Where Privacy Ends, Technocracy Begins

Ever since Technocracy was first dreamed up in 1932, personal privacy has been under attack.

Why? Because original Technocrats saw Technocracy as a system of "Social Engineering" and that meant knowing everything knowable about all citizens across society. They wanted to know everything about your energy consumption, all of your purchases, all of your health details and all of travels. It was lucky for us that they only had pencils and paper to create their self-styled Utopia.

Not today, though. Advanced technology is ubiquitous, ever-present and rapidly developing into a panopticon of surveillance where the "system" knows more about you than you know about yourself. Literally.

The U.S. Constitution is supposed to protect us from these Technocrat pariahs. In particular, the Fourth Amendment states,

> *The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly*

> *describing the place to be searched, and the persons or things to be seized*.

Well, Technocrats hated the Constitution in 1932 and nothing has changed.

WiFi-enabled smart meters now collect and transmit your energy usage to the energy-masters on a minute-by-minute basis, and they can calculate exactly where and how you are consuming all of your energy. All of your social media data is routinely hoovered up by a long line of corporate marketers and various government agencies, including the NSA, CIA and DHS. Your cellphone tracks 100 percent of your meanderings around town.

Then, there is the new field of 'predictive policing' that is reminiscent of the 2002 Tom Cruise movie, Minority Report.

Zachary McCoy went out on a bike ride and happened to inadvertently pass by a house that had been burglarized. Then he got a letter from Google that his local police department had served a "geofence warrant" that demanded Google release the private date of anyone who happened to be near the crime scene at the time of the crime, and McCoy's name was on the list.

Google knows and collects such things, you must realize, because of its users' GPS, Bluetooth, WiFi, phone apps and cellular connections. Now McCoy is considered a prime suspect in a crime that he had no idea was ever committed in the first place. Who on earth ever allowed any court to issue a "geofence warrant" in the first place?

In Utah, state leaders recently had a lapse of sanity when they granted full access to a myriad of state data to a private company:

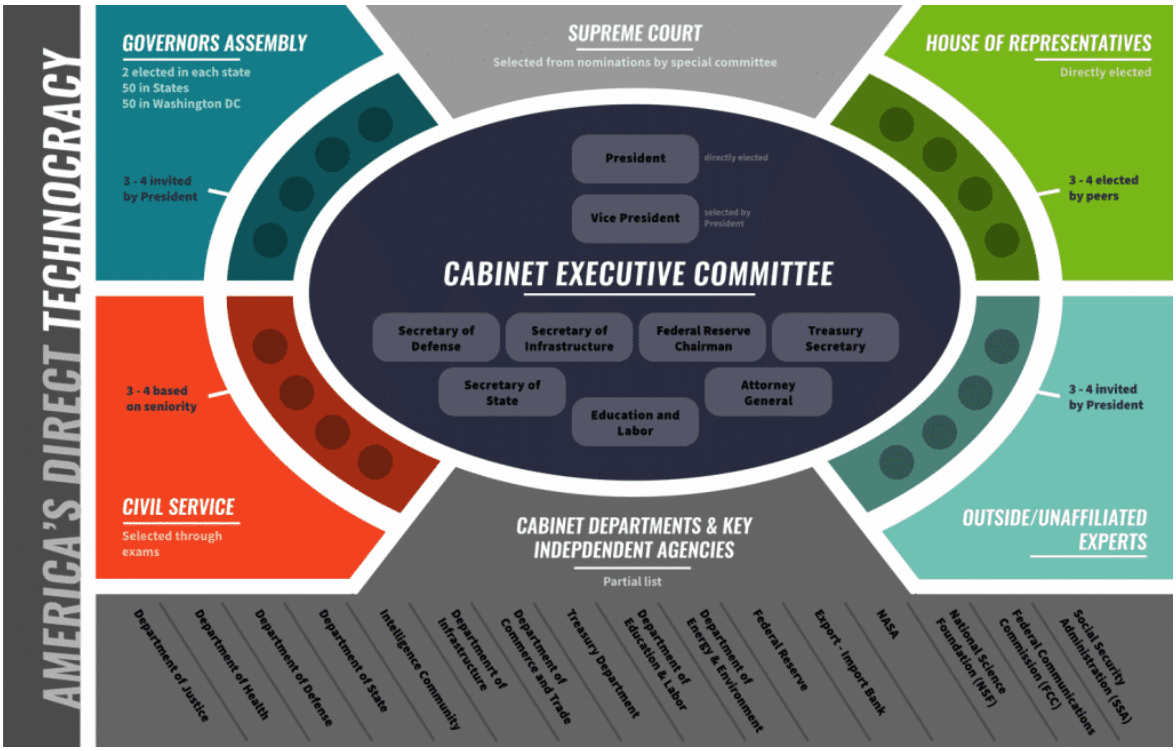
> *The state of Utah has given an artificial intelligence company real-time access to state traffic cameras, CCTV and "public safety" cameras, 911 emergency systems, location data for state-owned vehicles, and other sensitive data. The company, called Banjo, says that it's combining this data with information collected from social media, satellites, and other apps, and claims its algorithms "detect*

