THECITIZENLAB

Research and development at the intersection of
digital media, global security, and human rights

Contents

About the Citizen Lab

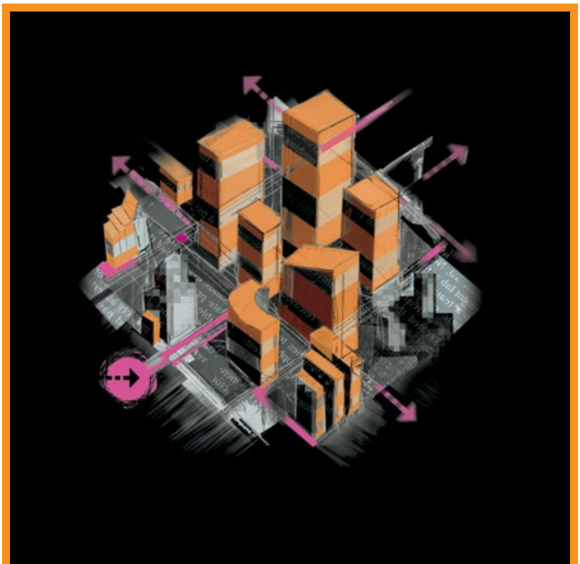
The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of **digital technologies**, **human rights**, and **global security**.

Our mission is to produce **evidence-based research** on cyber security issues that are associated with human rights concerns.

We use a **mixed methods approach** to research, combining practices from political science, law, computer science, and area studies.

We are **independent** of government or corporate interests and publish evidence-based, peer-reviewed research. We evaluate the ethical and legal implications of all of our projects.

Our **research** includes: investigating digital espionage against civil society; documenting Internet filtering and other practices that impact freedom of expression online; examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data; and analyzing privacy, security, and information controls of popular applications.



> *"The university has an important obligation to protect the Internet as a forum for open access to information and free expression. I see the mission of the Citizen Lab to help fulfil that obligation through careful, evidence-based research."*

— **Ronald Deibert**, Founder and Director, The Citizen Lab

Research

Since 2001, the Citizen Lab has researched and documented information controls that impact human rights and the openness and security of the Internet. Our goal is to inform the public while meeting high standards of rigour through academic peer review.

We study how governments and the private sector censor the Internet, social media, or mobile applications and have done extensive reporting on targeted digital espionage on civil society. We have produced detailed reports on the companies that sell sophisticated spyware and networking monitoring technologies, and document their abuse to raise corporate social responsibility concerns.

Our research can be broken down into several categories:

Targeted Threats: Investigations into the prevalence and impact of digital espionage operations against civil society groups and other high-risk targets.

Free Expression Online: Studies of Internet filtering, network interference, and other technologies and practices that impact freedom of expression online.

Transparency and Accountability: Examinations of transparency and accountability mechanisms that pertain to the relationship between corporations and state agencies regarding personal data disclosures and surveillance activities.

Apps and Privacy Controls: Analyses of privacy, security, and information controls of popular applications.

Targeted Threats

THE CITIZEN LAB CONDUCTS comparative analyses of targeted threats against civil society through close partnerships with human rights organizations that face a growing spectrum of online threats, including: Internet filtering, denial of service attacks, and targeted malware attacks. These groups can be particularly vulnerable to such attacks due to limited IT resources and lack of digital security awareness. Through this research, we are gaining a better understanding of the technical and social nature of these aggressions and the political contexts that may motivate them.

