Travel security guide for university researchers and staff

December 2019

This document is meant to be adapted as needed by institutions to complement their own policies and tools.

This document was produced by the *U15 Group of Canadian Research Universities* and *Universities Canada*. The original document can be found at www.univcan.ca/tools-for-navigating-changing-geopolitical-realities/.

The document is meant to be adapted as needed by institutions to complement their own policies and tools. In doing so, please reference the original document as follows:

> The U15 Group of Canadian Research Universities and Universities Canada. December 2019. *Travel security guide for university researchers and staff*. Retrieved from www.univcan.ca/tools-for-navigating-changing-geopolitical-realities/.

Table of Contents

The current environment

International travel for research is frequent and beneficial – not only to individual researchers but to the broader pursuit of knowledge through academic research and collaboration. Canada's researchers and universities are a strategic resource to Canada and advance our place in the world economically, politically and socially.

In an era of changing geopolitical realities, Canadian researchers travelling abroad may be targeted for their access to certain sources of information as foreign governments and businesses place a high priority on acquiring information related to research and innovation. This guide is not meant to cover general travel safety, but rather focuses on risks created due to the intersection of geopolitical dynamics and research areas. **This guide describes the nature of economic and geopolitically motivated threats to you or your research, provides basic steps you can take to mitigate risk and suggests actions you can take in case of incidents.**

It cannot be understated: international travel for research is a good thing! The information provided in this guide is meant to ensure researchers are aware of the risks associated with international travel and take the necessary steps to protect themselves and their research while abroad. For ease of use, a checklist is provided in Appendix A.

1. Five reasons Canadian researchers may be of interest and at risk

For researchers, the pursuit of knowledge and academic excellence drive them to collaborate across Canada and across borders. While travel is an integral part of collaboration, there are five factors that may put a Canadian researcher more at risk of being a target for theft and espionage while abroad.

1. **Your research:** While all research could be of interest to malicious actors, your research may be of more interest if it relates to:
   a. Canadian or foreign security practices, like military practices or law enforcement.
   b. Canadian or foreign commercial activities or intellectual property development.
   c. STEM and emerging technology fields.
   d. Health or other personal data (e.g. human genomics, interviews with key figures, etc.).
   e. Politically sensitive contexts (either domestic or international).
2. **Your access to indirect partners:** Information about fellow research partners, your institution, private industry partners and the Canadian government[1] can be used by malicious actors to target them.
3. **Your access to the United States:** Given the close relationship between Canada and the United States and the mobility that many researchers enjoy between Canadian and U.S. institutions, Canadian researchers occupy a unique strategic position. In some cases, Canadian researchers have privileged access to advanced U.S. technologies, which few others can legitimately procure. As a result, when travelling abroad, Canadian researchers may be seen as soft targets for access to U.S. institutions or research data.
4. **Where you travel to:** As a Canadian researcher, you have the privilege of being able to travel to many places around the world. While many of these countries are safe, some countries are riskier and the level of risk can change as global dynamics evolve.
5. **Who you travel with:** Researchers often have the opportunity to travel as part of delegations made up of other researchers, university senior leadership, business leaders or government officials. As part of a high-profile group, you may be more at risk of drawing attention from foreign governments or other actors.

Mitigation tips

- ❒ Assess the level of risk associated with your travel due to: your area of research, indirect partners or access to U.S. research, particularly in sensitive areas.
- ❒ Discuss any concerns with appropriate resource people within your university (supervisor, IT department, travel office).
- ❒ Consult the Government of Canada's travel advisory website and take relevant precautions associated with your destination.
- ❒ Make a travel plan and share it with an appropriate resource person at your institution.
- ❒ Register your travel at travel.gc.ca.
- ❒ Get travel insurance through your university travel service or another source.

1 Additionally, any relationship that you or your research has with organizations such as the North Atlantic Treaty Organization (NATO), the G7 and G20, the Commonwealth, la Francophonie, the Organization of American States (OAS), the Asia-Pacific Economic Cooperation (APEC), the Organization for Economic Cooperation and Development (OECD), the United Nations (UN) and the World Trade Organisation (WTO) may be of value.

2. Your personal profile

University researchers gain profile through the quality of their research and the new ideas that it generates. International travel is one way to build visibility and make valuable connections. Understanding what information is publicly available about you and effectively managing your personal profile in advance of your travel can help you mitigate risks associated with foreign governments or others who may be interested in you and your research.

There are four main ways information may be gathered about you before you arrive:

1. **Your research and social media profiles** can often outline detailed information about your research, your collaborators, your views, your contacts and your family. Assume interested actors may review your profiles before you travel.
2. **Visa and travel applications** may be aggregated with your social media and research profiles to assess the level of interest a foreign government and others might have in you or your work.
3. **Biometric data** will likely be gathered on you and may be stored and shared across jurisdictions.
4. **Border agents** gather, record and transmit information about the reasons for your travel. In addition, if you have been pre-flagged as a person of interest, you may be required to go through a secondary set of questions or search.

