

INSTITUT C.D. HOWE INSTITUTE

COMMENTARY
NO. 579

Open Banking in Canada – The Path to Implementation

Open banking, in which consumers control and can safely access their own financial data, is the next wave in financial services. Getting there requires a step-by-step approach. Here is a three-stage roadmap.

Thorsten V. Koeppl and Jeremy Kronick

The C.D. Howe Institute's Commitment to Quality, Independence and Nonpartisanship

The C.D. Howe Institute's reputation for quality, integrity and nonpartisanship is its chief asset.

Its books, Commentaries and E-Briefs undergo a rigorous two-stage review by internal staff, and by outside academics and independent experts. The Institute publishes only studies that meet its standards for analytical soundness, factual accuracy and policy relevance. It subjects its review and publication process to an annual audit by external experts.

As a registered Canadian charity, the C.D. Howe Institute accepts donations to further its mission from individuals, private and public organizations, and charitable foundations. It accepts no donation that stipulates a predetermined result or otherwise inhibits the independence of its staff and authors. The Institute requires that its authors disclose any actual or potential conflicts of interest of which they are aware. Institute staff members are subject to a strict conflict of interest policy.

C.D. Howe Institute staff and authors provide policy research and commentary on a non-exclusive basis. No Institute publication or statement will endorse any political party, elected official or candidate for elected office. The views expressed are those of the author(s). The Institute does not take corporate positions on policy matters.

About The Authors

Thorsten V. Koeppl
is Professor and RBC Fellow in the Department of Economics at Queen's University and Scholar in Financial Services and Monetary Policy at the C.D. Howe Institute.

Jeremy Kronick
is Associate Director, Research, C.D. Howe Institute.

Commentary No. 579
September 2020

Daniel Schwanen
Vice President, Research

$12.00
ISBN 978-1-989483-43-5
ISSN 0824-8001 (print);
ISSN 1703-0765 (online)

The Study In Brief

In Budget 2018, the federal government announced that it would review the merits of open banking. In January 2020, the Advisory Committee on Open Banking determined that the benefits of open banking outweighed the cost and what was needed was a plan for implementation. In this *Commentary*, we outline a possible plan, along three key themes:

- how to generate value for consumers;
- how to build a secure infrastructure for data sharing; and
- how to improve the regulatory framework to protect consumers.

With respect to value for consumers, we argue that constrained market experimentation should be the guiding principle. Third party providers (TPPs) should be allowed to start offering their services to consumers in a controlled environment where policymakers take into account potential risks that not all consumers may benefit from open banking.

On building a secure infrastructure for data sharing, consumers need to gain control over the data they generate. Technology needs to be standardized and improved so that consumers can manage data access in a ubiquitous, secure, and easy way. We argue in this paper for clear legislation for data privacy, a digital ID system, and a clear liability framework regarding data sharing and usage.

Lastly, on regulatory framework and consumer protection, Canada's regulatory framework needs to be brought into the age of Fintech. This will involve a new framework for handling consumer complaints from TPPs and a concerted effort by the federal government and the provinces to streamline financial regulation across jurisdictions and integrate such regulation across different areas.

Our message is one of cautious optimism that open banking will ultimately benefit Canadian households and businesses.

The development of a modern digital ID system and an overhaul of privacy laws are clearly pressing issues where open banking may very well provide a push in the right direction.

Our considerations and recommendations could move open banking along, but are unlikely to solve the regulatory fragmentation problem writ-large, a problem that hampers innovation in the financial services sector more generally. Therefore, open banking will very likely have to stay narrow at first in reach and in the types of activities allowed. In the long run, for open banking to become an unequivocal success, Canada will require a fundamental and extensive overhaul of its regulatory framework. Open banking may very well be the catalyst to achieve such change. If not, Canada is unlikely to realize the same benefits from Fintech that other countries like the UK and Australia are likely to enjoy.

