urban forum

Zoom and the EU security

Transcript of the Online Forum

In cooperation with

SINOPRESS

urban forum
Egon Matzner-Institut für Stadtforschung

Panelists

Speakers

Hannes Heide

Bernd Herger, BSc

Dr. László Flamm

MMag. Sascha Mundstein

Organizing Representatives

Dr. Bernhard Müller, BA, MPA
Urban Forum

Prof. Helena Chang, MA
Sinopress

Moderator

MMag. Alice Schmatzberger

10th July 2024

Impressum:
Urban Forum –
Egon Matzner-Institut für Stadtforschung

Tel.: +43/2622 21132 | Fax.: +43/2622 21388 E-Mail: office@urbanforum.at | www.urbanforum.at
Neunkirchner Straße 15/7, 2700 Wiener Neustadt
ZVR-Zahl: 169347700 | Titelseite: © Bigstock

Transcript

Moderator: Distinguished panellists, ladies & gentlemen, a warm welcome to the Online Forum on "Zoom and the EU security". This Forum is initiated and organised by Dr. Bernhard Müller, Secretary General of Urban Forum, Egon Matzner-Institute in Austria and Prof. Hui Chang, Overseas Researcher (Austria) of Non-Traditional Security and Peace Development Research Center, Zhejiang University. My name is Alice Schmatzberger. I'm honoured to be your moderator for today´s forum.

Today, we have the following distinguished panelists all with their respective expertise.

1. **Hannes Heide**, Member of the European Parliament
2. **Bernd Herger**, Vienna Education Academy
3. **László Flamm**, EuropaHaus Budapest
4. **Sascha Mundstein**, Harvard Graduate, IT Expert

Thank you all for joining us in this forum to share your experience, knowledge and expertise with us.

Before we start our rounds of talk, allow me to give a short introduction to today´s agenda concerning Zoom and the EU security:

A popular online video conference platform, Zoom has been widely used in Europe. But last year, the "Big Brother Award", a negative price for surveillance by the civil rights organization Digitalcourage in Germany, was given to Zoom in the "Communication" category. Based in the USA, Zoom is subject to the cloud act, the Patriot Act and the FISA Act, which means that it must pass on all data from non-US citizens to the US secret services. As a matter of fact, Zoom has presumably, in comparison to Cisco Webex Meetings or Microsoft Teams, much more power and scale in collecting personal and cooperate data. Out of security concerns, the majority of administrative institutions in Europe avoid using Zoom.

In today's discussion, we will concentrate on the question "Is Zoom compliant with EU data protection regulation?"

I would like to invite all panellists to offer your expertise opinions on this issue. But first, I would like to invite Mr. Hannes Heide to the floor.

Mr. Heide, as is known, the majority of administrative institutions in Europe avoid using Zoom. Instead, they use Cisco Webex Meetings. In fact, we know that before the corona time, EU-levelled online meetings forbade using Zoom. Why? Does it mean that in comparison to other online tools, Zoom raises more serious concerns about the compliance with data protection regulations for Europe?

Hannes Heide: Thank you very much for the opportunity to be with you, giving me the possibility to listen to your experiences, too. I hope my answer to your question will satisfy you and fulfill your expectations.

First of all, I would like to note that I can only talk about the use of videoconferencing tools in the European Parliament. The European institutions have been working with Cisco Webex for a long time, which is based on a contractual relationship combined with high security standards and permanent evaluation. This also includes the European Court of Justice, where a particularly high level of protection is required. The fact that a company's software is used by an institution on the basis of a contractual agreement is a completely normal procedure – for example, Microsoft products are consistently used as the operating system in the offices of the European Parliament.

However, I would like to point out that there is no longer an explicit ban on the use of Zoom in the European institutions: There are so-called "multimedia stand-up positions" in Strasbourg and Brussels, which allow MEPs to record short statements, video messages and interviews. In the Multimedia Stand-up positions, it is possible to participate in any kind of videoconference (Zoom, Skype, Webex) as journalist or when interviewing a MEP remotely. I recently used this tool myself for a live contribution in a conference, and I was completely free to choose which video conferencing tool I wanted to use.

