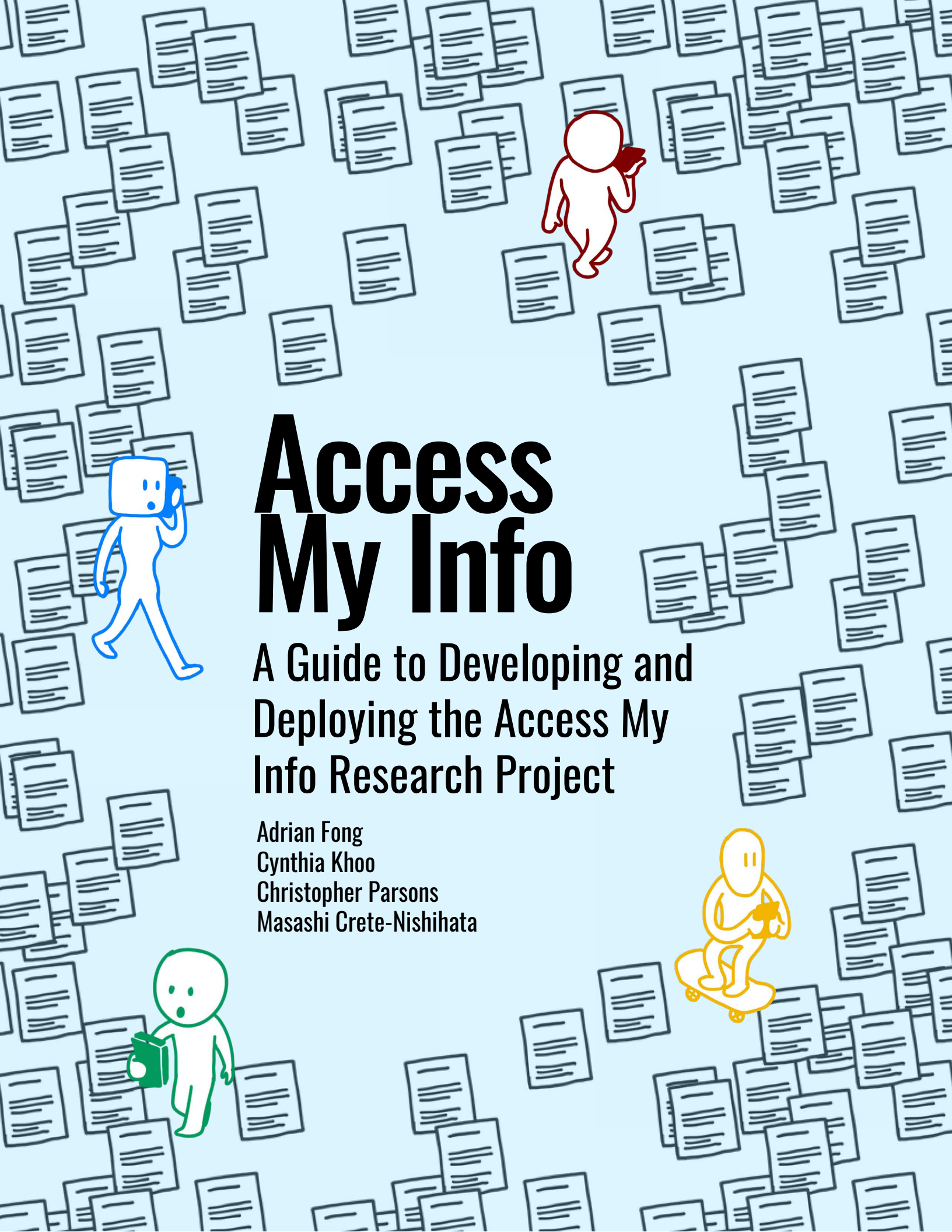


Access My Info

A Guide to Developing and Deploying the Access My Info Research Project

Adrian Fong
Cynthia Khoo
Christopher Parsons
Masashi Crete-Nishihata

This page has intentionally been left blank.

Copyright

Electronic version first published at citizenlab.ca in 2019 by the Citizen Lab.

The Citizen Lab engages in research that investigates the intersection of digital technologies, law, and human rights.

Document Version: 1.0

Legal Disclaimer: Please note that Access My Info does not provide any legal advice pertaining to an individual's data privacy rights or obligations. This applies to the AMI tool, AMI projects in general, and this AMI Playbook. If you are an individual seeking legal advice about your data rights with respect to a particular company, or who wishes to know if a specific company is violating your rights, we recommend that you consult a qualified lawyer.

About the Citizen Lab, Munk School of Global Affairs and Public Policy

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, 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 that combines methods from political science, law, computer science, and area studies. Our research 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.

About this Document

Access My Info has been made possible with support from the Privacy Commissioner of Canada and the Canadian Internet Registration Authority (CIRA)'s Community Investment Program. Case study research in Asia was supported by the International Development Research Centre (IDRC). We would also like to thank Mari Zhou for assistance in designing this publication.

Send all questions and feedback to: ami@citizenlab.ca.

About the authors

This analysis was researched and written by Adrian Fong, Cynthia Khoo, Christopher Parsons, and Masashi Crete-Nishihata.

Adrian Fong graduated from the Chinese University of Hong Kong with a Bachelor of Laws. He was a 2016 Google Policy Fellow at the Citizen Lab, in the Munk School of Global Affairs (as formerly named) with the University of Toronto. He is currently a lawyer in Hong Kong.

Cynthia Khoo is a Research Fellow at the Citizen Lab, and formerly their 2018 Google Policy Fellow. She is a digital rights lawyer called to the Bar of Ontario, and LL.M. candidate (Concentration in Law and Technology) at the University of Ottawa Faculty of Law, with a J.D. from the University of Victoria.

Christopher Parsons received his Bachelor's and Master's degrees from the University of Guelph, and his Ph.D from the University of Victoria. He is currently a Research Associate at the Citizen Lab, in the Munk School of Global Affairs and Public Policy with the University of Toronto as well as the Managing Director of the Telecom Transparency Project at the Citizen Lab.

Masashi Crete-Nishihata is Research Director at the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto.

Acronyms

AMI	Access My Info
CATSMI	Canadian Access To Social Media Information (project)
DAR	Data Access Request
DPA	Data Protection Authority
EU	European Union
FAQ	Frequently Asked Questions
GDPR	General Data Protection regulation
IP	Internet Protocol
ISP	Internet Service Provider
OECD	Organisation for Economic Co-operation and Development
PIPEDA	Personal Information Protection and Electronic Documents Act
UN	United Nations
UNHR	Universal Declaration of Human Rights

Contents

Contents

Executive Summary

Access My Info (AMI) is a research project that uses data access requests and complementary policy, legal, or technical methods to learn about how private companies collect, retain, process, and disclose individuals' personal data. A data access request (DAR) is a written query that an individual sends to a private company whose products or services the individual uses. DARs ask that company to disclose all of the data and information that the company holds on that individual, including when, how, to whom, and for what reasons a company shares or discloses the individual's data, and other details about the company's data protection practices and compliance with applicable privacy laws.

Accompanying the research methodology is often a web-based tool (the "AMI tool") that helps members of the public generate data access requests based on templates tailored to different industries. The AMI tool guides users through a step-by-step process to generate a DAR, which involves having users fill out a form after selecting which company they want to request their data from. The tool uses the information in the form to generate a data access request that the user then sends to the selected company as either a postal letter or email. The AMI tool does not collect any provided information and records only basic statistical information (i.e., company, language, jurisdiction, time and date of each request); users may choose to opt out of this minimal amount of data collection.

Access My Info projects typically rely on the existence of data protection laws and data access rights in order for the DARs to be legally binding. While such laws often vary per jurisdiction, they generally encompass individuals' right to know what personal data companies hold about them, to receive a copy of it, and to know why, how, with whom, and under what circumstances a company uses, retains, processes, or shares their data.

An AMI project can be used to gather information on the following questions:

1) **What personal data do companies hold?**
2) **How is personal data being used?**
3) **How long do companies retain personal data?**
4) **When and for what reasons do companies disclose data to third parties, and how do they transfer it?**
5) **What kind of data is subject to government or law enforcement requests?**
6) **To what extent do companies respond to data access requests and comply with data protection laws?**

By facilitating more data access requests through the automation tool, and collecting information received as a result of data access requests, researchers and the public can better understand companies' practices around their handling and governance of customers' personal data.

Researchers may add further depth and meaning to an AMI research project by supplementing the above core findings with complementary research and analysis. Such complementary activities include, for instance, analyzing each company's privacy policies and terms of service with respect to data protection for the purposes of comparing how companies respond to DARs as well as against legal obligations. Another option is conducting a technical analysis of the products or software produced by the given company and used by the person issuing the DAR; such analysis can be leveraged to determine how the company collects or secures user data on a technical level, regardless of policy statements or responses to user DARs.

Research teams have carried out AMI projects around the world, including in Canada, Hong Kong, Australia, South Korea, Indonesia, Malaysia, and the European Union. Such projects have typically resulted in formal reports, published academic papers, and conference presentations. Project teams have also leveraged their research findings, often in collaboration with civil society advocacy organizations, to create real-world impact and meaningful reform for user privacy, including encouraging Canadian telecommunications companies to begin publishing transparency reports and publicly spotlighting the privacy risks of connected fitness devices, which led some companies to reform their data handling practices. [1]

1 Colin Freeze, Christine Dobby and Josh Wingrove, "TekSavvy, Rogers break silence over government requests for data" (5 June 2014) Globe and Mail, online: https://www.theglobeandmail.com/technology /tech-news/teksavvy-opens-books-on-government-data-requests/article18999107/.

1. Introducing Access My Info

KEY POINTS

- **Access My Info is a multifaceted research project that is designed to render transparent companies' practices around user data, such as what data is retained and how it is used, and assess whether or not companies comply with applicable data protection laws. The project also reveals the extent to which users may meaningfully exercise their data access rights.**
- **Access My Info includes a web application (the "AMI tool") that partially automates the process of generating data access requests for an end user interested in requesting their data from a company whose products or services they use.**
- **Access My Info began in Canada in 2014, with a focus on the Canadian telecommunications industry. Since 2014, the project has also been run in Australia, the European Union, Hong Kong, Indonesia, Malaysia, and South Korea.**

1.1. Introducing Access My Info (AMI)

Companies increasingly collect, retain, control, and use more of our data than ever before. Internet service providers, social media platforms, web and mobile applications, email providers, and others collect and analyze their subscribers' and users' data in order to provide more personalized services, present targeted advertisements, make their products or services more engaging (for better or for worse), sell valuable data to third-party data brokers, or any other number of purposes. The majority of the public may not realize the extent to which companies collect their personal data, let alone precisely how it is used, analyzed, processed, stored, secured, and shared.

Access My Info (AMI) refers to a multifaceted research project. At core, AMI is a research project that uses Data Access Requests (DARs) to learn about how private companies collect, retain, process, and disclose individuals' personal data. It combines findings from

data access requests with legal and policy analyses, as well as technical knowledge, to analyze companies' privacy and data protection practices. These methods work together to answer a number of questions around users' data access rights and commercial technology companies' data practices.

1.1.1. How does Access My Info Work?

To view an example of the AMI Tool see the AMI Canada instance available at: https://accessmyinfo.ca

AMI research projects rely on the existence of data protection laws and data access rights to be effective. While such laws may vary per jurisdiction, they generally encompass individuals' right to know what personal data companies hold about them, to receive a copy of it, and to know why, how, with whom, and under what circumstances a company uses, processes, retains, or shares their data.

AMI projects centre around a web application (the "AMI tool"). This application provides a step-by-step wizard that helps a user generate a personalized formal letter that cites relevant data protection laws to request access to the information that a company stores, uses, retains, and/or discloses about that user. The letter can be saved as a PDF, printed, and mailed through the post or, where available, be directly emailed to a company's privacy officer. The tool does not send requests on the user's behalf; users must either mail the request physically or electronically after the tool generates their request. This design decision results in a commitment on the part of the user, as well as ensures that companies receiving the requests are less likely to dismiss them, because the requests are sent from individual users themselves, rather than be potentially (and mistakenly) regarded as a bulk of spam-like requests. This latter situation might follow should all requests come from one source.

GLOSSARY

AMI Project
refers to the totality of project components, including the research methodology, data access requests, the web-based tool, subsequent analysis, publications, and any additional related activities, such as potential advocacy work based on the research findings

AMI [Country]
refers to all of the pieces associated with an AMI project for that particular jurisdiction

AMI tool
refers specifically to the web-based software application that automatically generates data access requests for individuals

AMI website
refers to a website that hosts the tool and may include other documentation related to an AMI project, such as background information or reports from previous AMI projects

AMI research methodology
refers to the specific technique of leveraging data access requests and analyzing companies' responses to them, to draw conclusions about a company's or an industry sector's privacy practices.

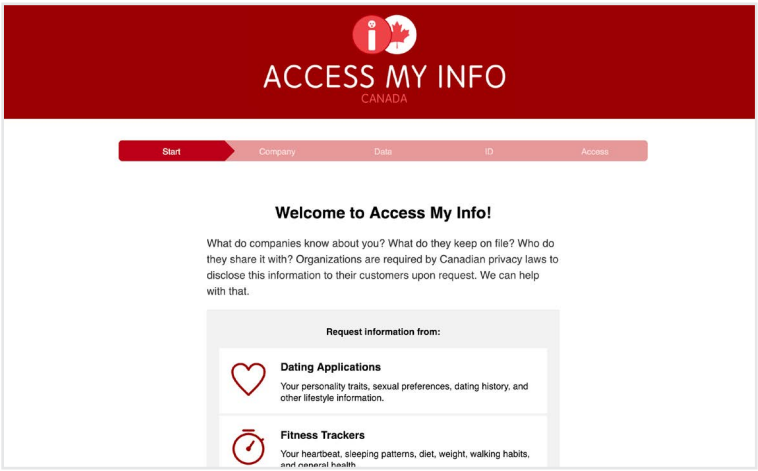


Figure 1. Screenshot of the AMI Canada instance, which can be found at accessmyinfo.ca

While a completed AMI project may consist exclusively of analyzing responses from companies, more fulsome AMI projects tend to also include legal or technical analyses of the selected companies' products and services, in addition to comparing their data practices to relevant data protection laws and their own privacy policies and terms of services.