SELECTED REPORTS:

- *Spying on a Budget: Inside a Phishing Operation with Targets in the Tibetan Community* (January 2018)
- *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware* (December 2017)
- *Reckless Exploits* (June – August 2017)
- *Tainted Leaks: Disinformation and Phishing with a Russian Nexus* (May 2017)
- *Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender* (August 2016)
- *Packrat: Seven Years of a South American Threat Actor* (December 2015)
- *Pay No Attention to the Server Behind the Proxy: Mapping FinFisher's Continuing Proliferation* (October 2015)
- *You Only Click Twice: FinFisher's Global Proliferation* (March 2013)
- *Backdoors are Forever: Hacking Team and the Targeting of Dissent?* (October 2012)
- *Tracking GhostNet: Investigating a Cyber Espionage Network* (March 2009)

Case Study — Reckless Exploits

In 2017, Citizen Lab published several reports that have triggered one of the largest surveillance scandals in Mexico's history. Working with Mexican civil society groups, Citizen Lab's role has been to investigate and verify that SMS messages received by civil society were tainted with exploits connected to the Israeli cyber warfare company, NSO Group. The messages included personalized and emotionally compelling content and included links which, if clicked by the recipients, would have silently installed NSO Group's Pegasus spyware on their devices. Such spyware would be capable of employing the device's phone and microphone to snoop on activity in the vicinity of the device, recording WhatsApp and Viber calls, logging messages sent in mobile chat apps, and tracking their physical movements.

Through a series of reports, Citizen Lab confirmed the use of government-exclusive technology to target journalists, lawyers, international human rights investigators, anti-corruption advocates, public health authorities, political opposition officials, and even a minor child.

The reports received significant media exposure, including **four separate front page stories** in *The New York Times*. Since the publication, the Mexican Government's Office of the Prosecutor has launched an investigation into abuse of this spyware.

Following the Citizen Lab's reports on Mexico, several United Nations officials together "called on the Government of Mexico to carry out a transparent, independent, and impartial investigation into allegations of monitoring and illegal surveillance against human rights defenders, social activists, and journalists."

In a related August 2016 investigation, Citizen Lab published "The Million Dollar Dissident" which outlined how NSO technology was being used to target Ahmed Mansoor, a human rights defender in the UAE. Citizen Lab determined that the espionage employed a sophisticated series of unpatched vulnerabilities ("zero days") in Apple products. Prior to the report's publication, Citizen Lab undertook a responsible disclosure to Apple, and their security team issued patches for all iOS, MacOS, and Safari products, affecting more than **1 billion Apple users worldwide**.

Free Expression Online

FREE EXPRESSION RESEARCH INVESTIGATES how information is censored and disrupted by state actors and private companies at the network layer (e.g., network shutdowns, network throttling, Internet filtering) and the application layer (e.g., content filtering and moderation, government requests for content removal). Reports in this stream have investigated incidents of: Sandvine/Procera Networks Deep Packet Inspection (DPI) devices to help deliver nation-state malware in Turkey and indirectly into Syria; information controls disruptions during Thailand's 2014 Coup; and the "Great Cannon", a tool in China used for large scale distributed-denial-of-service attacks.

SELECTED REPORTS:

- *Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?* (March 2018)
- *Managing the Message: What You Can't Say About the 19th National Communist Party Congress on WeChat* (November 2017)
- *Remembering Liu Xiaobo: Analyzing Censorship of the Death of Liu Xiaobo on WeChat and Weibo* (July 2017)
- *We (Can't) Chat: "709 Crackdown" Discussions Blocked on Weibo and WeChat* (April 2017)
- *One App, Two Systems: How WeChat Uses One Censorship Policy in China and Another Internationally* (November 2016)
- *Information Controls During Military Operations: The Case of Yemen During the 2015 Political and Armed Conflict* (October 2015)
- *China's Great Cannon* (April 2015)
- *Information Controls During Thailand's 2014 Coup* (2014)
- *Planet Blue Coat: Mapping Global Censorship and Surveillance Tools* (January 2013)

Case Study — Liu Xiaobo

On July 13, 2017, Liu Xiaobo, China’s only Nobel Peace Prize winner and its most famous political prisoner, died from complications due to liver cancer. He was detained in December 2008 for his participation with “Charter 08”, a manifesto that called for political reform and an end to one-party rule. In June 2017, eight years after his imprisonment, he was diagnosed with terminal liver cancer. The government of China rejected his request for permission to receive medical attention abroad, for which they were widely criticized.

