A threat to democracy

Mass surveillance

Pieter Omtzigt, Tirana, 27 May 2026

Table of Contents

A course on dictatorship

Today, we shall start the course ‘How to become a dictator 1.01’. It has been a popular course lately on planet Earth with quite a few gifted graduates. The course is not particularly new. After all, dictators and autocrats perform some of the oldest professions in the world.

After this introductory course, the course ‘How do I stay a dictator’ is compulsory for a certificate. After all, dictators know that becoming a dictator is not the hardest part, but staying one is. And it is compulsory to remain a dictator or, at the very least, make sure that a person you absolutely trust takes over the helm. That is why both North Korea and Azerbaijan have converged into a form of hereditary dictatorship.

In other historical periods, we would call them royal families. However, since they still want to pretend that they are a social state or a democracy, it is impossible to formalise it in the constitution.

If somebody else takes over, the former dictator risks spending the rest of his life in prison or, if he is lucky, in exile.

Lesson 1 of how to become and stay a dictator is very simple. You have to take two necessary steps.

The first is to take over the State's crucial institutions. So, make sure parliament, the judiciary, the media, and the armed forces are loyal to you.

The second step is to ensure that no one dissatisfied with your new government can topple it.
There are a few crucial differences between these two tasks. The institutions you need to take control of are known. The places of dissent are both known and unknown.

The second step has historically been very difficult and expensive. The dictatorships of the twentieth century established a vast apparatus to spy on and eavesdrop on all citizens.

Hitler took years to set up the SS, the Gestapo, the SD, and other parts of the state apparatus to monitor, quell, and crush dissent. Concentration camps were used against enemies.

Immediately after the establishment of the Soviet Union, Lenin founded the Cheka, which decades later would become the KGB. They ran it the same way: the police had both normal police tasks and political police tasks. Camps (Gulags) and mass informers were used to instil fear and control society. In certain waves, the oppression was extremely violent. In the great purge of 1937-1938, more than 700.000 people were executed.

Other dictatorships ran similar security apparatuses: the Securitate in Romania and the Stasi in East Germany. These methods were never just European: the Khmer Rouge in Cambodia or the Videla regime in Argentina had similar methods.

The security apparatus of these dictatorships was very large, and the costs were enormous. The Stasi in Eastern Germany employed 91.000 full time employees and hundreds of thousands of informers. It kept files on 6 million citizens, or 1 in 3 of the population.

Preventing dictatorships

After World War II, the political elites realised that establishing dictatorships had to be made more difficult through political design.

Hitler's takeover of German democracy had been relatively easy. The main act in the takeover had been a democratic, non-violent act.

After the fire at the Reichstag, he sensed his opportunity. He had a minority in parliament and needed a 2/3 majority for this law.

This one short law, the Ermächtigungsgesetz – enabling law - was passed on March 23rd, 1933. It enabled the German government to enact laws without the consent of parliament. It enabled the government to enact laws that were not in line with the constitution and to sign treaties without parliament's approval. It ended democracy in one vote.

From that point onwards, the real function of parliament had been abolished. The government was able, for instance, to abolish all political parties.

The remedy after the Second World War was clear: put up guardrails to prevent this from recurring.

One of the Guard rails was the establishment of the Council of Europe and the European Convention on Human Rights. Every citizen has access to the Court in Strasbourg if their rights are trampled on. Countries could start an interstate case against each other. The mechanism is not foolproof, but it helped restore democracy in Greece after the 1974 coup. It did not prevent member Russia from sliding into autocracy.

Guard rails were introduced in the countries themselves. Germany introduced eternity clauses in the constitution, which cannot be changed. It established an office of the public prosecutor, which is the most independent on earth. A strong constitutional court is a further check on the government.

The guardrails prevent easy takeovers and have been the focus of extensive academic research and political action.

Mass surveillance has become a market product

Political action and academic research have not focused as much on the second part: how to prevent a security apparatus from being built.

Taking over institutions has always been a challenge, and it still is, with or without guardrails. But setting up mass surveillance has rapidly become easy, cheap, and accessible to domestic governments, foreign governments, and other groups, including criminals.

Running mass surveillance requires neither massive financial resources nor mass human resources. It does not even require people on the ground close to potential targets. Until recently, physical proximity was necessary to plant devices. That is no longer the case.

