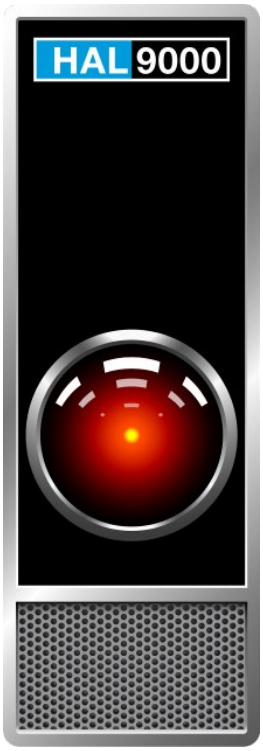
DIGITAL LITERACY
COMPUTER CLASSES

IS PRIVACY POSSIBLE?

DECEMBER 13, 2019

I AM COMPLETELY OPERATIONAL AND ALL MY CIRCUITS ARE FUNCTIONING PERFECTLY



Stop. Dave.

In the Bad Old Days, advertisers would have to *guess* what products and services you might be interested in and governments wanting to surveil your communications would have to dispatch agents to physically tap your phone lines and steam open your mail.

But wait – there's a better way! Nowadays, our communications zip across the Internet, bouncing between servers like electronic ping-pong balls, and our shopping is done not while pushing a cart around a big box, but while we're sprawled on our beds staring slack-jawed into our phones tapping and swiping away. To identify, profile, and micro-target you, no one need lift a physical finger. You allow corporations to record every website you visit and product you purchase, track your physical location at all times on a scale of meters, and listen to your every word through phones and tablets and smart speakers, ostensibly waiting like attentive butlers to do your bidding only when asked. You even have mysterious, hackable corporate cameras observing your every movement and activity as you stumble around your house – and *you purposely installed them!*

If you *like* this situation, congratulations. Carry on. If you don't, I can't help you disappear. But I can offer a few concrete steps toward ameliorating the worst of this current mishegas. Read on ...

ALL WE ARE IS ~~DUST IN THE WIND~~ DATA POINTS IN THE CLOUD

What's all this nonsense about privacy, you say. I browse the internet on my own laptop in my own bedroom, and no one is looking through the window or anything. The internet doesn't know who I am. It's just pages and sites and stuff. Anyway, nobody wants to invade my privacy. I'm not some spy!

Au contraire, my credulous friend. Your desultory wading through the digital tall grass leaves behind innumerable pieces of evidence dutifully vacuumed up and aggregated by hardworking algorithms to build a highly specific – to the point of creepiness – profiles of you. How do they do so?

INTERNET ACTIVITY

Don't trust him; he's a junkie!

Your browser: be it on a computer or magic rectangle, your window to the web is actually two-way glass. When you visit a website, almost without exception that website will politely request to place a **cookie** in your device's local storage. No, I'm afraid this is not a delicious snickerdoodle or elegant tuile; this is a bit of information that burrows into your device and waits. Waits to be activated, like the Manchurian Candidate. That makes it sound nefarious, but a cookie isn't necessarily so: don't you like not having to log into a site you just logged into two minutes ago but you closed the browser tab? Thank a cookie. How some sites, even if you don't create an account and log in, remember certain preferences you set? All thanks to the humble cookie. What else can a cookie do?

RUTHLESSLY PILFER YOUR PRIVACY, that's what. You frequently visit websites whose code includes visitors and parasites from third parties – for example, those fun little buttons that let you "like" random things on Facebook or Tweet them or Insta them or whatever. Those elements, when first loaded, place a cookie. The next time you encounter one, it politely inquires whether you're storing a cookie for the relevant service. If so, they've got you! The owning megacorp now gets a report that you visited this site at this time on this device, etc., etc.

"Ah, but it's to no avail," you say smugly, swirling your snifter of port. "I don't even *have* a Facebook account."

Oh yes you do. A *ghost* account. An account you didn't set up, and it's not for use on the service. Facebook made it to build their advertising profile of you. And you just added to it.

YOUR VOICE

We all love those smart speakers, don't we? Alexa, turn on some Wu-Tang Clan. Hey Siri, what's this embarrassing blemish on my keister? Hey Google, give me directions to the house of my co-worker I'm having an affair with. What could go wrong?