For an example of this, see the Citizen Lab's report, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*, available at: https://citizenlab.org/2016/02/fitness-tracker-privacy-and-security/.

To respect and protect users' privacy, the AMI tool only collects a limited amount of statistical information:

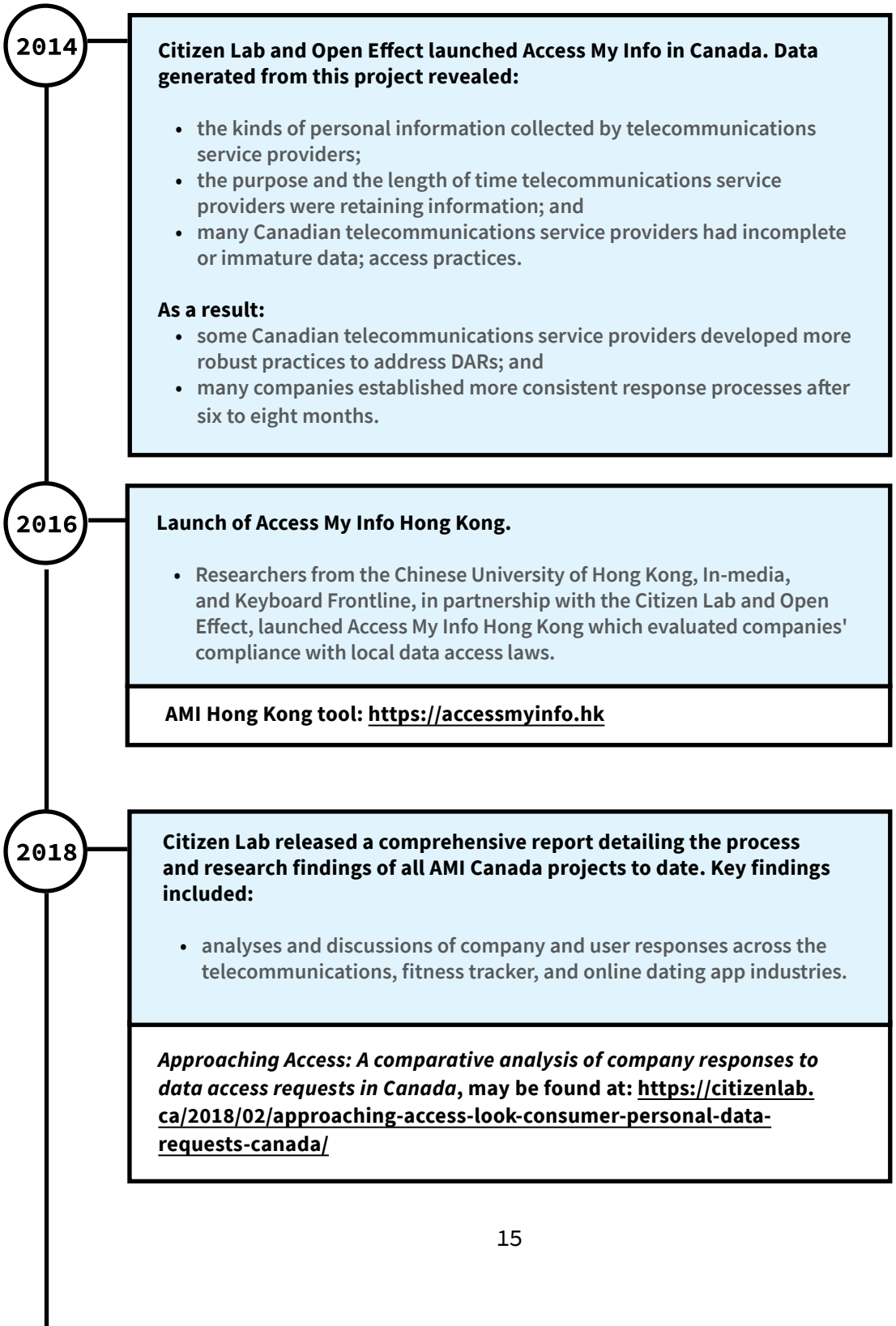
- the company for which a request was created;
- the language it was created in;
- the date and time of request, and;
- a hash-based message authentication code (HMAC). The HMAC is used as a privacy-friendly way of determining the uniqueness of a request. The HMAC is generated client-side, using browser-based cryptography to create a unique code associated with a particular user's request.

Users can opt out of this data collection. No other user-provided information is collected about the user as part of the AMI application.

Depending on the configuration of the web server hosting AMI, additional information may be collected in server access logs. AMI administrators should review their server's logging policy to minimize information collected and retained.

1.1.2. History of Access My Info

Below is a timeline of of the Access My Info project. A more detailed history of this project is available in the Appendix.



1.2. How to Use the AMI Playbook

The AMI Playbook was written to help interested groups develop and deploy a localized version of AMI for their respective jurisdictions. The target audience of this Playbook includes academics, activists and advocates, non-profit groups, technologists, data rights enthusiasts, or anyone else interested in running an AMI project, using the AMI research methodology, or deploying the AMI tool. The Playbook may also be useful for technology companies that collect or rely on users' data, as well as in-house privacy officers or in-house counsel who receive data access requests resulting from an AMI project, or to further inform such professionals' views regarding companies' obligations and best practices.

This guide is written and designed to provide clear, actionable recommendations for initiating and running an AMI project. To illustrate and increase familiarity with relevant materials and documents, the Playbook highlights a number of examples from past AMI projects. The Appendix contains further resources, including links to software development documentation and AMI research outputs.

This Playbook divides a complete AMI project into the following milestone phases:

1 **Privacy, Data Protection, and Data Access Laws**
2-4 weeks

2 **Developing and Deploying an Access My Info Research Project**
2+ months

3 **Collate results & write research report**
1-2 months

4 **Publicize findings & advocate for reform**
Variable

2. Privacy, Data Protection, and Data Access Laws

KEY POINTS

- **Privacy is globally recognized as a fundamental human right and takes on particular importance with respect to personal data in the digital age.**
- **Many jurisdictions have implemented some form of data protection legislation or frameworks, and which are often supplemented by judicial interpretations and a designated Data Protection Authority (DPA).**
- **For Access My Info projects, the most important part of any data protection law is the part that provides for users' data access rights, as these are the provisions that give force to the data access requests that users send to the selected companies for research.**

Strong privacy rights, data protection law, and data access rights are what make Access My Info projects effective. At the same time, shedding light on the current state of these laws and companies' compliance with them, potentially to improve them and to raise public awareness, is one of the primary goals of Access My Info. Given that AMI projects are focused on privacy and data protection compliance, it is advisable that those running an AMI project first familiarize themselves with the backdrop of privacy, data protection, and data access laws, policies, and regulations which are in force where the project is operating.

This section provides a high-level overview of the globally recognized right to privacy, specifically as expressed through data protection laws and data access rights in various countries.

Legal Disclaimer

Please note that Access My Info does not provide any legal advice pertaining to an individual's data privacy rights or obligations. This applies to the AMI Tool, AMI projects, and this AMI Playbook. If you are an individual seeking legal advice about your data rights with respect to a particular company, or who wishes to know if a specific company is violating your rights, we recommend that you consult a qualified lawyer.

2.1. Right to Privacy in the Digital Age

The right to privacy is an internationally recognized human right, and is enshrined in instruments such as the *Universal Declaration of Human Rights* (UDHR) and the *International Covenant on Civil and Political Rights* (ICCPR). Specifically, Article 12 of the UDHR states: "No one shall be subjected to arbitrary interference with his [or her] privacy, family, home or correspondence, nor to attacks upon his [or her] honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."[2] Article 17 of the ICCPR provides a nearly identical statement, protecting against "arbitrary and unlawful interference" with one's privacy.[3]

Privacy rights have become increasingly critical as people generate ever greater and more detailed streams of data in their daily activities. In November 2016, the United Nations adopted a resolution on "the right to privacy in the digital age" which, among other provisions, called upon all states to "respect and protect the right to privacy, including in the context of digital communications" and to "develop or maintain and implement adequate legislation, with effective sanctions and remedies, that protects individuals against violations and abuses of the right to privacy, namely through the unlawful and arbitrary collection, processing, retention or use of personal data by individuals, governments, business enterprises and private organizations."[4] The UN resolution also called upon all businesses to "inform users about the collection, use, sharing and retention of their data that may affect their right to privacy and to establish transparency policies, as appropriate."[5]

The right to protection in law against arbitrary or illegal state or business interference with one's privacy gives rise to state obligations to implement laws that protect individual privacy, including each individual's personal data.[6] This includes providing for and enforcing individuals' ability to know who has their data and what is being done with it (data access), as well as empowering individuals to correct or eliminate erroneous data about them (data accuracy or data correction).

---

2 United Nations General Assembly (1948), "Universal Declaration of Human Rights", United Nations (10 December 1948) <http://www.un.org/en/universal-declaration- 39 human-rights/> [UDHR].

3 United Nations General Assembly (1976), "International Covenant on Civil and Political Rights", United Nations (16 December 1966) < http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx> [ICCPR] at Article 17.

4 United Nations General Assembly (2016), "The right to privacy in the digital age" A/C.3/71/L.39/Rev.1, 71st Session, 3rd Committee, Agenda item 68(b): Promotion and protection of human rights: human rights questions, including alternative approaches for improving the effective enjoyment of human rights and fundamental freedoms, at Article 5.

5 *Ibid*., at Article 6(b).

6 See generally *Ibid.*

Data privacy primarily concerns protecting "personal data." The definition of "personal data" varies between countries, but generally means data or information that relates to an identifiable individual.[7] This could include a person's full name, social insurance number, passport number, location data, subscriber metadata held by their Telecommunications Service Provider (TSP), medical history, criminal records, employee records, personal bank statements, or personal itemized bills. Essentially, "personal data" refers to information relating to someone's physical, genetic, social, political, economic, cultural, or other identity—online or offline—that can be used to identify who a person is in the world.[8]

The next section summarizes the most common legal framework that countries have used to implement data privacy and data protection laws.

2.2. Data Protection Law

Countries around the world have enshrined data privacy rights in their laws. Graham Greenleaf, a senior academic who has studied data privacy laws around the world, reported that 120 countries had national data privacy laws by 2017.[9] Some countries contain multiple regimes—for example, Canada has both federal and provincial privacy and data protection legislation, whereas the United States lacks comprehensive federal privacy legislation, with individual states having instead adopted non-uniform state-based privacy laws.[10]

Although data privacy laws are unique to each jurisdiction, it is worth noting some general commonalities. Some commonalities include the legal authority that undergirds data protection rights, the establishment of data protection authorities, and the reliance on guiding principles. The following Subsections 2.2.1-2.2.3 briefly elaborate on each of these topics.

---

7 See, e.g., Office of the Privacy Commissioner of Canada, "Interpretation Bulletin: Personal Information" (11 October 2013), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/>.

8 See, e.g., EC, *Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (*General Data Protection Regulation), [2016] OJ L 119/1 [GDPR], at Article 4(1).

9 Graham Greenleaf (2017), "Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey", (2017) 145 *Privacy Laws & Business International Report* 10-13 <https://papers.ssrn.com/sol3 /papers.cfm?abstract_id=2993035>

10 See, for instance, the *California Consumer Privacy Act* of 2018. https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375

A Note on Terminology

An individual whose data is given to or collected by companies may be known as the "data subject", but the same individual can also be referred to as a person, customer, user (e.g., Internet user or user of the company's products or services), or other appropriate term under the circumstances (e.g., "voter" or "constituent" where the entity collecting personal data is a political party). The entity that collects and uses personal data may be a business, organization, non-profit entity, or otherwise, and known as a "data processor", "data operator", or "data controller". In some jurisdictions this entity is known as the "data user"; however, we avoid that term to mitigate confusion with Internet "users".

2.2.1. Statutory Framework and Judicial Interpretation

Data privacy law is most often statutory, with a specific legislative framework and various regulations providing for individuals' data protection rights. Such legislation often draws upon and interacts with codes of conduct, industry or government guidelines, and decisions by administrative tribunals. For example, Canada has the *Personal Information Protection and Electronic Documents Act* (PIPEDA); the United Kingdom has the Data Protection Act 2018; and the European Union has the General Data Protection Regulation (GDPR).

