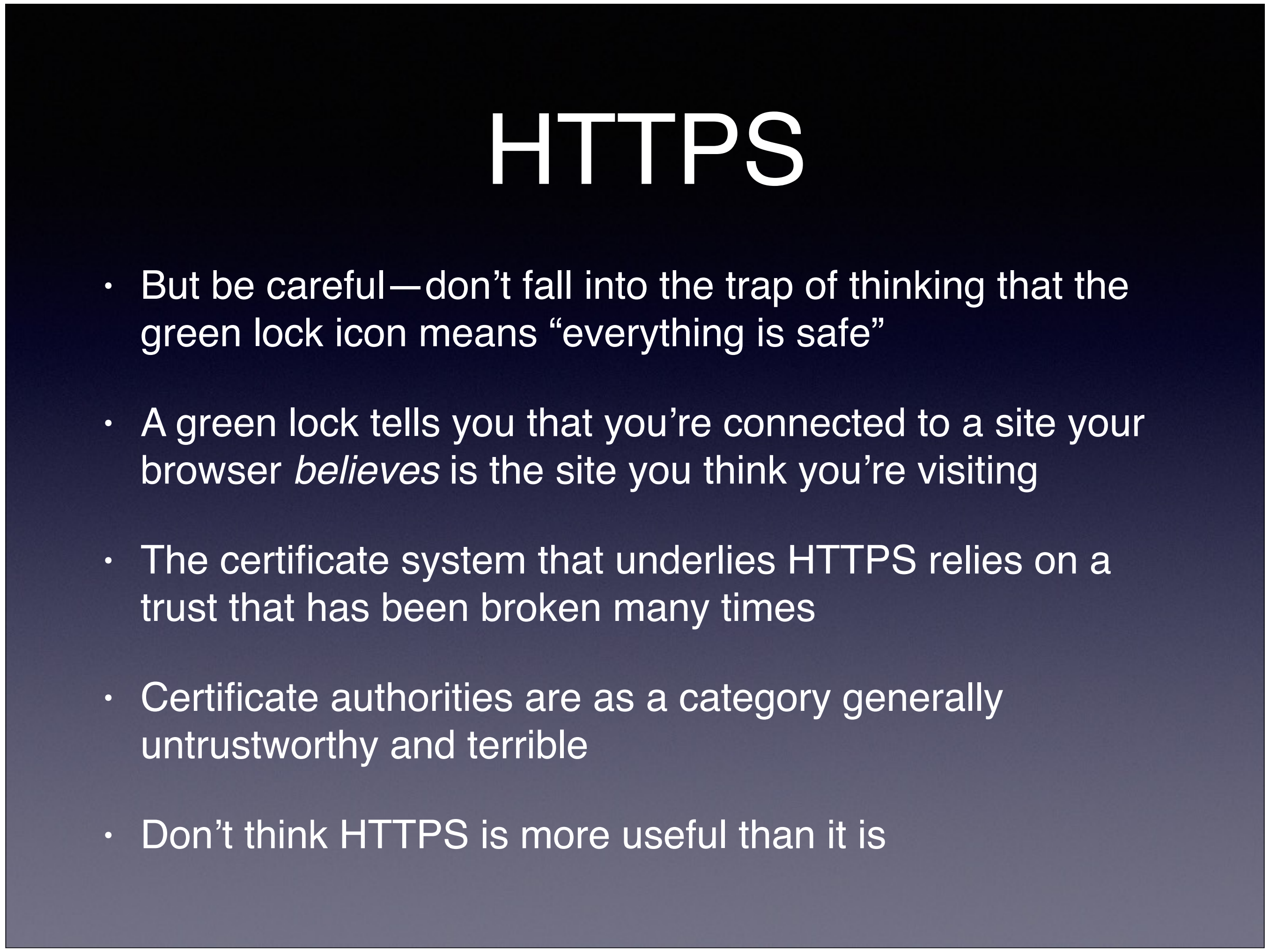
- HTTPS usage by popular web sites is steadily trending upward and this is a good thing
- Makes the web more proof against casual eavesdropping attempts
- “Encrypted by default” is a very pro-privacy stance to take



