HERE IS WHAT YOU MUST KNOW ABOUT HOW YOUR ELECTRONICS ARE ABUSING YOU!

If you're traveling this weekend, nestled in front of the fire, or just trying to offset the effect of sugar-coated holiday specials, we've got a reading list for you. These picks were recommended by team members at Purism and reflect our dedication to digital privacy, security, and freedom. With daily headlines about Big Tech scandals like Facebook's clandestine data-sharing, there's no better time to read up on these topics.

The choices below are listed in no particular order and, wherever possible, we link to author websites and privacy-respecting sources.

Reading about surveillance capitalism may not warm your heart, but it could put a fire in your belly and encourage you to #DemandFreedom in 2019.

The End of Trust **– McSweeney's Issue 54 (Nov. 2018)**

Compiled by the team at the Electronic Frontier Foundation (EFF) for McSweeney's, this collection features writing by luminaries like Cory Doctorow, Gabriella Coleman, Edward Snowden, Bruce Schneier, and many more. Among the gems within is a conversation between artist Trevor Paglen and journalist Julia Angwin, with Paglen having this to say about the intersection of freedom and privacy:

“I think I had the sense of growing up within structures that didn’t work for me and feeling like there was a deep injustice around that. Feeling like the world was set up to move you down certain paths and to enforce certain behaviors and norms [didn’t] work for me, and realizing that the value of this word formerly known as privacy*, otherwise known as* liberty*, plays not only at the scale of the individual, but also as a kind of public resource that allows for the possibility of, on one hand, experimentation, but then, on the other hand, things like civil liberties and self-representation.”*

Click Here to Kill Everybody: Security and Survival in a Hyper-connected World **– Bruce Schneier, W. W. Norton & Company (Sep. 2018)**

Schneier’s latest book is a sobering account of the pitfalls of modern technology. It covers a lot of ground, such as the huge gap between security and implementation in Internet-of-Things devices. The author has a gift for raising questions that cause the reader to rethink the underlying technology behind seemingly-simple tech, like network-connected baby monitors:

“They’re surveillance devices by design, and can pick up a lot more than a baby’s cries. Of course, I had a lot of security questions. How is the audio and video transmission secured? What’s the encryption algorithm? How are encryption keys generated, and who has copies of them? If data is stored on the cloud, how long is it stored and how is it secured? How does the smartphone app, if the monitor uses one, authenticate to the cloud server?”

American Spies: Modern Surveillance, Why You Should Care, and What to Do About It **– Jennifer Stisa Granick, Cambridge University Press (Jan. 2017)**

Granick gives the reader a real sense of just how big, and just how pervasive, U.S. intelligence programs really are. The author

doesn't stop with government programs, however, and calls out Big Tech for its major role in population surveillance:

"Spying is thriving not only because of technology, but also because of modern business models. Much of the modern privacy problem is the result of people giving up their data – knowingly or otherwise – to obtain cool new products and services."

Nothing to Hide: The False Tradeoff between Privacy and Security **– Daniel J. Solove, Yale University Press (Jan. 2013)**

This is a now-classic rumination on the deeply important role of privacy in autonomy and freedom. It quickly demolishes the "nothing to hide argument", a constant refrain in today's privacy debates, and continues to shed light on social and legal dimensions of surveillance. Here, Solove highlights contradictory perceptions of audio and video snooping:

"The electronic-surveillance statutes strongly protect against the government's eavesdropping on your conversations but don't protect against the government's watching you. This distinction doesn't make a lot of sense. Video surveillance involves similar threats to privacy as audio surveillance. As one court noted: 'Television surveillance is identical in its indiscriminate character to wiretapping and bugging. It is even more invasive of privacy… but it is not more indiscriminate: the microphone is as 'dumb' as the television camera; both devices pick up anything within their electronic reach, however irrelevant to the investigation.'"

Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance **– Julia Angwin, Times Books (Feb. 2014)**

Angwin is no stranger to the many facets of surveillance capitalism, and this book is just as prescient now as it was five

years ago. In that time, the author's concerns have been validated, with the pace of Big Tech's blunders only escalating. Angwin keeps the human element in constant view, giving vital context to headlines about privacy and data catastrophes:

"Skeptics say: 'What's wrong with all of our data being collected by unseen watchers? Who is being harmed?' Admittedly, it can be difficult to demonstrate personal harm from a data breach. If Sharon or Bilal is denied a job or insurance, they may never know which piece of data caused the denial. People placed on the no-fly list are never informed about the data that contributed to the decision. But, on a larger scale, the answer is simple: troves of personal data can and will be abused."