Note, however, that the judiciary has a role in interpreting legislation and thus may influence data privacy laws, and particularly where tort law, constitutional law, human rights law, or statutory interpretation is concerned. For instance, Chile does not have a national data protection authority and so relies on the courts to enforce its data protection laws. To see specific examples of data protection case law, for the 10th European Data Protection Day in 2016, Laraine Laudati, Data Protection Offer at the European Anti-Fraud Office, prepared a document summarizing numerous cases from the Court of Justice of the European Union which interpreted or impacted data protection law in the EU, between 2000 and 2015.[11]

2.2.2. Data Protection Authorities

Data privacy legislation often establishes a Data Protection Authority (DPA) responsible for overseeing the legislation's implementation and ensuring that people's data protection rights are upheld. The authority may also take an active role in monitoring companies and other parties that collect data, and ensuring that those entities comply with the jurisdiction's privacy legislation. The DPA may also be empowered to take enforcement action, handle

11 Laraine Laudati (2016), "Summaries of EU Court Decisions Relating to Data Protection 2000-2015", *European-Anti Fraud Office* (28 January 2016), <https://ec.europa.eu/anti-fraud/sites/antifraud/files/case-law_2001_2015_en.pdf>.

complaints, launch investigations of its own accord, or raise awareness about data privacy. Note that the DPA may not be a separate institution, but a role assigned to or a team housed within a pre-existing department or ministry (e.g., the Federal Trade Commission in the United States, or Ministry of the Interior and Safety in Indonesia). Each jurisdiction may also have multiple DPAs for different regions or industry sectors.

Examples of data protection authorities around the world include:

- Office of the Privacy Commissioner of Canada;
- Office of the Australian Information Commissioner;
- Privacy Commissioner for Personal Data (Hong Kong);
- Personal Data Protection Commission (Singapore);
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (Mexico);
- Dirección Nacional de Protección de Datos Personales (Argentina);
- Commission Nationale de l'Informatique et des Libertés (France); and
- Die Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Germany).

2.2.3. Principles-Based Guidelines

Data protection laws often rely on guiding principles, rather than legalistic specifications of conduct, to identify and establish what kinds of information or activity must be protected and how they are to be protected. Data privacy principles are typically referred to as general rules of thumb for best practices (albeit legally required best practices) and are less absolutist than other forms of statutory law and language. The rationale for principle-based approaches to privacy regulation is that such approaches avoid unduly hampering legitimate data collection and use. Lee Bygrave, author of *Data Privacy Law: An International Perspective*, identifies six core principles of data privacy which can be found internationally:

1) Personal data should be collected by fair and lawful means (principle of fair and lawful processing).
2) The amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data is gathered and further processed (principle of minimality).
3) Personal data should be collected for specified, legitimate purposes, and not used in ways that are incompatible with those purposes (principle of purpose limitation).

4) Personal data should be relevant, accurate, and complete in relation to the purposes for which it is processed (principle of data quality).

5) A company must make personal data policies and practices known to the public regarding the types of personal data it holds and how the data is used (principle of openness).

6) Personal data should be protected against unauthorized attempts to disclose, delete, change, or exploit it (principle of data security).[12]

2.3. Data Access Rights

Data access rights appear in most countries' privacy legislation, with such legislation empowering individuals to issue data access requests (DAR) to companies that collect, process, or retain their data.[13] In its most basic form, a DAR allows an individual to obtain the details concerning what a company is doing with their personal data, including specifically what personal data the company holds. DARs may also help requesters to ascertain if, and to whom, the company is selling or disclosing their personal data, how long the company will keep that data for, how that data is secured, and the purpose(s) of each of the above activities.

The right to access one's own data constitutes an essential component of protecting one's private life and fundamental freedoms associated with mental, informational, and physical privacy; data access rights are intrinsic to meaningfully exercising one's privacy rights.[14] An individual or regulator would find it difficult to protect a person's data and enforce data protection rights without first knowing who is collecting, storing, using, and sharing a person's personal data. Recognizing that every person has the right of access to data concerning them, the European Union and several other jurisdictions have explicitly provided for data access rights in various legislative frameworks which implement data protection laws.[15] Individuals may rely on these data access rights to discover what kinds of personal data companies hold about them, as well as how that data is used and disclosed.

Data access rights vary between jurisdictions and may place different specific obligations on the companies in each jurisdiction. However, broadly speaking, a data access right requires a business entity to disclose to an individual what personal information, if any, that the

12 Lee Bygrave, *Data Privacy Law* (Oxford: Oxford University Press, 2014), 1-2.

13 *Ibid*., 159-160.

14 See, *e.g.*, UDHR; and ICCPR.

15 See, *e.g.*, GDPR, at Article 15 ("Right of access by the data subject").

company retains about them, in addition to related information about how the company uses and stores that data.

Exercising one's data access rights normally involves issuing a DAR to one or more chosen companies. The Access My Info Tool helps individuals to generate such legally binding requests.

Data access right legislation may also empower the individuals to obtain a copy of all of their personal data and information that the company retains about them, as demonstrated in the following Hong Kong ordinance:

Hong Kong: Personal Data (Privacy) Ordinance, Cap. 486.

Section 18

(1) An individual, or a relevant person on behalf of an individual, may make a request-
(a) to be informed by a company whether the company holds personal data of which the individual is the data subject;

(b) if the company holds such data, to be supplied by the company with a copy of such data.

Figure 1: Hong Kong Personal Data (Privacy) Ordinance

Data access rights may also include the right to know for what purpose(s) one's personal data is collected, and to whom a company has disclosed that data, such as third-party businesses or law enforcement. The *Personal Information Protection and Electronic Documents Act* (PIPEDA) in Canada provides for these rights, among others:

Canada: *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Schedule 1, Section 4.2

Principle 2 — Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.3 The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4 When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5 Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

Figure 2: Canada's Personal Information Protection and Electronic Documents Act"

Some jurisdictions specify particular categories of data and information that individuals have the right to know about under certain circumstances. For example, the United Kingdom's *Data Protection Act* (2018), as well as all member states of the European Union, has enshrined in law an individual's right to know if a significant decision has been made about them through automation, without human intervention.[16]

Jurisdictions without Data Access Rights

Laws that provide a right to data access operate as the backstop of AMI research, insofar as such a right imposes legal pressure on companies to respond to DARs. As such, jurisdictions without such a right may experience significant additional challenges in obtaining meaningful research results through the AMI research methodology.

To support AMI in a jurisdiction without domestic data access rights, project leads and users of AMI may turn to (albeit non-binding) international frameworks to lend force and authority to their data access requests. This includes the *Asia Pacific Economic Cooperation Privacy Framework*[17] and the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*.[18]

It may also be possible to refer to bilateral or multilateral trade agreements that the jurisdiction has signed (if any) if such agreements include individual data protection rights. This may be the case, for instance, in future trade agreements involving the European Union, which prohibits companies and organizations in EU states from transferring their citizens' data to countries with lesser privacy standards than the EU. In addition, the EU's recent privacy reform legislation (enforced beginning in 2018), the General Data Protection Regulation (GDPR), applies to entities outside of the EU if they track European users' data or if they offer paid or unpaid goods or services to those in the European Union.

---

16 "Where a controller takes a qualifying significant decision in relation to a data subject based solely on automated processing — (a) the controller must, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing…" United Kingdom Data Protection Act 2018, s 14 "Automated decision-making authorized by law: safeguards" (where a "qualifying significant decision" is defined as a decision that produces legal or similarly significant consequences for the data subject, is required or authorized by law, and does not fall under an exception in the EU General Data Protection Regulation).

17 Asia Pacific Economic Cooperation, *APEC Privacy Framework* (2015), (August 2017) <https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015)>, at Articles 20-31.

18 Organisation for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (2013) <http://www.oecd.org/sti/ieconomy/oecdguidelinesonthe-protectionofprivacyandtransborderflowsofpersonaldata.htm>, at Article 13, page 15.

Data access requests may draw upon these instruments to establish reasons, with normative force, for why companies should respond to users' requests to access their own data. This approach may be more effective where multinational companies are concerned—in which case, it may also be useful to point out whether the company adheres to data access laws in the other jurisdictions where it operates.

3. Developing and Deploying an Access My Info Research Project

KEY POINTS

- **This section takes readers through the process of developing and deploying a full Access My Info research project, from design to public launch. The section is divided into five phases, with further step-by-step details provided within each phase:**
  - **3.1 Research Focus**
  - **3.2 Legal and Policy Research**
  - **3.3 Pilot Study**
  - **3.4 AMI Tool Set-Up**
  - **3.5 Public Launch**
- **While the phases and steps are presented sequentially and follow the most likely and recommended chronological order, be aware that many of the steps may be completed in parallel, particularly if allocated to different individuals. Research from certain steps may also inform each other, including steps that come before them, thus the process is to some extent iterative and researchers may find themselves revising or refining the results of earlier stages as they obtain more information in later phases.**

3.1. Research Focus

Access My Info research projects are meant to answer questions related to corporate responsibility, data protection, and privacy. Some examples of questions that researchers may investigate include:

1) What personal data do companies hold?
2) How is personal data being used?

3) For how long do companies retain personal data?
4) When and for what reason do companies disclose data to third parties, and how do they transfer it?
5) What kind of data is subject to law enforcement requests?
6) To what extent do companies respond to data access requests and comply with data protection laws?

The direction of research questions will help shape the approach to an AMI project, as findings will be primarily based on analyzing companies' responses to the data access requests that users issue.

These responses will be collected in at least two stages:

1) After the pilot study, which will act as a small test run of the larger AMI project. Section 3.3 describes how to setup a pilot study; and
2) After the public launch of AMI tool to all Internet users. Here, the tool will be open to members of the public, and will encourage those who use the tool to forward their responses from companies to the AMI research team.

One of the most important decisions to make at the outset of the project is: **what types of companies is the project investigating?** Examples of industries that other AMI projects have looked at include telecommunications companies, fitness trackers, dating apps, airlines, and social media networks.

We strongly recommend that researchers launching an AMI project for the first time select a single industry to begin with, as opposed to studying multiple industries at once. This narrowed scope has several advantages. First, companies operating in the same industry will likely collect similar types of data unique to their products or services, as well as conform to common industry data practices. Focusing on companies within one industry will thus simplify the process of formulating consistent data access requests and building the AMI tool.

For example, telecommunications companies would collect information such as IP address, website browsing history, and call logs; dating app companies would collect data such as people one has "matched" with, conversations, and dating preferences; and fitness trackers would collect information such as geolocation data from favourite running routes and biometric data such as heart rate logs. A different kind of data access request would have to be generated for each of these industry sectors, but once a request was formulated to

Ethics Approval

If conducting an AMI project in the course of academic research, or as part of an academic institution, the team may need to obtain ethics approval from the applicable university board or other appropriate bodies. This is because AMI projects involves collecting data from the public, as well as collecting and analyzing private and potentially sensitive information from individuals who volunteer their data access results.

target a particular sector, it would most likely work as a standard access request that could be sent to all companies within that sector, with few modifications.

Second, comparing results across companies from the same industry will likely result in more meaningful comparative outcomes, and focusing on a single industry will give researchers the time and space to delve more deeply into potential findings, as opposed to conducting shallower overviews across several different industry categories.

Third, if the public version of AMI reveals unforeseen glitches or obstacles that did not appear in the pilot study, then the consequences will be confined to one industry alone, as opposed to negatively affecting results across several industries at once. The team may then address those problems before expanding the study to other industries and companies.

The Office of the Privacy Commissioner of Canada provides an online guide to accessing one's personal information from a business, available at: https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/accessing-your-personal-information/.

The Hong Kong Privacy Commissioner for Personal Data provides similar guidance, in a short manual available at: https://www.pcpd.org.hk//english/resources_centre/publications/files/DAR_QnA_e.pdf.

3.2. Legal and Policy Research

The scope and effectiveness of the requests made in the course of AMI project rest largely on the legal and policy regimes around data privacy and data protection rights in the project's jurisdiction. This foundation is why completing a comprehensive review of the data rights and privacy law and policy landscape related to the chosen industry sector is critical to running AMI. We suggest reviewing Section 2 (Privacy, Data Protection, and Data Access Laws), above, before continuing this section.

The DAR that users send to companies through the AMI tool should make reference to the laws the request is relying on, as well as the laws that require or encourage the companies to respond with the requested data. If the team lacks legal expertise, we advise seeking legal assistance at this stage. Alternatively, the regional or national Data Protection Authority (DPA) may have published guides or

manuals available which summarize the law and that provide straightforward steps and information for non-legal experts to follow.

The following subsections review certain components of privacy law and policy that are generally common to most countries, and which should be examined as part of the foundation of AMI research. Gaining familiarity with each component is part of the preparation required for formulating the data access requests and launching the AMI tool in a particular jurisdiction.

3.2.1. Governing Data Protection Authority (DPA)

Identify the relevant Data Protection Authority (DPA) as described in Section 2, along with their scope of responsibilities and what legal power they possess to enforce privacy rights. Furthermore, studying the relevant DPA's website is a good place to start the legal and policy review, because the website will likely have useful resources to draw upon as a jumping off point for drafting a DAR letter, particularly for teams lacking legal expertise or familiarity with legal research. Moreover, such information can clarify the kinds of assistance the DPA can provide, as well as help to determine how strong the wording in the AMI data access request could be.

DPAs may be national (federal) or regional (provincial / state), as well as supranational (*e.g.*, at the level of the European Union). They may be a dedicated standalone department or institution, or may be a smaller unit housed within another department (e.g., digital economy, innovation, or consumer protection departments), or simply a function that another department takes on. For example, the United States has no dedicated federal privacy law or privacy authority, but many privacy issues and cases are brought to the Federal Trade Commission, often under section 5(a) of the Federal Trade Commission Act ("unfair or deceptive acts or practices in or affecting commerce").[19]

If possible, establish a dialogue with the DPA, to notify the DPA of the AMI project's intentions and to possibly seek guidance. The DPA can help by clarifying its positions on aspects of the law that are unclear, such as whether a particular type of information constitutes "personal data" or "personal information" of the kind that privacy law protects, or give greater context and informed perspectives on dealing with a particular industry in context of privacy. Maintaining a relationship with the DPA also helps to build credibility for the project; such credibility can be leveraged to increase the project's ultimate impact and may be useful in any attempts to engage with the companies being studied.