Globally, more than **half** of web browsing is HTTPS



HTTPS usage is trending **upwards** over time



HTTPS

- But be careful—don’t fall into the trap of thinking that the green lock icon means “everything is safe”
- A green lock tells you that you’re connected to a site your browser *believes* is the site you think you’re visiting
- The certificate system that underlies HTTPS relies on a trust that has been broken many times
- Certificate authorities are as a category generally untrustworthy and terrible
- Don’t think HTTPS is more useful than it is

HTTPS is good for telling you that the connection between you and a remote computer is encrypted and reasonably secure from eavesdropping. HTTPS is *terrible* at telling you that you’re actually connected to the remote site you think you’re connected to. Remember that when it comes to encryption between two parties, the encryption part is only half of the equation—encryption also needs a way of validating both parties’ identities and assuring you that you’re actually talking to the party you THINK you’re talking to, and not, say, a group of hackers that have falsely created an HTTPS certificate and are spoofing that party’s identity.

HTTPS provides for identity validation through the Certificate Authority system. These are organizations—mostly private companies, but some government entities too—that are empowered to issue the cryptographic certificates used by browsers and web servers to negotiate HTTPS connections. Ostensibly the CAs vouch for the identities of all parties by performing some kind of identity validation when they issue certificates; the flip side of this is that because of that position of trust, your browser trusts essentially everything a CA does. When a CA is compromised externally—or, as is more common, when bad actors inside of a CA are bribed or compromised—CAs can issue valid, trusted certificates that can be used by criminals or fraudsters. This has happened more times than I have fingers and toes, folks—the entire root CA system that underpins all of the encrypted sites on the web and represents literally trillions of dollars of commerce across the world…is basically a broken wreck.

Not much that can be done about it, and the reason we keep using it is that rebuilding an airplane in flight is really hard. But just be aware that while that green lock icon is desirable, it doesn’t mean you’re “safe.”

Bonus: Personal crypto

Easy

Whole disk encryption (BitLocker on Windows, FileVault on MacOS)

Harder

File encryption (TrueCrypt, others)

Messaging/voice call encryption (WhatsApp, Signal)

Annoyingly difficult or inconvenient as hell

Email encryption (PGP, GPG, S/MIME, others)

Whole disk encryption

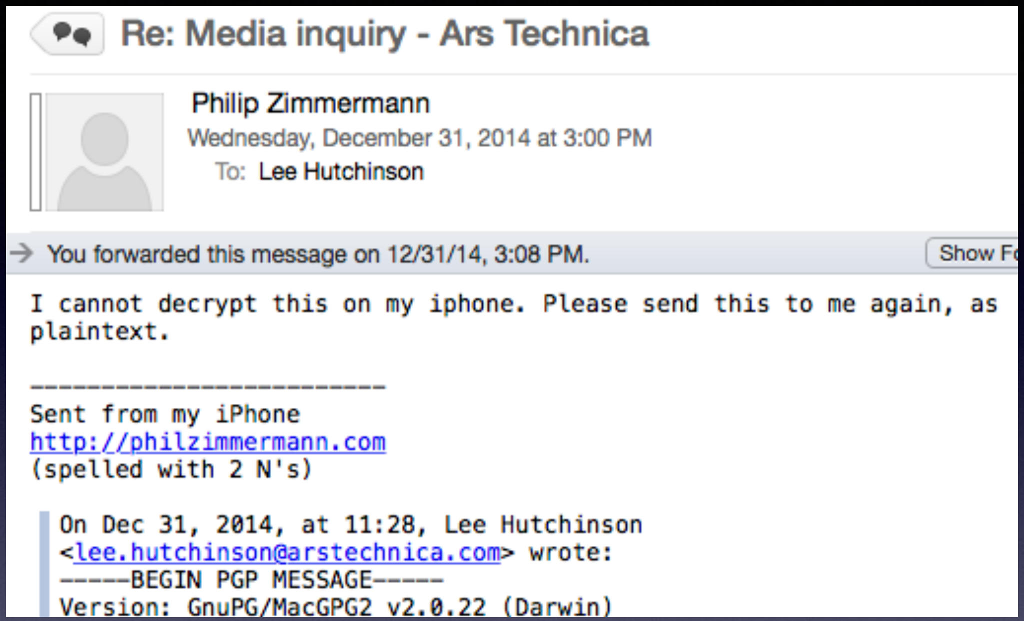
- If you have it, *use it!*
- Set it and forget it
- Primarily protects against theft and other physical threats:
  - Leave your laptop on the plane? Safe.
  - Someone steals your desktop? Safe.
- Will *not* help you against eavesdropping or keep you safe from online attacks, though

