Privacy 404

Filipe Cruz

Introduction

"*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*" Article 12, Universal Declaration of Human Rights, 1948.

Our right to privacy is enshrined in the Universal Declaration of Human Rights. The importance of privacy to an indvidual is well scientifically documented. Lack of privacy affects us physically, psychologically and emotionally. Having access to a space of our own that we consider safe and private promotes our self-confidence and the emotional capacity to deal with society demands.

Drawing the parallel to an increasingly connected world: data safety and digital privacy are essential for trusting the services that are critical to our life in community: access to education, medical assistance, legal system, money and banking, etc...

However, technology has made it now easier than ever to monitor and identify everything and everyone.

Video surveillance has been increasingly institutionalised by multiple governments, "for our protection". Almost a century after Orwell's published warnings, society in general continues to move in this direction. Being told to the public that "only those with something to hide would oppose it" and with recurring talk that many thieves, terrorists and paedophiles will only ever be caught if and when every street and person of our nation is under strict surveillance.

The critical follow-up question remains unanswered: Who watches the watchmen? Who will prevent abuses of power? Who guarantees that all the private information being collected will be securely encrypted and protected from unauthorised access and deleted when it is no longer being needed for the agreed upon purpose? It's inevitable that there will always be some sort of unauthorised system access at some point, while in turn private data has an ever growing commercial value. This conjecture makes our future... not very safe.

And then we have online social networks, which actively encourages the public sharing of information that should in many cases be considered private. There is still a big lack of awareness, interest or care from the users of such online platforms in avoiding sharing private information publicly. Because "it's convenient", because sharing creates relational bonds, because people crave public validation, because we now deal with matters in public that used to be considered private in nature. Because we're going to become millionaire "influencers" if we share, because "everyone else is sharing too". On the back-end companies also sell our private data to third parties so anyone can easily find our private information, or that of our families and friends. Suddenly nobody cares about the thieves, terrorists and paedophiles who could use this information to cause us harm, because it's more important that our followers know that today I ate the best pancake ever at this exact location and at this exact time with my friends Zé and Mariana and that their little boy who is 5 and a fan of Marvel comics loved it.

There are strong economic interests in selling more surveillance technology, artificial intelligence and personal data. There is strong motivation from security and military power to be able to monitor every street and every person. There is little political interest in enforcing international data protection and rules of privacy protection.

This is a topic that has bothered me for more than two decades. I was/am part of a number of groups that try to raise awareness of this type of issue and remind the government to protect us. For those who are interested, here are the references of two non-profit associations that work in favour of these causes in the public interest:

EFF - Electronic Frontier Foundation https://www.eff.org/

Based out of the United States but with strong international projection.

D3 - Defesa dos Direitos Digitais: https://www.direitosdigitais.pt/

Based out of Portugal, also paying attention to European directives.

I try to support these institutions as much as possible, with hope it'll make my son's future a little bit better than what things are now. It's currently impossible to live in society without having our private data collected by several public and private systems, under prejudice of not

being allowed access to transport, shipping, employment, communications, healthcare, finance, etc... Having a mobile phone and internet access is becoming mandatory for a lot of small everyday comforts, without knowing to what extent our privacy is being respected by telecoms operators, their employees and even possible unauthorised access. We pay to have a personal tracking device with us at all times.

I spent a lot of nights with insomnia, thinking about this topic, pondering what I could do to improve the world in this regard for the next generation. Where we don't have to hard choose between living off-grid and marginalized by society or living integrated but exploited and under control. I have no real power to influence politics. So all I can do is try to influence culture. I've written down my dystopian thoughts about what our future might look like in a few years' time. I present them here in two short, somewhat related stories, both of which are just some food for thought in the genre of speculative science fiction.

I hope they are interesting reads from a literary point of view, but above all I hope they manage to make you consider some of the real dangers behind the lack of digital privacy that is creeping into our society. Or maybe even offer some ideas on potential ways to tackle some of the problems that we'll have to deal with? Or maybe not? Who knows? I just wrote things and wanted to share them. Anyways, hope you find them interesting!

Occurrence in Rua da Lapa

Temporal Geo-referencing:

2133696921 - Avenida Álvares Cabral, Lisbon

2133697620 - Rua da Lapa, Lisbon

Actors:

Nuno Benite 54636775

João Serzedo 62819311

Contextual narrative reconstruction (narrator profile 424):

Once upon a time there was Lisbon on the 12th of August 2037. Driving down Avenida Álvares Cabral at 14:35 was a white vehicle with two blue stripes. It was one of the latest hybrid car models from Public Security Police. It had a built-in centralised global communication system that allows it to send and receive proximity notifications to all devices active in the area; it also had an auto navigation system with a 98.9% confidence level, which Nuno Benite prefers to keep switched off to drive the car himself, so that he "has something to do" while he's out on patrol. 3 known access vulnerabilities.