Policy Area: Financial Services and Regulation.
Related Topics: Banking, Credit and Payments; Competition; Consumers' Interests and Protection; Financial Innovation and Technology; Financial Stability.
To cite this document: Koeppl, Thorsten V., and Jeremy Kronick. 2020. *Open Banking in Canada – The Path to Implementation.* Commentary 579. Toronto: C.D. Howe Institute.

C.D. Howe Institute Commentary© is a periodic analysis of, and commentary on, current public policy issues. James Fleming edited the manuscript; Yang Zhao prepared it for publication. As with all Institute publications, the views expressed here are those of the authors and do not necessarily reflect the opinions of the Institute's members or Board of Directors. Quotation with appropriate credit is permissible.

To order this publication please contact: the C.D. Howe Institute, 67 Yonge St., Suite 300, Toronto, Ontario M5E 1J8. The full text of this publication is also available on the Institute's website at www.cdhowe.org.

Every time a person or business makes a payment or engages in a financial decision (for example taking out a mortgage or using a debit card to make a purchase), data are generated within the financial system. As financial institutions create internal records while intermediating these transactions, they gain plenty of valuable data about their customers.

Financial institutions are thus in an enviable position. Data possession is a massive competitive advantage as it provides critical customer information. Consequently, financial institutions profit from this information to charge customer-specific prices, or by selling the information to third parties.

Open banking changes this dynamic fundamentally, by putting customers (be it households or businesses) back in charge, allowing them to decide when a provider can access their financial data from institutions that have collected them. If customers so choose, they can give a third-party provider (TPP), or for that matter any other financial institution, open access to all the data from their bank or non-bank financial institution. Put another way, open banking breaks the monopoly banks and non-bank financial institutions currently have on their customer data.

The big idea behind open banking is, therefore, that giving customers of financial institutions control over when and how to share their financial data would help spur the development of the types of tailored products and services that create a more innovative and competitive market – one that ultimately benefits the consumers of financial services.

In Budget 2018, the government announced that it would review the merits of open banking. The minister of finance appointed an Advisory Committee on Open Banking (henceforth Committee) to undertake the review. The first stage consultation paper was released in January 2019. One year later, after extensive consultations, the Committee recommended (while replacing 'open banking' with 'consumer-directed finance') "the development of a framework to enable consumer-directed finance."[1]

The report clearly establishes that open banking is to proceed only along the dimension of data sharing that accompanies existing financial services. It is not to encompass new service providers that carry out direct, potentially new, financial transactions for customers. This distinction is often labelled as "read" vs. "write" options for open banking and is important to keep in mind for our discussion. Open banking will still rely on transactions of the existing institutions at the core of the financial sector such as banks, investment brokers and insurance companies. However, under the "read-only" option that Finance has outlined, new service providers will, for example, be able

The authors thank Farah Omran, Parisa Mahboubi, Rosalie Wyonch, Julien Brazeau, Senator Colin Deacon, Victor Gomez, anonymous reviewers and members of the C.D. Howe Institute's Financial Services Research Initiative for helpful comments on an earlier draft. The authors retain responsibility for any errors and the views expressed.

1 Finance (2020).

to provide households and small businesses with financial advice.[2]

The second stage in the path to open banking in Canada will involve the Committee and the Department of Finance exploring "in greater depth some of the themes raised by stakeholders…. liability, accreditation, governance, the question of how "screen-scraping" of customer data should be dealt with, and how to build an ecosystem that is accessible to all participants" (ibid). From there, the Department will generate a white paper for further consultations.

Unfortunately, the likelihood seems remote that any implementation of open banking will occur in the desired one- to two-year timeline the Committee suggests, given the time it will take to generate a white paper, go through further consultations, and determine which recommendations to implement. Hence, there is a real concern that some TPPs will go ahead and offer significant open banking-like services during this delay with little to no regulatory guidance, thereby putting households and businesses at risk.