Encrypt files

- A little more complicated
- Can encrypt files or folders with a password, can be emailed/copied/transferred and decrypted by recipient on another computer
- But ask: do you really need to do this?

Good old PGP/GPG

- Encrypted email is old technology
- Works well, but high barrier to entry
- PGP = Original proprietary version, currently sold by Symantec
- GPG = Version that normal people use (but still interchangeably called “pgp” because it’s more confusing that way—based on OpenPGP)
- NOT a single-click encrypt/decrypt process
- Requires working knowledge of non-beginner cryptographic processes (maintaining pub/priv keys, performing out of band verification, key signing)



Re: Media inquiry - Ars Technica

Philip Zimmermann
Wednesday, December 31, 2014 at 3:00 PM
To: Lee Hutchinson

You forwarded this message on 12/31/14, 3:08 PM.

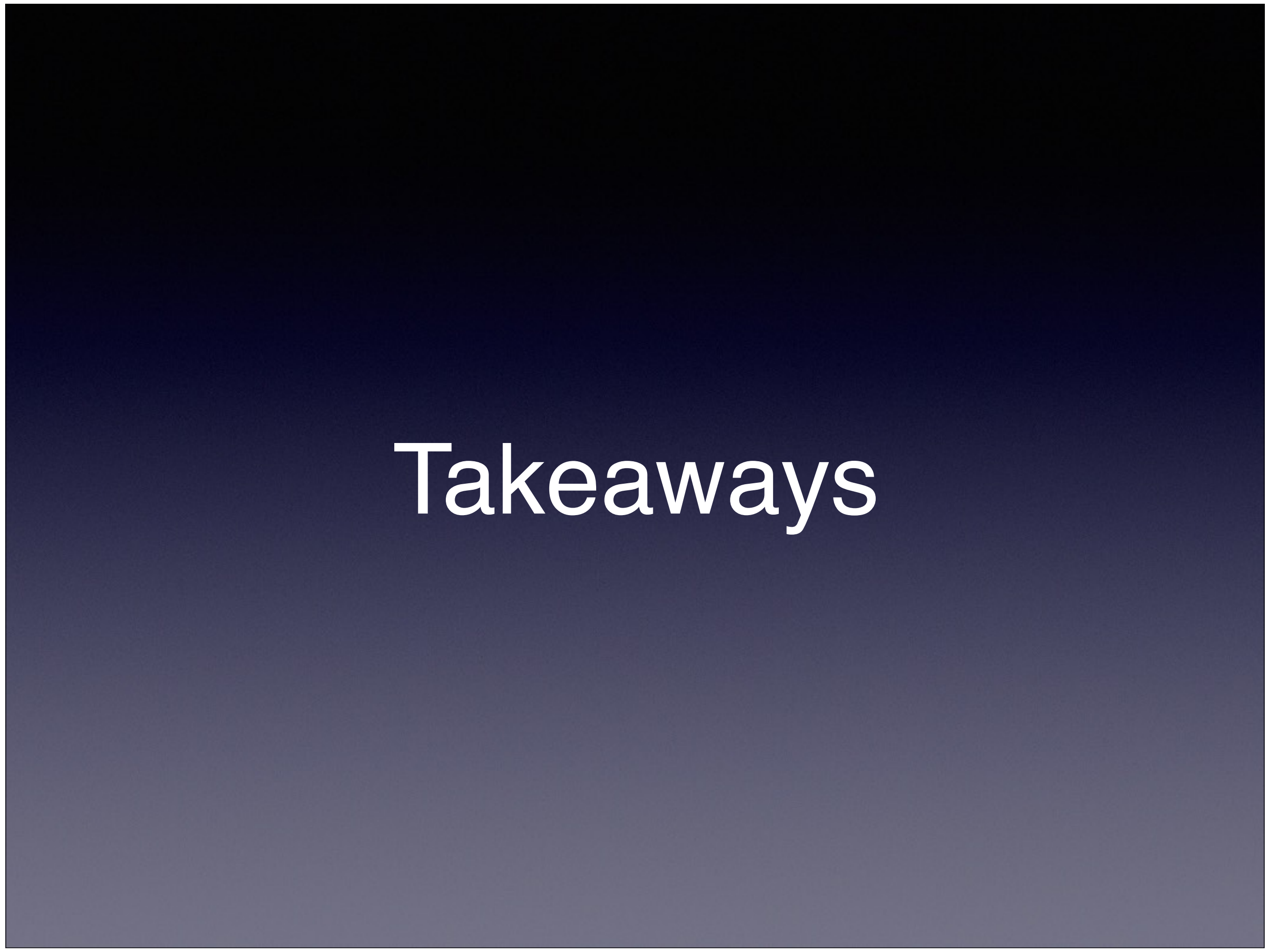
```
I cannot decrypt this on my iphone. Please send this to me again, as
plaintext.

-------------------------
Sent from my iPhone
http://philzimmermann.com
(spelled with 2 N's)

  On Dec 31, 2014, at 11:28, Lee Hutchinson
  <lee.hutchinson@arstechnica.com> wrote:
  -----BEGIN PGP MESSAGE-----
  Version: GnuPG/MacGPG2 v2.0.22 (Darwin)
```