As designed, these speakers keep an ear open but only activate when you trigger them with their wake-up phrases. Designs don't always work. From a privacy standpoint, the thing to note here is that some percentage of the recordings, legitimate and erroneous, are farmed out to human contractors to listen to and check for accuracy. To improve the algorithm. All glory to the algorithm!

YOUR FACE

Oh yeah? *Your* face, pal! Do you have one of those trendy new Rings or Nests or other corporate surveillance cameras in your house? I'm sure that's a great idea. And you have read the news stories about hackers berating children with racial slurs through those speakers? And you have read about Amazon's Neighbors program, giving a) police easy access to surveillance footage and granular detail about Ring owners and b) the neighborhood a chance to express their worst selves by making sure gossip flies fast and furious when suspicious people are about? You know, suspicious people … *the ones who aren't white?*

Facial recognition looms on the horizon. Although it's still not quite ready for mass surveillance, your constant contributions to the data cloud is helping tone the algorithms. China is doing very great work in this field, and it's making destroying the culture and lives of the Uighurs much easier.

THE VERY GENES IN YOUR NUCLEI

Won't it be interesting to see if you're related to Rasputin? Or if perhaps you *do* have a claim to all that Nigerian prince money you keep hearing about? Several companies are leveraging the power of genetic analysis to give you interesting information of highly varying accuracy about your ancestry. Many of these companies also simply hand this stuff over in bulk to any law enforcement interested in combing through it (or perhaps anyone else, for that matter). But they caught the Golden State Killer that way, right? Isn't it worth it?

Ask the aforementioned Uighurs, herded into concentration camps and downtrodden by an oppressive, dystopian Chinese government *really leading the way* on abuse of technologies like genetic testing.

WHAT DO I DO ABOUT IT?

BECOME A POWER BROWSER

On a computer, your browser may already be starting to fight the good fight. Newer versions of **Firefox** and **Safari** are building out their capabilities to identify and block third-party cookies and even attempt to thwart browser fingerprinters (using every scrap of

information a site can glean from what your browser tells it about itself to try and zero in on you). Google's **Chrome** is meandering haltingly toward stronger protections too, except of course for encouraging you to sign in to it and hand everything you do wholesale over to Google. **Brave**, a new-ish browser headed by an original Firefox architect, blocks ads and trackers from the get-go. It has a scheme you can opt into that serves you more anonymized ads and pays you to look at them in trendy imaginary cryptocurrency funny-money. But you don't *have* to do that part. I don't!

There are **extensions** available too: **Privacy Essentials**, by the non-tracking search company DuckDuckGo, and **Privacy Badger**, by the Electronic Frontier Foundation, are set-and-forget guardians that will intercept and block (or discard) those nasty little cookies. Privacy Essentials also includes as much information as is known about a site's privacy practices in easy-to-understand language. Both extensions, thankfully, do meaningful work without needing a lot of care and feeding and maintenance.

Have a mobile device? Brave makes a mobile browser, as does DuckDuckGo. Extensions don't work with mobile devices, so just switch to a new browser.

If you're really concerned about privacy, you could use a browser that works through the Tor network – a distributed set of nodes that allows you to reroute your every internet request through encrypted tunnels to emerge somewhere else in the world and also find hidden resources within the Tor network – yes, often crime stuff, but there are *some* legitimate purposes … Downside? Be prepared to be treated rudely by many websites suspicious of Tor traffic. You'll be doing a *lot* of CAPTCHAs.

WEST COAST BEST COAST

There's a new law in town – technically, in the State of California as of January 1, 2020. The **California Consumer Privacy Act** will give you the opportunity to find out what data companies hold on you and the power to make them delete it, and opt out of its sale. We shall see what happens with the rubber hits the digital road, but it's encouraging if you're concerned with privacy.

BUT YOU DON'T HAVE TO TAKE MY WORD FOR IT

Doo doot doot! Let's give you some digestible resources to continue your studies, shall we? This isn't exhaustive by any means; simply some *entrepots* to your own investimigashuns.

Recode, recently folded into Vox Media, has launched an initiative called **Open Sourced**, including rundowns on the issues at stake. I think it's worth keeping an eye on. "Old Media" outlets like the Washington Post and New York Times also cover these areas, of course, and have broken several important stories lately. Check Wired too; this stuff is in their wheelhouse as well.

This all is a balancing act; find where you're comfortable. And look out behind you! ;)