June 2022

Who's Watching What?

The **metaverse** might be the next shiny new toy for bored internet users. But for Big Tech, advertisers, PR firms, and even intelligence agencies, it's a brave new world of opportunities for acquiring and utilizing personal data produced by those same users.

Anyone who uses the internet should be resigned to the fact that one's own personal data is exchanged for services. Platforms and advertisers also gather this information on their own sites to offer individually-targeted choices. It's just how it all works nowadays.

But people may be surprised to find out just how much information about themselves is out there, who may be collecting it and why. Because today, personal information is not only valuable, it's been weaponized.

Gotta catch 'em all

The most useful aspect of the metaverse will likely be **augmented reality**, where visual input of the real world is overlaid with info about it. Translations of signage, for instance, notes about local features, and so on could be quite helpful. Then again, if dominated by commercial interests, the metaverse could become an advertising hellscape of inescapable spam baited with intimate facts.

Augmented reality apps have been around for several years now, and some of the biggest have been location-based quest games. Most are made by one company spun off from Google called **Niantic**, including the one most people have heard of, **Pokémon Go**. The story around this popular game vividly illustrates both the tangled purposes and potential dangers inherent in the modern online world and especially the metaverse.

The CEO of **Niantic** is **John Hanke**, a man who talks with almost religious zeal of his company's mission to build a **planet-sized platform** for augmented reality hardware. Hanke started out with a firm called Keyhole, which made 3D interactive maps of the planet. Google bought it in 2004 and soon renamed their product "**Google Earth**".

Once Niantic budded off from Google, they created a number of games, all similar, starting with a sci-fi one called **Ingress** (still enjoyed today even by SWCP staff) then using data generated from that to build Pokémon Go and so on. For games are Hanke's way to digitize the planet with crowdsourcing by playing games in places all around the world.

Pokémon (from the Japanese for "pocket monsters") is a **popular franchise** around the world. The game is all about catching, training, and having small fictional creatures fight each other. Players interact in these games with these animated characters within real-world scenes of the actual locations captured by the cameras of players' smartphones.

To catch critters and do other things to gain points, people have to physically visit special portals called **Pokéstops**. Players must be connected to the gaming servers, constantly sending in their GPS data, and are encouraged to scan around Pokéstops with their phones for extra points and Pokémon.

Just to play the game required a great deal of access. But Pokémon Go soon raised alarms with the huge swath of **permissions** it demanded from the user's Google accounts. These included the ability to read the player's email and respond, accessing their cloud documents, search and location history, etc.

Niantic responded the way Big Tech often does, apologizing for the unintentional little mistake and promising that no ill-gotten data was kept. But the incident was enough to get the company mentioned as one particularly bad example in **Shoshana Zuboff**'s 2019 book ***The Age of Surveillance Capitalism***.

Surveillance capitalism is the economic system of getting and selling personal infor-

mation for profit. This data is not intended to improve lives but to predict individual behavior in order to better sell things – be it toilet paper or political allegiances. It's all about **targeted advertising**; and the data created is valuable to many parties, including spies.

Pokémon Go was criticized for its commodification of player data. One way was to team up with merchants to sell stuff to players near their shops, using Pokéstops to lure them in. Of course, the game also sells loads of merchandise through their **own sites**.

Zuboff claimed that it's not the personal data itself being gathered that is important as much as its predictive power. Targeted ads make online consumption so alluring and easy that they subtly undermine free choice.

From the start, **rumors** circulated that the wildly-popular game was a **spying device** of some kind. **John Hanke**, the driving force behind it all, had some backstory of his own that was not reassuring in this regard either.

Keyhole's software, which eventually became Google Earth, the basis of Pokémon Go, was partially funded by **In-Q-Tel**, the not-so-secret venture capital arm of the CIA. Hanke had also been centrally **involved** in the whole Google car WiFi scanning fiasco.

Conspiracy theories quickly sprouted, from it being a sinister government plot to get people to exercise to **Chinese worries** that it was a tool to spy out their secret bases. Many Pokéstops did seem to be placed near embassies and other sensitive areas. Many countries have **banned** it outright or restricted it from certain locations like churches.

Microsoft's now-retired **Photosynth** image tool combined photos taken by crowds into 3D models of sites. With Pokémon's dataset, it could **crowdsource** espionage.

Too much? Then consider that the Ukrainian Security Services says that the Russian intelligence agencies have developed a **game** like Pokémon Go. Ukrainian kids became unwitting Russian agents as they scanned through their towns taking pictures of military equipment and facilities, looking for virtual boxes that reward finders with digital cash.

Yet Ukraine's own volunteer hacktivists have been using smartphone dating apps to score lots of good info on troop movements from lonely Russian soldiers. It seems sex is still a very effective spying tool, though it must keep up with changing times, too.

Connecting lots and lots of dots

Whether the intent is to sell, spread misinformation, or spy, targeted advertising is a powerful secret tool. The reason most people are not more concerned about it is that it almost always must be used quite carefully to avoid alarming those being manipulated.

For instance, **Target** once found that it could tell exactly when a woman became pregnant by what she bought, but they also had to be very discreet with their targeted ads as not all pregnancies are met with joy.

Data does not dwell in a vacuum. Every fact and feeling a human has is connected to all others, even if the link is completely unknown. Early on, **Amazon** discovered that sharing "people who bought ***x*** also bought ***y***" got more folks to buy product ***y***. They didn't know ***why*** it worked. But even if there was no logical connection between ***x*** and ***y*** that humans could see, their algorithms could somehow spot one in the data and use it anyway.

Meta, that is, Facebook, gathers an immense amount of data from around the web. It uses this to **sort users** into categories based on dozens of criteria. A typical user might belong to 10 or more. Each one can be used to specifically target that individual. And as the Facebook **Cambridge Analytica** scandal showed, a single data point can reveal much more – a **beer preference**, for example, may reveal inner political leanings which once spotted can be subtly influenced at will.

To function, Meta's virtual reality devices will have to **record** every twitch a user makes, and so the data becomes even more intimate. And there's no telling how it will all be used.