19 See, *e.g.*, Federal Trade Commission, "Privacy & Data Security Update (2016)", *Federal Trade Commission* (January 2017) <https://www.ftc.gov/reports/privacy-data-security-update-2016>.

Note, however, that establishing contact with the DPA may only be helpful if the DPA is a trusted independent authority that meaningfully recognizes, upholds, defends, and enforces privacy rights to the extent its powers allow, and that would see the value in a project such as AMI.

3.2.2. Legislation, Case Law, and Regulatory or Industry Guidelines

Identify relevant privacy legislation, which will comprise laws that the country's regional and/or national legislature(s) have written and passed in the form of bills and statutes or regulations. Legislation is distinct from case law, which is decided through the courts.

Relevant legislation may exist as a standalone data protection statute or within a larger legislative regime, such as a comprehensive freedom of information and privacy law, consumer protection legislation, or human rights law.

After identifying the relevant legislation, an AMI team should research relevant case law to know how that legislation has been interpreted and applied by the courts or administrative tribunals and appeal boards, or the DPA, when the legislation has been challenged. For example, the legislation may state that companies must handle "personal data" a certain way but not specify whether or not an IP address, geolocation history, or subscriber metadata is legally considered "personal data". If the legislation itself does not define any key terms,[20] then the courts or a regulatory adjudicator such as the DPA must fill in the gaps.

Reviewing case law and past cases or investigations by the DPA can also be useful to learn more about the personal data that companies collect, as well as further details about their data protection practices. For example, if a case states that the police obtained a court order that required a telecommunications provider to release a user's IP address and list of visited sites, that strongly indicates that users' IP addresses and browsing history are types of data that telecommunications companies collect and retain for a certain amount of time.

Note that whether cases form binding precedent may depend on the legal system. Decisions and guidelines issued by the DPA may be legally binding, depending on the powers the DPA was given legislatively (or powers confirmed judicially, if there is relevant case law on the issue). It is worth recognizing that the DPA's positions and cases may hold persuasive power even if its decisions do not possess the binding character of law. Such decisions may also

20 Legislation usually includes a dedicated definitions section near the beginning, which defines key terms that appear in the law.

provide useful indicators to determine the extent of past compliance or violation of data protection principles for companies that have been the focus of earlier attention by the DPA, which may inform the research strategy.

Lastly, if any of the selected companies or their industry as a whole publishes transparency reports or their own data protection guidelines, it would also be useful to review those for more information about the company's or sector's data protection practices. Such a review may inform the data access requests and the AMI project and tool generally.

Throughout the legal, policy, and industry guidelines research, it is helpful to note what laws, policies, and regulations must or could inform the scope of the AMI project and the data access requests that the project team will ask users to send. Also note specific laws or policies that would be useful to reference within the data access request itself in order to emphasize the legal force behind users' data access requests and further encourage companies to respond accordingly.

The following points are the most important to document:

1) What laws govern an individual's access to personal information held by commercial data operators (the companies)? Do any particular rules govern how or when an individual can request access to their data held by a company? Are there laws governing how companies must respond to such requests, such as time limits, what specific content to include, and in what format(s)?
2) What types of data are protected? If "personal data" is protected, how is it defined and what constitutes personal data? How have the courts and the DPA interpreted "personal data" in the context of specific industries or activities?
3) How does the law protect personal data—are there strict legislative provisions, is it based on broad principles-based guidelines, perhaps a combination of the two, or another framework altogether?
4) Are there specific guidelines or provisions concerning the collection, recording, processing, storage, alteration, use, direct marketing, transfer to third parties, sale, or disclosure to government authorities or other parties, retention periods, and destruction of personal data? Note each of them separately and be clear what the requirements for each specific activity is.
5) Do specific industries have particular rules they need to follow? Are there any relevant guidelines issued by the DPA that apply either generally or in reference to a specific industry or representative company?

6) What is the jurisdictional scope of the legislation? Does it apply when personal data is collected from individuals in the country, by foreign companies?

7) Does the relevant data protection law or legislation mandate that each company must designate a privacy officer or any other designate to handle data privacy concerns?

3.2.3. Data Access Request: Process and Contents

Developing the text for the DAR template is one of the most important steps of an AMI research project. Drafting a template requires understanding the scope of the data access rights that users have under relevant laws and regulations, including how and to what extent companies must respond to a DAR. Technically a user *can* request as wide a scope of data as they might wish, but the law may only enforce a subset of the data requested. Knowing which requests are legally enforceable and which are not will increase the credibility of the data access request and any follow-up communications with the company.

Note what the law says about the following in particular, and incorporate the information into the template data access request and analysis of companies' responses:

User's Data Access Request

1) What is the scope of a data access request (DAR)? Does it give a person the right to:
    a) be informed whether companies collect and store their personal data;
    b) receive a copy of that data;
    c) identify what purposes the data is collected and stored for;
    d) identify to whom the data has been or may be disclosed to; and/or
    e) any other information regarding the data?
2) Is a specified form required to make a DAR? Does the request have to be in writing?

Company's Response to Data Access Request

1) What response is required from a company? Are there rules around content, length, format, level of detail, or deadlines?
2) Is there a requirement for the reply to be in a specific data format (e.g., machine-readable as well as human-readable)?

3) Does a company have to respond within a certain number of days and in a specified manner? Can they request an extension for their response and, if so, under what circumstances?

4) Can a company charge a fee? What is the fee that a company can charge? Is there a maximum amount?

5) When can a company refuse to supply the requested data (if at all)? Does the legislation allow for exceptions when requesting certain types of data?

6) What happens if the user finds that false, misleading, or incomplete material has been supplied?

7) When can an individual file a data correction request? In what manner?

8) Are there any other substantive or procedural requirements to making a data access request?

Company Requirements for Data Access Requests

Research each selected company to see if they have placed their own requirements on data access requests that must be met before the company will process them, and determine if those requirements are legitimate or can be ignored, as well as whether adhering to such requirements would be onerous to integrate into the data access request and eventually the AMI tool. For instance, if the company provides a specific form to fill out and states it will only process requests sent through that form, researchers must determine, perhaps in consultation with the DPA, whether the company's designated form is:

1) a valid requirement, which companies may ignore if not met;

2) a baseless requirement, insofar as companies cannot refuse a DAR if the request is made in good faith and otherwise contains the necessary information to process the request; or

3) merely a guideline the company suggests.

Especially in jurisdictions that provide data access rights, many companies will likely have a designated privacy officer or specific contact for users to inquire about their privacy concerns. DARs for an AMI project should be addressed, and sent, to this person or contact for each company.

3.2.4. Complaint Mechanisms and Avenues of Legal Redress

The law or the relevant DPA may provide mechanisms of redress if a data access requestor considers that a company's response has not complied with the country's data protection

laws. These mechanisms may not be immediately relevant to the AMI project, unless the researchers or users intend to submit complaints in the event of non-compliance, or intend to later advise members of the public in submitting complaints. However, awareness of these mechanisms is important to obtaining full understanding of the legal and policy landscape of a potential AMI project. Knowing available legal remedies also adds strength to the DARs when and if all parties involved understand that the law provides for potential redress and a specific resolution process if a company, for instance, ignores a DAR or responds in a way that breaches the company's obligations under data protection or privacy laws.

It is also possible that the companies themselves will possess internal resolution processes that customers may go through before taking a complaint to the DPA. Note these as well, particularly to assist with troubleshooting DARs during the pilot study and/or the public version of AMI.

Look into any complaints procedures that the chosen companies or selected industry utilizes, and note the following:

1) Is there a specific procedure for dealing with complaints? Is this outlined in a privacy policy, or customer service policy, or terms of service? What are the requirements for launching a complaint?
2) Is mediation, arbitration, or any form of negotiation between the company and data requestor required before the data requester may issue a formal complaint?
3) Is there any fee requirement for formally issuing beginning a complaint process with the company?

If there is a DPA in the jurisdiction, research the following questions:

1) Would the DPA launch an investigation upon receipt of a complaint from a user about a company not complying with their obligations in response to the user's DAR? Is this process automatic or does the DPA screen complaints to determine if there is a basis for an investigation?
2) Is there a set procedure for investigations? How will the DPA determine if the user's complaint is well-founded or if there is a case to be made against the company?
3) What is the redress mechanism if the investigation shows that the company violated the law? Does the DPA have the power to take remedial or corrective action such as enforcement notices, civil penalties, or criminal penalties?

Conversely, can the DPA dismiss the claim and deem the case resolved if the investigation shows that the company did not violate the law?

4) Is there an option to file class complaints to the DPA, where a number of data subjects (*i.e.*, people whose data was collected, used, or disclosed) jointly complain about misconduct from the same company under similar circumstances?

5) Is there a right of appeal or review of the DPA's actions and final decisions, either through an administrative tribunal or through the courts?

By the end of this phase, the AMI team should have a comprehensive understanding of the relevant jurisdiction's data protection laws, including applicable legislation, case law, regulations, and company or industry-specific guidelines and policies. All of this information will inform drafting data access requests in full as part of the next phase of the Access My Info project: the Pilot Study.

3.3. Pilot Study

The pilot study is an important preparatory stage that is intended to test the DAR templates and gather baseline response data from the selected companies. The pilot study can help an AMI research team identify and address unforeseen problems and obstacles before a public launch of the project using the AMI tool.

The pilot study involves a number of volunteers generating data access requests manually (*i.e.*, writing letters to the companies without use of the AMI tool) and sending them to the project's selected companies. As this occurs before any public campaigning, researchers arguably increase their chances of obtaining an accurate representation of companies' usual data access and data protection practices.

Without first completing a pilot study, the project runs the risk of compounding potential confusion and issues by generating a the high volume of data access requests sent through the AMI tool; such confusions or issues may negativelymay negatively impact the quality of the research data collected. However, once researchers have themselves gone through, or taken collaborative volunteers through, the entire data access request process from start to finish, they will be in a better position to predict how companies will respond to the public's requests and can move forward to the next stage of AMI accordingly.

Post-pilot-study adjustments might include, for example, refining or revising the DAR template, preparing a page of Frequently Asked Questions (FAQ) to assist the public with expected challenges in obtaining responses to their requests, noting particular rules, specifications, or lessons to build into the AMI tool in generating the DARs, or even redirecting the focus of the project altogether.

Completing a pilot study will also ensure that a minimum number of results is collected for the project, in the event of a low user response rate or in case few or no users agree to forward their DAR responses to the AMI team. However, relying on pilot results alone may be of limited use depending on the project's research goal, due to the small sample size and non-randomized nature of the study (i.e., the volunteers may be in the researchers' immediate networks, such as friends, family, or coworkers, who may not represent the average member of the public with respect to the topic being researched).

The rest of this section will take you through each stage of the pilot study:

3.3.1. Recruit and Prepare Committed Volunteers

1) Create the materials necessary to brief and prepare volunteers to ensure they are fully informed going into the pilot study. This may include preparing an oral and written explanation of AMI research projects and what research participants would be expected to do as part of the project, a brief outline of the legal framework around DARs, an explanation of what a DAR request is and a sample request, and a list of the companies selected for the study.

2) Recruit volunteers who are willing to commit to the full term of the DAR for as long as possible, including following up with the company if necessary. Volunteers should be long-term customers of one or more of the selected companies (e.g., minimum of 1 year) in order to obtain a meaningful response or range of data from the companies receiving their data access request(s). Ensure that volunteers are comfortable with sending their identification information to the selected companies since such information will be required for the company to confirm it is sending data records to the person who controls the data in question.

3) Ensure that volunteers are fully aware and informed of all that their role at this stage will entail, and that they are committed to seeing the pilot study through. A useful exercise is hosting an AMI volunteer orientation workshop to ensure that the volunteers are fully aware of the potential significance of their undertaking, including what may happen upon the submission of their DARs, and the need to follow up with the company as well as regularly update the AMI team about their interactions with the company. Volunteers must be aware of, and agree to, the time commitment, as the full process may take up to several months or longer. They must also agree beforehand to forward their results from the company to the AMI project team, particularly as obtaining these responses is the primary purpose of the pilot study.

4) Confirm at least two to three (2-3) volunteers to send data access requests for each company that is included in the AMI research project. This number of volunteers is suggested because it means that the trial phase is not jeopardized if a volunteer exits the project.

5) Volunteers should send their DARs to the different companies on approximately the same date and in the same manner. Doing so will allow for meaningful comparisons between different users' responses from the same company and will also facilitate comparisons across and between companies.

6) Volunteers should forward all responses (or copies of the responses) they received from companies replying to their data access requests to the AMI team. This data includes documentation from the companies, as well as detailed descriptions of any non-written interactions between the company and the volunteer, that are relevant to the data access request. Volunteers, or the AMI researchers, should note, for example, the time and date of the company's initial response, the method of contact (e.g., phone, email, postal mail), and the specific contents of the response. It is useful to send periodic (e.g., weekly) follow-up reminders to the volunteers for updates if they are not in ongoing contact after issuing their DARs.

3.3.2. Create the Data Access Request

The previous section (Section 3.2: Legal and Policy Research) should result in the team obtaining all of the information they need to create a full DAR template for the specific industry sector chosen. The researched laws, cases, regulations, and guidelines should indicate to the AMI team whether the data access request must be in a specific form or

Sample Data Access Request Letter for Companies in the Canadian Telecommunications Industry

[User's Mailing Address]

[Date]

[Mailing Address for Company's Privacy Officer, or Closest Appropriate Personnel]

To: Privacy Officer at **[Company]** **[Use the officer's name if available]**

Re: Data Access Request for **[User's Name]**

I am a subscriber to your telecommunications service, and am interested in understanding the kinds of personal information that you maintain and retain about me. So this is a request to access my personal data under Principle 4.9 of Schedule 1 and section 8 of Canada's federal privacy legislation, the Personal Information Protection and Electronic Documents Act (PIPEDA).