Let me briefly introduce my work in the European Parliament so far. I have been working in the Committee for Culture and Education, which also deals with media freedom. I have been also working in the Regional Development Committee and in the Budget Control Committee. For the security in the European Union, I have worked as a coordinator and a

shadow rapporteur in the Investigative Committee on Surveillance for the use of surveillance fibre in the European Union. This might have a bit of relationship and a connection with today's topic.

As I said, I cannot confirm that there is a general ban on the use of Zoom in the European Parliament. For the back streaming from committees and from plenary sessions, we stand by the European Parliament itself with its own infrastructure, on cameras and on sound systems. If connected with experts or lecturers, it's primarily done with Webex. But it's also possible with other tools. Another example of my own group, the S&D group, uses Interactual because of the possibility for simultaneous translation. But within Interactual, other translation services can use this tool, too, like Zoom.

This is my experience as a Member of the European Parliament. If there is an official use in the parliamentary work, we use Webex. But it's open for us which tool or system we use in other situations.

Moderator: Thank you very much, Mr. Heide, for this insight into the practice of the European Parliament. If I got it right, there is a diversity of potential platforms you are able to use, a diversity concerning online media applications. But there is also security standard under permanent evaluation, is that right?

Hannes Heide: Yes. If you have a look at my apps, you see that I have 5 platforms.

Moderator: Thank you again, Mr. Heide! We know now more about the present situation within the EU concerning the use of different online media platforms.

In this context, I would now like to invite Mr. Bernd Herger to offer his expertise from the technical aspect of Zoom.

Mr. Herger, Zoom enjoyed rapid increase of popularity during the pandemic years. Meanwhile, it has been found with severe security gaps, e.g. the undesirable penetration of internet trolls into video conference talks, data protection injuries such as the sale of Zoom account details via the Dark Web etc. Is Zoom technically negligent or immature?

Bernd Herger: Zoom's popularity grew significantly during the pandemic, which highlighted the importance of secure online communication. Initially, Zoom faced serious security issues, such as "Zoom-bombing," where internet trolls disrupted meetings, and the sale of account details on the Dark Web. These incidents suggest that Zoom was technically careless and perhaps not fully developed in its early stages.

Firstly, Zoom's security setup was not designed to handle such a massive increase in users. The simple sharing of meeting IDs without additional checks made it easy for unauthorized individuals to join meetings. This lack of strong security measures led to significant problems and privacy violations.

Additionally, Zoom had several privacy issues, such as data not being fully encrypted initially. There were also reports of data being shared with third parties without explicit user consent, raising serious concerns about data protection practices.

However, Zoom has responded to these issues by implementing several security improvements. These include end-to-end encryption, better authentication methods, and enhanced privacy settings. Today, there are many settings that users must configure to ensure their sessions are secure. For example, meeting hosts can now require passwords, enable waiting rooms, and restrict screen sharing to specific participants.

Nevertheless, the responsibility for security does not lie solely with Zoom. Users also play a crucial role. It is essential for users to use strong, unique passwords, regularly update their software, and carefully configure their privacy and security settings. Without active participation from users, even the best security measures cannot provide complete protection.

As an example, I have personally experienced an attack during a Zoom session where disturbing images were shown. But this session was publicly advertised, making it easy for malicious individuals to disrupt it. While it was a distressing experience, it is not fair to blame Zoom entirely. The session's public nature made it vulnerable, and unfortunately, there is a lot of criminal energy in the world.

Moderator: So, during the Pandemic, its easy access gave Zoom – despite security concerns – the market power. Zoom was, however, not prepared for this sudden quantity of users. In your opinion, Mr. Herger, Zoom has to guide its users more through the security modulation, while its users should take more care in using the platform, e.g. in password setting, etc. Thank you very much for this valuable input, Mr. Herger!