Mitigation tips

- ❒ Review your research and social media profiles before you travel so you are aware of what information is publicly available about you. Take steps to limit exposure through social media if appropriate.
- ❒ Limit the information you provide on travel applications and visas to only what is required. Refrain from offering additional personal or professional details.
- ❒ Limit the information you provide to border patrol agents to only what is required.
- ❒ If a secondary search is requested:
  - Know that you have the right to consular services, should questioning become inappropriate.
  - If you are dual citizen, understand in advance how best to exercise your rights.

3. How your research may be accessed

Sharing research results is part of the fabric of advancing the academic enterprise, and participating in global conferences are ideal forums for doing so. However, every researcher has a vested interest in making sure their ideas are not taken without their knowledge or used in ways they – or their subjects and partners – did not consent to.

When you travel, there are three main avenues that less scrupulous foreign governments, businesses and other actors may seek to use your information without you knowing:

1. People-to-people connections;
2. Physical intrusion; and
3. Cyber intrusion.

This guide will take each of these avenues in turn and provide a checklist to mitigate risks.

3-A. People-to-people connections

Networking at conferences and sharing research interests, current results and future directions are normal and important objectives of international travel. However, it is important to be aware of how and when these normal activities might cross over into research theft or espionage.

1. **Elicitation:** A legitimate researcher, student or business person under duress – or someone who is impersonating one – engages you in what appears to be harmless or random conversation, but their aim is to subtly extract information about you, your work and your colleagues.
2. **Cultivation:** A relationship is cultivated with you by another researcher, student or business person in an attempt to extract information from you.
3. **Taxi drivers, waiters and bartenders:** In some contexts, everyday people in everyday roles may be employed by governments or groups who are seeking to gather information on foreigners.
4. **Sexual entrapment for blackmail:** Sexual entrapment refers to an individual seducing someone and putting them in a compromising position where they could be blackmailed. This often involves the recording of an intimate encounter, which is then either used to blackmail or publicly embarrass the victim.

Mitigation tips

- ❒ Be vigilant and monitor the progress of associations, particularly new relationships and connections with foreign nationals. Always be heedful of discussions regarding your work, even if seemingly benign.
- ❒ Refrain from talking about sensitive parts of your research in public places or with contacts you have just met.
- ❒ Refrain from offers of companionship while travelling and be aware of risks associated with sexual activity (eg. age of consent and sexual orientation) in the country where you are travelling.
- ❒ If you are a victim of elicitation, cultivation or entrapment or suspect that someone is trying to victimize you, notify the Canadian consulate in your area immediately and file a report with the appropriate person at your institution, either immediately or when you return. In case of emergency abroad, contact the Government of Canada collect at: 1-613-996-8885 or sos@international.gc.ca.

3-B. Physical intrusion

The risk of theft when travelling is not new. Being aware of the increased risk that a researcher may face because a foreign government or other actor is interested in their research can help safeguard both the researcher and their work.

1. **Hotels:** Hotel staff may be direct or indirect government agents. They could break into your hotel room to steal or copy documents or facilitate entrapment and blackmail. They could also enable others to do so. Though you may not notice that someone has surreptitiously entered your room, some travellers have returned to their rooms to find individuals searching through their belongings or conducting unnecessary maintenance activities. There are also reports of individuals who have suspected they were drugged and who awoke to find that their hotel room had been searched, smartphone stolen and sensitive documents missing.
2. **Conference spaces:** Conference and event spaces may be bugged or surveyed. As with hotels, staff may be direct or indirect government agents.
3. **Cars:** Though vehicles and cars are often thought to be safe places for work conversations, they may be bugged or equipped with locating devices, allowing external actors to track and monitor your movements.
4. **Eavesdropping:** In some contexts, conversations may be monitored in public places and on public transportation. Eavesdropping activities can range from the strategic positioning of an unobtrusive bystander, to the use of concealed sophisticated audio and visual devices.

Mitigation tips

- ❒ Consult with your IT department before leaving. Use burner phones or travel safe devices whenever possible. (See 3-C for more on cyber hygiene.)
- ❒ Do not travel with unnecessary documentation (contact lists, electronic files, etc.) or devices.
- ❒ Do not advertise where you are staying or your room number.
- ❒ Do not leave the keys for your room at the front desk of your hotel.
- ❒ Keep your radio on in your room when you are not there.
- ❒ Refrain from using hotel or conference computers or public phones as they may be monitored.
- ❒ Do not surrender your electronic devices at the conference.
- ❒ Refrain from talking about sensitive elements of your current or future research.
- ❒ If you are a victim of robbery or suspect someone wants to rob you, notify the Canadian consulate in your area immediately and file a report with the appropriate person at your institution, either immediately or when you return. In case of emergency abroad, contact the Government of Canada collect at: 1-613-996-8885 or sos@international.gc.ca

3-C. Cyber intrusion

Digital devices allow us to share information and keep in touch with professional contacts. However, they also provide opportunities for data and identity theft, both while away and once you return home. As best practices in cybersecurity are rapidly evolving, consulting your IT department regarding current policies and practises at your institution before you travel is key. Some overarching risks are noted below.