I am requesting a copy of all records which contain my personal information from your organization. The following is a non-exclusive listing of all information that [name of company] may hold about me, including the following:

- All logs of IP addresses associated with me, my devices, and/or my account (e.g., IP addresses assigned to my devices/router, IP addresses or domain names of sites I visit and the times, dates, and port numbers)
- Listing of 'subscriber information' that you store about me, my devices, and/or my account
- Any geolocational information that you may have collected about me, my devices, and/or associated with my account (e.g., GPS information, cell tower information)
- Text messages or multi-media messages (sent and received, including date, time, and recipient information)
- Call logs (e.g., numbers dialed, times and dates of calls, call durations, routing information, and any geolocational or cellular tower information associated with the calls)
- Information collected about me, or persons/devices associated with my account, using one of your company's mobile device applications
- Any additional kinds of information that you have collected, retained, or derived from the telecommunications services or devices that I, or someone associated with my account, have transmitted or received using your company's services
- Any information about disclosures of my personal information, or information about my account or devices, to other parties, including law enforcement and other state agencies

If your organization has other information in addition to these items, I formally request access to that as well. Please ensure that you include all information that is directly associated with my name, phone number, e-mail, or account number, as well as any other account identifiers that your company may associate with my personal information.

You are obligated to provide copies at a free or minimal cost within thirty (30) days in receipt of this message. If you choose to deny this request, you must provide a valid reason for doing so under Canada's PIPEDA. Ignoring a written request is the same as refusing access. See the guide from the Office of the Privacy Commissioner at: http://www.priv.gc.ca/information/guide_e.asp#014. The Commissioner is an independent oversight body that handles privacy complaints from the public.

Please let me know if your organization requires additional information from me before proceeding with my request.

Here is information that may help you identify my records:

Full Name: **[Name]**
Account Number: **[Number]**
Email Associated with Account: **[Email address]**
Phone Number Associated with Account: [Phone number]

Thank you, and I look forward to your response.

Sincerely,
[Name]

Figure 4: Sample Data Access Request template provided in Christopher Parsons (2014), "Responding to the Crisis in Canadian Telecommunications" Citizen Lab (1 May 2014) <https://citizenlab.org/2014/05/responding-crisis-canadian-telecommunications/>.

follow particular rules. The DAR template letter may look something like the following example, denoted in Figure 4. This letter was used at an early stage of AMI Canada, focusing on telecommunications companies.

As mentioned, the specific types of data requested will likely differ from industry to industry. Note as well the specific references to Canada's data privacy laws and the legal obligations that the company is subject to with respect to the data access request.

3.3.3. Process Initial Responses from Companies

Responses from the companies will vary depending on the sophistication of their data access systems and practices. Responses may include differences in the content sent back to the user, level of detail in the provided data, length and detail of the response, formatting, or whether a company responds at all.

At this stage, the responses by the companies need only be noted and kept for future analysis.

Below is the outline of an ideal response to a data access request, by TekSavvy, an Internet Service Provider (ISP) in Canada that responded to requests sent during the original iteration of AMI Canada. This response was considered satisfactory by the Canadian AMI research team because it addressed the companies' policies as specific to the request and then provides the data requestor with a specific record of their data retained by the company.

Follow-Up and Challenges to Data Access Requests

Excerpt of Sample Response from TekSavvy to Data Access Request Letter

RE: Request to Access Personal Information

Dear TekSavvy User:

Thank you for requesting a copy of records containing information directly associated with your name, phone number, e-mail, or account number. This is TekSavvy's response.

It consists of:

A. background about this response;
B. a description of our policies and practices with respect to the management of personal information, including responses addressing each type of specific record you asked about;
C. an overview of the attached report, in light of the above; and
D. a PDF containing records responsive to your request.

Items A through C are set out below. Item D is provided in a separate document.

[The rest of the letter proceeds as outlined above. To read, access the full letter at: https://perma.cc/5Q-YP-FKB9]

Figure 5.

Ideally, every company will have responded fully to every data access request in complete compliance with applicable data access laws, and there will have been no issues or barriers for the user making the request. However, challenges may occur and obtaining a full response may require persistence on the part of the volunteers and researchers. Table 1 identifies and provides recommendations for handling likely challenges in the event they arise, based on the experiences of prior AMI projects.

Challenge	Details and Recommended Responses
Company contacts data requester by phone instead of sending a written response	**Companies may call the data access requestors to confirm their identity, inquire more about the DAR they submitted or its purpose, or otherwise ask for more information. Companies may also call to state how much the DAR will cost. Calls can sometimes have a dissuasive effect on the data requestor, who may not have the requested information at hand or may be taken off guard by a high fee. Such calls can also be dissuasive because an answered phone call requires an immediate response and some volunteers may not be prepared to answer the company's questions or otherwise respond without notice.** **When receiving these calls, volunteers should ask the companies to provide any queries in written form (i.e., through email or postal mail). The volunteer should also record the date, time, and contents of the call. If the company insists on asking questions through the telephone it may be better to ask the company to call the volunteer back another time, so the volunteer can consult with the researchers and be better prepared to speak with the company representative.**
Company provides an answer that is not responsive to data access request, or is otherwise incomplete or inadequate	**Companies may answer a volunteer's DAR by providing a response that the volunteer or the AMI team does not consider to be complete or adequate. This may happen for any number of reasons and does not necessarily indicate bad faith or intentional circumvention on the part of the company.** **One reason is that companies may lack adequate internal processes for managing users' data in a way that makes it easy or quick to respond to DARs with all of the requested data. This may not reflect well on the company as far as data protection obligations go, but neither does it suggest deliberate evasion of the data access request itself.**

Challenge	Details and Recommended Responses
	For example, a previous AMI project focusing on the telecommunications industry discovered that telecommunications companies had procedures in place for processing customer service logs, billing data, or phone call records, but not for any other kind of data collected. If the researcher(s) or volunteer(s) believe(s) that the company may hold data that it has not presented to the data requester, then a polite enquiry may be in order. The enquiry could focus on whether all of the user's data given in the response is all that the company collects, or if the company collects additional data that did not get processed. Companies may also fail to respond to specific questions set out in the data access request, such as the identities of third parties that the user's data is shared with, as well as the frequency of disclosure. If the company does not cite a specific legal justification for not responding to a particular line of enquiry, the volunteer may follow up by pointing out the deficiency and reiterating the request for the missing information. If the company answers the repeated request with another inadequate or incomplete response then that may form the basis of a possible complaint to the DPA (if provided for in that jurisdiction), or the volunteer may wish to see if there is a way to launch and escalate a formal complaint through the company's internal processes.
Company requires volunteer to pay high fees to process data access request	Companies may sometimes request fees for complying with a DAR. If the applicable data protection law makes provisions for the companies to charge fees, then paying the fees may be an inescapable element of DARs issued as part of an AMI project. If, however, the statute does not state that companies have the right to charge fees, then there is a strong case that companies must comply with the DAR without charging the data requester. Other times, the legislation will allow for charging the user "at minimal cost", "reasonable fees", or "fees directly related to and necessary" to comply with the request. In these cases, the DPA may have issued decisions or guidelines which give an interpretation of what constitutes a minimal, reasonable, or related and necessary fee. Companies may base the requested fee on a fixed-cost model ("It will take $[X] to complete this request") or an hourly model ("It will take [X] number of hours at $[Y]/hr."). Data privacy legislation may provide grounds for making a complaint if the total fee is excessive. If the company requests what seems to be a disproportionately high fee for complying with the DAR, the volunteer may send the following response:

Challenge	Details and Recommended Responses
	"The [name of applicable legislation] states that access to my data should be provided "at [minimal/reasonable] cost". I do not consider the quoted fee to be in line with the spirit of the law. Given that your company is obligated to grant its [users/customers] reasonable access to their personal data, this procedure appears to put an inordinate burden on the inquirer. I am willing to pay a minimal fee as provided for in the legislation, but hope that [company] is able to comply with my data access request at a more affordable cost. Otherwise, I am aware of my right to lodge a complaint with the [Data Protection Authority]." **Another strategy is for the volunteer to adjust their request to obtaining only a sample of their data from the company, instead of a complete record. Such a request will still allow volunteers (and AMI researchers) to better understand the general character of the data that the company holds, though will forego obtaining a complete historical record of all the information the company holds on that volunteer.** **Practically speaking, a sample set of records might amount to asking for all records related to a single month's worth of activities, instead of all activities throughout the entire time the volunteer has been a user of the company's services:** *"Given the cost your company has associated with fulfilling my request for complete data records, I would like to modify my original request to obtaining a sample in the form of all data associated with one month's worth of activity. I also request that [company] waive the data access fee, given this significant reduction in the scope of my request and in light of the applicable law."*
Company does not respond at all to data access request	**If the company does not respond at all before the legally mandated deadline, the volunteer may follow up by reminding the company of their duty to respond. The reminder may take into account, if the volunteer or researchers are aware, whether the company failed to respond due to non-malicious circumstances such as not having a data protection or privacy department or team, being under-staffed or under-resourced, not having in-house legal or regulatory expertise, or if the data access request never made it to the appropriate person, or other bureaucratic issues. The volunteer may send the company a polite note reminding them:**

Challenge	Details and Recommended Responses
	"I am writing in regard to my request dated _____ for access to my personal information held by [Company]. I have yet to receive a response, and would like to remind you of your legal obligation to respond to my request within [statutory period]. In this case, that means the deadline to receive a response to my request [was/is] _____. Please respond to my request within the next [X] days. I am also aware of my right to lodge a complaint with the [Data Protection Authority] should I not receive a response within the indicated timeframe." **If the company still fails to respond after the reminder, then the volunteer may consider raising a complaint with the DPA.**

Table 1. Recommendations for handling likely challenges in the event they arise, based on the experience of prior AMI projects.

3.3.4. Debrief, Evaluation, and Recommendations for Next Phase

After completing the pilot study, the team should debrief and evaluate the entire process they and the volunteers went through with each company, highlighting any problems which arose either in the DAR process or in any other aspect of the project methodology. There may have been specific or common obstacles that prevented volunteers from obtaining their data records. Such obstacles may need to be resolved before launching the public version of AMI, particularly if the remedy can be built into the AMI tool or an obstacle preempted in the automatically generated DARs.

Consider the following when evaluating the pilot study, noting lessons for the public AMI phase:

1) What did the AMI team learn from the pilot study? Was anything unexpected or unforeseen?
2) Did all the volunteers successfully access their data as a result of their respective requests? For those who did not, what were the reasons for this?
3) Of the companies who responded, did any return data records that were inconsistent, unreadable, incomplete, or otherwise inadequate or non-responsive? Were there commonalities among deficient responses (e.g., did they all miss the legal deadline, were they all missing the same kinds of data,

did they all require persistent follow-up from volunteers, did they all quote high fees)?

4) Were there any issues of legal interpretation that needed the assistance of lawyers, the data protection authority, or another regulator? Did any other legal issues arise?

5) Did any informational or data access gaps emerge, that the data access requests could not address, and which did not seem provided for through other processes or laws?

6) Did the companies raise any obstacles that could not be solved (e.g., demanding high fees, or a prohibitively complex process)?

7) Did any of the companies' responses violate the letter or spirit of applicable data privacy laws?

8) Did the pilot study reveal complications or issues in the project methodology that need to be addressed before public launch?

9) Was the overall pilot study successful, in that it provided meaningful results that let the research team move to the next stage of the AMI research project? If not, can the shortcomings be addressed?

10) Having completed the pilot study debrief and evaluation, what are all of the tasks that must be completed (and issues resolved) before moving to the next stage of AMI?

3.4. AMI Tool Set-Up

Project leads should begin preparing the public-facing AMI tool required to launch AMI to the public following the completion, or even during the undertaking, of the pilot study. This tool is a central component of the AMI research project for at least two reasons.

First, the AMI tool is the central portal through which AMI researchers will obtain the data for their research. The tool facilitates collecting higher volumes of data by streamlining the process for generating DARs and increasing accessibility to a broader audience, through public availability and a user-friendly interface. This is important due to the necessarily limited nature of results from the pilot study, arising from its experimental and first-time nature, as discussed above.

Full details on the tool, its technical requirements, and source code are available on Github: https://github.com/citizenlab/ami.

Details on the general design of the tool can be found in the Access My Info Software Design Document, available at: https://openeffect.ca/wp-content/uploads/2017/01/ami-design-doc.pdf.

Second, a key objective of most AMI projects is to raise awareness about data access rights, related legal and policy issues, and companies' privacy practices among members of the public. Complementarily, AMI projects are intended to equip the public with the ability to exercise their data access rights, such as through the AMI tool.

3.4.1. Technical Requirements

The AMI tool is an open source web application. Deploying the tool requires an individual who is familiar with the core technologies it relies on: HTML/CSS, JavaScript, and if the optional statistics tracking module is used, PHP and MYSQL. AMI can be hosted on any web server. If the statistics module is used, server-side support for PHP and MYSQL is required

Figure 6 features a series of partial screenshots to illustrate what a completed AMI tool may look like as a user moves through the process of generating their DAR. These images are taken from the AMI tool used for AMI Canada, at a stage when the project had expanded beyond the telecommunications industry to study several industries at once.

3.4.2. Tracking Responses

The AMI tool, by default, does not collect identifying information about users. The AMI tool only collects the following statistical information:

- the company for which a request was created;
- the language it was created in;
- the request jurisdiction;
- the date and time of request, and;
- a hash-based message authentication code (HMAC) that functions as the request ID.