Today, we have also an expert from EuropaHaus Budapest, Mr. László Flamm. I'm curious about the use of Zoom in Hungary, Mr. Flamm. Do Hungarians pay much attention to the data collection by online video conference platforms like Zoom? Is Zoom frequently used by Hungarian companies and administrative institutions?

László Flamm: As for the attention to data collection, it was not typical of Hungarians before the outbreak of Covid-19. However, the situation changed in the months following the Pandemic.

On March 13, 2020, the Hungarian government decided to close physical schools to switch to digital distance education. Furthermore, home-office was introduced, in whichever sector it was possible. As a result, Zoom became one of the most popular services in Hungary.

But in a short time, serious problems arose from the use of Zoom, which the company itself acknowledged, too. More and more security and data protection concerns as well as questionable practices about the Zoom were identified one after another. Violation of users' privacy connected to database preservation and non-erasable data were mentioned in this regard, which drew the attention of security experts, various domestic Hungarian and international organizations such as the FBI.

As a result of the proliferation of security concerns by an immense number of Hungarians, special attention to the importance of security and data collection by the Hungarians increased very quickly. This trend was particularly felt in large corporations, and in the world of education including schools, colleges and universities, too. They have been widely and frequently exposed to undesirable internet trolls and data protection injuries.

Moderator: Thank you very much for sharing with us, Mr. Flamm. It seems there are many questions to the security of using Zoom. I would like to now invite Sascha Mundstein to deepen the look into this. Mr. Mundstein, you are an IT expert in industry. What is your opinion on the technical security of Zoom? What does industry think about it?

Sascha Mundstein: From my experience in various IT-departments in industry and numerous software companies, I can echo the general sentiment that Zoom is not trustworthy.

We have observed the accelerated growth in the use of Zoom during the COVID pandemic, and it stands to reason that the company had problems adjusting to this fast expansion. As is common in many cases, security then comes as an afterthought.

Zoom, in particular, is subject to US laws so it keeps recordings and logs of all activities and conversations, which is required by the US legal authorities but illegal according to European law. From a technical point of view, when a customer demands the deletion of data, it is simply marked as deleted but can still be retrieved. Another blatant dishonesty by the company was that they claimed "end-to-end" encryption on their website, which means that the company and anyone in between does not have access to the exchanged data. At the state of their technology in 2020, it was all but impossible to encrypt a video conversation with more than four participants. They quietly removed the claim from their website.

Other companies do offer real client-side end-to-end encryption, but these are usually paid services.

Most larger companies have abandoned Zoom in favor of more established market players, such as Webex and Teams. (Teams has its own problems, but the dominant position of Microsoft has led to significant market share right off the start.) Webex has been in the market for more than ten years and is used by the German military and big many big corporations and government agencies. Solid video communication solutions in terms of security will not be free, but with affordable paid subscriptions, a high degree of privacy protection is possible.

Moderator: These hard facts sound shocking. Thank you very much for your input, Mr. Mundstein!

Allow me now to pose a follow-up question to Mr. Heide. During the Pandemic where free movement was much limited, the European Commission began to use Zoom platform for "non-sensitive online workshops and webinars", despite the fact that Zoom is not an officially approved IT solution for use by the Commission's departments. How to define non-sensitive and sensitive in the context of EU meetings, Mr. Heide?

Hannes Heide: Before explaining the view on the definitions of non-sensitive and sensitive content, I would like to tell you what kind of meetings take place within the European Parliament, which might explain what is sensitive or non-sensitive. There is high interest in the work of the European Parliament that information being available, and that everybody has the opportunity to follow debates, plenary sessions and committee sessions.

So, there are a lot of cameras in all our meeting rooms. They're not there for security reasons. They are there so that citizens can have the opportunity to follow the debates. But we have other kinds of meetings, for example, meetings of the political groups where one talks about content strategy and the political work. It's clear that there is no interest that they be public and that people get in. For such meetings, there is only limited audience. We have working groups on different committees on different issues and topics. We have negotiations on political level as well as on technical level, which of course should not be in public. And we have coordinators' meetings. These are the people on political level who negotiate on reports, on papers and even on acts of law.

