The Impact of Spyware on Fundamental Rights, Democracy, and Electoral Processes

Intervention before the European Parliament's PEGA Committee of Inquiry

Thursday, 27 October 2022

Intervention by Iverna McGowan, Secretary General of CDT Europe

CHECK AGAINST DELIVERY

Mr. Chairman, Members of the Committee, Members of Parliament, esteemed colleagues. I would like to begin by thanking the Committee of Inquiry for this invitation to address you today. Hearing the views of civil society will be crucial to ensuring human rights compliant and binding solutions to the threats that Spyware poses to human rights, democracy and the rule of law.

For those of you who are not familiar with the organisation that I represent, the Centre for Democracy & Technology Europe is a not for profit organisation that advocates for the promotion and protection of democracy and human rights in European tech law and policy. We champion policies, laws, and technical designs that protect against invasive, discriminatory, and exploitative uses of new technologies. We advocate for private companies to be more transparent, accountable, and respectful of human rights. Our work also focuses on curtailing government censorship and enabling all people to access and share information of their choosing without harassment or undue interference.

My intervention today will focus on three points. Firstly, I would like to examine more broadly the implications of unlawful surveillance for democracy, human rights and civic space; secondly, I will lay out some of the particular challenges that spyware can pose in the context of electoral integrity; and thirdly, I will provide some reflections in relation to the EU Dual Use Regulation. I will conclude with some concrete action points that the Inquiry could forward in line with its mandate to prevent such infringements on rights going forward.

Unlawful Surveillance and the Threat to Human Rights and Democracy

As you heard from our colleagues this morning, unlawful surveillance violates the right to privacy, and can also violate the rights to freedom of expression, opinion, association, and peaceful assembly. The European Court of Justice insists upon a strict necessity and proportionality test on State-led surveillance before it can be deemed to be lawful. Indeed, both the European Court of Human Rights and the European Court of Justice insist upon the limitation of surveillance only to what is strictly necessary. It is important to understand then, that surveillance that has been conducted through the use of state-hacking tools such as those that NSO group provided is an extraordinarily invasive and generalised form of surveillance, and

therefore would *de facto* not meet either of the Courts' standards, nor the requirements under international human rights law. This is why it is particularly worrisome that this Inquiry has already heard that such tools have been both used within the EU, and exported out of the EU.

We must also remember the reasons why our Courts so staunchly uphold the right to communicate securely, and so carefully consider any derogations from it. The right to communicate securely is a foundation upon which the key pillars of democracy are built. This includes press freedom, the presumption of innocence, privacy and freedom of expression and association, and indeed the very ability to hold free and fair elections.

A vibrant and critical civil society is a prerequisite for a strong and resilient democracy. The pandemic has fast-forwarded digitalisation meaning that across the globe, hundreds of thousands of people are now organising online to fight racism and to protect the planet. However, there has also been a backlash against these demands for societal change and against the power of online organising. Civil society actors across Europe have witnessed online smear campaigns and the stigmatisation of their organisations, staff, as well as personal attacks on those working on the frontlines to protect the rights of others. Already in 2019, the EU Fundamental Rights Agency Report on civic space in the EU found that three of the four most common threats and attacks on civil society actors took place online. It can be seen as no small coincidence then that the primary victims of the PEGASUS scandal were journalists, whistleblowers, human rights defenders and political opponents. These actors all have crucial roles to play in defending democracy and human rights, but it is because of this very role, speaking truth to power at their own peril, that such actors are likely targets of smear campaigns and related hacking operations. Spyware such as PEGASUS poses an existential threat to civic space and with it our democracies and the rule of law.

Unlawful Surveillance and the Threat to the Integrity of Electoral Processes

A vibrant civic space is also imperative to running free and fair elections, as is the ability to communicate securely. Being spied on can inhibit people's ability to organise and campaign and has a detrimental impact including a chilling effect on freedom of expression and association.

Hack-and-leak operations can pose a serious threat to election integrity. It should be stressed that information lawfully obtained about any candidate that would be in the public interest is a normal part of the cut-and-thrust of election campaigning and important to a vibrant democracy. At the same time, as my fellow speaker has attested to, hack-and-leak operations - where information is unlawfully obtained through spyware or phishing attacks and which are often accompanied by smear campaigns - must be examined more critically. As we have heard, in Poland in 2018 PEGASUS spyware was used to hack political opposition members, and then that information was doctored before being used as part of a smear campaign. In 2016, Russian hackers released hacked emails from Democratic officials, rocking the U.S. presidential election. In 2017, a similar hack-and-leak operation released thousands of documents on Emmanuel Macron, just hours before the start of the French election period media blackout. The methods and actors that carried out these different hack-and-leak operations may be different, but the

tactics and the impact are similar. A week is a long time in politics; an hour can be a very long time in the context of an election. The timing of such hack-and-leak campaigns tends to be at the 11th hour, just before polling starts, therefore inhibiting the victims from restoring their reputation in time before the vote. Effective remedy after an election has already been called is also more difficult to achieve. According to the international election standards principle of equal suffrage, it is imperative that different arms of the State remain impartial towards candidates and political parties. As we can see then such Spyware poses an extraordinary danger to elections whether used by unauthorised actors or by governments against political opponents or dissidents. This is why it is all the more important that we regulate effectively to control the dissemination and use of these tools in accordance with human rights standards. The EU Dual Use Regulation is designed to help control the export of such surveillance technologies, but what about their use within the EU?