Nuno, 34 years old and of average height, is the kind of person who goes to the gym twice a week, not because he needs to, since he has the exact same equipment at home, and the "boss" actually keeps him on a tight leash with all this new technology that knows where we all are at all times, there's nothing he could do without her knowing really. So he only goes to the gym to socialise with his male friends and "see the sights" of his girl friends. Enjoying the views, while looking and thinking is still not a crime. He wears the usual bald look, worn by many other police officers, and says it's because it suits him, but in reality it's because it's just less work to upkeep. He doesn't drink alcohol, because "that's for the broken". A term legitimately used by many good people to reference "that class" of others who insist, the poor things, on not being "a part of

the system", but who also then don't accept to just live inside the colony that was created for them in Alentejo. They are always out here creating problems for traffic and pestering people to leave technology and regain their privacy. Nuno says he became a police officer "just because". Possible conversion rate 0.12

In the driver's seat, connected to the immersive system for central communication, was João Serzedo, 25, of medium height who is a little shorter, but not by much. He jogs every other day (when he's not late for work). He's not in a relationship "because it's never happened" and although he has been a little disappointed with his first six months as a police officer, he still believes that he is improving society a bit every day on the job. João says that he became a police officer because it was his dream from an early age, but he never revealed on record exactly why. Possible conversion rate 0.67

Audio transcript of the event:

- Notification of an occurrence at Rua da Lapa number 12, we are the nearest unit.

- OK, what kind of event?

- Can't you see it projected?

- You know I don't like having that rubbish on while I'm driving. Just tell me what kind.

- Occurrence of domestic disturbances with PEPO 3.8. - Potential for escalation to punishable offences, calculated in real time by the authority system, based on machine learning prediction models applied against the local history collected with sensory fusion of various devices in access to the premises: smart lights, smart TV, mobile phones, fridge, entrance display, vibrators, washing, drying and ironing machines, etc.

- It's not some kid practising neo punk, atrophying the whole system again, is it?

- No, it's a male couple. There are no other people registered in the flat. The sensory fusion in the neighbouring systems confirms it.

- If the neighbour's devices registered it then they are already paying a fine, why do we need to go there?

- PEPO 3.8, damn it!

- OK, let's go and visit the upset lovebirds before they get seriously hurt. I'd leave them alone. My grandmother used to say "between husband and husband, nobody puts a condom" hahaha...

- Yes, you're a first-class respecter of all privacy! Speed it up, here it says it's already escalating to physical aggression. I'm going to switch to direct access to the audio of one of the phones...

- ... piece of shit! I saw it on the system, Raquel showed me! Who was that bitch who was here from 11.10 to 11.52? You fucking cunt! My father warned me that you couldn't be trusted, that you had probably had some broken friends! All that bullshit of ...

- ... nothing happened, shut up, you're activating the systems!!! How did Raquel give you access without permission??

- ... I don't care about the fine, you lying bastard piece of shit! I want you out of ...

- ... keep your voice down, shut up! Let me explain! Stop it! Fuck!

- ... stop this, you cunt ...

- HAHAHA! He threw his fucking phone at the other guy!! These guys are crazy!

- It must have broken on impact, it stopped transmitting. I can monitor the heartbeat through the digital watches, but I can't hear it through the fridge, damn firmware updates.

- What about the other mobile phone?

- It's fake privacy, it's transmitting expected audio, not real, the sensory fusion rectifier detected this flaw in the synchronisation pattern when they started arguing.

- Whoa! He's a terrorist!

- You can't assume he's a terrorist for trying to exercise privacy.

- Only those who have something to hide need privacy! And you heard what the other guy said, he's probably got broken friends! He's a terrorist for sure! Call in the technophobia unit.

- We must have proof.

- We should already have it, that Raquel he mentioned must be some kind of management entity, either for the flat, the building or the street. Send it a request for access to the building's or flat's video surveillance channels, we have probable cause to make the request.

- I have the IDs, but I don't know which one is Raquel.

- Fucking right to privacy mania, always getting in the way of our work, what was wrong with just stating the name of the entity in the access logs?

- You know there's still discrimination. Even if it's illegal to intentionally switch off servers, there are still a lot of people who think that the wealth of the dead shouldn't be tied up in the hands of their artificial entities, but returned to society instead! I'll send the request to the 3 of them, they're obliged by law to respond to law enforcement agents in a timely manner of 5 mins per bandwidth.

- Those laws only passed because they were paid for by some rich folks, that should be illegal, those aren't people, their inheritance should go to the state and a small tax on the family to cover the clean up of their state systems footprint, as it always was before!

- It's the law we have, we have to enforce it. I've already received two replies, the flat organisation is configured not to keep long-term records...

- How convenient! That shit right there, that's what should be actually illegal! Fucking politicians.

- Focus please. The entity that manages the street does not identify itself as Raquel, but in accordance with the law it provides limited access to the surveillance cameras it is responsible for, with a view of number 12. Street management entities are obliged to keep the records.

- Alright, send it now to the technophobia unit. Look, number 12, this is it. Let's go separate those lovebirds.

The transcript ends at 14:47.

Probabilistic conclusions of the report:

It is probable with a 74.5% confidence rating that the operative Tomás Farto 737480283 is being held in technophobic rehabilitation or is in transit to it, without inconspicuous access to the untraceable communication modes required by our current operations security and privacy standard. All links to him are prohibited until further notice.

It is probable with a 12.2% confidence rating that the entity Marques Fino 120937211, resident of Rua da Lapa 12, is likely to have an operational relationship with the system. All operatives should avoid future relationships.

It is probable with a 89.7% confidence rating that the operative Cláudia Mota 232549282 is considered a suspect of illegal inter-operation and is being monitored with increased computing power to detect anomalies in the behavioural pattern. All connections to her are prohibited until further notice.