How hard is it?

(Phil Zimmermann is a the creator of PGP and a world-renowned expert in cryptography and cryptographic applications)

Other methods

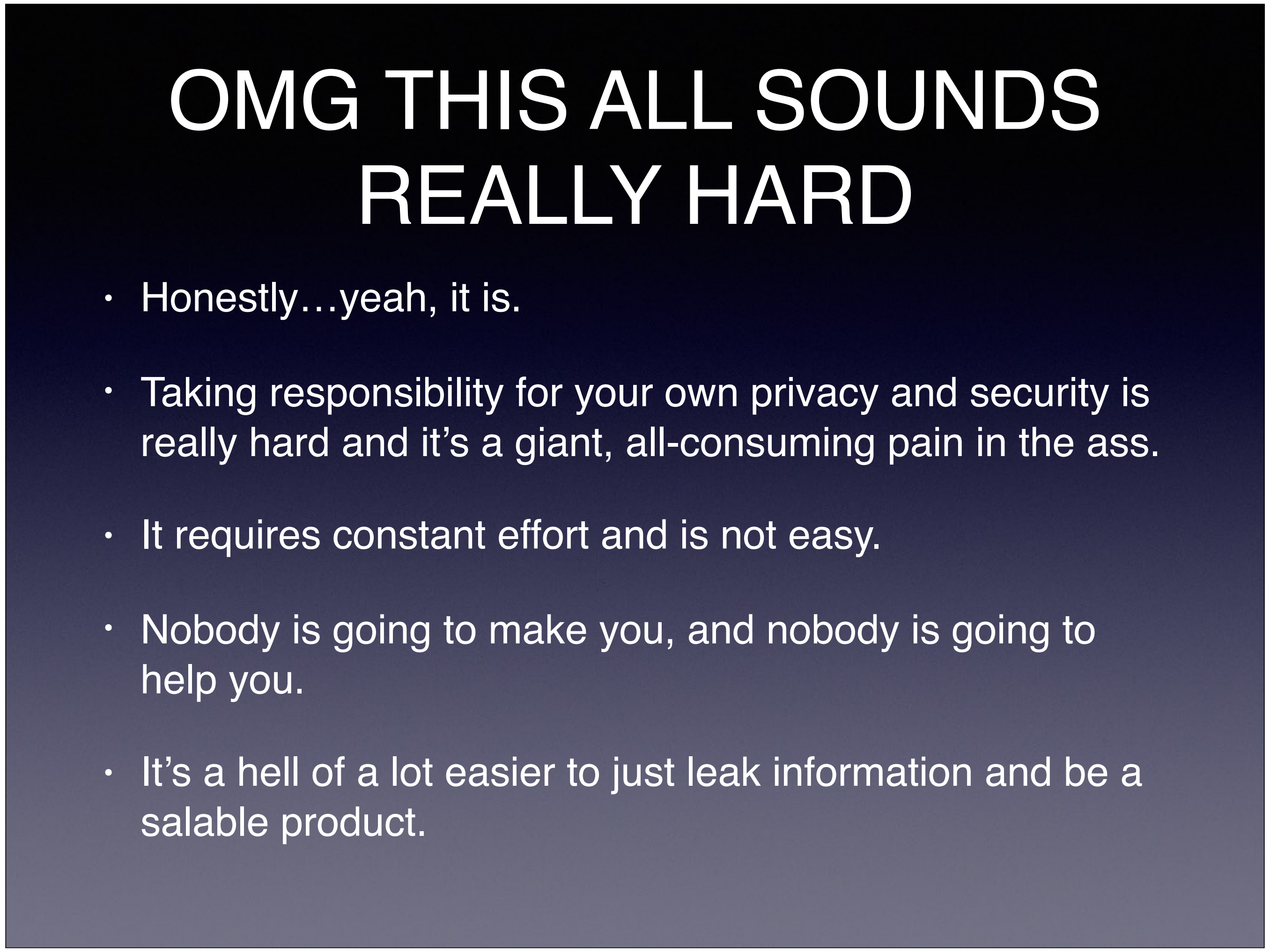
- S/MIME is easier for businesses because you can set it up with Active Directory, but still very challenging for normal people & has many of PGP’s usability issues
- Bitmessage and other peer-to-peer applications are easier but not in wide use
- Ask yourself: should I be using email for this?