1. **Intercepting your communications:** Wireless communications can be monitored in any country. Local authorities may have access to telecommunication networks, which means that they can access information on your devices such as call logs, contact lists, documents, messages. They may even be able to listen in on and/or record phone calls. Data can also be intercepted via technical means by the Internet Service Provider. A smartphone, tablet, desktop or laptop can all be intercepted and eventually "taken over." These vulnerabilities can persist long after you return home.
2. **Identity fraud and phishing:** Your information could be used by an attacker to impersonate you and send targeted emails with malicious software, such as ransomware, to others on your professional network. This could have significant costs to your colleagues or your institution.
3. **USB devices:** USB drives and devices are often used by malicious actors to gain access to or otherwise compromise computers. Any device that can be plugged into your computer's USB drive is a potential threat.

Mitigation tips

- ❒ Consult with your IT department before you travel. Make sure all electronics have the latest anti-virus, encryption, firewall and program patches. Use burner or travel specific devices. Follow guidance for use of Virtual Private Networks and other safeguards for accessing the Internet while away.
- ❒ Before you travel, carefully consider what data you need. Bring the minimum.
- ❒ Encrypt and transfer data onto a separate external storage device and keep it with you at all times while travelling. Keep data passwords separate from the media.
- ❒ If your devices are out of your sight at any time during travel, assume that the equipment has been compromised.
- ❒ Do not plug an external device, including USB keys, cameras or digital picture frames, into any of your equipment.
  - Should you find it necessary to plug an external device into your equipment for presentation purposes at a conference, you should consider that your device has been compromised.
- ❒ If possible, do not access cloud data storage sources while travelling.
  - If access to cloud storage is necessary, be sure to only do so on personal and secure devices.
- ❒ If your device is lost or stolen, notify your IT department immediately.
- ❒ Upon your return home, take appropriate steps to clean your hard drive or other devices, especially if you think your device may have been compromised. Have all external devices scanned for viruses before using them, including gifts and conference swag.

Appendix A – Travel security checklist for university researchers

Before you travel:

- ❒ Assess the level of risk associated with your travel due to: your area of research, indirect partners or access to U.S. research, particularly in sensitive areas.
- ❒ Consult the Government of Canada's travel advisory website and take relevant precautions associated with your destination.
- ❒ Discuss any concerns with appropriate resource people within your university (supervisor, IT department, travel office).
- ❒ Make a travel plan and share it with an appropriate resource person at your institution.
- ❒ Consult with your IT department before leaving.
  - Use burner phones or travel safe devices whenever possible.
  - Make sure all electronics have the latest anti-virus, encryption, firewall and program patches.
  - Discuss guidance for use of VPNs and safeguards for accessing the Internet while away.
- ❒ Do not travel with unnecessary documentation (contact lists, electronic files, etc.) or devices.
- ❒ Before you travel, carefully consider what data you need. Bring the minimum.
- ❒ Encrypt and transfer data onto a separate external storage device and keep it with you at all times while traveling. Keep data passwords separate from the media.
- ❒ Register your travel at travel.gc.ca.
- ❒ Get travel insurance through your university travel service or another source.

While you are away:

If you are a victim or suspect someone is trying to victimize you, notify the Canadian consulate in your area immediately and file a report with the appropriate person at your institution, either immediately or when you return. In case of emergency abroad, contact the Government of Canada collect at: 1-613-996-8885 or sos@international.gc.ca.

People to people connections

- ❒ Refrain from talking about sensitive parts of your research or potential future research in public places, or with contacts you have just met.
- ❒ Be aware of the potential for elicitation, cultivation or entrapment. Monitor the progress of associations, particularly new relationships and connections with foreign nationals and refrain from offers of personal companionship while travelling.

Physical intrusion

- ❒ Do not advertise where you are staying or your room number.
- ❒ Do not leave the keys for your room at the front desk of your hotel.
- ❒ Keep your radio on in your room when you are not there.
- ❒ Refrain from using hotel or conference computers or public phones as they may be monitored.
- ❒ Do not surrender your electronic devices at a conference or hotel.

Cyber intrusion

- ❒ Do not let your devices out of your sight at any time during your travel. If this happens, assume that the equipment has been compromised.
- ❒ Do not plug an unknown device, including USB keys, cameras or digital picture frames, into any of your equipment.
  - Should you find it necessary to plug an external device into your equipment for presentation purposes at a conference, you should consider that your device has been compromised.
- ❒ If possible, do not access cloud data storage sources while travelling.
  - If access to cloud storage is necessary, be sure to only do so on personal and secure devices.
- ❒ If your device is lost or stolen, notify your IT department immediately.

When you get back:

- ❒ Upon your return home, take appropriate steps to clean your hard drive or other devices especially if your think your device may have been compromised. Have all external devices scanned for viruses, including gifts or conference swag.
- ❒ Notify your colleagues, resource person or travel expert of any suspicious or criminal activity that occurred during your trip. Seek guidance as to whether you should contact authorities.