UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

Testimony of Ronald J. Deibert to the House of Commons of Canada's Standing Committee on Procedure and House Affairs regarding its study of Parliamentary Duties and the COVID-19 Pandemic

April 29, 2020

I am Ron Deibert, Professor of Political Science and founder and director of the Citizen Lab* at the University of Toronto's Munk School of Global Affairs & Public Policy. Our research at Citizen Lab includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities. I submit these comments in a professional capacity representing my views and those of the Citizen Lab.

***

As much of the world moves into work-from-home rules and self-isolation, technology has become an essential lifeline. However, this sudden dependence on remote networking has opened up a whole new assortment of security and privacy risks. In light of these sudden shifts in practices, it is essential that the tools relied on for sensitive and high risk communications be subjected to careful scrutiny.

In what follows, I first provide a summary of the Citizen Lab's recent investigation into the security of Zoom's video conferencing application, and the company's responses. I then discuss a broader range of digital security risks that are relevant to the work-from-home routines that MPs and their staff are following. Finally, I conclude with six recommendations.[1]

Citizen Lab Research on Zoom Security

On April 3, 2020, the Citizen Lab published a report on a technical analysis of the confidentiality of communications on the popular video chat application Zoom.[2] On April 8, we released a followup report with details of a security vulnerability in Zoom's waiting room feature.[3]

---

[1] Thanks to Christopher Parsons, Lex Gill, and Josh Gold for comments and assistance.
[2] Bill Marczak & John Scott-Railton, "Move Fast and Roll Your Own Crypto: A Quick Look at the Confidentiality of Zoom Meetings," *The Citizen Lab*, April 3, 2020, https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
[3] Bill Marczak & John Scott-Railton, "Zoom's Waiting Room Vulnerability," The Citizen Lab, April 8, 2020, https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/

Our initial report found that the encryption in Zoom did not seem to have been well-designed or effectively implemented, and that its public documentation made several misleading claims about Zoom's encryption protocols that did not match what we observed in our analysis. I invite those with interest to see the full details as outlined in our report.[4]

We also found potential security issues with Zoom's generation and storage cryptographic information. While based in Silicon Valley, Zoom owns three companies in China where its engineers develop the Zoom software. In some of our tests, our researchers observed encryption keys being distributed through Zoom servers in China, even when all meeting participants were outside of China. A company primarily catering to North American clients that distributes encryption keys through servers in China is very concerning, given that Zoom may be legally obligated to disclose these keys to authorities in China.

In our report published on April 3, we noted that we also discovered a security issue with Zoom's "waiting room" feature. Specifically, we found Zoom servers provided both the encryption keys and a live video stream of the Zoom meeting to all users in the meeting's waiting room, even if the waiting users had not been approved to join the meeting. This issue would enable an arbitrary, unauthorized Zoom user in a waiting room to intercept and decrypt the "encrypted" video content.

In response to our research and concerns raised by other parties, Zoom has taken a number of actions regarding security.[5] Zoom has committed to a 90-day process to identify and fix security issues, including a third-party security review, enhancing their bug bounty program and preparing a transparency report.

In direct response to our research, Zoom acknowledged the concerns we raised about their use of non-industry standard encryption and committed to making improvements, including working towards the implementation of end-to-end encryption. Zoom also acknowledged that some Zoom users based outside of China would have connected to data centres within China, and indicated they had immediately put in place measures to prevent that from happening.

---

[4] In our report of April 3, we found that Zoom documentation claimed that the app uses "AES-256" encryption for meetings where possible. However, in our testing, a single AES-128 key was used in ECB mode by all meeting participants to encrypt and decrypt audio and video. The use of ECB mode is not recommended because patterns present in the plaintext are preserved during encryption. What this finding means is that the encryption in Zoom does not seem to have been well-designed or implemented.

[5] Colleen Rodriguez, "Zoom Hits Milestone on 90-Day Security Plan, Releases Zoom 5.0," *Zoom Blog*, April 22, 2020, https://blog.zoom.us/wordpress/2020/04/22/zoom-hits-milestone-on-90-day-security-plan-releases-zoom-5-0/

On April 8th, Zoom released a new version of their client that added additional security features. Zoom CEO Eric Yuan indicated in a video webinar that this new version fixed the waiting room security issue we identified.[6] He also announced that Zoom had established a CISO Council and Advisory Board to assist with their privacy and security practices, and had hired former Facebook Chief Security Officer Alex Stamos as an advisor.

