DC. DIPLOMATIC COURIER
A GLOBAL AFFAIRS MEDIA NETWORK
www.diplomaticourier.com

GLOBAL ECONOMY

THE MANY-HEADED HYDRAE OF SURVEILLANCE CAPITALISM

BY ANDREA BONIME-BLANC .

Photo by Jurgen Jester via Unsplash.

FEBRUARY 1, 2022

In an era of exponentially transformative technology, surveillance capitalism—the creation and sale of technology-enabled products and services based on the collection, use, and possible abuse of data—is a growing problem, but one that businesses can mitigate, writes Andrea Bonime-Blanc.

SSurveillance capitalism is a many headed hydrae—when you cut off its heads, additional ones sprout up. In this era of exponentially transforming technology this is a big problem—for everyone.

Oversimply put, "Surveillance Capitalism" is a recent technologically enabled form of capitalistic economic power where the capitalists (tech firms) harvest private data (largely unbeknownst to its donors (us)). In exchange, we (the donors) get "free" social media or platform experiences like Facebook, Instagram, Twitter, TikTok. And, in turn, the tech firms then monetize our "free" data via advertising and other data selling techniques into millions and billions in revenue.

But, for a more fulsome and dramatic definition of "Surveillance Capitalism" as well as an amazing treatise on the topic, take a look at author Shoshana Zuboff definition in her great book, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.

In all of its constantly, rapidly evolving and bleeding edge characteristics—surveillance capitalism falls squarely into public and private governance discourse as well as the overall environmental, social and governance (ESG) discussion or what I like to call ESGT – ESG + technology. Indeed, if there ever was an ESGT issue that was mostly about technology it is the phenomenon we are calling "surveillance capitalism"—the creation, sale and profit making of technology enabled products and services that are based on the collection, use and abuse of data.

While this is not a brand-new issue, it is sufficiently evolved, transformational, ferociously mutating, and impactful that it requires constant attention from actors and stakeholders in business, society, and government. Business and other entities are caught willingly or unwillingly in this crossfire and must understand the challenge and consequences. And "spyware" is one of the more troubling manifestations of the many heads of the surveillance capitalism hydrae.

SPYWARE: SURVEILLANCE CAPITALISM ON STEROIDS

NSO, an Israeli-based, privately held technology company founded in 2010 is until recently primarily known for its proprietary spyware Pegasus, which is capable of "remote zero-click surveillance of smartphones" and was supposedly sold only to and used by governments and law enforcement (and, by implication, not the "bad guys" according to NSO). It is a technology that is surreptitiously embedded into people's phones without their knowledge, and which tracks their every move, content, and communications. What could go wrong?

Apparently, just about everything. An obvious problem is that not all governments or law enforcement agencies are created equal in terms of observing proper rule of law or human rights protections. While one

can posit that authoritarian regimes and the usual underworld suspects (criminals, hackers, and spies) will not comply, sadly, democratic governments, their agencies, and politicians cannot be trusted either nor can private interests for that matter. Witness the recent revelations of the use of Pegasus by ruling party Polish government officials against out-of-office democratic political party contenders in (mostly) democratic Poland.

Not surprisingly, NSO isn't the only game in town—they're the ones recently caught in the act. In this December 27, 2021 opinion piece called "The Spyware Crisis is Much Bigger than NSO Group", the Editorial Board of the Washington Post sounded the alarm on this topic not only because it is a seriously important topic but they have been directly affected by this scourge in the case of murdered WaPo journalist Jamal Khashoggi whose wife had Pegasus implanted into her phone months prior to his murder.

But theirs isn't the only case—journalists, non-governmental organizations have had Pegasus inserted into their phones. As WaPo concludes in their editorial: "The roster of victims runs a gamut, suggesting that the only real selection criterion for these companies is whether a client is willing to pay."

Thus, is born another nuance in the story of Surveillance Capitalism. The implications for all manner of business, NGOs, educational and research organizations everywhere couldn't be clearer: when and if a competitor, hostile government, criminal, or underworld entity wants to get protected information and data from one or more of your people, all they need to do is to pay NSO (or one of their competitors) for this kind of "surveillance".

Meta (formerly known as Facebook) just issued an alarming "Threat Report on the Surveillance for Hire Industry" in which, among other things, they conclude that a "global surveillance-for-hire industry" has emerged that targets individuals for the collection of data, intelligence and the manipulation and compromise of their devices and accounts. The Report calls these entities "cyber mercenaries" and (like NSO in its public statements) claim to only target "criminals and terrorists". However, this months-long study showed that the net of people caught in this mostly nefarious practice includes human rights activists, political opponents in both democratic and authoritarian regimes as well as journalists and other private citizens.

WHAT ARE WE TO DO?

So, what is a business or for that matter any other form of legitimate organization to do in the face of this serious and super challenging new threat? Depending on where an entity "sits" geographically and virtually, its mission, its main stakeholders, its human capital footprint and supply chain, its leadership at both management and board levels has a critical and proactive role to play.

And there are a few things leaders of every type of entity—whether in business, NGO, education, research, media—can do, to wit:

1. Deploy appropriately sophisticated and effective cyber-security protections at all key entry points guarding crown jewels (including data)

2. Establish disciplined governance, quality and ethical filters and protocols to prevent/disable the implanting of dangerous software and/or misuse of data

3. Scrub - and have the talent to understand how to scrub and evaluate - supply chain software coming in and going out

4. Prevent the illegal (and even legal but problematic) use of spyware in the workplace (in and out of the office including WFH) to track employee movements, productivity, communications, and other activities

5. Understand that external surveillance tech may very well be deployed against its own employees, executives and board members by nefarious competitors, officials, criminals or other bad actors and be prepared from a crisis management standpoint to deal with it

6. Have a transparent policy framework, related training and communications for all affected stakeholders explaining what the entity does to protect them, providing reporting helplines and protocols to protect against data and tech misuse and abuse

7. Gauge the challenge of maintaining high ethical, legal and transparency standards in the various countries you are present in – you will be challenged and thwarted in authoritarian countries (and maybe even in some democratic or hybrid ones)

8. Understand the essential nature of private/public collaboration while being cognizant of the dangers thereof especially in less than democratic countries

A final and critical component for dealing with the multiplying challenges of surveillance capitalism and related tech issues is that all entities need to have tech savvy executives and boards who understand the need for a permanent, cross-functional, transversal team of internal and external experts looking at these interconnected issues as they affect the entity, the sector, and the stakeholders in real time and continuously.

Anything short of this is seriously insufficient in today's world of complex interconnected ESGT risks and opportunities. These issues aren't going away, if anything they will continue to multiply like the many headed hydrae, until further notice.

About Andrea Bonime-Blanc:
Dr. Andrea Bonime-Blanc is the Founder and CEO of GEC Risk Advisory, a global ESG and cyber strategist, board member, life-member of the Council on Foreign Relations, international keynote speaker and author of several books and many articles.

The views presented in this article are the author's own and do not necessarily represent the views of any other organization.