Following his death, news articles reported cases of social media in China blocking references to Liu Xiaobo. Citizen Lab analyzed censorship related to Liu and his death on two of China’s most popular platforms: WeChat and Weibo.

On WeChat, we collected keywords that triggered message censorship related to Liu Xiaobo before and after his death. Before his death, messages were blocked that contained his name in combination with sensitive content, such as issues related to his medical treatment or requests to receive care abroad. However, after his death, we found that simply including his name was enough to trigger blocking of messages. In other words, WeChat issued a blanket ban on his name after his death, greatly expanding the scope of censorship.

We further documented censorship of images related to Liu on WeChat after his death, and **for the first time found images blocked** in one-to-one chat. We also found images blocked in group chat and WeChat Moments (a feature similar to Facebook’s Timeline), before and after his death.

Transparency and Accountability

USERS OF INFORMATION TECHNOLOGIES now depend on and share their data with a plethora of private companies, many of whom are required by law to retain or disclose information to comply with government agencies' requests or demands. These data retention and sharing practices often lack transparency and impact user privacy.

Additionally, policies and practices based on national security interests have, and continue to be, enacted by governments. These policies and practices pertain to use and operation of technologies and may have negative impacts on human rights.

By examining the transparency and accountability mechanisms relevant to corporations and state agencies, we strive to support policies that better protect individuals and their personal data.

SELECTED REPORTS:

- *Approaching Access: A Look at Consumer Personal Data Requests in Canada* (February 2018)
- *Analysis of the Communications Security Establishment Act and Related Provisions in Bill C-59 (an Act Respecting National Security Matters), First Reading* (December 2017)
- *An Analysis of the International Code of Conduct for Information Security* (September 2015)
- *Canada's Quiet History of Weakening Communications Encryption* (August 2015)
- *The Governance of Telecommunications Surveillance* (May 2015)
- *Shutting the Backdoor: The Perils of National Security and Digital Surveillance Programs* (October 2013)

Case Study — Bill C-59

The Government of Canada introduced new national security legislation in the summer of 2017. Bill C-59 (the National Security Act) raised the prospect of significantly changing Canada's national security agencies and practices, including Canada's signals intelligence agency, the Communications Security Establishment (CSE).

Since the Bill was first proposed, a range of civil society groups and academics have called for significant amendments to the proposed Act. A co-authored report by the Citizen Lab and the Canadian Internet Policy & Public Interest Clinic (CIPPIC) represented the most detailed and comprehensive analysis of CSE-related reforms to date. Calls for amendment principally focused on:

- Concerns related to the new "active" and "defensive" cyber operations powers, which could let the CSE use its expertise to engage in state-sponsored hacking
- Improving the review and oversight frameworks to ensure that they provide an adequate level of protection given the risk to the Charter-protected rights of Canadians and persons in Canada, as well as internationally recognized human rights abroad
- The risk that the proposed Act would normalize mass surveillance activities, which are neither inherently necessary nor proportionate
- The sweeping exceptions to the CSE's general prohibition on "directing" its activities at Canadians, including exceptions that would allow the CSE to acquire "publicly available" information, a definition broad enough to include information stolen or otherwise illegally obtained by the seller

This analysis was produced to help members of parliament, journalists, researchers, lawyers, and civil society advocates engage more effectively on these issues and was included in **parliamentary committee debates** and highlighted in dozens of media reports.

Apps and Privacy Control

MOBILE APPLICATIONS HAVE BECOME a central means for civil society to communicate, organize, and act. However, applications that have amassed huge user populations in some regions of the world remain largely understudied by security researchers, leaving users with limited information on their relative privacy and security. Our research in this area has investigated end-to-end encryption of popular chat apps, the leaking of data from fitness trackers, and the security of mobile payment systems.