It is important to underscore that we did not test Zoom's HIPAA/PIPEDA-compliant healthcare plan, or the ZoomGov software that is used by some government agencies. These platforms would require additional analysis.

While it is encouraging that Zoom is working to improve their product, the sudden reliance by a very large number of people on a platform that was never designed for highly-sensitive communications is symptomatic of a much larger set of problems related to work-from-home routines.[7] It is imperative that we evaluate all of the risks associated with this sudden change in routines, and not just those associated with one particular application.

Security Risks Related to Work-From-Home Environments

Legislators working from home are connecting using devices, accounts and applications through widely differing home network setups, as are their staff. These networks may be shared with roommates and family members, whose own digital security practices could collaterally affect their own security, and the devices which are being used are likely loaded with applications that can access large volumes of sensitive information. Whereas in the pre-COVID era, these devices were routinely brought back into the government's security perimeter where sensors might detect aberrant network behavior, this will no longer be the case. Consequently, adversaries might linger on networks and devices indefinitely, and obtain more data from targets than in a pre-COVID world.

The communications systems that we rely on have rarely been designed with security in mind. Security has either routinely been regarded as slowing the speed of innovation or impossible to impose on essential systems that have chronic failings and which would require total redevelopment of communications infrastructures to become "secured." The consequence is that there is a vast array of unpatched systems that leave persistent vulnerabilities for malicious actors to exploit. These risks extend right down into the most fundamental layers of our shared infrastructure. For example, telecommunications and cell phone networks still rely on a decades-old information exchange

[6] "Ask Eric Anything," (YouTube Video), *Zoom*, April 8, 2020, https://www.youtube.com/watch?v=TeohYK-hsO4
[7] See John Scott-Railton, "Another Critical COVID-19 Shortage: Digital Security," *Medium*. March 23, 2020, https://medium.com/@_jsr/another-critical-covid-19-shortage-digital-security-374b1617fea7

protocol, called SS7, that has been shown to be highly insecure and prone to abuse and illegal surveillance, including when sending second-factor authentications over mobile phone networks.[8]

Meanwhile, governments and criminal enterprises have dramatically increased their capabilities to exploit this ecosystem for a variety of purposes. Almost all nation-states now have at least some "cyber espionage" capabilities, with many in the top-tier being exceedingly well-resourced and routinely spending billions of dollars on clandestine influence and intelligence-gathering operations. There is a vast and poorly regulated private market for cyber security that includes numerous companies that provide "off-the-shelf" targeted espionage and mass surveillance services.[9] Citizen Lab's research has shown that the market for commercial spyware in particular is proflierating widely, and is highly prone to abuse (including being linked to targeted killings),[10] with sophisticated hacking tools ending up in the hands of despots and dictators.[11] These relationships may well open the door to the same tools being deployed against legislators and their staff in jurisdictions like Canada. As a result, the government must be wary of seemingly less competent adversaries punching well above their weight by using private and commercial hacking tools.

At the best of times, these problems present extraordinary challenges for network defenders. But parliamentarians and their staff are now at even greater risk. Not surprisingly, threat actors are already capitalizing on this new environment. Phishing and malware attacks have targeted and disrupted hospitals in the Czech Republic, the U.S. Department of Health and Human Services, and the World Health Organization. On April 14, a leading U.S. cybersecurity firm revealed that a "Canadian government health organization actively engaged in COVID-19 response efforts, and a

[8] Stephanie Kirchgaessner, "Revealed: Saudis suspected of phone spying campaign in US," *The Guardian*, March 29, 2020, https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us

[9] For further detail, see testimony by Ron Deibert on this subject to the Senate of Canada on November 30, 2016, here: https://sencanada.ca/en/Content/Sen/committee/421/ridr/52951-e.