Free Software, Free Society, 3rd Edition **– Richard M. Stallman, Free Software Foundation (Oct. 2015)**

Stallman's status as an icon in the Free/Libre world is often the focus of press. Bootstrapping GNU and the Free Software movement was no small feat, but there is too little focus on Stallman's writing. The author's philosophy is grounded in practical concerns and explained with a clear and mindful tone that few writers possess. This most recent edition of Stallman's collected essays describes just how important liberty is in the contemporary digital context:

"If 'cloud computing' has a meaning, it is not a way of doing computing, but rather a way of thinking about computing: a devil-may-care approach which says, 'Don't ask questions. Don't worry about who controls your computing or who holds your data. Don't check for a hook hidden inside our service before you swallow it. Trust companies without hesitation.' In other words, 'Be a sucker.'"

Defending Politically Vulnerable Organizations Online **– Sean Brooks, Center for Long-Term Cybersecurity (July 2018)**

In this report from the Center for Long-Term Cybersecurity (CLTC), Brooks provides a broad overview of the cybersecurity landscape. This is a great introduction for industry professionals and consumers alike, though it focuses on civil organizations that are often targeted for political reasons. The report's citations are a valuable resource in their own right, providing context as well as technological solutions. The author is quick to point out lackluster investment in cybersecurity in both the public and private spheres, describing the vicious cycle this creates:

"The broad asymmetry between attackers and defenders online is unsurprising; politically vulnerable organizations lack resources and are therefore particularly under-protected. This problem is not unique to politically vulnerable organizations. Many public and private organizations have underinvested in cybersecurity and have become soft targets for criminals and other bad actors. Online attackers have continued to develop their offensive capabilities, exacerbating the mismatch."

Bad Blood: Secrets and Lies in a Silicon Valley Startup **– John Carreyrou, Penguin Random House (May 2018)**

This story of the rise and fall of biotech startup Theranos is a page-turner, described here with all the detail of investigative journalism. Carreyrou's most interesting passages are those where the author describes the culture of Silicon Valley, where fraudulent CEO Elizabeth Holmes was desperately trying to fill the mold of her Big Tech heroes:

“For a young entrepreneur building a business in the heart of Silicon Valley, it was hard to escape the shadow of Steve Jobs. By 2007, Apple’s founder had cemented his legend in the technology world and in American society at large… to anyone who spent time with Elizabeth, it was clear that she worshipped Jobs and Apple.”

The Doomsday Machine: Confessions of a Nuclear War Planner **– Daniel Ellsberg, Bloomsbury USA (Dec. 2017)**

Decades after the legendary whistleblower disclosed the Pentagon Papers to the American public, Ellsberg’s warnings will still ring alarm bells and shock the reader. Through first-hand accounts, the author chronicles the nuclear program of the 1960’s and the dangers of the present day, describing the contrasting roles of secrecy and transparency, as well as their relationship to trust:

“Like discussion of covert operations and assassination plots, nuclear war plans and threats are taboo for public discussion by the small minority of officials and consultants who know anything about them. In addition to their own sense of identity as trustworthy keepers of these most-sensitive secrets, there is a strong careerist aspect to their silence.”

The Participatory Condition in the Digital Age **– Electronic Mediations Book 51 (Nov. 2016)**

This collection of articles spans the gamut from street protests to online “hacktivism” to Free and Open-Source collaboration. The editors expertly summarize the transdisciplinary tone of the volume in an introductions that’s worth contemplating in its own right. Among other issues, Gabriella Coleman describes Kate Crawford’s work on the power and scale of spying:

“Ubiquitous surveillance facilitated by [information and communications technology or ICTs] – what Crawford designates as ‘algorithmic listening’ – and the gathering of personal data currently operated by web-based corporations (commercial surveillance) and governments (the NSA program, for example) are not simply matters of privacy but also of scale and lack of accountability.”

Privacy and Big Data: The Players, Regulators, and Stakeholders **– Terence Craig & Mary Ludloff, O’Reilly Media (Sep. 2011)**

Published at a time when “Big Data” was more of a buzzword than a factor of everyday life, this book is a quick and easy introduction to the perils of the data economy. The lessons would seem dated if they weren’t still applicable, and there’s perhaps nothing more prescient than the fact that data can not only be sold by Big Tech to business partners, it can be given away:

“While the IP stakeholders have been busy redefining “privacy” for their own ends, Google, Yahoo, Facebook, and others have been equally busy making billions of dollars collecting your data and using it for targeted advertising. Of course, any company or organization that collects data can offer it for sale or free.”

Habeas Data: Privacy vs. the Rise of Surveillance Tech **– Cyrus Farivar, Melville House (May 2018)**

Farivar exposes the role of common, household tech in the global surveillance apparatus, diving into the court cases and legal precedent that shapes the scope and limits of privacy and security. Above all, the author steeps his analysis in history, with quotes from legal heavyweights like Louis Brandeis, here discussing wiretaps in a famous dissenting opinion:

“‘The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping,’ Brandeis wrote. ‘Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurences of the home.'”