Collecting and Storing Private Data Using Web-Based Tools

The same principles of privacy protection apply to both physical and digital data. The key questions to ask when collecting or storing data using web-based applications include:

- Who has lawful access to the data?
- How might personal data be compromised and how do I mitigate risk?
- What do participants need to know for their consent to be informed?

The following outlines areas of consideration for safeguarding participant privacy when using online tools and applications. These guidelines apply to data that contain personal information only. Information does not have to directly identify a participant to be considered personal - it may include an address, date of birth, government identification number, description, personal history, or even an IP address. While all research data should be protected, potential risks to personal information should receive more thorough scrutiny.

Who has lawful access to the data?

While research data collected at Alberta universities are not subject to access to information legislation (FOIP, sec. 4(i)), they may be requested by law enforcement and security agencies through other legal channels. The means to do so vary considerably between countries, and jurisdiction may not always be clear. Importantly, American agencies may be able to request any data held by companies and organizations that operate in the US, even if the data are not held within that country. Canadian privacy legislation may provide some protection for these data, so storing research data in Canada is often a better, though not foolproof, option when it comes to protecting data from access by *foreign* governments.

There is no guarantee that any data stored using an MRU institutional Google Suite account or transmitted using Gmail will be held in Canada. Those data may be subject to the laws of the United States. Further, data transmitted between Canadian destinations may cross borders in transit, although major service providers (e.g. Google) generally encrypt data in transit. Check the website of the software provider for information about the location of servers, the home country of the provider, and any digital privacy protections the provider uses.

How might personal data be compromised and how do I mitigate risk?

The biggest risk to research data is through loss or theft of portable computing devices. These include computers, phones, and portable memory devices. Smaller devices (portable hard drives, memory sticks, etc.) should always be encrypted. Computers and smartphones should be password protected, at minimum. If research data are stored on cloud services, be aware of all devices that are connected to cloud accounts and ensure they are secure. For example, if data are stored on Google Drive, take note of all phones, tablets, and computers that can access that Google account and ensure that those devices have protections that reflect the sensitivity of the data, including multi-factor authentication, encryption, or strong passwords.

Another potential risk to be aware of is unauthorized access to the data through hacking, fraud, or extortion. It is important to note that any networked device, including your office workstation, may be compromised through malware or ransomware. Use the same protections mentioned above to protect your data, but also be aware of suspicious emails. Contact ITS to report those emails or for more information about cybersecurity.

Generally, established internet companies incorporate better security measures into their tools than smaller organizations do. Closely examine the policies associated with any unfamiliar or less established tools you use to collect or store participant information. Are data encrypted in transit (look for https in the URL)? Does the tool use third-party servers (e.g. Amazon Web Services)? Does the company retain the data after its been deleted?

What do participants need to know for their consent to be informed?

In addition to a FOIP statement, participants should be aware that some data may be subject to request by law enforcement and security agencies outside of Canada. This includes any data collected through online forms or surveys, stored using cloud services, recorded during video conferencing, or transmitted by email, particularly if the company operating the service is primarily located outside of the country. This generally does not include data gathered and stored exclusively on local devices, stored on MRU servers (e.g. H drive), or collected using services entirely located in Canada.

Normally, participants will be made aware of how their personal information will be managed and the digital and physical security measures in place to protect their personal information. The amount of detail provided about the risks of unauthorized access to data will depend on the audience and sensitivity of the data, but usually participants should be informed or reminded of the potential risks to privacy associated with using online services.

It is suggested that the following statement be included in consent letters in cases where data are collected or stored using services hosted or owned outside of Canada:

> Your information will be [collected or stored] using [software name and company location]. The information you submit may be subject to laws in force outside of Canada. As with any information transmitted via the internet, there is some risk that data may be intercepted by unauthorized parties and, therefore, privacy cannot be absolutely guaranteed.