Countries use spyware and other modern technologies (AI, drones), but so do criminal groups, like drug cartels. They possess huge capabilities in terms of mass surveillance, used to secure their own terrain and supplies, and to attack law enforcement agencies or any unwanted guests or journalists.

Mass surveillance is used to some degree by corporations, which track all internet activity via cookies, store data on your phone calls and travel destinations, and even ask for your permission to track you on your phone permanently.

Just consider, for instance, how weird that is: before the introduction of smartphones, no parent could track every move of a child. It is a sign of growing up and becoming independent that you are invisible to your parent for longer periods. Nowadays, large corporations can follow every mouse click, obtaining very private information about our deepest preferences, desires, and secrets. Showing the websites you visit, I can guess whether you are addicted to gambling or porn, what your political preferences are, and your sexual preferences.

If you tell me your AI questions, I can see which diseases you fear, maybe whether you have a fight with your husband or friend.

Mass surveillance is ubiquitous and comes in many forms.

The number of devices usable for eavesdropping has exploded

Anybody who can hack the mobile phone and see all the text, listen to all the conversations, check every bank statement and payment, read every mail, see the medical and tax data, basically knows everything. Since the rise of Pegasus, these devices have been perfected and are now available to everyone.

Any device with a camera and a microphone can, and has been used, for eavesdropping. That means modern televisions, computers, doorbells, robot lawn mowers, and robot hoovers. And these are devices you bought yourself.

The public space is full of cameras with face recognition technology, so either the government or anyone who can hack systems can set up rudimentary systems of mass surveillance.

You do not even need to hack. In the US, televisions now send a screenshot of the screen back to the manufacturer every minute under their user license. If you are using it as a big screen for your journalistic investigation, then surveillance is legal!

Countries eavesdrop elsewhere

The ability to eavesdrop does not stop at borders. The Snowden revelations show that the United States has mass surveillance programs for the whole planet.

Israel admitted that it had hacked the cameras in Tehran and could make accurate observations without people on the ground.

It is not infallible

Israel clearly has one of the most advanced surveillance systems in the world and applies it to Gaza. Yet, it missed the October 7 massive security attack and Hamas invasion of Israel proper.

Technology itself, without proper human intelligence, clearly failed to spot it and prevent the Hamas atrocities.

Why should we be worried?

I may tell you why this is so worrying. Eavesdropping does not occur only in autocracies. Extensive eavesdropping practices take place in countries that qualify as democracies.

For 22 years, I was an MP in the Netherlands and a Member of the Parliamentary Assembly of the Council of Europe. For the last few years, I have been a member of the parliamentary supervisory committee for the Dutch secret services.

Over the last 12 years, I have conducted extensive research into eavesdropping within the Council of Europe and have spoken to whistleblowers and people who have been subjected to eavesdropping.

In 2014, I wrote a report on Massive Surveillance and Snowden for the Parliamentary Assembly of the Council of Europe, and I was the first MP to hold a hearing with him via video. The extent of his revelations in 2013 is still mind-boggling.

Over the last few years, I have written reports in Europe on Pegasus and similar software to hack phones. For that, I spoke to many victims and questioned all 47 Member States.

We noticed that many countries hacked phones of political opponents: Poland, Greece, and Spain are well-known examples, but the practice was widespread. Both left and right-wing governments are implicated, countries we consider democratic and autocratic.

The public's casual acceptance of eavesdropping is shocking.

Richard Nixon, president of the United States, had to resign over Watergate, in which the Republican Party eavesdropped on the Democratic Party and won the presidential elections.

The present-day methods are, if anything, more intrusive. The political consequences are way less consequential. In Poland, the PiS government hacked the phones of political opponents during election times, used and abused the material, won the elections, and continued governing.

The present-day methods are incredibly effective. It suffices to describe just one of them.

China and Uygurs

Since at least 2017, China has had an incredibly efficient, massive surveillance program in place against the Uyghur people. They are Turkic Muslims living in the Xinjiang region.

The Chinese authorities use mass surveillance. Using data from mobile phones, biometric data such as iris and face scans, tracking cars, and tracking every payment and movement, algorithms are used to select people.

Examples of suspicious behaviour include: not socialising with neighbours, using encrypted apps like WhatsApp, donating to mosques, or using more electricity than usual.

Based on this data and on ethnic profiling, the Chinese authorities have detained hundreds of thousands and possibly more than a million people. This detention is arbitrary, and ill treatment and sexual violence take place, as well as forced labour. People disappear, and family members living abroad face intense pressure.