[10] Research by The Citizen Lab has revealed several cases of targeted killings linked to targeted espionage and surveillance software, including the murder of Saudi journalist Jamal Kashoggi. For further information on this, and other cases, see for example: Miles Kenyon, "Dubious Denials & Scripted Spin: Spyware Company NSO Group Goes on 60 Minutes," *The Citizen Lab*, April 1, 2019, https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/.

[11] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak, and Ron Deibert, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," *The Citizen Lab*, September 18, 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

Canadian university conducting COVID-19 research," had been victims of ransomware attacks.[12] These reports are likely only scratching at the surface.

While it is laudable that a platform like Zoom has received a lot of attention about security risks, we should not lose sight of the fact that our entire communications ecosystem contains numerous insecurities, and that there are a multitude of bad actors searching for and seeking to exploit them.

Recommendation #1: Where possible extend digital security resources developed for the House of Commons (HoC) to all Canadians

Remote work for the HoC will require a significant investment in additional digital security support, resources, and capacity. These teams were already engaged in actively protecting members of the HoC and are now dealing with a significantly broader set of home network and device setups, while simultaneously defending against a tsunami of targeted malware and other attacks that are outside of the government's formal security perimeter.

To partially combat new threats, the CSE's Canadian Centre for Cyber Security has begun sharing information with infrastructure providers to reduce the likelihood of phishing or malware successfully exploiting devices and systems.[13]However, the details of this program (and others like it) presently lack public accountability or transparency, and it has not been independently audited. If these are rolled out without proper safeguards, such systems can end up undermining free expression, privacy, and other rights. Wherever possible, the HoC and the rest of government could share mitigation techniques or signatures to Canadian infrastructure owners *in a transparent and accountable way* to both improve the home security of MPs and HoC staff, as well as all other residents of Canada.

Additionally, distributing and encouraging the use of educational tools to all parliamentarians, their staff, and all residents of Canada could help boost awareness and help mitigate risks.[14]

Recommendation #2: Evaluate and issue guidance on work-from-home best practices, including those for video conferencing applications.

---

[12] James McLeod, "Canadian coronavirus response workers targeted in ransomware attack, says U.S. cybersecurity report," *Financial Post*, April 14, 2020, https://business.financialpost.com/technology/canadian-coronavirus-response-workers-targeted-in-ransomware-attack-u-s-firm

[13] Canadian Centre for Cyber Security, "Canadian Shield – Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic," April 23, 2020, https://www.cyber.gc.ca/en/canadian-shield-sharing-cyber-centres-threat-intelligence-protect-canadians-during-covid-19.

[14] Some resources to consider include the Citizen Lab's *Security Planner* (https://securityplanner.org/) and the Electronic Frontier Foundation's *Surveillance Self Defense* project (https://ssd.eff.org/en).

The Government of Canada should issue detailed guidance on work-from-home best practices that includes a detailed evaluation of video conferencing applications. The latter could include recommendations on scenarios for use of some applications for specific purposes but not others. Such guidance could be made available to Canadians to assist medium and small businesses, as well as individual residents of Canada, make decisions that are informed by security expertise from the government. Although some guidance has been issued already,[15,16] these are dated, and largely insufficient to the tasks at hand.

By way of contrast, the U.S.'s NSA has issued public guidance that identifies various criteria to consider when using a video conferencing service.[17] These criteria include, *inter alia*, whether the service uses end-to-end encryption; whether they share data with third parties; and whether or not the service's source code has been shared publicly. Other assessments consider questions of transparency and privacy, for example whether firms issue transparency reports or have clear privacy policies.[18]

Recommendation #3: Support independent research on digital security and the promotion of secure communications tools.

At a time when daily life significantly depends on technological systems, there should be more high quality, independent research that scrutinizes these systems for privacy and security risks. To assure Canadians that the digital appliances and networks upon which they depend are secure, researchers must have the ability to dig beneath the surface of those systems, including into proprietary algorithms, without fear of reprisal.