It is probable with a 12.1% confidence rating that the operative Yassmir Vulkov 832812922CC is suspected of illegal interoperation and is being monitored with increased computing power to detect anomalies in the behavioural pattern. The connections remain active in accordance with our current security and privacy standards.

It is probable with a 6.2% confidence rating that the operative Afonso Polido 7408206931CC is considered a suspect of illegal inter-operation and is being monitored with increased computing power to detect anomalies in the behavioural pattern. The connections remain active in accordance with our current security and privacy standards for operations.

It is probable with a 89.1% confidence rating that the entity Raquel Valente 213038263CC, cyberbrain regent of number Rua da Lapa 12, has operational relations with the system. All operatives should avoid future relationships.

I'm a hacker, living in the streets anonymously

I'm a hacker, living in the streets anonymously. What are my days like? The mornings are humid, the afternoons dark, the nights are full of buzzing lights. The partial lockdown laws have helped me go unnoticed in most of the metropolis I've visited in recent months. During the day I dress up as a delivery courier. I rarely deliver anything. Sometimes I have to, in order to gain access to a building with particularly high security. But usually people just let me in and don't look twice. The obligatory mask helps a lot. I travel by bicycle or electric scooter, the kind that are rented by the hour electronically. I enter the target building and pretend to be confused, looking at my tablet, like all couriers do when they're looking for confirmation of an address, I stand in a corner away from the cameras while I search the target network, when I find it, I access it however I can access it, I install whatever I need to install, I listen to whatever I need to listen, I copy whatever I need to copy. Later, I transfer a confirmation of the target's achievement to a public dropbox on the internet via my own VPN and the next day I'm paid the rest of the agreed upon amount.

"*Another anti-corruption protest turned violent, right here behind me in Square of Rossio, yesterday late afternoon the police were called in to control the crowd who threw stones and Molotov cocktails at them, they were dispersed with water cannons but they promise to return to the protests on Monday. One more in the dozens of demonstrations that have been organised all over the country in recent months. The protesters' demand is clear: parliament must approve the expedite court of immediate resolution for cases active corruption. Let me remind you that the parliamentary elections are scheduled for six months from now and the voting forecasts continue to favour the new anti-corruption party formed just over two months ago that emerged in the wake of yet another statute of limitations expiring in the active corruption investigation linked to the third bailout of the new bank with known deep links to members of the government. If the elections were held today, the latest polls indicate they would get 35 per cent of the vote.*"

When I was four I unlocked my father's mobile phone, I wanted to play Angry Birds. He slapped me across the face for going through his things without permission. When I was 7, perhaps as a joke, he threw me his old broken phones upon my bed, they no longer worked and no one wanted to buy off him for parts, he told me to play with those instead of his working phone. None of them would switch on or charge, on one of them the screen was broken and the battery was swollen, while the other had drowned in a toilet. I went to the Indian's shop with them, borrowed his repair kits in exchange for what I couldn't salvage, spent three hours there dismantling, testing and reassembling them, it took longer than I expected, but at the end of the day I managed to get one of the phones working by replacing the broken parts! When I got home my father was waiting for me, he belted me for being late for dinner and he took the repaired phone from me, I never saw it again, he must have sold it, he didn't give me any money for it either. Thanks to my father I learned never to trust anyone in life, ever. I considered it an important lesson. Nowadays I strictly abide by the rules of encrypted, disposable internal independence. This keeps me safe.

At night I have an anonymously reserved corner by the docks to sleep in, it's too humid for my liking but it'll do for a few days. They hand-deliver food for the homeless to us. They don't ask questions and abide by the current sanitary laws of wearing masks and social distancing. The place is good enough to sleep for a few hours. I can charge the batteries of my devices there and watch the news. I live in an organically developed bubble of systematic prudence. I stay in the nooks and crannies of the city that have no cameras and people don't ask questions. As long as these corners have access to electricity, they're very precious! Anyone who knows how to look on the dark web will find several websites where they rate city corners in respect of the offered anonymous privacy. I realise that the rating can be a decoy to find the people who don't want to be found. So I strictly abide by the rules of encrypted and disposable internal independence. This keeps me safe.

"*The Associação Transparência e Integridade presents us the figures, and they are clear: the money embezzled from the state budget in publicly known cases of active corruption that have lapsed from lawful prosecution this year, would have paid the Unconditional Basic Income*

1.67 times the current national minimum wage to all 11 million Portuguese! Think about what I've just said, if there was no corruption in Portugal we could not only eliminate poverty and the vast majority of crime derived from poverty that exists in Portugal, but we could also all choose which thing in life we really want to work in, regardless of whether it's generating money for some employer or not. We could work at the pace that suits us best. We would have time for our families again, we'd reduce the stress caused by the profit-focused business world, we'd eliminate precarious work and the jobless crisis. With only the savings of 1 year of the known government corruption, which is known, but our courts have allowed to lapse in bureaucracy or incompetence."

They told me that my mum died of an overdose of Metartropine shortly after I gave birth. They don't know the side effects, there aren't enough studies yet.

My father also used Metartropine, all his UBI experiment money was spent on Metartropine, when he didn't have money to buy more he would steal from his friends, until he didn't have any friends left. My grandmother knew about the situation and looked after me for a while. I remember her letting me play with her computers, as long as I never connected them to the internet. But I would connect them anyway when she wasn't there, and that's how I met Victor.

