

Mini Review
Volume 11 Issue 3 - June 2024
DOI: 10.19080/ARR.2024.11.555811

Ann Rev Resear Copyright © All rights are reserved by Doepp Manfred

The Danger of the Computer Becoming like Man is not as Great as the Danger of Man Becoming like the Computer (Konrad Zuse)



Doepp Manfred*

Holistic Center, 13 Haupt St., Abtwil 9030, Switzerland Submission: June 09, 2024; Published: June 14, 2024

*Corresponding author: Doepp Manfred, Holistic Center, 13 Haupt St., Abtwil 9030, Switzerland

Keywords: Smartphones; Electro smog addiction; Pocket spy; Operating systems; Privacy

Abbreviations: PVS: Phantom Vibration Syndrome; FOMO: Fear of Missing Out; PtSS: Post-Textual Stress Syndrome; MAIDS: Mobile and Internet Dependency Syndrome; CSAM: Child Sexual Abuse Material; IAB: Internet Architecture Board; BLE: Bluetooth Low Energy

Introduction

We pay for the convenience that smartphones offer us by giving up our freedom. The devices not only spy on us, they also shape our consciousness. What do we prefer - freedom or control? Availability stress or relaxation? Some privacy or total transparency? Informal self-determination or the feeling of being used for commercial purposes? To feel safe or to be exposed to constant attacks on our minds? The answer to all these questions should be simple. Yet, day after day, the majority of people make the choice that is harmful to them. The smartphone has become a pocket-sized tyrant. For many, it is addictive, and for the few who could still do without it with an easy heart, the device is increasingly being forced upon them by structural constraints. Just as the smartphone has become indispensable, the dangers and impositions associated with its use are growing. Programmers are working at full speed on applications that not only increasingly spy on us, but also attempt to deform our minds in the interests of the prevailing narratives. The devices configured by Apple and Google are far more than just "useful tools" - they are surveillance devices, data octopuses and weapons of psychological warfare all rolled into one.

The Situation

Many people harbor vague suspicions. Many have noticed one or two indications that such a suspicion may well be justified. Despite this, very few people manage to objectively analyze their behavior and change behaviors that they have once internalized.

Habits and routines are difficult to get rid of. Especially when they develop into addiction or compulsion. This happens not only with alcohol and drugs, but in an almost epidemic way (together with an "electro smog addiction") with something that can be called a "pocket spy": the cell phone or smartphone.

While the excessive use of the device in practically all situations in life has undoubtedly become a socially harmful bad habit - not to say a plague or epidemic - the addictive factor of the ever more potent companion is not even the biggest problem. After all, addictions can be overcome, albeit laboriously and slowly, but not the fact that the devices are used for the seamless observation, manipulation and transformation of society. This is because they have long since eaten too deeply into the socio-economic structures of our time. For the majority of the population, everyday life seems almost impossible to organize without a smartphone. Whether communication, news, weather forecast, route planner, payments, two-factor authentication, photo collection, video streaming or music archive - the mobile companion works.

However, the misleadingly positive and progressive lifestyle image of this useful all-rounder belies its intentions. These are revealed when we take a look at its development, the corporate structures behind it, a few frightening figures on its effects on people and society and, above all, what smartphones with Android/Google or iOS/Apple operating systems are doing without the user's help or knowledge.

Concrete

To put this into context: over 60% of all internet traffic and 55% of global website access now takes place via cell phones (as of April 2024). 98% of devices run on either Android or iOS. 92.3% of all internet users access the internet from their pocket computer. 6.92 billion people currently own such a device. At the end of 2023, that is a good 86% of the world's population, who spend between two and almost six hours a day on it, depending on the region. The alarming global average for people aged 16 to 64 is currently almost seven hours of screen time per day. 35.2 percent of iPhone and Android customers' usage time is spent on social media (as of 2021, and rising). Smartphones have hardly been used for making calls since 2012. "Smartphone penetration", as market penetration is referred to in the sales jargon of the telecommunications industry, seems to be an increasingly accurate description of general developments in view of these figures. Because the device is raping the brain.

Nevertheless, the cell phone has taken the world by storm. At first it was the enthusiasm for the new, the joy of mobile telephony, the "toy". Or Gameboy. Then came the SMS. Closely followed by mobile e-mail and the ability to access the Internet on the move. Then came the first iPhone. What this technological progress has done to an essentially social being since 2007 can be seen today at bus stops, restaurant tables, in school playgrounds or among groups of lonely display junkies. The effects are devastating. The playful, light flair of the handheld radio feeling was quickly lost. What the device primarily triggers today is stress, pressure, compulsion and anxiety.