Presently, researchers can come under legal threat when they conduct this research, to the detriment of improving security for all users, including MPs and their staff who are at home. As such, we recommend that the Government of Canada pass legislation which explicitly recognizes a public

[15] Canadian Centre for Cyber Security, "Considerations when using video-teleconference products and services," April 3, 2020 (amended April 14), https://cyber.gc.ca/en/alerts/considerations-when-using-video-teleconference-products-and-services.
[16] Canadian Centre for Cyber Security, "Cyber Hygiene for COVID-19," March 18, 2020, https://cyber.gc.ca/en/guidance/cyber-hygiene-covid-19.
[17] Existing assessments of various video teleconferencing applications could be built on. See, for example, guidance from the US National Security Agency issued on April 24, 2020: (https://media.defense.gov/2020/Apr/24/2002288652/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-LONG-FINAL.PDF).
[18] See, for example, assessments by Freedom of the Press (https://freedom.press/training/blog/videoconferencing-tools/) and Google engineer Gary Belvin (https://medium.com/@gdbelvin/covid-19-and-cybersecurity-e9ee5cba6de7)

interest right to engage in security research, and prohibits organizations or individuals from legally threatening residents of Canada who are involved in such public interest research.

Recommendation #4: Implement a Vulnerability Disclosure Process for Government Agencies, including the House of Commons

Vulnerabilities disclosure policies (VDPs) establish terms and processes by which researchers can communicate the presence of vulnerabilities in organizations' systems or networks without fearing legal repercussions. American institutions, such as the Department of Defense,[19] have already adopted a VDP and additional American institutions are developing them. Canada should follow this model, so that researchers can identify and work with the government of Canada to mitigate vulnerabilities, instead of declining to communicate them out of fear they may experience legal (or other) threats. This recommendation is in line with a report issued by the HoC Public Safety and National Security Committee in 2019, where it recommended that, "the Government of Canada support responsible vulnerability disclosure programs."[20]

Recommendation #5: Transparent and Accountable Vulnerabilities Equities Process

The Communications Security Establishment (CSE) currently has a process by which it evaluates whether to conceal the presence of computer software vulnerabilities for use in its own intelligence operations, or to disclose a given vulnerability to ensure that all devices are made secure from it. However, the CSE is formally alone in making decisions over whether to retain or disclose a vulnerability.

We recommend that the Government of Canada broaden the stakeholder institutions who adjudicate whether vulnerabilities are retained or disclosed, especially in light of the enhanced risk that all government workers are at given their work-from-home situation. We also recommend that the Government of Canada follow international best practice and release a full vulnerabilities equities process policy, so that residents of Canada can rest assured that the CSE and its government will not retain vulnerabilities that could seriously compromise the security of Canadians.

[19] Department of Defense Cyber Crime Center, "DoD Vulnerability Disclosure Program (VDP), November, 2016, https://www.dc3.mil/vulnerability-disclosure.
[20] SECU, "*Report 38: Cybersecurity in the Financial Sector as a National Security Issue*", Adopted by the Committee June 17, 2019, https://www.ourcommons.ca/Committees/en/SECU/StudyActivity?studyActivityId=10450263. See recommendation 7, page 38.

Recommendation #6: Support for Strong Encryption

In 2019, the HoC Public Safety and National Security Committee recommended that "the Government of Canada reject approaches to lawful access that would weaken cybersecurity."[21] Given the potential for adversaries to take advantage or poorly-secured devices and systems, we recommend that the Government of Canada support the availability of strong encryption so that MPs, their staffs, and residents of Canada can be assured that the Government is not secretly weakening this life-saving and commerce-enabling technology, to the detriment of all Canadians and our allies.

---

*The Citizen Lab is an interdisciplinary laboratory focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. We use a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. We are currently investigating topics about digital security risks related to the COVID pandemic, including detailed analyses of security and privacy issues related to contact tracing apps, investigations into COVID-related censorship[22] and disinformation practices, and comparative analyses of health-related emergency measures that may adversely impact human rights.

[21] SECU, "*Report 38: Cybersecurity in the Financial Sector as a National Security Issue*", Adopted by the Committee June 17, 2019, https://www.ourcommons.ca/Committees/en/SECU/StudyActivity?studyActivityId=10450263. See recommendation 8, page 39.

[22] Lotus Ruan, Jeffrey Knockel, and Masashi Crete-Nishihata, "Censored Contagion: How Information on the Coronavirus is Managed on Chinese Social Media," *The Citizen Lab*, March 3, 2020, https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.