I met Victor724 through a forum on the dark web. He taught me how to change my digital identity periodically (without any backtracking traces) in less than 10 minutes. He taught me how to register with other people's credentials. How to access things you shouldn't access. He gave me Predator's source code to analyse. I never met Victor in person, and one day he disappeared from the internet. Maybe he got caught, or changed his identity more radically. He stopped contacting me. I had to change my identity too. We lost contact. Maybe he's still hanging around dark web forums under a different name, like I am. I miss talking to him, he's the only person on the internet who knows my biological name. I don't believe his real name was Victor though.

When the services found out I was living with my grandmother, they cut off my father's UBI experiment. He didn't like this and forced me to move back in with him in order to get it back. My grandmother gave me

a computer, but my father sold it to buy Metartropin. I got upset, did some calculations and then I killed him. I didn't do it on a whim, I simulated my life forecast with a neural network on a school computer, trained it to maximise my short-term survival and the results were clear, it was better that my father wasn't included in my life plan. The UBI wasn't working for him.

They didn't find the body, nobody came to investigate. Anyone who asked me about him I answered that he had disappeared, which didn't surprise them. They asked me for the money he owed them, broke into the house, took what little furniture I had left, came back a couple of more times but there was nothing left to take so they did the same to my grandmother, she complained to the authorities about it, so they killed her.

The day after they found her dead body the authorities came to me. They informed me that I could not live alone, asked me about my father and tried to convince me to come with them when I told them he was gone. I had been planning to ghost the system entirely for some time, when investigations had begun at school looking into the activities of illegal access practices detected on the network. Now I finally had the motive to put the plan into practice. So I left the house, stopped going to school and since then strictly abide by the rules of encrypted and disposable internal independence. This keeps me safe.

"It seems the p*roposed Unconditional Basic Income won't be enough to live in Lisbon! These are the conclusions of a study carried out by the Catholic University and released today: property speculation and a lack of life goals continue to drive many people to despair in the capital. The numbers of disappearances, petty crime, suicide and drug addiction continue to rise despite financial support for subsistence. Metartropine in particular has spread in popularity, with a special focus on retired housewives and unemployed young. Don't miss tonight at 10pm the panel discussion on RTP2 with João Martelo, secretary of state for the implementation of the Portuguese UBI in debate with RTP's political commentators.*"

I don't have an identity card or any data in the system. If I'm asked for documents, I reply "I've lost them" or "I left in a hurry and must be in

the other jacket". I have a laundry bag, a couple of hoodies and shirts from the different carriers and a towel for when I need to wash up. To access Hacker Trade I connect to the McDonalds router network, every day with a different spoofed mac address, every day in a different McDonalds, sometimes in another establishment, but there are many McDonalds scattered around. I establish a secure private connection and stay connected for exactly 18 minutes and 26 seconds, more than enough time to synchronise my transfers, accept something local at Hacker Trade and illegally maximise my bike rental time while I have lunch and delete the access logs. The dark web says that at 20 minutes they can trace Hacker Trade's connection, so I'd rather not risk it.

I pay for everything in cash, I shower in the social sports hall, they have coin lockers to store my electronics! But even so, I always keep everything encrypted and rigged to self-destruct if illegal access is detected. I keep a record at BIOS level of all the physical connections made and check that the pattern of talcum powder sprinkled on the screws remains consistent before using the electronics again, we have to be careful with direct physical access to the hardware, it's a common attack vector.

"*The law must be honourable and not be afraid to go look where it needs to look. Privacy is only relevant to those who have something to hide!*"

Just in case, for the most critical missions, I rent second-hand equipment, easily resold on the black market. I have a quick method of preparing the equipment for any new anonymous illegal disposable use. The first thing I do is physically switch off the camera, microphone and GPS. Factory reset the BIOS and operating system, install an encrypted sandbox with the basic toolkit that I've reviewed and compiled myself with the latest security updates. Everything ready to install or delete and leave in less than 5 minutes. No digital footprint. I always assume that all the networks I access will be compromised and looking for me. I only carry out missions with my connection properly camouflaged.

Often I don't even read the target's profile. I have the network ID, I know the expected security standard, the mac address and the target description. If the objective isn't clear, I don't accept. If I have no known vulnerabilities for the expected standard, I don't accept. If the security

standard on ground level is higher than the expected in contract, I cancel. If it takes longer than expected to find the objective, I cancel. If someone unexpected is connected to the network or is actively accessing the machine, I cancel. I don't mind losing reputation points in Hacker Trade with cancelled missions. It even helps me stay under the radar. All I care about is abiding by the rules of encrypted, disposable internal independence to ensure that I'm not linked to the crime of improper access. This keeps me safe.