Even a superficial search immediately reveals six to nine "medical achievements", i.e. diseases of civilization, that can be attributed to improper smartphone use. From smartphone acne and video shoulder to cell phone neck, PVS (phantom vibration syndrome), FOMO (fear of missing out), PtSS (post-textual stress syndrome) or MAIDS, the "Mobile and Internet Dependency Syndrome". Un reflected usage behavior, the distraction dictate of the platform economy, is changing our thinking, physicality, brain capacity, eyes and our emotional and social abilities. Not to mention the "mental health crisis" triggered by intensive social media use, especially among teenagers. In light of the bare figures and emerging long-term effects, it should therefore be indisputable that the supposedly practical everyday helper has not really advanced the human species in evolutionary terms.

Dangers

In the frenzy of permanent accessibility, the fact that smartphones are not only causing us massive physical and social damage is unfortunately being lost. Knowledge is power - and nobody knows as much about postmodern man as Google or Apple.

The companies not only know all our contacts, movement data, songs, photos, videos, bank details, account balances and email attachments, but also our search queries, political views, worries, sexual preferences, confidential messages and intimate conversations. This information not only paints a detailed picture of each user's social network, but also a psychological profile that could hardly be more accurate. Digital advertising providers in the USA collect over 72 million data points per child up to the age of 13. Facebook collects more than 50,000 entries per user. The most harmless result of this data collection is targeted advertising that is displayed to us on platforms and websites based on data and user behavior.

The effects of data misuse - see the Cambridge Analytica scandal -, mental manipulation, electronic ID cards, digital currencies, algorithmized censorship, social credit systems, ${\rm CO_2}$ budgeting and geofencing are much more serious. All projects that would not be possible without smartphones. Anyone who permanently transmits their location to a control center is easy to control. Even some music tracks can no longer be played when you are traveling. "Not available in your region", it says. Geofencing exclusion in a nutshell.

Smartphones naturally monitor and document their owner's position even if all GPS functions are deactivated or the device is switched off completely, as an article on NSA surveillance techniques from 2013 or a report from Princeton University from 2017 show. The option to switch off location and tracking services or background updates in the smartphone menus only applies to service and third-party apps. However, many still transmit data regardless of this. Such location data is preferably sold to governments and secret services.

The location services from Google and Apple cannot be switched off, nor is it clear what happens to the data. For example, a travel route across a country is documented to the exact meter on Google Maps, even though all tracking functions may be deactivated and it may not be possible to establish a data connection with the smartphone unless you are near a hotel hotspot and activate locally available credit cards for data. Following this program, it is easy to program digital money or modern cars so that they only work within a predefined radius. This turns the smart grid into an invisible cage.

The goals pursued by the digital-financial complex of corporatism are exemplified by the latest developments for Android smartphones. Take Google Play Protect, for example, an operating system software that warns of "harmful" or "unknown" third-party apps, scans them and prevents them from being installed. Ostensibly for the safety of the user. However, it doesn't take much imagination to imagine that even unwelcome apps from Odysee, Rumble, RT, Al Jazeera or anonymous crypto wallets quickly end up on the list of malicious software and can no longer

be used.

Apple made headlines in 2021 with the announcement that it wanted to install "client-side scanning" on iPhones and iPads. This extension would enable the tech company to scan all photos uploaded to iCloud. This should make the distribution of child pornography - CSAM (Child Sexual Abuse Material) - more difficult. At the time, the Internet Architecture Board (IAB) issued an urgent warning about this scandalous paradigm shift in terms of privacy and data encryption. After some uproar, Apple officially withdrew from this project. However, the software was installed anyway. Today, the program can be found on every Apple device with a current operating system. However, it is not active, according to Apple, the fact-checking industry and various tech bloggers.

However, this is not correct, as you can see from the comments of cyber security expert Rob Braxman. The function is just well disguised. On closer inspection, it becomes clear that every photo taken with an iPhone, iPad or Mac is scanned locally. How else would the device be able to identify faces and suggest them for special albums? Each image is provided with so-called neural hashes, unique identifiers that are transferred and cataloged when uploaded to the cloud. Privacy for photos no longer exists. Because even if the cloud services are deactivated, Apple devices secretly transmit the transcripts of the neural hash database to the control center at night. And images in the cloud cannot simply be deleted either. If you click on "Delete" in the context menu of a photo, the photo is not actually deleted, but only the user view is hidden. It is not known how long Apple and Google keep the data on their servers. Presumably for a long time. Because as a test by "Copy Trans" shows, photos that were supposedly deleted years ago can also be downloaded from the iCloud.