Users can opt out of this statistical recording.

The AMI tool statistical reporting tracks the number of unique requests which were generated for each company. However, these statistics do not indicate the actual number of people who then printed, downloaded, or copied the generated DAR and then sent it to a company using either email or postal mail.

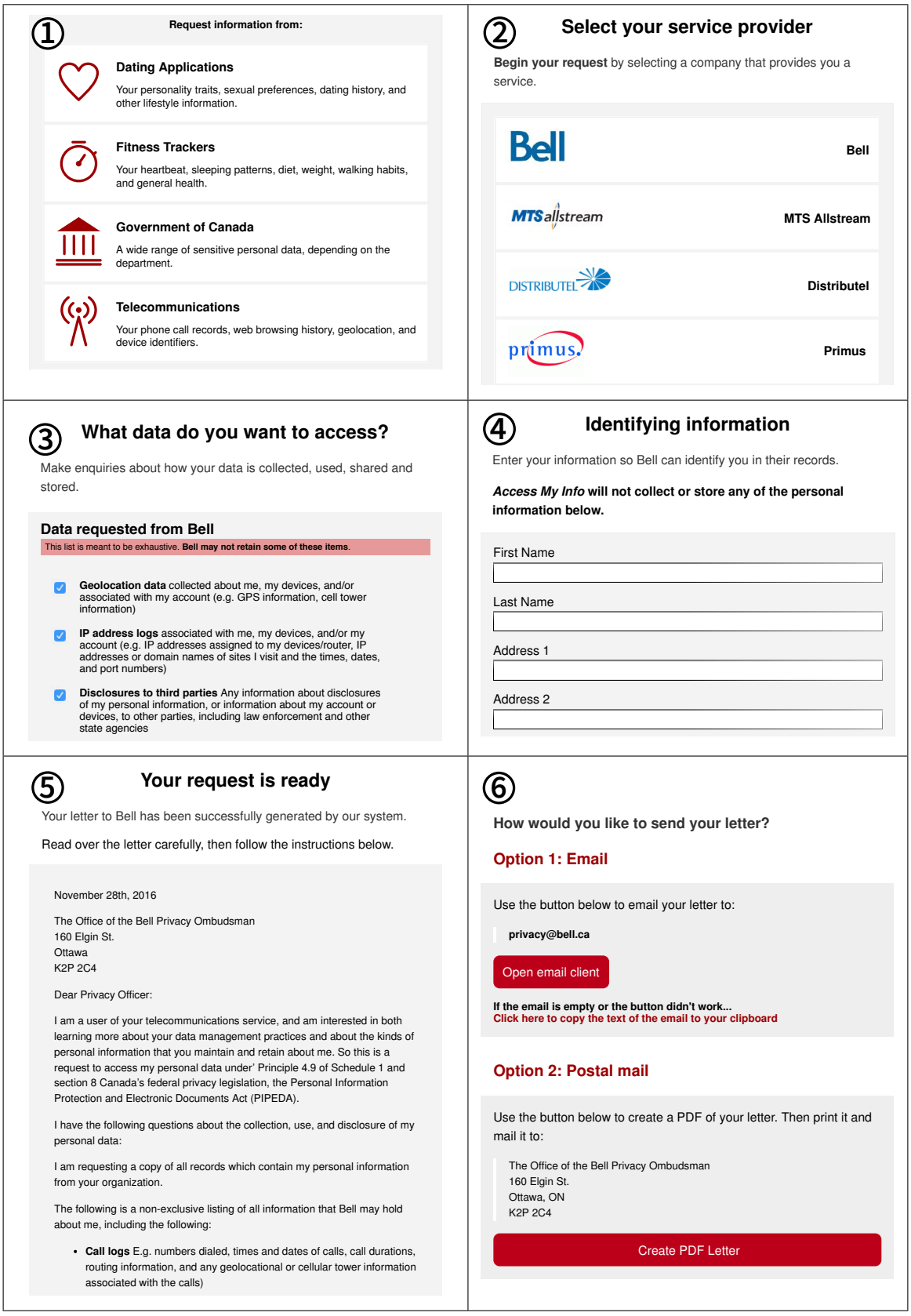


Figure 6: user interaction stages in the AMI front-end

The tool should include a contact email address inviting users to send the responses they receive from the companies to the AMI researchers, as well as invite users to contact the AMI team if they encounter problems in the process of after sending a DAR, or if they have any questions about the AMI tool itself. The AMI researchers can track commonly reported problems and draw comparisons between companies, or eventually between industry sectors, as a result of facilitating and engaging in response follow ups with participants.

3.4.3. Company Research and Information

To facilitate users sending requests to companies, the following information should be obtained for every company listed in the AMI tool:

1) Name of the company (full formal business name and more well-known name);
2) Name and title (if possible) of a designated privacy officer at each company—if there is no privacy officer, then use contact information given for privacy concerns; and otherwise use other available contact information that seems the most appropriate for this kind of request;
3) Email address of privacy officer or chosen contact;
4) Company mailing address (in case the requester chooses to send their generated request using postal mail); and
5) Any rules that the company applies to DARs (e.g., formatting or what user information to include)—where possible, these rules should be automatically integrated into the DAR that the AMI tool generates for that company; otherwise, the AMI tool should make these rules clear to the user at the relevant stage of the interface, so that they can follow them once the tool generates their DAR.

3.4.4. Local Customization to Research Jurisdiction

Customizing the AMI tool to the specific jurisdiction in which it will be deployed involves a number of considerations. We would recommend at least the following:

1) **Language:** Depending on the official and common languages in the jurisdiction, it may be necessary to translate the AMI tool into another language. This will entail translating the user interface, the legal summary, and any other information required to educate and fully inform visitors to the website, particularly if

they are to then use the tool and volunteer their information or results to the researchers. Based on previous experiences we recommend that one member of the AMI team be in charge of the language translation to ensure consistency.

2) **Branding (Colour and Logo):** You may wish to redesign the aesthetic look and feel of the AMI tool from the original and create a new logo. This will not only distinguish your project from AMI projects in other jurisdictions and make it easier to recognize, but may also potentially increase the local public's receptiveness and potentially increase the use of the tool and participation in the project.

3) **Messaging:** Effective communication strategies and styles vary depending on cultural, political, and social context. Where an AMI project is deployed may impact how related content should be communicated to users. Ensure you know your audience and tailor AMI to their needs.

3.4.5. User Instructions

We recommend the following guidelines when writing the user instructions for your AMI tool:

1) Use clear and simple instructions that include a minimal amount of technical language and jargon. At the same time, be careful not to oversimplify when it comes to explanations of the tool, data access requests, the broader research project, or relevant law and policy.

2) Warn users of the different types of results they may receive, including the various forms of pushback they may encounter from companies, and provide guidance on how to respond to such pushback efforts.

3) Encourage users to be persistent in their data access requests if they feel comfortable doing so.

4) Make clear what user information, if any, the AMI tool is collecting or sending to the AMI project researchers, and allow users to opt out of this if possible—and certainly if your local privacy laws require this.

5) Encourage users to volunteer to complete the follow-up survey, as well as encourage them to forward the responses they receive from companies to the AMI project. Emphasize the rationales and objectives driving the AMI research project, the desired outcomes and benefits for the public and the users themselves, and the value of companies' responses to this research and its goals.

3.4.6. AMI Team Contact Information

The AMI tool should have public-facing contact information so that users and other visitors to the website can contact the research team for more information, such as if they are having trouble using the tool, wish to deploy their own AMI project or tool, or wish to write a media story about AMI. This information may also be used by companies to inquire about the project and offer a chance to open dialogue with the subjects of research, such as the companies' privacy officers.

3.5. Public Launch of Access My Info

The final phase of an AMI research project involves launching the AMI tool to the public, alongside promoting the AMI project and raising public awareness in order to drive people to use the tool. The AMI team may wish to host a press conference, issue a press release and statement, or give a heads-up or send an advance or embargoed release to journalists who cover privacy, technology, human rights, business, or digital society issues, or who cover the industry that the AMI project is investigating. The team may also wish to consult a grassroots campaigning or public relations expert on tailoring the project's public messaging to the applicable jurisdiction, industry sector, and other relevant contexts.

We highly recommend that the AMI researcher(s) partner with public interest groups, advocacy organizations, academics, journalists, activists, and other related individuals and organizations to help amplify the AMI project's reach. These partners can also help better and more widely communicate the project's purpose, importance, and impact of both the process of facilitating members of the public sending data access requests, as well as of the eventual results and findings from companies' responses.

Below are resources and example materials from the public launches of AMI Canada and AMI Hong Kong, which may assist with your AMI project's communications and media strategy.

Access My Info Press Releases and Blog Posts

AMI Canada Blog Post (Citizen Lab): https://citizenlab.org/2014/06/access-information-using-ami/

AMI Canada Blog Post (Open Effect):https://openeffect.ca/access-my-info/

AMI Canada Press Release (OpenMedia): https://openmedia.org/en/press/new-access-my-info-tool-empowers-canadians-learn-what-information-their-telecom-collects

AMI Hong Kong Blog Post (Citizen Lab): https://citizenlab.ca/2016/05/access-my-info-launched-hong-kong/

AMI Hong Kong Facebook Post (AMI Hong Kong): https://www.facebook.com/AccessMyInfoHK/posts/1673353586265058

Media Coverage of Access My Info (Canada and Hong Kong)

"Are internet service providers keeping tabs on your browsing?"
Craig Desson, Toronto Star (5 March 2015)
https://www.thestar.com/news/privacy-blog/2015/03/are-internet-service-providers-keeping-tabs-on-your-browsing-.html

"Want to put a snooping government back in its place? Click here"
Marni Soupcoff, National Post (18 June 2014)
http://news.nationalpost.com/full-comment/marni-soupcoff-want-to-put-a-snooping-government-back-in-its-place-click-here

"It's time to ask your telco how it's tracking your data, Hong Kong activists say"
Josh Horwitz, Quartz (9 May 2016)
https://qz.com/678923/its-time-to-ask-your-telco-how-its-tracking-your-data-hong-kong-activists-say/

"Telecom companies fail to provide sufficient responses to personal data requests, transparency advocates say"
Kris Cheng, Hong Kong Free Press (6 May 2016)
https://www.hongkongfp.com/2016/05/06/telecom-companies-fail-to-provide-sufficient-responses-to-personal-data-requests-transparency-advocates-say/

Access My Info Press Kits

AMI Hong Kong Press Kit: https://accessmyinfo.hk/#/press-kit

AMI Canada Press Kit: https://accessmyinfo.ca/#/press-kit

4. Analyzing Results

KEY POINTS

- **Follow up with all of the users who agreed to be contacted by the AMI team after they created their Data Access Request (DAR) using the AMI tool to ensure as complete collection of all available research data as possible.**
- **During this stage of an AMI Project, the research team will engage in comprehensive analyses of all of the data and information compiled throughout the project, particularly the user survey responses and data access responses from companies (provided a meaningful number of users forward the responses they received to the AMI team). Outputs at this stage may include blog posts, press articles, academic papers, conference presentations, and other publications through which to share the research findings.**
- **The research team may wish to add a privacy policy analysis to the project, which involves reviewing each company's public privacy and data processing policies and comparing their contents to a) what the law requires; b) what each company stated in its responses to users' data access requests; and c) what the company's practices demonstrably entail, regardless of its policy or other statements.**
- **The research team may also wish to add a technical analysis to the project, which involves reverse engineering or otherwise examining each company's product(s), device(s), or service(s) using technical expertise to assess what the company's technology does in practice with users' data, regardless of corporate policy or other statements.**

This section discusses the process of collecting as many company responses as possible from users, as well as obtaining additional relevant information from users such as the details of their experiences going through the data access request process with the selected companies.

For a complete example of what the potential final product of an AMI research project may look like, refer to the Citizen Lab's report, *Approaching Access: A comparative analysis of company responses to data access requests in Canada.*

This report includes a copy of the user survey that Citizen Lab used, in addition to a full analysis of users' responses as well as findings from comparing companies' responses in multiple industry sectors. It is available at: https://citizenlab.ca/wp-content/uploads/2018/02/approaching_access.pdf.

4.1. Collecting Company Responses and Qualitative Data from Users

After users agree to submit their contact details to the researchers for follow-up communications, as described in Section 3, researchers should follow up as soon as possible by sending reminders for updates as well as a survey to ask for details about each user's experience with their data access request(s). The AMI team may wish to consult more detailed guides on formal survey methodology and best practices if it does not already have experience with conducting research surveys.

The AMI team should seek the following information from users who have completed the DAR process through the AMI tool, and who have volunteered to provide such information for research purposes. Users who completed DARs for multiple companies should ideally complete a separate survey for each company they requested data from.

Questions to ask users who completed DAR requests:

1) Did the data requestor receive all of the information that they think they had a right to receive?
2) Did the company explain its privacy policies regarding each type of data requested, including use, collection, storage, security, transfer, sale, disclosure, and purpose? How did participants assess the level of detail of the explanation?
3) Did the company (1) confirm that it collected user data; (2) explain the type of data collected; and (3) deliver a copy or records of all of the requested data?
4) What were the forms of contact between the data requestors and the companies? What were the contents and nature of these exchanges, and the date(s) and time(s) they occurred?
5) For companies that provided data records to the user, what method(s) did the company use to send the information? For instance, was the data provided securely, such as through a passworded .zip file with a separate password key, or sent in plain text over a commercial email provider such as Gmail?

6) For companies that provided data records to the user, what format(s) was the data provided in? For instance, were the data records provided as scanned images in PDF or were they provided as machine processable spreadsheets?