The UN concluded in 2022 that this may constitute crimes against humanity. The United States went further, both under Trump-1 and Biden, and determined that China commits genocide.

Earlier this year, I visited China, and to my surprise, CloudWalk, the company that conducts mass surveillance and is blocked in the US, demonstrated its technology to us.

On large screens, officials can track people in flats in real time using face recognition. It felt dystopic, worse than the books of Orwell or Huxley.

In the pictures, you see their sales room to sell this technology for scanners at customs, on money machines, and even for the sale of drinks. There is no doubt that there is a big market for it.

Democracies

The key worry is that both dictatorships and democracies are using eavesdropping to a greater extent than publicly acknowledged.

There are two reasons democracies resort to mass surveillance: it is cheap, and they face legitimacy problems. And sometimes there are real concerns about security, in large-crowd situations, like in football stadiums.

On top of that, the Corona period accelerated the use of mass surveillance methods.

The methods are cheap

Eavesdropping methods have become both more invasive and cheaper, as we noticed before. It has also been possible to run several programs without adequate democratic supervision.

Democracies are backsliding

Democracies get their legitimacy both from the democratic process and from the outcome, that is, do the policies deliver the public goods or not?

Let’s start with what you think is the basic idea of democracy, and then measure how major Western democracies are failing.

Process legitimacy

We think of democracies as countries where citizens elect their representatives in a parliament, unicameral or bicameral. The executive is either elected directly by a popular vote or is a logical outcome of the parliamentary elections.

Major laws, like the budget, are approved by a majority of MPs.

The executive is itself subject to the law and is not exempt from it.

Most democracies have built-in pressure valves to ensure outcomes remain available in exceptional circumstances. A budget is always needed, and the judiciary should not be able to derail the executive, so democracies build in escape clauses for exceptional circumstances. These have been normalised.

Let's take the three Western democracies with a permanent seat at the United Nations.

The French constitution, in article 49,3 allows the French government to pass laws without the approval of parliament. The instability of the Fourth Republic led to the introduction of this clause in 1958. Parliament can only reject the law by a vote of no confidence, that is, by dismissing the government of the day (but not the president). In essence, the majority of budget laws, social security laws, and major reforms now pass this way. This means that parliament is not fulfilling its primary function, namely approving annual budgets. Politicians do not have to take responsibility for spending and outlays.

Parliament not adopting a budget was meant to be the exception and has become the rule.

In the UK, Prime Ministers like Thatcher, Major, and Blair governed for more than a term, won an election, executed policies and reforms, and were judged on them at the next election. Since David Cameron's resignation in 2016, the UK has frequently changed Prime Ministers. Liz Truss was PM for less than two months. Truzz and Sunak never even managed to obtain a mandate at a general election. The result is that the electorate does not elect the leader, who can be in power long enough to change policies and show the results. This essential part of the election and policy implementation has effectively broken down.

Changing a Prime Minister was meant to be the exception and has become the rule.

In the US, the constitution grants the president the power to pardon federal offenses. Trump is the first president to use mass pardons and has used them for the January 6 insurrection.

Recently he struck a deal with his own attorney general on a leak of his tax return, which not only granted him a large sum of money but also shield him, his family and his company from scrutiny by government agencies for the rest of his life. Together with many other actions, he has ended being subjected to almost any law in the United States.

Pardons were meant to be the exception and have become the rule. That rule is now accompanied by a large ban on investigations of the president.

Outcome legitimacy

Apart from procedural legitimacy, outcome legitimacy has also decreased substantially.

Governments have borrowed large sums of money, and all three have state debt well above 100% of GDP. This is unheard of, except in the aftermath of a war. Yet, large social problems persist, and governments are no longer able to deliver the public goods the electorate desires.

The combination of a lack of outcome legitimacy and procedural legitimacy makes it attractive for a government to control the population.

A democracy was meant to be exactly the opposite, namely, the population scrutinises the executive!

Normalisation of mass surveillance – COVID-19

During the COVID-19 pandemic, many countries introduced surveillance systems to monitor the behaviour of all their citizens. Poland, for instance, used facial recognition software to monitor home quarantine. Almost all countries had curfews.

This is not the place to discuss the necessity or effectiveness of these measures.

States that acquire certain powers and instruments rarely relinquish them voluntarily afterwards. So both the public and the states became accustomed to what should have been an exceptional situation.