Corporations

Google is going one step further. As the "Medium for Digital Liberties" www.netzpolitik.org explains on May 16, 2024, the company plans to scan - and store - all of its users' calls in future in order to be able to warn its customers about telephone fraudsters. Data retention was yesterday. In addition to the tech companies, the transatlantic surveillance circles in the EU, the UK and the USA are of course now also working on laws that legalize client-side scanning and total surveillance without cause. Even if such undertakings reduce the right to the protection of personal data or the presumption of innocence to absurdity and projects such as the so-called chat control are illegal according to general legal understanding.

But worse is always possible. Smartphones that can be unlocked with facial recognition software such as "Face ID" - as if the fingerprint reminiscent of police fingerprints wasn't enough take an infrared image of their surroundings every five seconds. Even when the screen is locked or covered. According to Apple, this is necessary to be able to unlock the device quickly by looking at the screen. The photos taken by Face ID are converted into mathematical structures and stored on the phone. A device that

sends unsolicited, invisible data packets "home" every night at around three o'clock a.m.

However, the cameras on modern smartphones can do completely different things. For example, they follow the owner's gaze in order to anticipate their actions or receive commands. Analyze their facial expressions. Apple calls these "attention-sensitive functions". Anyone who feels uneasy about the increasingly biometric entry controls at airports should therefore probably not use a smartphone. The pocket spy is also listening, constantly. How else would "Siri" know when you want something from her? But here, too, the "experts" and the media complex are playing it down, claiming that it is pure coincidence that advertisements and social media content reflect exactly what has been discussed around the device in the last few hours. In this context, «USA Today» admits that the phone is listening, but that this data is only processed locally and no voice recordings are transmitted to Apple, Google or Amazon. And that is actually correct. Because the amount of data would be too large. Instead, smartphones transmit text files with transcripts, which anyone can see today when they record a voicemail with iMessage and it immediately appears as text. They deliberately omit this aspect.

In addition, the AI-based applications "to prevent domestic violence" or "danger prevention", 136 of which were examined in a study published in March 2023, will only function as promised, namely autonomously, if the smartphone constantly uses its cameras, microphones and motion sensors to monitor its surroundings. In future, the individual device will no longer pose the biggest problem for freedom-loving contemporaries. For some time now, pocket spies have been monitoring not only their respective owners, but also their surroundings. The devices communicate with each other, exchanging information such as IMEI numbers, IP addresses and contact details. iPhones have offered this function across the board via the operating system since September 2020 (iOS 13.7). The information collected via Bluetooth Low Energy (BLE) formed the basis for the contact tracing apps during the coronavirus crisis. The German Corona-Warn-App also used the non-transparent data pool. The program was able to read out all encounters from the past 14 days via an interface. By the end of 2020, more than 20 countries had already developed tracking applications to read the movement and encounter data collected by Big Tech and display it in their COVID apps. China sends its regards.

In other words, iPhones have been recording every contact with another iPhone for almost four years and using this data to create network maps of their owners' movements and encounters. Although this function can be deactivated in the smartphone menu, it is naive to assume that the device does not still collect the relevant data. According to Apple, this information should only be stored locally and automatically deleted after 14 days. The example cited above with the supposedly deleted iCloud photos that can be restored years later shows what to make of such statements.

Google followed suit and implemented a similar data octopus. Since the end of 2020, Android devices have also been recording every encounter with other Android devices. This created two huge mesh networks in which machines communicate with each other without the owner's intervention. In Germany, 66.1% of smartphone users use Android - 33.2% use Apple's iOS (as of March 2024). This means that 99.3% of the population is mapped. For some time now, the two operating systems, which previously spied on each other separately, have also been able to understand each other. Not only does this secretly herald a paradigm shift in terms of total surveillance, such a mesh network also creates the basis for the militarization of smartphone infrastructure, because this network can not only collect and send data, but also receive commands. Malware could be installed for 99.3 percent of the population at the touch of a button, a blackout could be simulated or a specific radio frequency could be generated. This could stimulate nanoparticles and smart dust to react in certain ways.