7) Was the company equivocal or clear regarding its disclosure of personal data to government authorities or other third parties? Did the company's response identify the specific entities they had shared the user's data with, or provide any relevant details such as when, why, and for how much the data was disclosed to other parties?

8) Did the company ask the user to pay a fee for processing the request? If so, how much was the fee? How did the user respond to the fee requirement, and what did the company do afterwards?

9) Did the company display any particular attitude towards the user or their data access request? For example, were interactions positive, neutral, or negative, and what led the user to consider the interactions were of that nature?

Other examples of completed AMI reports and publications:

Early Findings From AMI Requests: https://citizenlab.ca/2014/10/early-findings-ami-requests

Every Step you Fake: https://openeffect.ca/reports/Every_Step_You_Fake.pdf

4.2. Conducting Analysis and Reporting Findings

The project's core analysis and development of research findings occur in this stage. The analysis is based on the data and information collected through research and from users and companies throughout all of the earlier phases of the project. While the analysis and reporting phase necessarily occurs last, the research team should spend time early on thinking through what kind of analysis they intend to do and what findings they are most interested in at the outset of the project. Such early thinking about the AMI tool's design or the way data access responses are collected may help the team to best either structure data as it is obtained or mitigate administrative hurdles that must be undertaken before the analysis of data can begin (e.g., recording responses in a particular spreadsheet format that is setup prior to receiving data from participants).

Alternatively, researchers may wish to, or may have to, wait until after they have finished collecting all the user surveys and company responses that will be analyzed, and then review the contents to determine where the most meaningful findings and analyses lie. The

decision of orienting research analysis from the outset or upon the conclusion of obtaining empirical data will all depend on the specifics of the particular AMI project, jurisdiction, chosen industry sector, team members and their expertise and familiarity with the process and chosen companies, and other contextual factors.

The AMI research team may present their analysis and findings in a number of different ways, such as in blog posts, article, op-eds, working papers, conference presentations, academic papers for publication, short videos, or any other means of communicating with the public. There may also be more than one report or publication generated from the AMI research project, such as a report on early findings and then a follow-up report with deeper and more comprehensive analysis.

4.3. Expanding the Scope of AMI Analysis with Complementary Research

One way of broadening the scope of the AMI project and adding depth and meaning to the project's findings is to supplement the project results with complementary analysis. Two kinds of additional analysis fit particularly well with Access My Info: an analysis of the selected companies' privacy policies, and a technical analysis of each company's products or services and their functions, effects, and capabilities with respect to user data.

4.3.1. Privacy Policy Analysis

The privacy policy and terms of service analysis includes reviewing all of the privacy policies and terms of service of the selected companies. Such reviews should reveal what the companies state their policies are in terms of collecting, using, and disclosing customers' data. While large companies may be expected to have a professionally written policies, smaller companies may not have an adequate privacy policy or terms of service in place that outlines in detail their procedures for handling users' personal data. This absence of any policy may also be recorded as a result.

Note that some companies may not have standalone privacy policies and, instead, have embedded the equivalent content into their terms of services.

This kind of policy analysis should be used to determine what each company's privacy policy (or terms of services) says about the following elements of processing and handling users' personal data:

1) Collection of Data (types and amount of data collected);
2) Use(s) of Data and Purpose(s) of Each Use;
3) Disclosure, Transfer and Sale of Data to Third Parties (e.g., commercial affiliates);
4) Disclosure of Data to Government Agencies or Law Enforcement;
5) Retention of Data (Methods, Duration, and Purpose);
6) Security of Data (Methods);
7) Data Access and Correction (Process); and
8) Designated Privacy Officer (Name and Contact Information).

The AMI researcher(s) would then compare each company's official privacy policy with:

1) What privacy and data protection law requires of the company's privacy policy;
2) What the company presented as their policy for each piece of information that the volunteer users requested, in its responses to DARs; and
3) What the company's processes and practices appear to be in practice, regardless of what its privacy policy or terms or service or response to a user states.

For example, perhaps a company's privacy policy states that the company only collects users' data for one particular purpose, but the company reveals in responding to a user's data access request that the data is used for other purposes not mentioned in the privacy policy. Similarly, a company may state in its terms of service that it only collects user-provided registration information, while results from the data access requests revealed that the company also automatically collects geolocation data and IP addresses.

Researchers may also record the published-on date of the privacy policy or terms of service if that information is available, as well as the date they accessed the privacy policy in recording their analysis. Doing so helps researchers to track any changes to the policy, particularly if it is only available on a company's website and they are able to unilaterally change its contents without clear and obvious notice to customers. We recommend archiving the privacy policy or terms of service at time of access, such as saving a screenshot, saving it as a PDF, or using a web archiving service such as the Internet Archive's Wayback Machine, perma.cc, archive.fo, or archive.is.

One example of the privacy policy analysis done as part of an AMI project, to great effect, was the Canadian Access to Social Media Information Project (CATSMI). CATSMI reviewed the privacy policies of several social networking websites to analyze their stated positions on how they collected user information, what information they made available to the social networks' users and third-parties, as well as how that information was disclosed, and the conditions for providing user information to government agencies or law enforcement. The research team also examined whether members of these social networking sites could access their own data records held by the company and correct misleading or incorrect data by relying on provisions in Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA), despite the fact that many of these companies were not based in Canada.

The full version of *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security* is available at: https://openeffect.ca/reports/Every_Step_You_Fake.pdf

A blog post summarizing main findings from the report is available here: https://citizenlab.ca/2016/04/every-step-you-fake-final-report/

Open Effect built a dedicated webpage hosting an interactive version of the report, available here: https://openeffect.ca/fitness-trackers/

4.3.2. Technical Analysis

Completing a technical analysis for each company involves determining and recording how their products and services work on a technical level, with particular attention paid to collecting, using, and making available (deliberately or inadvertently) users' personal data. This includes examining the data that is actually collected by the company's technology, regardless of what its privacy policy or response to data access requests state, as well as investigating the level of security and encryption deployed around use, storage, and disclosure of personal information. Note that this type of analysis requires technical expertise in order to analyze how the product or service works and specifically what it does on a technical level. Teams undertaking a technical analysis may potentially engage in activities designed to reverse engineer or deconstruct the company's products or services; they should be aware of, and consult a qualified lawyer about, the legal implications of such activities before undertaking these research activities.

A technical analysis may answer some of the following questions:

1) What categories of data does a technical analysis reveal that each product or service actually collects?
2) What technical security mechanisms are in place for each product, device, or service with regard to data collection, storage, security, and transmission practices?

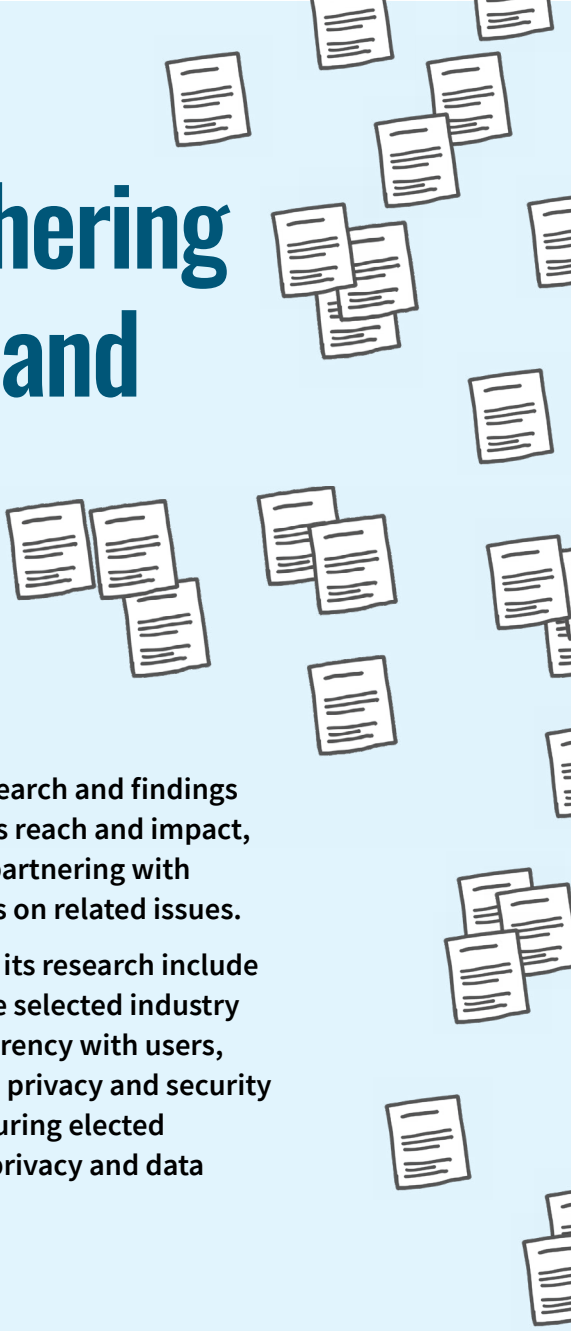
3) What data, or categories of data, could an unauthorized third-party obtain by targeting security mechanisms that the company has put in place (if any)?

4) What is the level of ease with which unauthorized third-parties of various skill and determination could access user data?

In 2016, Open Effect and The Citizen Lab published an Access My Info report focused on the fitness tracker industry, *Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security*.[21] This report included a technical analysis of fitness tracking devices—excerpted in the sidebar—in addition to a privacy policy analysis, legal analysis, and findings based on responses obtained through the AMI tool. The report found that the examined fitness tracking devices collected a wide range of personal information that was then transmitted back to each company's servers. Researchers also discovered a number of security vulnerabilities around sensitive information, such as geolocation data.

21 Andrew Hilts, Christopher Parsons & Jeffrey Knockel (2016), "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," Open Effect <https://openeffect.ca/reports/Every_Step_You_Fake.pdf>.

5. Publicizing and Furthering Impact of Research and Analysis



KEY POINTS

- **The project team should consider publicizing their research and findings from the Access My Info project to amplify the project's reach and impact, such as through communicating with journalists and partnering with grassroots advocacy groups who run public campaigns on related issues.**
- **Possible outcomes of a well leveraged AMI project and its research include raising public awareness, persuading companies in the selected industry to improve their data protection practices and transparency with users, causing the local data protection authority to launch a privacy and security reviews of the industry sector(s) under focus, or pressuring elected officials to engage in legislative reform to strengthen privacy and data protection laws.**

5.1. Research Communications and Impact

For those interested in furthering the impact of the Access My Info project or who wish to advocate for change in light of research findings, there are many ways to amplify research results and to assist others in using AMI research for advocacy purposes. AMI project teams have routinely partnered with grassroots advocacy groups and other non-profit organizations to bring issues into the public spotlight, such as transparency to government surveillance practices which are facilitated by telecommunications service providers.

Similarly, AMI research results have been used to help achieve various policy and public education objectives, such as:

1) Building public awareness about data privacy rights by sharing findings with the public through press conferences, print and electronic media, and other user-friendly formats;
2) Pressuring the data protection authority to clarify the law and its interpretation;
3) Encouraging the data protection authority and companies to develop and implement better industry practices;
4) Demonstrating the extent to which companies are (or are not) complying with data access laws;
5) Creating momentum for legal or policy reform in data privacy and data protection; and
6) Persuading industry to establish initiatives such as voluntary transparency reports, or persuading the data protection authority to impose transparency reporting as a new requirement of collecting, processing, or retaining personal information.

Potential partners for disseminating or mobilizing Access My Info research results and increasing the project's impact include journalists, activists, human rights groups, technology and digital policy specialists, advocacy groups, non-governmental organizations, and academics in related fields.

Examples of Impact from Access My Info Projects

AMI Hong Kong

After AMI was launched in Hong Kong, a joint meeting with the researchers, data protection authority, industry, and a legislative official was held to consolidate the results of AMI and chart a path forward. The purpose of the meeting was to ensure that everyone was on the same page in relation to AMI. The DPA clarified aspects of the law related to the industry. The meeting also culminated in a discussion of a possible industry initiative to launch transparency reports.

AMI Canada: Telecommunications Providers

Following the release of AMI in Canada and a significant number of requests made by users, Canadian telecom companies began publishing transparency reports that addressed some of the questions that were asked in

AMI data access requests. The research team believes that through repeated AMI requests the companies could see that openly publishing information about data handling practices in transparency reports would be an easier way to reply to users and likely reduce the number of subsequent requests received.

AMI Canada: Fitness Trackers

Access My Info Canada's fitness tracker research garnered media attention from around the world when it was released in 2016. [22] Later that year, the Office of the Privacy Commissioner of Canada announced that it would be joining a "global privacy sweep" of connected devices, or the Internet of Things, taking responsibility particularly for examining the data and security practices of connected health devices such as sleep monitors and fitness trackers. [23] The AMI project was likely only one of many influences leading to this outcome; however, the high-profile public engagement and media attention helped to keep the issue top of mind for regulators (such as data protection authorities) and the public alike.

22 See, *e.g.*, Jordan Pearson (2016), "Courts and Insurance Companies Need to Realize Fitness Data Can Be Spoofed", Vice/Motherboard (2 February 2016) <https://motherboard.vice.com/en_us/article/xygdyq/courts-and-insurance-companies-need-to-realize-fitness-data-can-be-spoofed; Jon Fingas (2016), "Your fitness tracker probably has security issues", Engadget (2 February 2016) <https://www.engadget.com/2016/02/02/fitness-tracker-security-flaws/; Stephanie Mlot (2016), "Is Your Fitness Tracker Leaking Data?", PC World (3 February 2016) <https://www.pcmag.com/article2/0,2817,2498807,00.asp; "Sicherheitsrisiko Fitness-Tracker", GQ.de (10 February 2016) <https://www.gq-magazin.de/auto-technik/computer-gadgets/studie-sicherheitsrisiko-fitness-tracker; Geoffray Sylvain (2016), "Les bracelets connectés trahissent vos données personnelles", Aruco (9 February 2016) <https://aruco.com/2016/02/open-effect-securite-donnees-bracelets/; and Ana Rita Guerra (2016), "Pulseiras de fitness permitem seguir usuários via Bluetooth, excepto Apple Watch", Bit Magazine (3 February 2016) <https://www.bitmag.com.br/2016/02/pulseiras-de-fitness-permitem-seguir-usuarios-via-bluetooth-excepto-apple-watch/>.