Takeaways

We made it!

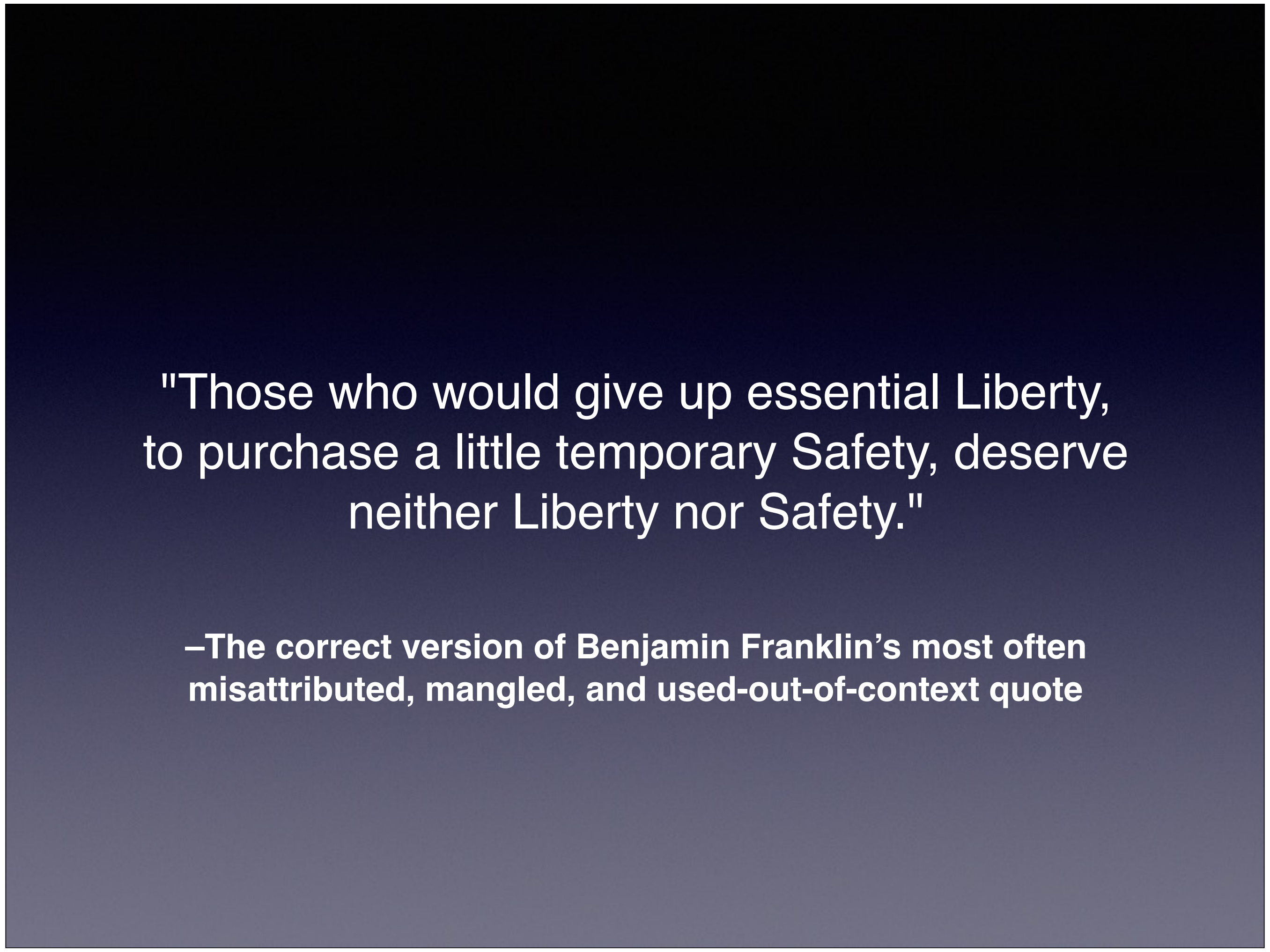
Okay, let’s wrap this real quick with some takeaways.