In this context, it is worth noting that the iPhone is by no means the brainchild of a brilliant inventor - even if Steve Jobs liked to think of himself as such - but of military technology. Jobs just used it cleverly and marketed it. Mariana Mazzucato dedicated an entire chapter of her book "The Entrepreneurial State", published in 2013, to this story. In the book, the author shows that many of the innovations of our time that are generally celebrated as private-sector masterpieces can actually be traced back to an interventionist state. Batteries, sensors, chips, Siri, touchscreens - all financed and developed by the US government and US military. A graphic published by Business Insider in 2014 illustrates the extent of this. As recently as 2012, DARPA itself warned that cell phones, if widely used, would be an ideal weapon for covert attacks on the population.

Google only exists, as it were, thanks to research budgets provided by the CIA and NSA for the development of mass surveillance tools. An internal company video from 2016 illustrates Google's vision of being able to "change society" with "total data collection". As explained by Yasha Levine in his book "Surveillance Valley" published in 2018, this applies not only to Google, but to all big tech companies. Even CBS News was able to read in 2011 how intensively In-Q-Tel, the CIA's investment vehicle, was involved in the founding of Google, Facebook, and co., and how the secret service has used the companies for its own purposes ever since. Headline of the CBS article: "Social Media is a tool of the CIA. Seriously."

Protection?

The fact that you can no longer escape this permanent smartphone surveillance by Google and Apple even by using encrypted messenger services is illustrated by the AI service program Recall recently presented by Microsoft. It will soon be rolled out for Windows and will help users to search for files. To do this, Recall takes screenshots every few seconds and

records everything that happens on the computer. Microsoft CEO Satya Nadella tried to reassure the immediately furious data protectionists that the data would only be stored locally, would be encrypted and would be deleted after three months. Not very reassuring. After all, if a hacker gains access to a computer, all they have to do is call up Recall to gain access to passwords or other sensitive data. Above all, however, a program like Recall shows that even technically secure messengers can be monitored quite simply. To do this, you don't have to intercept and decrypt their messages on the server, but simply take a photo of them on your smartphone and convert them into text files for transmission.

What Needs to be Done?

To summarize, it can be said: If you want to protect your privacy, you should switch off your smartphone. Or get rid of them. Because the devices configured by Apple and Google are surveillance cameras, data octopuses and weapons of psychological warfare - not useful tools.

This category tends to include the so-called «dumb phones», which can only be used to make calls and send text messages. Reminiscent of the early 2000s, these devices do not bother the owner with countless unnecessary applications or never-ending notifications. No updates. What's more, the devices don't lead a secret life of their own. When they are off, they are off. In most cases, the battery can even be removed. What's more, such rustic cell phones do not constantly report their location to a control center. These arguments seem to be convincing more and more people. The Nokia 3310, which was launched in 2017, already sold twice as many units in 2023 as in the previous year. Communication and tasks that were previously handled via smartphone are being shifted back to the PC. The immediate effects of this approach on daily routines and quality of life are considerable.

If you can't or don't want to do without a smartphone, you should look for alternatives to Google and Apple. The iPhone is out of the question, as the iOS operating system cannot be modified or replaced. However, Android can be customized and used without Google services. Smartphone alternatives can also be operated with other operating systems such as Graphene OS, which respect the user's privacy - as long as you no longer download your apps from the Google Play Store, but from F-Droid, Aurora or APK Pure, for example.

A Murena Fair phone or Volla Phone, for example, is a suitable end device. An Above Phone in the USA. The Volla Phone is supplied ex works with two optional operating systems, one developed inhouse and the other Graphene OS. This gives you control over your own data. And after a short familiarization phase, not using Google services is no longer a problem - because there is a monitoring-free open-source alternative for practically every Google app. Tips, tools, tutorials and further information on protecting your privacy on your PC or phone can be found at Rob Braxman or in the Privacy Academy store.

Annals of Reviews and Research

Conclusion

If you don't want to be a slave to your devices in the "media age", you have to actively address these issues and change your routines. Whatever you intend to do, you should do it now. You

have to escape this network of total surveillance, leave the matrix while you still can. Because the seductive convenience of the surveillance economy comes at a high price: freedom. And smartphones have long been collecting more data about their owners than a secret service could ever do by conventional means.



This work is licensed under Creative Commons Attribution 4.0 License

DOI:10.19080/ARR.2024.11.555811

Your next submission with Juniper Publishers will reach you the below assets

- Quality Editorial service
- Swift Peer Review
- · Reprints availability
- E-prints Service
- · Manuscript Podcast for convenient understanding
- · Global attainment for your research
- Manuscript accessibility in different formats (Pdf, E-pub, Full Text, Audio)
- · Unceasing customer service

Track the below URL for one-step submission https://juniperpublishers.com/online-submission.php