23 Office of the Privacy Commissioner of Canada (2016), "Canada examines health devices during 2016 'Internet of Things' global privacy sweep", Press Release (11 April 2016) <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_160411/>; and Office of the Privacy Commissioner of Canada (2016), "2016: Internet of Things/Health Device Sweep", Office of the Privacy Commissioner of Canada (11 April 2016) <https://www.priv.gc.ca/en/about-the-opc/what-we-do/international-collaboration/international-privacy-sweep/2016-internet-of-thingshealth-device-sweep/>.

Figure 7.

Appendix

A1. History of Access My Info

The Citizen Lab and Open Effect first launched Access My Info in Canada in 2014[24] to investigate companies' data protection practices after reports surfaced that Canada's telecommunications companies had received nearly 1.2 million annual requests for subscriber data from law enforcement agencies.[25] Data generated from this AMI research project helped researchers to understand precisely what kinds of personal information telecommunications companies collected, how long telecom companies were retaining information, and for what purposes. The project was meant to increase public understanding of what information telecommunications companies were gathering and retaining about users, as well as to garner an understanding of companies' relative willingness to share such information with their customers.

The Canadian launch of AMI revealed that many Canadian telecommunications companies had incomplete or immature data access practices, and included companies:

- Phoning users who had requested their data, rather than respond in writing;
- Requesting high processing fees, despite data access legislation mandating "minimal cost";
- Providing inaccurate data;
- Providing the data to the wrong customer; or
- Not providing full records as the law mandated.[26]

Because most of the data that customers previously requested from the telecommunications companies usually revolved around customer services records (in order to make claims), these companies seemed to lack practices around providing other types of personal data after receiving a request. Following the initial launch of AMI Canada, along with other efforts to encourage companies to explain their data management practices, some Canadian telecommunications companies developed more robust practices to address DARs; many established more consistent response processes after six to eight months.

---

24 *Ibid.*

25 Laura Payton (2014), "Private data given to feds limited to 'basic' information, Bell says," CBC News (30 April 2014) <https://www.cbc.ca/news/politics/private-data-given-to-feds-limited-to-basic-information-bell-says- 1.2627043>.

26 Andrew Hilts and Christopher Parsons (2014), "Early findings from AMI requests," Citizen Lab (6 October 2014) <https://citizenlab.ca/2014/10/early-findings-ami-requests>.

In May 2016, researchers from the Chinese University of Hong Kong, In-media, and Keyboard Frontline, in partnership with the Citizen Lab and Open Effect, launched Access My Info Hong Kong. AMI Hong Kong focused on Hong Kong-based Internet and telecommunications service providers. The project sought to understand and evaluate whether those companies complied with local laws when subscribers attempted to exercise their data access rights.

In June 2016, a second AMI Canada research project expanded the selection of companies to include the fitness tracker and online dating industries. In February 2018, The Citizen Lab released a comprehensive report detailing the process and research findings of all AMI Canada projects to date, with the report providing analyses and discussions of company and user responses across the telecommunications, fitness tracker, and online dating app industries.

A2. Access My Info Canada

AMI Canada Tool: https://accessmyinfo.ca

Andrew Hilts, Christopher Parsons, and Masashi Crete-Nishihata, "Approaching Access: A look at consumer personal data requests in Canada" (12 February 2018), online: The Citizen Lab <https://citizenlab.ca/2018/02/approaching-access-look-consumer-personal-data-requests-canada/>.

- This is the most recent and most comprehensive report to come out of AMI Canada. It covers a three-year AMI study of telecommunications companies, online dating companies, and fitness tracker companies operating in Canada.

Andrew Hilts, Access My Info Software Design Document, Open Effect (2017) <https://openeffect.ca/wp-content/uploads/2017/01/ami-design-doc.pdf

- This document describes the process of designing, developing, and deploying Access My Info on a technical level. It goes through the steps, design principles, requirements, and considerations that were involved in building the AMI Tool, as well as details the technical implementation of the tool in context of the broader AMI project. See also the GitHub repository at: https://github.com/citizenlab/ami-frontend

Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security" The Citizen Lab (5 April 2016) <https://citizenlab.ca/2016/04/every-step-you-fake-final-report/

- Open Effect released a report describing major security and privacy issues in several leading wearable fitness tracking devices and accompanying mobile applications. The research examined offerings by Apple, Basis, Fitbit, Garmin, Jawbone, Mio, Withings, and Xiaomi.

Andrew Hilts and Christopher Parsons, "Early findings from AMI Requests" The Citizen Lab (6 October 2014) <https://citizenlab.ca/2014/10/early-findings-ami-requests/

- This post provides a summary of early findings from users in Canada creating data access requests for telecommunications companies, using the Access My Info tool. It discusses several themes that emerged from an initial analysis of company responses to such requests.

Andrew Hilts and Christopher Parsons, "Access Your Information with AMI" The Citizen Lab (16 June 2014) <https://citizenlab.ca/2014/06/access-information-using-ami/

- This post first identifies the individual and collective benefits of using the Access My Info tool to request access to one's personal data held by Canadian data operators. It then discusses technical design decisions that went into the tool's development and implementation.

A3. Access My Info Hong Kong

AMI Hong Kong Tool: https://accessmyinfo.hk

Stuart Hargreaves and Lokman Tsui, "IP Addresses as Personal Data Under Hong Kong's Privacy Law: An Introduction to the Access My Info HK Project" (14 November 2017) J L Inf & Sci 25:2, available at: <www.jlisjournal.org/abstracts/Hargreaves_Tsui.25.html. >

- This is a published paper based on the work of AMI Hong Kong, which introduces the project and explores whether IP addresses should be classified as "personal data" under the data protection regimes in Hong Kong and in the European Union. The paper is also available on SSRN at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3074243.

Amitpal Singh, "Access My Info Launched in Hong Kong" The Citizen Lab (10 May 2016) <https://citizenlab.ca/2016/05/access-my-info-launched-hong-kong/>

- This is a blog post announcing the launch of AMI Hong Kong, which focused on telecommunications providers in Hong Kong.

A4. Privacy and Data Protection Law and Policy

A4.1. General Resources

"Data protection in the EU," European Commission, online: <https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en.>

David Zetoonny, "Data Privacy and Security: A Practical Guide for In-House Counsel," IAPP (2018), online: <https://iapp.org/media/pdf/resource_center/In-House-Counsel-2018_BryanCave.pdf.>

"Global Privacy and Information Management Handbook," Baker McKenzie (2018), online:<https://globaltmt.bakermckenzie.com/global-privacy-matrix. >

Lee Andrew Bygrave, Data Privacy Law: An International Perspective (Oxford: Oxford University Press 2014).

A4.2 Data Access Requests

"Accessing your personal information," Office of the Privacy Commissioner of Canada (2 March 2018), online: <https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/accessing-your-personal-information/.>

"Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users," Guidance Note, Privacy Commissioner for Personal Data, Hong Kong (June 2016), online: <https://www.pcpd.org.hk/english/publications/files/DAR_e.pdf.>

"Guide to the General Data Protection Regulation (GDPR)," Information Commissioner's Office (United Kingdom), online: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/.>

A4.3. Defining "Personal Data"

"PIPEDA Interpretation Bulletin: Personal Information," Office of the Privacy Commission of Canada (11 October 2013), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_02/. >

"The Ordinance at a Glance," Privacy Commissioner for Personal Data, Hong Kong, online: <https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html. >

"What is personal data?," European Commission, online: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. >

"What is personal data?," Information Commissioner's Office (United Kingdom), online: <https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/. >

Access My Info Checklist

Quick Reference Guide

What Is Access My Info?

Access My Info (AMI) is a research project, research methodology, and research tool in one. AMI leverages user data access requests to private companies to learn more about how those companies collect, retain, process, and disclose individuals' personal data. The AMI tool is a web application that automatically generates written data access requests for individuals to submit to selected companies.

Access My Info Checklist

The Access My Info Checklist is a companion document to the Access My Info Playbook, which is a comprehensive step-by-step manual to designing and implementing a full AMI project from beginning to end. This Checklist condenses all of the key steps of an AMI project, each of which the Playbook discusses in detail. Use this as a quick reference guide or checklist when planning your own AMI project.

1. Research Focus

- ❒ **Decide what specific research question(s) you intend your AMI Project to answer.**
- ❒ **Decide what companies or industries the AMI Project will focus on.**
- ❒ **Secure ethics approval if necessary (e.g., if implementing AMI as part of a formal research project at an academic institution).**

2. Legal and Policy Research

Research relevant privacy and data protection legislation, case law, regulations, and policies, noting those that will add legal or persuasive force to your data access requests.

- ❒ Seek legal assistance if your team lacks relevant legal expertise.
- ❒ Check the local data protection authority's (DPA's) website for guides and resources.
- ❒ Review case law to determine how the courts or tribunals have interpreted legislation.
- ❒ Review cases, investigations, and precedents set by the DPA.

- ❒ Review any transparency reports or data protection guidelines published by any of the companies that your AMI Project is focusing on.

- ❒ **Identify the local data protection authority (DPA) and establish the scope of their powers, to note in cases where companies do not comply with data access requests or data protection laws.**

  Note: Only reach out to the DPA and give them notice of your AMI Project and obtain additional insights if you believe that the DPA is an independent trusted authority that meaningfully protects privacy rights.

3. Data Access Request (DAR)

Determine the contents of the data access requests that will be used throughout the project.

- ❒ Note what the law says about the contents and process of a data access request, and about how companies must respond, and incorporate those insights into the template DAR.

- ❒ **Research each company you have selected for the AMI Project to see if they have their own requirements that user DARs must meet. Determine if those requirements are valid.**

- ❒ **Identify the privacy officer at each company and address all DARs to each respective officer, or otherwise to the designated contact each company provides for addressing privacy enquiries.**

- ❒ **Prepare strategies to troubleshoot DARs if companies return unsatisfactory responses or are uncooperative. Are there internal complaint mechanisms, and what can the DPA do in response?**

4. Pilot Study

Recruit and prepare volunteers to send DARs to the selected companies.

- ❒ Ensure volunteers understand the scope and duration of their commitment.

- ❒ Secure multiple volunteers per company, in case any withdraw, and to obtain a fuller view of each company's responses and data protection practices.

- ❒ All volunteers should send their DARs at the same time, for research consistency, and forward their responses from companies to the AMI research team.

- ❒ **Create the data access requests (DARs) based on legal and related research in earlier phases.**

- ❒ Collect and store responses from companies as volunteers send them to you.

- ❒ Follow up with volunteers and assist with responding to companies' challenges to DARs (e.g., inadequate, incomplete, or non-responses; demanding high fees; or declining to provide responses in writing).

- ❒ Debrief and evaluate results of the pilot study to determine adjustments to the AMI methodology or revisions to the DAR template before progressing to next stage of project.

5. Set Up and Deploy The AMI Tool

- ❒ If not already on the team, obtain assistance from someone familiar with javascript, Wordpress, and node.js, which are the core technologies of the AMI Tool, an open source web application.

- ❒ Consider procuring a server to host the web application, if needed.

- ❒ Customize the AMI tool, language, and content to the relevant jurisdiction and industries.

- ❒ Obtain and integrate all of the necessary information which is related to the targeted companies, such as contact information and company-specific criteria or required user information for data access requests.

- ❒ Provide a clear notice to users of what data the AMI tool collects and for what reason.

- ❒ Encourage users to opt in to being contacted by AMI researchers, to follow up on their DAR experience and ask them to forward copies of their responses from companies.

- ❒ Provide a way for users to contact your AMI team and invite them to do so if they encounter problems after submitting a DAR.

Refer to full documentation for further details on implementing the AMI Tool:

- ❒ Technical requirements and source code: https://github.com/citizenlab/ami

- ❒ Designing the tool: https://openeffect.ca/wp-content/uploads/2017/01/ami-design-doc.pdf

- ❒ Include user instructions and a Frequently Asked Questions (FAQ) guide. You may use the one available at (URL), modifying the contents as needed for your specific project and jurisdiction.

6. Public Launch of Access My Info

- ❒ **Create and implement a media and public communications strategy to bring the desired amount of attention to the AMI project possible to the AMI project and AMI tool, so as to encourage members of the public to submit DARs.**

  For example, issue a press release and statement, contact journalists, host a press conference, and/or partner with a civil society or grassroots advocacy organization to amplify reach.

7. Analyzing Results

- ❒ **Ensure that you have followed up with all users who agreed to be contacted by the AMI team.**

- ❒ **Comprehensively analyze all materials and data collected, including companies' responses to DARs, DAR-related correspondence between users and companies, and users' experiences.**

- ❒ **Consider supplementing the core analysis with a privacy policy analysis and/or technical analysis.**

- ❒ **Write up analysis and findings in a formal report or paper.**

8. Publicizing Research and Furthering Impact

- ❒ **To increase the impact of your project, consider collaborating with grassroots advocacy groups, journalists, activists, or policymakers who may use your research findings to bring certain issues into the public spotlight and advocate for legal, policy, or industry reform.**