What is needed is a clear roadmap that outlines the best way forward for introducing open banking in a timely fashion that protects the interests of Canadian households and businesses. This map needs to be clear on how market forces, government initiatives, and adjustments to the legal and regulatory framework should work together to achieve broad benefits for consumers. This *Commentary* provides such a roadmap along the central themes put forward by the Committee and the Department of Finance, which can broadly be defined as:

- how to generate value for consumers;
- how to build a secure infrastructure for data sharing; and
- how to adjust the regulatory framework to protect consumers.

A clear roadmap significantly reduces the uncertainty created by a long, drawn-out process of consultations. For creating value in financial services, one needs to rely on market experimentation. Such experimentation can take place in an orderly fashion only when a clear roadmap is laid out so that innovative ideas can develop in parallel to a regulatory framework and infrastructure.

Within this parallel process, policymakers will have to address two main concerns. First, new TPPs cannot just recapture above normal returns or "rents" from incumbents by gaining new dominant market positions. This is not a new issue, but paramount in the context of new financial technology or "Fintech" in general, and open banking in particular. Second, new services offered by TPPs need to give broad access to households and businesses to ensure that the benefits are widespread. To the extent the market provides this on its own, no government intervention is needed. However, policymakers should be vigilant about whether the benefits are accruing to only a select few of Canada's society.

Hence, we need to adjust the regulatory framework in such a way that the benefits of open banking are realized broadly across Canada's economy, while protecting financial customers through a clear liability framework. This change involves cooperation across regulatory concerns, including anti-trust, privacy and financial stability. But what complicates this matter greatly in the Canadian context is that financial services regulation is fragmented both functionally and geographically. We suggest here a gradual approach that introduces open banking step-by-step across

2 To be clear, there can still be entry into the financial sector to carry out new financial transactions or offer new financial products. Such entry, however, is well-governed by the existing federal and provincial regulatory framework.

different financial services starting with ones that have the least regulatory hurdles.

Lastly, to build the appropriate infrastructure, governments will need to lead the way. Data access raises issues of data control, privacy protection and security. At present, we do not have the necessary infrastructure in place for open banking to succeed. Three priorities need to be addressed. First, we need to establish through legislation clear control of data for financial customers. Second, we need to ensure standards for safe access and safe storage of data. And, third, we need to build a digital ID system that allows households and businesses to control access to their data.

We proceed in this *Commentary* by first describing the technology of open banking and summarizing the results of the consultation process that has been initiated by the Department of Finance. We then outline a roadmap for open banking that centers around the economic, technological and regulatory themes.

The Technology of Open Banking

At its core, open banking is really about data control and data sharing. As such, we begin with a review of the status quo for data sharing, and discuss how open banking will change it. At present, a TPP can access consumer data with consent through a process called screen scraping. Under screen scraping, a consumer signs in, gives access to the TPP who collects the screen display, and uses that information to provide a particular service. This approach is convenient, on the one hand, as all it requires is consumer login information. On the other hand, it can also be burdensome in the case of data aggregation across a number of financial institutions. Even worse, consumers have no control over the scope of the data accessed, or how it is being used. Customers may also run afoul of their terms of agreements with their financial institutions, meaning they bear the risk of identify theft, fraud, and more.

Enter application programming interfaces, or APIs. APIs are the digital infrastructure created by incumbent financial institutions that enables data sharing across systems, and gives consumers control on scope, duration, and breadth of the data accessed by the TPP. APIs would not require consumers to hand over their personal login information. Figure 1 provides a breakdown of the two methodologies.