OMG THIS ALL SOUNDS REALLY HARD

- Honestly…yeah, it is.
- Taking responsibility for your own privacy and security is really hard and it’s a giant, all-consuming pain in the ass.
- It requires constant effort and is not easy.
- Nobody is going to make you, and nobody is going to help you.
- It’s a hell of a lot easier to just leak information and be a salable product.

Some of this stuff I’ve gone over isn’t terribly hard, but a lot of it is difficult, time consuming, and annoying. You’ve got to decide for yourself what you will and won’t do. Your own feelings about the acceptability of government surveillance (and government in general) will inform your choices, as will your feelings about being reduced to an ad-consuming blob that can be mined for personal data, which is how the majority of online companies see you. Certainly nobody is going praise you for withdrawing from social media and going on the offense to advocate for your own privacy—a lot of people will see it as being antisocial, or worse, “making a fuss”—like you should somehow be obligated by your own sense of politeness to happily let Amazon or Google or Facebook treat you like a commoditized data point, plaster ads over every surface of your life, and sell your personal information to any company that wants to buy it.



"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

–The correct version of Benjamin Franklin's most often misattributed, mangled, and used-out-of-context quote

This is the last slide - show of hands one last time for everyone who had a sinking suspicion I was going to wind up quoting Franklin at one point or another here!

OK, yeah, I'm perpetuating the problem and using this quote out of context, since Franklin originally said it as part of a dispute in Pennsylvania about taxation and defense spending. And as smart as Franklin was, it's pretty clear that he couldn't have envisioned specifically the future in which we live, where everybody effectively carries the collected knowledge of all humankind around in their pockets—or the essentially effortless surveillance state that is the modern world, vacuuming up actions in public and private and incorporating them into databases both public and private. But there's a broadly applicable kernel of truth here, and that kernel is that liberty is more desirable than commoditization—that giving up control over your privacy in return for being able to effortlessly tag friends on facebook or automatically re-order toilet paper on Amazon isn't just a horrifyingly bad trade, but that it's a fundamentally un-*American* trade.

In closing: you wouldn't walk around with your social security number and credit card tattooed on your forehead in real life. Don't do it online, either.

http://www.npr.org/2015/03/02/390245038/ben-franklins-famous-liberty-safety-quote-lost-its-context-in-21st-century