As a Member of the European Parliament, I am not an expert in this field. Our IT experts at DG ITEC, which means directorate-general for innovation and technological support, are highly qualified and reliable when it comes to assessing security issues related to technical infrastructure. And the European Commission is constantly re-evaluating the contractual agreements that involve the international transfer of personal data. The assessment is based on various parameters. And as you have mentioned and as you are aware of, the re-assessment is closely linked to Zoom's end-to-end encryption white paper. The Commission clearly stated the following:

"Given the company's recent commitment to security, controls and improved encryption, the Commission considers the risks of using Zoom for non-sensitive conferencing or educational purposes mitigated".

Coming back to the question of what is "sensitive" or "non-sensitive", I would like to point out that a lot has changed in the post-Covid era. For the past two years, all plenary sessions and committee meetings have been held in person again, which is why most of the video conferences I have attended since then have been more informal in nature. In my experience, the ratio of which video conferencing tool be used is very balanced and it usually depends on which medium one of the two sides has premium access to. As Cisco is a contractual partner of the European Parliament, Webex can be used by MEPs without restriction and is therefore often preferred for the organization of webinars.

Moderator: Thank you for offering us the insight of the EU regulations, Mr. Heide! I didn't know much of it until you made it clear for us all.

Tackling further with the IT aspects of today's topic, I'd like to invite once more Mr. Herger to the floor. Mr. Herger, according to the analysis by IT experts, the stored information by Zoom for companies includes the name of the administrator and the account ID, billing data and the profile, the recording location of the file, the users' operating systems and much more. How does this conflict with the EU regulations?

Bernd Herger: Well, the EU's General Data Protection Regulation (GDPR) imposes strict rules on data collection, processing, and storage to protect individual privacy. Zoom's extensive data collection, including administrator names, account IDs, billing data, and various user device details, raises significant concerns regarding GDPR compliance.

The GDPR requires that personal data be collected only for specific, clear, and legal purposes. Zoom must clearly define why each piece

of data is collected and ensure this is communicated transparently to users. For instance, storing data such as MAC addresses and IP addresses must have a justified purpose that aligns with the services provided.

Plus, the principle of data minimization under GDPR mandates that only the necessary data for the intended purpose should be collected. Zoom needs to demonstrate that all the collected data is essential for its services. Collecting excessive data without clear justification can be considered a violation of GDPR.

Moreover, GDPR emphasizes the need for strong security measures to protect stored data. Zoom must ensure that the collected data is safeguarded against unauthorized access and leaks. This includes implementing encryption, regular security audits, and limiting access to sensitive information.

An essential aspect of GDPR is obtaining informed consent from users. Users must be clearly informed about what data is being collected, how it will be used, and who it will be shared with. Users must actively consent to this data collection.

Processing data without explicit user consent can lead to serious GDPR violations.

While Zoom strives to comply with GDPR, users also bear significant responsibility. Choosing providers with transparent privacy policies and European standards is crucial. By making informed choices, users can help steer the market towards better data protection and security practices.

BUT a major issue is the lack of strong European alternatives to Zoom. Many major platforms in all fields are from the USA, China, or Russia, such as Meta, TikTok, and Telegram. Europe has yet to develop competitive IT products, leading to reliance on foreign providers whose privacy standards might not meet European requirements. This highlights the need for greater investment and innovation in the European tech sector to ensure better alignment with GDPR and enhanced digital sovereignty.

It is becoming increasingly difficult to extend European laws to other parts of the world. To protect European users' privacy and security effectively, it is essential to have strong European competitors in the IT sector. This would reduce reliance on foreign services and ensure that data protection aligns with European standards.

The development of robust European IT solutions is, therefore, not just a matter of convenience but a necessity for maintaining control over our data and ensuring compliance with our laws.

Moderator: This is a clear and very important statement made by you, Mr. Herger! Thank you so much for this initiative. The development of robust European IT solutions is indeed a necessity, as you said.