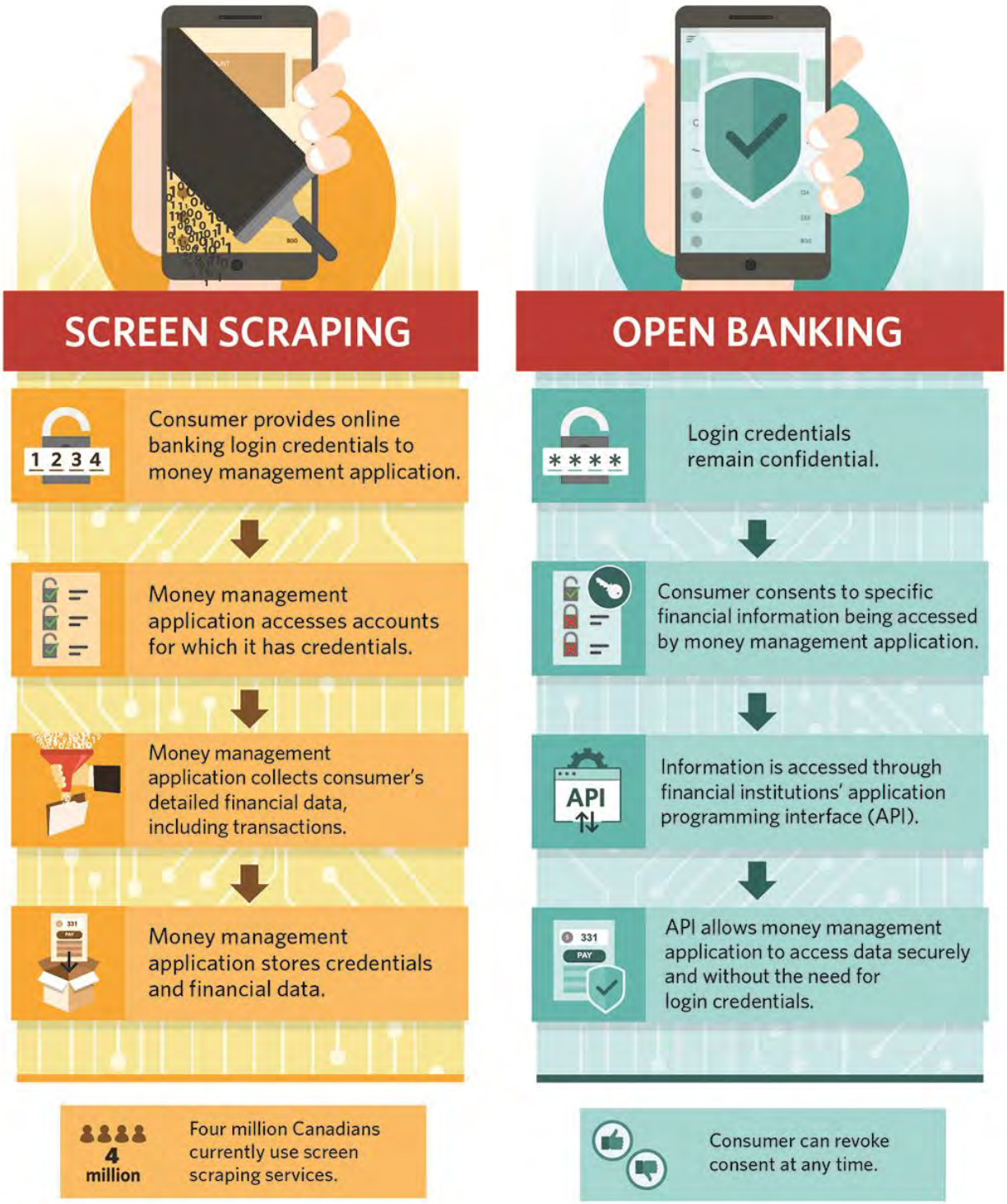
As we have seen from other jurisdictions, including the UK and EU, there are two key criteria for designing APIs: standardization, and ease of use. Standardized APIs allow safer access to customers' financial data because TPPs do not have to customize their systems for each individual financial institution. We have already seen that the lack of standardization has threatened to stifle the growth of open banking in the EU (see Kronick and Hui 2018).