SELECTED REPORTS:

- *Safer Without: Korean Child Monitoring and Filtering Apps* (September 2017)
- *Analysis of End-to-End Encryption in LINE* (August 2017)
- *Cashless Society, Cached Data: Security Considerations for a Chinese Social Credit System* (January 2017)
- *Harmonized Histories? A Year of Fragmented Censorship Across Chinese Live Streaming Applications* (November 2016)
- *A Tough Nut to Crack: A Further Look at Privacy and Security Issues in UC Browser* (August 2016)
- *Baidu's and Don'ts: Privacy and Security Issues in Baidu Browser* (February 2016)
- *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security* (February 2016)
- *A Chatty Squirrel: Privacy and Security Issues with UC Browser* (May 2015)

Case Study — Parental Monitoring Apps in South Korea

Beginning in 2015, the Citizen Lab began publishing a series of reports which document serious privacy and security concerns with mobile applications that allow parents in South Korea to monitor activity on their children's phones. These parental filtering apps were developed following the South Korean government's April 2015 mandate that requires "harmful content" to be blocked on the mobile phones of minors. South Korea is the first jurisdiction to pass such legislation.

Citizen Lab's analysis of five different monitoring applications demonstrated that they did not follow best security practices for data transmission, data storage, or user authentication. In fact, the findings showed that the children who used them were at risk of having their messages intercepted, personal data compromised, and even communication records falsified.

These results emphasize the need for independent, comprehensive, and public audits of all child monitoring apps available in the South Korean market. The mandated use of these apps also underscores broader public policy issues regarding privacy and the rights of children and parents.

As a result of these reports, **some apps were pulled from the market**, while others were updated to address some of the problems Citizen Lab identified. Following the publication of Citizen Lab's reports, the South Korean government introduced a bill which would allow parents to opt-out of using these applications.

Global Research Network

The Citizen Lab is committed to supporting a global community of researchers through our Cyber Stewards Network, various fellowships, and events.

Cyber Stewards Network

The Cyber Stewards Network is a global network of organizations and individuals that use evidence-based research for policy advocacy to ensure and promote a secure and open Internet. The Network builds bridges between researchers and activists in the global North and South to form a space for peers to collaborate and organize at local, regional, and international levels.

CLSI

The Citizen Lab has convened the annual Citizen Lab Summer Institute on Monitoring Internet Openness and Rights (CLSI) since 2013. The workshop is a meeting place for researchers and practitioners from academia, civil society, and the private sector who are working on Internet openness, security, and rights. CLSI is not your average academic workshop: the goal is to form collaborations and work together on projects through intensive participant-led sessions. Collaborations formed at prior CLSI workshops have led to publication of high impact reports on Internet filtering in Zambia (2016), a security audit of child monitoring apps in South Korea (2015), and an analysis of the “Great Cannon” (2014), a tool in China used for large scale distributed-denial-of-service attacks. Publication of the *Great Cannon* report, which was a collaboration between Citizen Lab, Princeton University, and UC Berkeley, was covered on the front page of *The New York Times* and was the subject of a lead editorial from *The Washington Post*.

Cyber Dialogues

From 2011 – 2014, the Citizen Lab organized the annual Cyber Dialogue series of conferences, designed to bring together roughly 100 stakeholders from government (including law enforcement, military, intelligence, and foreign affairs), private sector, and civil society to discuss issues concerning the security of cyberspace. Among the attendees were representatives from Canada, US, UK, Germany, NATO, EU, AT&T, Facebook, Google, Bell Canada, Privacy International, EFF, and many others.

Security Planner and Access My Info

While the majority of the Citizen Lab's work focuses on high-risk individuals and organizations, we also produce platforms that help everyday Internet users better navigate the digital world.

Access My Info

Access My Info (AMI) is a web application that enables users to find out what a variety of different companies know about them. It guides users via a step-by-step wizard to generate a formal letter that requests access to personal information. This letter can then be sent via postal mail or email to the respective company's privacy officer, or attached to the federal government's Access to Information request tool.

Security Planner

Security Planner is an easy-to-use guide with expert-reviewed advice for staying safer online. It provides recommendations on implementing basic online practices, like enabling two-factor authentication on important accounts, making sure software stays updated, and using encrypted chats to protect private communications. More advanced users can receive advice on where to go for more help.