I always try to minimise the time of physical contact with the target's WiFi network. On more complicated missions I sometimes hide a small machine inside the perimeter to attempt to crack the access to the network with a little more access time, or just wait for a certain packet to be transmitted, but in general in less than a minute my software manages to find the target network and apply the vulnerability that relinquishes access. From there it's trivial, I access the router and have a list of the devices by IP, if the router doesn't have the password by default (or has been configured to only be accessible by ethernet cable) I run an nmap on the local network that contacts all the IPs, looking for a response from the target mac address. I've already got metasploit ready to look for a vulnerable communication protocol, just run it, sometimes it takes a while, it depends on the operating system: a Windows Home Edition (5 seconds) is slightly different from a Windows Professional (7 seconds) or a Windows Server (15 seconds), sometimes they also use Macs (10 seconds) and there's always someone with a Linux Ubuntu (15 seconds) who doesn't know how to configure it properly (5 seconds), sometimes I also find other toys online, a Raspberry Pi (5 seconds), one or another Android phone (20 seconds) or iPhone (15 seconds), but my favourite is always IoT devices, those lights, surveillance cameras, toothbrushes, fridges, vibrators and vacuum cleaners with free access to the network, installed without any security in their configuration (less then 2 seconds to root). Perfect for installing a backdoor for later access to the network if the need ever arises. If the computers are properly secured (which is rare), I use my own machine to attack the router and sniff the web traffic. All I have to do is pick up an unencrypted packet with a login and password to some website and I can usually get something. As a last resort, if they're only using encrypted communication, I can also set up a man in the middle proxy, pretending to be the website they are visiting

and exploit vulnerabilities in the browser itself: Chrome and Firefox (20 seconds), Opera, Brave (10 seconds), Internet Explorer (5 seconds), Edge (10 seconds). Once I have access to the browser, I have to escalate my privileges to administrator on the operating system, another 5 seconds. When I enter the machine using this method, I sometimes notice they might be running a virtualised machine, it's a pain, have to activate another module to gain access to the host system in VirtualBox (5 seconds) or Parallels (5 seconds) or VMWare (10 seconds), it depends on what they're using really and the settings they've activated, but ultimately all of them have known kernel vulnerabilities and metasploit takes care of if easily if it's configured to do so. Most missions are completed in less than a minute.

"It's *been an historic night, celebrating a month since the new law has been passed, the cases continue to come in by the dozens every day, the core of new judges that have been assigned to enforce the law haven't stopped dealing sentences, more than 137 cases have already been processed, 8 members of the government were sacked today alone on the culmination of another intense case reveal. And it's not just Portugal that is celebrating, there are reports of dozens of demonstrations of solidarity with the Portuguese revolution taking place all over the world, demanding their own governments to enact similar laws.*"

Sometimes I stop in front of the interactive installation dedicated to the unknown hacker, in honour of all those who made the great clean-up of 2025 possible, the political revolution that forced the resignation of 84% of the members of the Portuguese Parliament, the vast majority of which were brought to light through Hacker Trade. I was one of those hackers. The cases were investigated and executed immediately, under the new expedite law for corruption cases.

The promised legal reform worked. As soon as the law was passed, there was a cascade of clean-ups, all the corruption that had been institutionalized in the public system for decades started getting washed away. Overnight it no longer mattered whether the information had been obtained legally or illegally, it only mattered if it was true, and the judge who didn't comply with the expedite law was the next to be deeply investigated and it's case show up in the hands of another judge. There was a boom in requests for investigations in the Hacker Trade, for

hackers to investigate certain suspicions that everyone knew about but that the public prosecutor's office had never obtained definitive proof of by legal means. It became an anti-corruption battle royale, everyone had skeletons in their closet, and everyone was scrutinised until only the naked survived in public office, those few who maintained their trustworthiness in the face of all the scrutiny of their privacy, as revealed by the Hacker Trade.

An anti-system had finally been put in place to replace the law of due process democracy. It brought together interested parties from across the political spectrum: populism, liberalism, socialism. All the social tensions that seemed to be suffocating our tenuous civilisation were answered in this cannibalistic self-destruction of political corruption. In a few weeks the political landscape changed radically. The largest private companies declared bankruptcy in the face of the enormity of the cases of illicit profiteering brought to light. State-owned companies were forced to sack most of their active managers and open positions to the naked. The young graduates finally found the motivation to train in their areas of interest and leave university with a more resolute job security. All they had to do was surrender any and all of their right to privacy.

The lack of prison capacity to accommodate the huge wave of arrests brought chaos to the system and inevitably forced also a political reform of the prison system aswell. The model of house arrest without a right to privacy was quickly introduced. Prisons now only house repeat offenders of violent crimes.

The unconditional basic income was revised, now highly rewarding the naked for their honesty.

Police investigation was quickly privatised by systems like the Hacker Trade. Many that were convicted of corruption have returned to school, in order to find something else they are passionate about, without participating in more corruption schemes. Others simply retired earlier or disappeared from the system, emigrated somewhere.

The wave of interest in this new socio-political model adopted in Portugal infected Europe and quickly spread to the rest of the world. Governments in several countries were quickly forced by social protest to either adopt similar laws or escalate their efforts of censorship and

active repression towards those who advocated for it's adoption. Many countries were driven into dictatorships or civil war as a result. Worldwide migration increased.

The Hacker Trade continued to grow exponentially in supply and demand... It reached it's plateau when the hackers themselves began to fall victim to investigations by other hackers. The supply of professionals decreased significantly as the risk of reprisals increased. After four years, the market for hacker investigators begins to level off.

Now the hot topics of conversation on the dark web is on how to reclaim the right to privacy that we lost in order to destroy corruption from society? The liberalisation of privacy seems now irreversible and is most concerning to the community.