However, those standards need to ensure the safety and security of customer data, while also not being so complex that customers think twice about engaging in open banking. The UK has clear standards but the authorization and authentication journey for financial customers – especially private households – has been too complex, requiring too many unnecessary steps on a complicated interface that is not user-friendly (ibid).

We raise the issue of technology because as we are about to see, the open banking framework the Department of Finance is considering is largely about data sharing.[3] Understanding how things are done will lead to clarity on what regulatory requirements are necessary for customers to reap

3 On July 29, it was announced that many Canadian financial services companies, including most of the big banks, have signed on to join the Financial Data Exchange (FDX), which will allow for a "common technical standard to share customer data" (Bradshaw 2020).

Figure 1: Screen Scraping versus Open Banking – Money Management



Source: Report of the Senate Standing Committee on Banking, Trade and Commerce entitled *Open Banking: What it Means for You* (Senate 2019) via the Library of Parliament.

the benefits in a safe and secure way, with the necessary recourse should things go wrong.

Review of the Committee Report on Open Banking

The Department of Finance announced in Budget 2018 that it would study the merits of bringing open banking to Canada. The announcement laid out a two-stage process and created the Advisory Committee on Open Banking (the Committee). The first-stage consultation, using information gathered from the experiences of other countries, began in January 2019, and asked whether open banking should be implemented. In January 2020, the Committee released the findings of this first stage. We get into the details next, but in short, it was determined that the expected benefits of open banking do in fact exceed the costs. The plan for Stage 2 involves a deeper dive into some of the big themes of Stage 1 (we will come back to this as well), followed by a consultation paper that will look at what needs to be done to implement open banking.

But let's step back and briefly review the questions and answers to the Stage 1 consultations.

The Committee was meant to "represent the broad interests of Canadians."[4] Assessing whether to implement open banking, the Committee was to evaluate how open banking might fit into three core financial-sector policy objectives:

1. "Efficiency: the sector provides competitively priced products and services, and passes efficiency gains to consumers, accommodates innovation, and effectively contributes to economic growth.
2. Utility: the sector meets the financial needs of an array of consumers, including businesses, individuals and families, and the interests of consumers are protected.
3. Stability: the sector is safe, sound and resilient in the face of stress."

More specifically, the consultation document (Finance 2019) set out to answer three questions:

1. "Would open banking provide meaningful benefits to and improve outcomes for Canadians? In what ways?
2. In order for Canadians to feel confident in an open banking system, how should risks related to consumer protection, privacy, cyber security and financial stability be managed?
3. If you are of the view that Canada should move forward with implementing an open banking system, what role and steps are appropriate for the federal government to take in the implementation of open banking?"

Critically, the Department of Finance focused specifically on financial transactions data – think withdrawals or chequing account balances – from federally regulated banks that are squarely in the purview of the minister of finance. The consultation document did acknowledge, however, that any conclusions reached could also apply to other types of consumer data, and as such, we sometimes take a broader perspective in this *Commentary*.

The document was also clear on the difference between the core part of open banking, which is the sharing of financial transactions data (the "read" option), and payments initiation (the "write" option), whereby TPPs make payments out of accounts belonging to households and/or businesses. While such "write" capabilities of open banking are indeed happening in some jurisdictions, it adds a layer of complexity. The document was clear that, should open banking proceed on the "write" option as well, it would have to do so alongside the ongoing Payments Canada modernization framework.

4 See Finance (2019) for more.

In January 2020, the Department of Finance released the findings from its consultation process. The conclusion: Canada should move forward with implementing open banking.

Through its consultations, the Committee quickly realized that, while a cost-benefit analysis on open banking made sense as a starting point, data sharing is already happening. It is likely that some 3.5- to 4-million Canadians use some kind of data-driven services either for personal or for business reasons, and typically through screen scraping.

