The topics we’ve covered in this class so far have painted a pretty dark picture of our right to privacy, and I think it would be difficult to come away from that without feeling at least a little bit concerned about what the consequences will look like. But I think the national conversation on the topic of privacy will ultimately land on the redefining of what privacy means in the digital age.

I say that because what I’ve learned in class so far absolutely caused me to want to minimize my digital footprint, and while I think the real only partial solution is to just ditch technology and I mean all technology, it’s not practical without sacrificing a lot in terms of access and experience. So, while I’ve begun to tighten down on privacy options on my devices, it’s an admittedly slow process, one that’s perpetually being negated by further participation in online and connected activities. I think the understanding of just how futile it really is to eliminate your online footprint, and the true effort involved to even come close (developing new skill sets, learning about how programs and networks and even how the hardware functions at a really deep level), acts to deflate any sense of motivation to prioritize going through over 2 decades of an online footprint to achieve some semblance of privacy. But I have set the privacy settings on new devices and installations more strictly and will continue to do so moving forward. I’m also planning on going through the articles from this week’s readying again and implementing a lot of those changes.

However, the next question is a bit more difficult to answer. While researching last week’s topic, I ran across the concept of Data Capitalism, and there are some good arguments for data collection from that perspective. If data is functionally the new oil, and our American way of life was built on oil through the global dominance of the petro-dollar since the mid-20th century, wouldn’t it be reasonable to assume then that moving forward, to maintain global economic dominance would mean having control of the data more than others, including hostile nations? In any reasonable outlook of the near- to mid-future, there will only be unstoppable growth in surveillance technology, methodology, and scope.

So in knowing that, I think the question is not how much information is safe or appropriate, but rather how much is absolutely necessary. To know what is necessary, necessarily forces someone to consider more deeply what kind of life they both want to have and are willing to sacrifice to have. How much are they willing to be excluded from society, how many of society’s benefits are they willing to go without? I think just the bar for entry at this point in participation is having a digital presence that can be reached by a protocol that is ubiquitous so not one would be unable to contact you, so an e-mail. For most people, that’s going to be through Google’s Gmail. Sure, other services exist, and I can see Outlook/Microsoft and Apple being in the same category, but generally one of these is the bare minimum, with all security and privacy setting set to their most strict levels. Then to be able to function at all online, you’d need a way to spend money online, which again there are alternatives, but most people are going to have a bank account and a few credit cards. So maybe that’s equally as important as an email. From that point, it really comes down to services that facilitate or improve an area of your life which you’re not willing to sacrifice. Those services will also need that information. These three things will get a person by through most situations. I just think it should be severely limited after that point, only to necessities. I would add things like VPNs to that list.

I think I answered the 3rd question above with answer #2, heh, but to expand, the real answer to actions I could take gets really complicated. To be able to hide yourself properly, you really need to understand the innerworkings of cellular and data networks, mobile operating systems, computer code, white-hat hacking, and a whole lot more. There’s a very complex set of interwoven skills and knowledge someone would have to acquire. But at a base level, it’s fairly easy, though tedious, to implement protections is frequently used services’ user settings, like two factor authentication, utilize things like ad-blockers and VPNs, and focus on adjusting usage habits. Limit who can see posts, only engage with services that will be frequently used, frequently check on privacy monitoring like viewing active devices on an account, turning off location tracking and contact sharing, and other general privacy and security settings.

However, all these things should be done with the understanding that you’re only putting a slight restriction of the \*flowrate\* of your data through government and corporate hands. In today’s world, without a major reorganization of how we live in modernity, or just living in a cave, there’s not really anything we can do to completely anonymize and protect ourselves from data collection and mass surveillance.

Sources:

* These 11 Facebook Privacy Teaks Put You Back in Control – Fast Company (<https://www.fastcompany.com/90368822/these-11-facebook-privacy-tweaks-put-you-back-in-control>)
* What Does Google Know About Me – Gabriel Weinberg (<https://www.quora.com/What-does-Google-know-about-me/answer/Gabriel-Weinberg>)
* How the NSA Betrayed the World’s Trust – Mikko Hypponen (<https://www.ted.com/talks/mikko_hypponen_how_the_nsa_betrayed_the_world_s_trust_time_to_act/transcript>)