> *anomalies" in the real world. The lofty goal of Banjo's system is to alert law enforcement of crimes as they happen.*

Banjo calls this "Live Time Intelligence" and in the lofty and noble name of solving crimes as they happen, they will suck up every piece of data on everyone in the entire state! No problem though, because "It claims it does this while somehow stripping all personal data from the system, allowing it to help cops without putting anyone's privacy at risk."

"Somehow"? Um, since when is state data not completely tied to individual citizens? Well, "Duh!"

You can see where this is headed and it's nowhere that you want to go. To this writer's humble logic, citizens in every community in America should get out their torches and pitchforks and storm their city halls to put an end to this nonsense… while there is any time left to do so.



Parag Khanna Says Save America By Imposing Technocracy

Parag Khanna's book, Technocracy in America, would turn the nation upside down, but he misrepresents Technocracy as some kind of benevolent partnership between democracy and civil experts.
His argument is disarming and provocative, but wrong on all counts. He does not acknowledge that the U.S. Constitution is what made America great in the first place, so it is easy for him to say that replacing it with a pseudo-constitution would 'fix' our problems. TN Editor

If the American Century is the past, geopolitical analyst Parag Khanna studies the future. A "new global order has arrived," he declared in a hotly debated 2008 essay, "Waving Goodbye to Hegemony," marking the rise of Europe and China as new pillars of a multipolar world. The intervening years have largely proved him correct.

Khanna, of course, has a uniquely global perspective: born in India, raised in the United Arab Emirates, educated in New York and Washington. A policy-wonk wunderkind, he held jobs at the Council on Foreign Relations, World Economic Forum, and the Brookings Institution before publishing his first book at the age of 30. Critics bristled at his precociousness, but Khanna barreled on, picking up fellowships and consulting gigs, hosting an MTV show, and advising U.S. special forces in Iraq and Afghanistan.

The rise of Donald Trump has, in many ways, accelerated the trends Khanna identified earlier in his career—and made him even more skeptical of American governance. Now in his 40s and living in Singapore, the peripatetic think tanker hopped on the phone with *Fast Company* to talk politics, power, and how to save the presidency from the president.

Fast Company: Let's start by talking about what's broken in the

American political system. If there's one thing that both parties agree on, it's that Washington is too polarized, too partisan to function. What's your diagnosis?

Parag Khanna: There's a difference between politics and government. I'm not trying to be a hairsplitting academic, but I want it to be clear that these are not synonymous terms. So when we say things like, "What's broken in American government?" We turn right away to politics, as if fixing politics would fix government.

But that is a very, very critical point. One of the most important ways to diminish the corrosive impact of partisan politics and money in politics and so forth is to have a government that has its own independent characteristics and bureaucracy and institutions.

FC: You tackle some of these issues in your 2017 book, *Technocracy in America*, which offers some pretty radical solutions.

PK: Critics sometimes get confused by the term technocracy, which is in no way antithetical to democracy. On the contrary, I advocate radically more democracy. One obvious step is to lower the voting age, which is something that's being considered or initiated in countries like Switzerland and elsewhere. The most significant step would be mandatory voting, such as exists in Australia. Perhaps the only way to genuinely ensure the statistical legitimacy of an election is to have a high voter turnout. Some even propose that younger peoples' votes should count more than those of the elderly.

Then the question is, how do you faithfully translate the will of the people into actual policy, or at least into policy options?

So that is the kind of thing that can also be legislated and structured. If you look at California or Switzerland or New Zealand, there are essentially parliamentary committees to take various citizen initiatives and to consider the proposals in committees, to reconcile them and put them forward as potential legislation.

Compare that to the national American system, in which candidates run on a particular platform but then have to make lots of broad

compromises and wind up doing very little on any of the aspects of their agenda.

FC: And voters end up feeling exhausted or ignored.