Recommendations in Security Planner are made by a committee of experts in digital security and have gone through a rigorous peer-review evaluation, led by the Citizen Lab. Security Planner is supported by a community of organizations, including non-profits, educational institutions, and foundations, and never accepts funds or services in exchange for making a recommendation.

Profile and International Recognition

RONALD J. DEIBERT is Professor of Political Science and Director of the Citizen Lab at the Munk School of Global Affairs, University of Toronto. He is a former founder and principal investigator of the OpenNet Initiative (2003 – 2014) and a founder of Psiphon, a world leader in providing open access to the Internet. Deibert is the author of *Black Code: Surveillance, Privacy, and the Dark Side of the Internet* (Random House: 2013) — which has been turned into a feature-length documentary by Nick De Pencier — as well as numerous books, chapters, articles, and reports on Internet censorship, surveillance, and cyber security. He was one of the authors of the landmark *Tracking Ghostnet* (2009) and *Great Cannon* (2015) reports, and co-editor of three major volumes with MIT Press on information controls (the "Access" series).

Ron Deibert and the Citizen Lab routinely make world news. Since 2006, Citizen Lab reports have been featured **22 separate times** on the front pages of either *The New York Times*, *The Washington Post*, *The Globe and Mail*, or *Toronto Star*, including **four separate front page stories** in *The New York Times* in 2017 alone.

In recognition of his own work or that of the Citizen Lab, Ron Deibert has been awarded the University of Toronto's President's Impact Award (2018), Foreign Policy's Global Thinker Award (2017), the Electronic Frontier Foundation Pioneer Award (2015), the Neil Postman Award for Career Achievement in Public Intellectual Activity (2014), the Advancement of Intellectual Freedom in Canada Award from the Canadian Library Association (2014), the Canadian Journalists for Free Expression Vox Libera Award (2010), and the Northrop Frye Distinguished Teaching and Research Award (2003). In 2013, he was appointed to the Order of Ontario and awarded the Queen Elizabeth II Diamond Jubilee medal for being "among the first to recognize and take measures to mitigate growing threats to communications rights, openness, and security worldwide."

About the Munk School of Global Affairs and the University of Toronto

The **Munk School of Global Affairs** unites people who are passionate to address the problems of a fast-changing world with an aspiration to create a unique, world-leading research, teaching, and public engagement site. It is the home of world-renowned researchers and more than 40 academic centres, labs, and programs.

Founded in 1827, the **University of Toronto** has evolved into Canada's leading institution of learning, discovery, and knowledge creation. It is proud to be one of the world's top research-intensive universities, driven to invent and innovate.

The University of Toronto is dedicated to fostering an academic community in which the learning and scholarship of every member may flourish, with vigilant protection for individual human rights, and a resolute commitment to the principles of equal opportunity, equity, and justice.

Contact Information

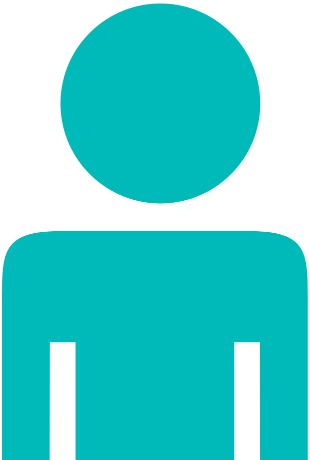
MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

THE CITIZEN LAB

315 Bloor St West
Toronto, Ontario, Canada
M5S 1A3

inquiries@citizenlab.ca
(416) 946 – 8903
https://citizenlab.ca/
@CitizenLab
citizenlab.uoft



Lifting the lid off the Internet since 2001

MUNK SCHOOL OF GLOBAL AFFAIRS
UNIVERSITY OF TORONTO

THECITIZENLAB

315 Bloor St West
Toronto, Ontario, Canada
M5S 1A3

inquiries@citizenlab.ca
(416) 946 – 8903
https://citizenlab.ca/

@CitizenLab
citizenlab.uoft