Micro-targeting

Another factor that can have implications on election integrity is the harvesting and exploitation of user data from social media accounts for purposes of targeting ads and other election-related content. We must include this particular type of unlawful harvesting and surveillance of people online in our analysis given its serious implications for election integrity. The Cambridge Analytica scandal resulted in disclosures and uses of data at the expense of user privacy on a mass scale. By responding to seemingly innocuous quizzes via their Facebook pages, users unwittingly gave access to third-parties that harvested their data. Installed Spyware similarly results in unconsented disclosure of data, and when installed on a broad basis, as with Pegasus, can lead to massive privacy violations. Stolen data can be used to manipulate what content and information people see online. User surveillance and targeting in this way can have a devastating impact on universal suffrage, the right to vote to all adult citizens, regardless of wealth, income, gender, social status, race, ethnicity, or any other restriction.

This is because such targeting can be used to conduct voter suppression campaigns, whereby the personal data is used to target people and discourage them from exercising their right to vote. Minorities and communities of color are unfortunately a typical target of this particular technique. With the use of personal and demographic data it is possible to run a campaign providing false information on election procedures or dissuading a targeted group from exercising their right to vote. The EU is already taking action in response to this challenge, through the EU Digital Services Act and now the Online Political Ads proposal. Together with numerous other civil society organisations and the European Data Protection Supervisor, we have recommended a phasing out of targeted advertising based on pervasive tracking and prohibition of microtargeting in the context of political advertising. Phasing out of tracking and micro-targeting will require restrictions on the use of Spyware as well as robust implementation of current EU legislation on data protection.

Potential of the EU's Dual Use Regulation

The United Nations Office of High Commissioner for Human Rights has called for States to impose a global moratorium on the sale and transfer of surveillance technology until they have

put in place robust regulations that guarantee its use in compliance with international human rights standards. With this, and the objectives of this Inquiry in mind, our organsation is in the midst of conducting research into the implementation of the EU's Dual Use Regulation. We hope that this research can inform better on how export controls could be tightened, and on the broader question of what other measures might be necessary to protect human rights. The Regulation is essential to the integrity of the EU's Foreign human rights policy, and in the future could be a tool to ensure that the findings and recommendations of this Inquiry can go beyond the European region and take on global proportions. This Inquiry has already heard allegations that PEGASUS spyware was partly exported from EU countries. During the negotiations on the recast of the EU's Dual Use Regulation and since, CDT and our civil society partners already highlighted some of the shortcomings with the recast Regulation namely:

- The very narrow definition of cybersurveillance items.
- The weakness of the catch-all-call control clause which can be easily vetoed by member states.
- The lack of precision regarding which human rights concerns should be taken into account both when applying the new catch-all control clauses, and when member states are deciding whether to approve exports of cybersurveillance items.
- Insufficient transparency measures.
- Language on due diligence that is not in line with human rights norms.

I would like to briefly focus on this last point for a moment. The United Nations Guiding Principles on Business and Human Rights require that companies take proactive steps to ensure that they do not cause or contribute to human rights abuses within their global operations, and to respond to any human rights abuses when they do occur. In order to meet that responsibility, companies must carry out human rights due diligence to "identify, prevent, mitigate and account for how they address their human rights impacts." Since this revision of the Dual Use Regulation much has happened in the development of the concept of due diligence under EU law. The results of our research will provide the opportunity for more in-depth analysis, but we can already consider the need to strengthen the due diligence obligations on States and private companies with regard to export controls.

Members of the Inquiry, while the regulation of surveillance technologies is an essential step, we must also ensure that Europe protects the technology that enables secure communications in the first place. Regulation of technologies used to gain access to private communications can only be effective if the communications are, in fact, private. We are concerned that the detection requirements in the proposed Regulation on Child Sexual Abuse now before Parliament would make it impossible for providers to offer private messaging services when they are encrypted end-to-end. I would welcome any questions you may have about the privacy impact of this proposed regulation.

Conclusions & Points of Action for the Inquiry

Esteemed colleagues. As I hope I have demonstrated today, the right to communicate securely is a keystone in the arch of European democracy. I would appeal to the Inquiry to focus both on the broader need for safeguards on security of communications, rule of law checks on State surveillance as well as the particular aspect of surveillance technologies.

Our recommendations to this Inquiry would be:

Strengthen Oversight Over State Surveillance

- Insist upon the upholding of international human rights standards with regard to State-led surveillance, and ensure independent, impartial investigations where there is reason to believe this is not the case.
- Be critical about whether law enforcement itself is sufficiently independent and impartial to lead such investigations given its possible implications in what has already occured.
- Call on the European Commission to broaden the scope of its annual rule of law report to include an analysis on reprisals against journalists and human rights defenders, and include reports of unlawful surveillance against members of civil society.
- Highlight the critical importance of tools such as end-to-end encryption to the protection of civic space and democracy more broadly.

Increase Accountability of Corporate Actors

- Phase out targeted advertising based on pervasive tracking and prohibition of microtargeting in the context of political advertising.
- Revise and strengthen the provisions of the EU Dual Use Regulation on corporate due diligence and on human rights impact assessments.
- Consider what further regulation would be required to control domestic trading of Spyware.

Immediate Actions to Stop Adverse Effects of Spyware

- Call for a moratorium in the EU and for exports out of the EU on the sale and transfer of surveillance technology until they have put in place robust regulations that guarantee its use in compliance with international human rights standards.
- The EU should put NSO on its global sanction list and take all appropriate action to prohibit the sale, transfer, export, import and use of NSO Group technologies, as well as the provision of services that support NSO Group's products, until adequate human rights safeguards are in place.

Members of the Inquiry. We implore you to act urgently, as if democracy and human rights depend upon it - because they do.