"*This was the third scheduled demonstration against the so-called destruction of privacy, closely followed, right next door, by a counter-demonstration with protesters in favour of tightening anti-corruption measures. Tempers flared a little in the afternoon, and the public security police were called in to prevent any unrest. On one side there were demands for a return to the right to privacy as originally provided for in the constitution. On the other side there were shouts of order to continue moving forward with the new republic and that to stop the revolution now would have us return to the rot we had, so say the protesters.*"

As long as this access vulnerability to Exces' local routers is left unpatched I'll be staying in Paris, everyone has an Exces router here. France is still in a state of fog regarding their legislative transparency revolution. The situation has not reached the level that it did in Portugal yet but it is considered inevitable by the experts on the news. The number of missions available on Hacker Trade for Paris keeps increasing. Some vulnerabilities that longer to get noticed and patched and all routers are slightly different. Moving to another country usually means rebuilding your zero day vulnerabilities portfolio, but every now and then it's worth the change of scenery. I strictly adhere to the rules of encrypted and disposable internal independence. It keeps me safe. I don't use vulnerabilities that nobody else is exploiting yet, that would be uniquely identifiable. When I find a new zero day, I sell it anonymously

on the black market! Only when enough other hackers are using them in the wild do i I start using it myself.

"*Another group of anarchists were identified today and put under house arrest. A cell of 12 operatives who were anonymously plotting an illegal demonstration for the restoration of privacy in Portugal. They were pointed out to the police via the well-known Hacker Trade portal.*"

I don't like missions where I have to delete my steps. I've heard rumours that some teams, perhaps in charge of national security or private projects have access to this type of software, but I've never seen it working and don't trust it's security or effectiveness. They could be sniffing traffic or monitoring changes to the logs. It's much easier to pretend that it's normal traffic than to to delete log entries inconspicuously. When they are missions to pretend I was never, I don't accept them. Those who accept them tend to end up getting caught. Some hackers label them as the "real challenge" that determines the real skills, to me it's a honeypot to lure the best and catch them. I strictly abide by the rules of encrypted and disposable internal independence. It keeps me safe.

"*Under discussion in the parliament assembly today was the request to change the model for dividing and taxing privatised services. The liberal bloc refers to numbers from the recent Catholic University study on the impact of the UBI in our country over the last five years: There's still a long way to go, we need to give private companies more hiring support.*"

Some cities only accept electronic systems of payment, which means I have to use rotating access to accounts previously compromised by others to receive and conduct payments, it can be dangerous, the algorithms developed to detect suspicious transactions are always changing, there is no way of knowing if we have been flagged, I always assume that my transactions trigger some alarm somewhere. Transactions in person are also dangerous, with all the cameras everywhere. If I pay electronically from a physical location I inevitably leave a digital trail for the cameras to investigate. On the other hand, getting real money to pay cash also comes with its own set of challenges, the only advantage is that that you don't have to do it as often if you withdraw a large amount of cash. But obviously withdrawing large

amounts is also likely to trigger algorithms of suspicious behaviour. I ended up having to rely on local black market contacts. Which is very risky, I don't recommend it. I've had to move cities several times because of this. In Eastern Europe it's beautiful, everything becomes easier when there are cryptocurrency machines with guaranteed anonymity in various parts of the city. The volatility of the value is significant, but at least I don't have to hack communications towers to get the 2FA mobile phone codes needed for a transfer, which opens another way for someone to triangulate my position. It's a shame there aren't as many contracts available on Hacker Trade for Eastern Europe now, otherwise I'd stay there full-time. When I had to withdraw money physically I did it with disruptive regularity, never at the same ATM, except when I repeated an ATM on purpose to confuse the pattern detection. I implemented a recurrently counter-intuitive pattern generator for that. Even then I only went to the ATM at night, wearing hoodie and my dynamic screen mask that randomly generates fake identities. They are becoming illegal in most countries but it's worth the risk. If the card code isn't processed under 23 seconds at the ATM, I walk. I've lost a few cards because of this, but it's better to play it safe and strictly abide by the rules of encrypted, disposable internal independence. It keeps me safe.

"*Historical figures today pointed out by the ACP (Anti-Corruption Party) government spokesman, the famous Hacker Trade whistleblower portal has reached the lowest numbers of missions transacted on Portuguese territory in the last decade, I quote the spokesman: Clear signs that the anti-corruption revolution has fulfilled its objective, we now live in a transparent country, when there is nothing left to point out that we don't all already know, we stop needing people to point it out for us.*"

I tried to get a full proof new identity with verifiable background checks a few months ago. It wasn't deep enough, it was compromised by a hacker when I used it to access healthcare to treat a tooth that had been bothering me. I had to abandon that identity and now the system has my appearance (and partial dental records) in the suspect records. Took me several months to put the identity together, losing it was painful. That's when I decided to hitch-hike back to Paris, even though there are barely any Hacker Trade jobs left there now.

Prices have become quite competitive to obtain new identities, especially the credible ones, they are in high demand, governments and especially hired hackers are more strict with their background checks now, everyone is looking for a payday revealing forged new identities. I see some for sale but I always wonder if they are not a decoy, so I keep trying to make my own.