PK: You need to have strong independent institutions that are able to pursue universal agreed-upon policies in a long term way that transcends particular election cycles. In the United States, there's this problem where we pass Obamacare and then we try to repeal Obamacare. Or with infrastructure, after the financial crisis, we agree that we're going to spend trillions on infrastructure, then we issue the infrastructure bonds—and bonds are meant to have a 30-year maturity—then we terminate those bonds within two years.

I mean, that's the kind of behavior you expect from Argentina, right? So once you decide that something is in the long-term national interest, the key is to invest authority in parastatal entities—bodies run independently of the government but reporting to it. Social Security and Fannie Mae, and the Consumer Financial Protection Bureau, are supposed to be run like this.

There's nothing radical or abnormal about creating a national infrastructure governance authority, for example, once you've decided you're going to spend trillions of dollars on roads and bridges. In fact, no citizen or bondholder in their right mind would ever invest on something that important if it were subject to day-to-day politics.

Think about Norway and it's oil fund: it's independently managed, but it has a supervisory board consisting of democratically elected lawmakers and the prime minister, and they're overseeing it and receiving reports annually. It's as democratic as it gets, but it's independently managed by experts.

FC: What you call technocracy, then, is more like government by civil servants.

PK: Technocracy is a term that originates in 19th century France, after the country was humiliated in the Franco-Prussian War in the 1870s. The Third Republic wanted to find a way to overcome their decadence. And

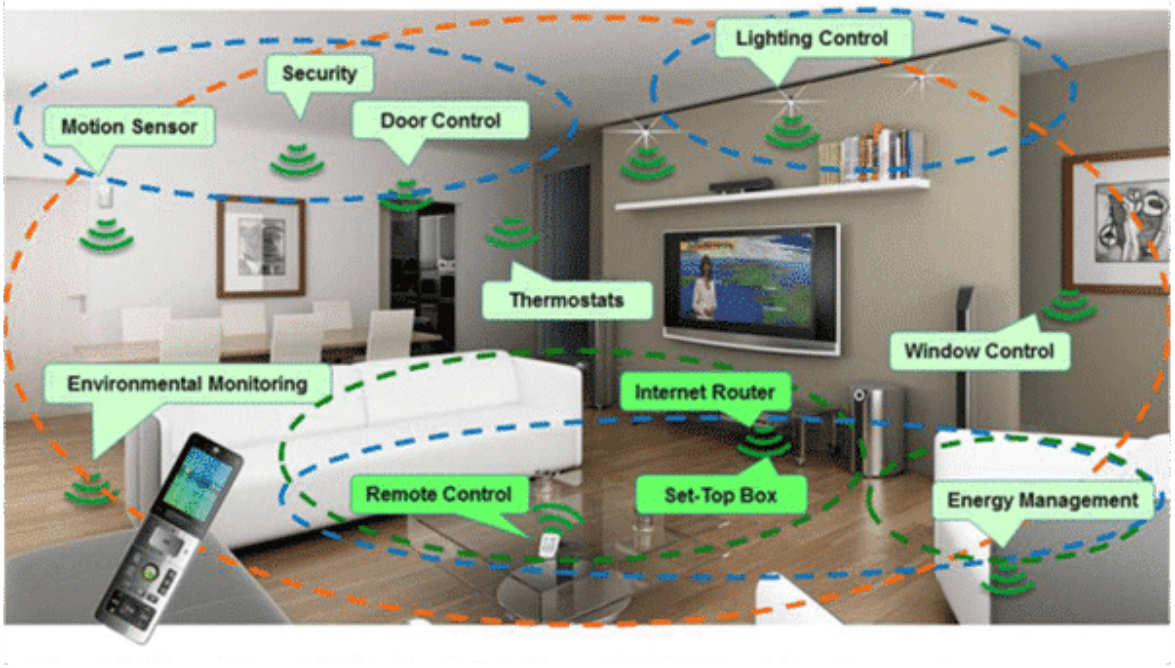
so they created the famous Grandes écoles academies that are meant to train government elites across a wide range of fields.

So the first thing around technocracy is that it is about public administration, a strong civil service—competent, meritocratic, independent management of the state. The second aspect is utilitarianism. In other words, the moral function of a technocratic regime is the welfare of the people. The greatest good for the greatest number. Otherwise, it becomes a system that's subject to elite capture. Finally, you need feedback loops between the civil service and the people.

The word technocracy fell into disrepute in the mid 20th century when it came to be associated with the Soviet Union and Communist China—apparatchiks and mandarins driving their economies into the ground. Then it got tied up with the idea of the "best of the brightest" dragging us through the Vietnam War.