Whistle-blowers are crushed

States react strongly to revelations of mass surveillance. I have communicated with all Western states on this topic, and the responses have been strong.

There are good reasons for this: governments know that mass surveillance is illegal under their own laws, and they know it turns upside down who would control whom.

And most of the time, eavesdropping is also done partly in the interest of state security, and that always provides an excuse.

Several cases will illustrate this reaction.

Edward Snowden

Edward Snowden was a contractor of the US security agency NSA. The access he had to NSA documents was a rather big breach of internal security.

His revelations require hours, but a few key takeaways.

The NSA had direct, secret access to data from major internet firms. There was hardly any oversight on it. The NSA collected metadata on phone records on a massive scale. Basically, there is mass surveillance on the US population at large.

The NSA tapped straight into the internet backbone and collected worldwide data, including American data, and used it.

And the NSA spied on foreign heads of state, including US allies.

The result: Snowden was charged under the Espionage Act, a broad, vague law that carries huge penalties and chilling effects. He was forced to flee to Hong Kong and then to Russia and has never been home since.

Julian Assange

WikiLeaks published leaked documents, showing, for instance, how in 2007 the US killed many civilians, including two Reuters reporters in Baghdad, in a military strike.

The Vault-7 disclosures showed the enormous capacities of eavesdropping.

Assange had to go into hiding in the Ecuador Embassy in London. He was apprehended in 2019 and spent 5 years in high-security prison Belmarsh in the UK, as the US requested extradition. The chilling effects of this case are clear.

Alexander Litvinenko

Alexander Litvinenko was a former Russian Spy who was poisoned by Polonium in the UK and died a truly agonising death. The European Court of Human Rights ruled that the Russian state is responsible for his death.

Many people forget why the Russian regime committed this act.

Putin, a KGB man, became Prime Minister in 1999 and later the acting President. This was a chaotic period in Russia. He was unknown. Within two months, bombs in and around Moscow

killed 300 people. Putin blamed Chechen rebels and started a war there. He restored order and was elected president.

Litvinenko claimed that the KGB was behind the bombing. His claims are credible because, in a case where bombs did not go off, the KGB was caught red-handed placing explosives.

He wrote a book about it, which was prohibited, and duly fled the country.

Special care for victims and support networks

Being the subject of eavesdropping causes enormous stress: every detail of your life can be leaked to the press. You lose control over your own life.

The workshop on coping with this stress during this conference is an absolute necessity, I can tell from personal experience. Talking about it, even with close friends, can be difficult.

An agenda

You probably expect solutions from me for this situation.

The honest answer is that there is no quick solution, as eating from the forbidden fruit has been an irresistible temptation in human history. And however poisonous this fruit is, it tastes extremely good.

Showing the poisonous nature is the only option. It will not come from international politicians.

Yesterday, there was the first statement of a head of State with great moral authority, the Pope, who describes the dangers eloquently:

“171. A further risk, less visible but no less serious, is the social control enabled by the massive collection of data and the use of algorithmic systems. When every action — movements, purchases, relationships, and preferences — leaves a trace, a new form of power emerges: the power to profile, predict, and influence behaviour, often without individuals being fully aware of it. If such kinds of data are used to make decisions affecting concrete opportunities — such as access to credit, employment, or essential services — there is a risk of undermining freedom and discriminating against the most vulnerable. Furthermore, control is exercised not only through explicit prohibitions, but also through the architecture of visibility: what is amplified or rendered invisible, what is rewarded or penalised, ultimately shapes opinions and choices, fostering conformity and self-censorship.

For this reason, freedom in the digital age is not merely a matter of interiority but also a public concern. It calls for clear rules, transparency, the possibility of recourse, and proportionate limits

on the use of intrusive technologies, so that technology will remain at the service of the human person and not become a form of control over consciences."

So, what could we do:

1. Keep describing the dangers, including the chilling effects

2. Raise support for international measures. Even the leading voices in Silicon Valley, such as Elon Musk, have called for a moratorium on development. So, you are not alone.

And treaties on banning land mines or banning biological warfare once seemed impossible, until they were done. Sure, maintaining those obligations is extremely difficult to control, but without a discussion, we will not get there.

3. Engage with politicians, especially those who have been subject to these methods. They understand the consequences.

This conference could not be timelier. Thank you for organising it.