My dream now is to be still live anonymously but with a social security number, a history of studies that is resistant to scrutiny, a paid taxes record, a history of house rent and a dental record that fails the algorithm matching percentage for my real teeth that the dentist will still consider a common mistake and treat me without triggering an alarm. The older I get, the harder it becomes to come up with a real fake identity, systems keep changing and there's always an hacker like me trying to find holes in other people's stories to earn their credits. I've been looking for vulnerabilities in various systems, to see if one day I can create my own identity without being detected. But a lot of others have thought of the same thing, they've created systems with redundancies and stricter access controls, they're in another league of hacking, I can only move forward when I have access to all systems at the same time. While I was trying to try to find a vulnerability for the social security servers, the healthcare system's security got updated and now I have to start looking for vulnerabilities there aswell...

Maybe I could just stop being a hacker, stop living in the streets anonymously. Just walk to the social security office, give them my real name and ask them to regularise my situation. Compromising all the rules of internal encrypted and disposable independence that are keeping me safe. I'd probably get matched to some Hacker Trade contract in a few minutes. Maybe they'll put me in a glass house with no access to the internet and a bed with no humidity spots... Sometimes I think it probably wouldn't be that bad as a retirement plan, I could maybe go back to school and participate in tech papers that I can't currently submit. Maybe Victor is even monitoring those databases and I'd get back in touch with him? But more likely, I'd be recruited for forced labour in mercenary cybersecurity so I'll keep abiding by the rules of encrypted, disposable internal independence. This keeps me safe.

Good practices for the real world

These tales are speculative fiction, but much of the technology mentioned in them is real. Here's a good practices guide to help you reflect and consider ways to improve your own digital privacy security:

Physical access to the user's machine

The simplest way to digitally spy on someone is to have physical access to their machine or private network where it is connected.

With physical access one can either steal the machine (to access it later with more time and leisure) or install devices that read the network traffic from the machine (with a low probability of being detected), it can also make it easier to access the data on the computer's hard disc (if it isn't properly encrypted), and it may even be possible to install software on it that allows a third party to see and hear everything that happens on the machine.

It is advisable for machines with important private data to be kept in places with proper physical access control. Behind doors with locks, under private surveillance cameras, installed in places where it is not trivial for someone to access or manipulate without being identified.

It is also advisable to encrypt the data on the disc (using Veracrypt for example), keeping regular encrypted backup copies of the most critical information and storing them in duplicate in physically separated but equally secure locations.

And most obviously, having a secure password to access the computer.

Mobile phones are also machines, they can also be accessed and manipulated. Treat them with equal care. Evermore mobile phones are a prime target for vulnerabilities and attacks.

Operating system

Everything we do on the machine can be observed by the operating system installed. There have been recurrent reports of Microsoft, Apple, Google and other operators abusing access to private data. Because they

are the most widely used systems, they are also constant targets for new malicious software applications.

New anti-virus applications or Artificial Intelligence assistants want to access all the data in the operating system "so they can help us", so make sure these surveillance systems aren't installed when you don't need them. There is no guarantee that they will respect and protect your private data.

The least privacy-intrusive and spyware-targeted operating system is still Linux, and there are several distributions to choose from with greater or lesser focus on privacy and data encryption.

Equally important is to use different accounts for different types of access. All properly protected with a secure, separate access password. Don't leave your machine with your sessions open for others to use. They don't need access to your bookmarks, password files, automatic logins, emails, private documents, etc.

Browser

Most online activity nowadays involves using a web browser to navigate different pages. Most browsers store browsing cookies that can be used in conjunction with machine and browser information to uniquely identify the person using the computer.

Logging to your browser in the cloud to share shortcuts and accesses from your sessions on another computer can be useful, but it also opens the possibility of unauthorised access by third parties. All that information is stored in servers located in an unknown to you data center that could be accessed by third parties if they are not being properly protected.

Most web pages also host adverts as a way of monetising their content, these adverts are used as an additional layer of identification of the user, collecting data about your browsing habits which is then sold to third parties.

For better online security and privacy it's recommended using browsers without cookies (incognito mode), using ad blockers (such as adblock), or browsers with a greater focus on privacy (there are several free ones in constant development, find one that best suits your use).

Email

For convenience, most people use free email accounts from major operators. Many of them don't use encrypted traffic when transmitting emails.

Unencrypted traffic can be read by Internet service operators or other malicious agents present on the network. It is also known as common practice for large operators to parse the content of your emails to improve their algorithm for selling you adverts, train AI models, etc. With no guarantees of who actually has access to your information, while they are known to have agreements with certain government agencies to have backdoor access to your accounts. The PRISM project exposed by Snowden in 2013 is just one example of what we now know.

For those who have nothing to hide, it doesn't really matter who is reading your private emails, but if you live in a country where journalism and democratic activism are actively repressed, there is a real danger in sending an email with content that someone in power doesn't appreciate.

The most private alternative is to use your own properly encrypted email servers (which come with their own challenges and costs) or use email services such as protonmail that have a known record for prioritising privacy.

Another best practice is to use separate mobile phones and email accounts for different uses. The most obvious example is to separate your personal life from your work environment, but apply the same logic to other points of interest that don't require your personal information. Multiple email accounts are more of a hassle to manage and set up, but they ensure that there is no cross-referencing of information between your different online personas focusing on different interests.