But it was used very wrongly all along in the same way that today, if you were to confuse technocracy and authoritarianism, you'd pretty much be missing the point. Some of the most technocratic countries are Germany, Switzerland, Finland, New Zealand, and Canada.

Read full story here…



Protecting Your Digital Life In The Age Of IoT

Unless specifically demonstrated otherwise, you should assume that every electronic device in your home is capable of ratting on you in one form or another. Here are some steps that can protect you. TN Editor

The Internet of Things (IoT) device universe is expanding. This statement echoes for the fifth year in a row—only the numbers change as they grow bigger. Indeed, as the universe of IoT devices grows, so do the dangers they bring. With Gartner's predicted 20 billion IoT devices by 2020 and 25 billion by 2021 comes not only lack of certification for IoT security (ISO/IEC 27030 is still in draft version and there are no clear dates when it can be released) but also real dangers right now from interconnected, insecurely designed, and not properly updated and maintained IoT.

Such constant expansion clearly demonstrates the attitude of those who participate in the IoT market. New models are introduced with shiny new functionality, but secure design, and extensive quality assurance and testing remain low on the priority list.

17 entry points to a connected home

Each new component added to the network poses a new possible risk and widens the attack surface for each household. This attack area for households is already large. On average, there are 17 devices connected to the internet for a single household, including computers, phones, gaming consoles, smart TVs, watches, cameras, NAS devices, printers, and thermostats.

This means every household has 17 devices on average that are:

- Collecting your private data
- Sending your private data for further analysis to the cloud
- Serving as a possible entry point to the network
- Disrupting internet services by participating in DDoS (distributed denial of service) attacks

Our data shows that almost 43 percent of devices are using an operating system (OS) that is no longer supported. This does not mean immediate danger and exploitability because of differentiating OS lifecycles, but it does suggest a huge number of interconnected devices out there that are possibly no longer maintained by vendors, though they still exist in the local network as part of a device base. Even if we approximate that no more than a quarter of these devices are really vulnerable, that's an impressive 10 percent of the overall device universe left to be exploited, posing real danger.

The risks posed by rogue devices

The most dangerous scenarios point toward devices that are unsupported, discontinued, or no longer maintained. They might still be storing sensitive user data after they are left connected to the internet with their ports forwarded.

Remote access attempts executed by malicious outsiders or host discovery scanners and unauthorized attempts to access the open port make up more than 65 percent of overall suspicious and malicious activities registered daily. Based on CUJO AI data attempts to check open ports or scan for possible vulnerabilities, this kind of activity

happens at least 10 times a day per household. Apart from the direct danger to sensitive user data, no longer used and forgotten devices can serve as a trampoline or proxy inside the local network.

Other typical scenarios include leaving default credentials when connecting the device to the network. Given that IoT device configuration is often too complex or there's no way to change the default built-in credentials, this is usually left "for later" and never done at all. The same considerations come with vulnerability patching and firmware updates.

IoT devices were often overlooked as minuscule, unimportant details of the overall network. This view has changed completely after the initial Mirai botnet attack. Hundreds of thousands of low calculating power devices can be coordinated together to unleash a huge, volumetric DDoS attack.

And there are several considerations when talking about IoT device security and protection:

- How to protect them on the perimeter?
- How to protect devices inside the network?
- How to distinguish legitimate device behavior from malicious?
- How to protect the device that is no longer maintained by the vendor itself?

What can be done to secure the home?

With the evolution of a chaotic IoT device market, new problems arise. How do you deal with the massive amount of discontinued and possibly no longer used devices still connected to the network and partially alive in zombie mode?

Cloud services used by such devices can be no longer available, patches are no longer released, and the manufacturer has shifted to a different type of product. And this problem will become more and more relevant with the practically unregulated expansion of the IoT device market. Parts of the internet become an interconnected landfill.

How to minimize the impact?

- Monitor your household by identifying what devices are in your network. Review them occasionally to dismiss ones that are no longer used, thus decreasing the attack surface for your home network.
- Change the default credentials, especially for IoT devices. Secure them with strong passwords according to the latest recommendations.
- Deploy protection to the edge of the home network to disallow malicious outsiders access to your inner network while at the same time disallowing your devices from participating in illegal activities or communicating with malicious nodes.
- Utilize security solutions driven by artificial intelligence that are capable of proactive protection for deterministic IoT devices by analyzing their behavior and determining typical vs anomalous behavior.

Read full story here…