Mr. Flamm, allow me to raise another question to you: Supposedly a so-called VPN in front of Zoom can disguise the IP address. Is this an option which gives Zoom an argument for using the software in accordance with the data protection requirements of the EU?

László Flamm: In my opinion, the mere use of a VPN in front of Zoom does not automatically guarantee compliance with the EU's data protection requirements. Here's why:

First, purpose and legal basis: Zoom would need to clearly define the purpose for using a VPN in its data processing activities. The legal basis for processing personal data (such as IP addresses) must align with the General Data Protection Regulation principles.

Second, transparency: Zoom should inform users about the use of VPNs and their impact on data processing. Transparency is crucial under the GDPR, and users should be aware of how their data is handled.

Third, data minimization: Zoom should minimize the collection and processing of personal data, including IP addresses. And as I mentioned earlier using a VPN can help protect user privacy, but Zoom must still adhere to data minimization principles.

Fourth, security measures: While a VPN enhances security, Zoom must also implement other security measures to safeguard personal data. Encryption, access controls, and regular security assessments are essential in this respect.

Fifth, international data transfers: If Zoom processes data across borders, for example between servers within EU and outside the EU and European Economic Area, then Zoom must comply with GDPR provisions related to international data transfers.

In summary, while using a VPN can contribute to data protection, I would say that Zoom's overall compliance depends on a comprehensive approach that considers legal requirements, transparency, and security practices. And Zoom does not meet the EU data protection requirements. There are also connections and interplay between civil rights, data protection and privacy and security risks. These connections are multifaceted and critical in today's era of digital transformation. In my opinion, the use of Zoom weakens the connections between the European citizens' sense of security and respect for their privacy.

However, it should also be noted that the EU does not have its own app like Zoom, Google Meet or Microsoft Teams. Therefore, it would be necessary that the EU found its own development company and better support a common European IT industry.

Moderator: Now the consensus on this forum is more and more clear: Zoom is being used by the European Parliament for "non-sensitive" conferences, even though there are, in the eyes of IT experts at least, quite serious technical gaps away from the EU data protection requirements. As Mr. Herger and Mr. Flamm pointed out, the EU should have its own IT solutions instead of using platforms like Zoom to guarantee the security of the EU citizens. Mr. Heide, as a member of the EP, maybe you can bring up our consensus at the EU meetings when the opportunities arise? Thank you, Mr. Heide!

Dear panelists, I would like to sincerely thank you for sharing your in-depth expertise and experience today at this forum on the subject of "Zoom and the EU Security"! To close today's forum, allow me to give the floor to Mr. Müller from Urban Forum for his closing remarks. Mr. Müller, the floor is yours.

Bernhard Müller: Ladies and gentlemen! I am delighted that Urban Forum has once again cooperated with Prof. Helena Chang

from SINOPRESS for successfully organizing an international online forum in 2024.

The beginning was not easy for webinars. But we are happy to have been able to hold these forums since April 2021 and have always had great experts from different European countries, as we do today again.

During the forum today, we mentioned that the civil rights organization Digitalcourage delivered the "Big Brother Award" last year to Zoom in the "Communication" category. The ground is that Zoom, based in the USA, is subject to the cloud act, the Patriot Act and the FISA Act, which means that it must pass on all data from non-US citizens to the US secret services.

This fact might be little known to the public. As a result of the Pandemic and the restricted ability to hold events, Zoom has experienced a real boom as it is really easy to use.

Today, we discussed the technical and legal details as well as the concerns of the European Union. As a guest speaker today, Hannes Heide, member of the European Parliament, presented his view on the things at European level in great details. From a European perspective, we should endeavor to provide and to operate a communication platform in accordance with European standards, legislation and data protection guidelines. The debate on Zoom shows that our continent is often looking for its way between the world's major powers and sadly, has not yet found one.

However, a strong Europe is essential for a peaceful, social, ecological and prosperous world. With the international online forums, we as organizers strive to make a small contribution to the mutual understanding of each other and to a willingness in talking across national borders.

Again, many thanks to all for the valuable contributions to the discussion! Wish you a relaxing summer!

10th July 2024