Avoid obvious names for disassociated e-mail accounts. If you use first and last names or always the same login name on all your accounts, it becomes trivial for third parties to associate the person with their e-mail or to guess their login name on other websites.

If you're creating an account on a website that you'll never use again, consider using a disposable temporary email account generator, there are several available online.

Another of the most common problems with using email are phishing emails, where someone sends a message asking the user to click a link or run an application or script. These types of emails are designed to trick people and their dangers are real: these links typically contain vulnerabilities that allow third parties to gain remote access to your machine and private information. It is important to always consider the legitimacy of who is sending you an email, and when possible use email servers with spam filters that flag or filter out this type of malignant content.

Internet access network

The Internet access network is one of the most exploited layers for violating privacy. Both at the local network level and at the Internet service level.

If the traffic leaving your computer isn't encrypted, any machine with access to the local network can read it. The internet service provider itself can also read any traffic that passes through its system. And even when the data is encrypted in transmission and we have guarantees that our used internet service provider is not spying on its users, nor is it compromised by any third parties who might be doing so, and it does not have any agreements with the government to facilitate access to this type of information, the entry and exit points of the encryption may still be compromised, eavesdropping, or serving as an access identifier: If we know that a person accesses their computer 3 times in one day using an anonymization service and 3 times the same day at coinciding times some activity appears on a given website, after a certain number of coincidences we can infer with some certainty that the activity comes from that person being monitored. Advances in pattern recognition systems makes these things trivial to monitor.

There are various protections that can be used to minimize the problem, but they all involve trade-offs and none of them are 100% secure. Using a trusted VPN or routing your traffic through Tor helps a lot to anonymize your traffic, but they are not invulnerable solutions and using

them slows down all your browsing due to the extra steps that it requires to go through, so it's quite inconvenient to use when you just want to quickly check something online.

Other recently announced projects such as Veilid promise better security in the future but are still under development.

Social networks

Social networks are some of the most popular websites on the internet right now. They are dangerous on several levels. The most obvious one are the users voluntarily sharing in public forums information that should be considered private.

Another issue is requiring multiple accesses on different machines and public networks (when using someone's WiFi on a mobile phone for example), which all increases the chances of one of them being compromised and someone gaining access to your account and it's data.

The third major issue is the common setting of weak access passwords, usually so that they can be easier to remember or entered faster or even shared amongst multiple users. Reusing the same password on several websites, another serious security issue commonly being exploited.

Some social network websites have password recovery questions that can in some cases be obtained by someone who vaguely knows the person. And often these systems do not enforce 2FA (two factor authentication) to confirm access.

If all this wasn't enough, the messaging systems of these websites are typically unencrypted (any machine on the network can read the message), they are recurrent targets of malicious attacks due to their popularity (which means a greater chance of our private data being accessed illegitimately) and most of them have agreements with the government to facilitate access to any accounts suspected of criminal offences without any accountability for potential abuse.

This type of websites also tend to require you to submit a photocopy of an identity document and a telephone number of yours to confirm that you are a real person. Thus retaining important identifying information about their users that should not be legally required to use the website.

I recommend not using these types of websites. If you can't live without them there are some frontend alternatives to guarantee access to the content with better anonymity / privacy, check for example the projects Invidious or Piped.

Mobile phones

Mobile phones are increasingly the target of security attacks. They are computers all the same and have the similar vulnerabilities that desktop and laptop computers do. In some cases perhaps even more so, as they have more services that transmit private information activated by default. GPS being the most obvious, the operator knows where the mobile phone is at all times.

The phone number always being officially associated with a real identity with an associated name and proof of address in the system makes the mobile phone a conspicuous unique identifier. This makes mobile phones with disposable numbers the only way to have any real privacy.

But there are other uses for mobile phones that also leave a trace:

- the active bluetooth or WiFi hotspot service can be used to geotag the person's travel history in more detail than GPS already does, airports and large shopping centres have systems that actively use this data

- the memory of visited WiFi networks can indicate georeferenced associations to third parties in forensic analysis

- telephone contact details stored "in the cloud" on unknown servers can be obtained by third parties

- private messaging conversations via services that are not encrypted by default leave the entire conversation open to eavesdropping by third parties

- the compulsory 2FA by SMS on certain web pages requires you to have your mobile phone switched on and with you at a moments notice

The mobile phone turns out to be one of the most vulnerable points of individuals' digital privacy in today's society. It's fascinating how everyone carries one in their hand or pocket, just ready to be lost or stolen.

Conclusion

It's quite inconvenient to guarantee our digital privacy and anonymity online.

Real anonymous privacy would imply a strict separation of accesses in machines, networks and accounts that could identify the user. It's not enough to use your neighbour's internet and believe you're now invisible, you have to use another computer, another phone number, another email account and social network accounts. Effectively be someone else located somewhere else, at the same time that you're not being monitored for doing anything suspicious.

In day to day use, we don't have to be that radical in order to avoid the most common problems; we can easily reduce our risks and concerns with some simple actions and habits:

- Avoid publishing private data on public websites

- Use secure complex passwords, don't reuse logins and passwords on multiple websites

- Do not give temporary access of your account or machine to others

- Use more privacy-aware operating systems, browsers and applications

The most important thing is to be aware of the problems and dangers that come with all the advances in technology that we now use on a daily basis. Stay informed and always demand your right to privacy.