In light of this finding, the questions under consideration changed slightly with the Committee positing the following (Finance 2020):

- "Will the market develop sufficiently to satisfy objectives of benefiting consumers, promoting innovation and ensuring financial sector stability?
- Alternatively, could a framework that sets the ground rules for data sharing in banking and financial services improve consumer protection, deliver broader benefits to Canadians looking to manage their finances and promote innovation in the data and digital economy?"

The Committee found that the risks around open banking – consumer protection, privacy issues and cybersecurity – arise in many ways, because there is no formal framework currently in place for open banking to develop through experimentation within the financial industry. We fully agree with this view and stress that putting an appropriate framework quickly in place will help mitigate many of these risks.

The Committee identified the following principles that could underlie such a framework (ibid):

- "Consumer-directed finance should be focused on enabling consumer choice and meaningful control. Consumers, including small businesses, should be able to securely direct and control the use of their data in ways that benefit them.
- Consumer-directed finance should give consumers confidence and engender trust. It should be secure; respect and enhance privacy; and, be an improvement over the status quo. If something goes wrong, there must be a clear and straightforward accountability mechanism for consumers and a means to ensure that liability rests with the appropriate party.
- Innovation should guide the development of consumer-directed finance, founded on a safe, secure and standardized data-sharing mechanism. While privacy and cyber security concerns are real and must be addressed, equal weight must be given to ensuring the growth of a vibrant financial ecosystem and technological innovation."

The proposed framework "could require participants to use a more secure form of technology and set rules for how market players must design for and meet requirements for cybersecurity, privacy and consumer protection" (ibid). It must also be accessible for as broad a range of stakeholders as is possible, be done in consultation with regulators across industries and the country, and include a liability framework that ensures that TPPs assume liability risk.

To this end, the Committee identified the following key themes that must be tackled in the Stage 2 consultations around implementation: accreditation that ensures consumer protection but also a competitive market; governance; what to do with screen scraping; and, making the system available to everyone. We largely agree with the themes for further investigation but a better way to think about these themes for implementation is along the following lines: economic (consumer surplus); technological (infrastructure); and regulatory (consumer protection). Our roadmap for implementation will follow these updated themes.

A Roadmap for Fast and Secure Implementation of Open Banking

We start from the premise that open banking will be based only on "read" functionality, which involves

data aggregation and sharing, but not the initiation of transactions.[5]

The Department of Finance's decision to go read-only avoids the additional layer of complexity and uncertainty imposed on the system if TPPs were allowed the "write" option where they also can undertake payments, investments, credit and insurance intermediation.

Augustin Carstens, the general manager of the Bank for International Settlements (BIS), recently noted[6] that the main concern about Fintechs is to make sure that they are truly adding value and not only exploiting regulatory loopholes. For example, Fintechs that exist simply to take deposits out of the banking network, paying no interest to consumers but investing the money back in banks or money market funds earning interest, and then providing services (e.g., payments) outside the heavily regulated banking network provide no real value.[7]

The Department of Finance's decision to allow only the "read" option on the part of Fintechs can be seen as an attempt to avoid such problems. By making open banking read-only, the idea is that only TPPs that provide true value-added will survive. Activities that include only the "read" option are still far ranging, including the aggregation of consumer data to provide investment advice, access for small businesses to low-cost loans with fast adjudication, or simple advice on where to earn a higher return on consumer deposits. All transactions will still take place through financial institutions within the existing regulatory framework, thereby allowing households and businesses to profit from such services while avoiding regulatory arbitrage.

In what follows, we develop a roadmap for implementing open banking in Canada in such a "read-only" world following the three themes identified above.

Offering Value to Consumers

The guiding principle for open banking should be constrained market experimentation. What this means is that TPPs and incumbents can start offering new services to consumers in a controlled environment. We focus first on the value proposition for consumers. The next two sections will focus on the infrastructure that is necessary to make such experimentation feasible and the controls that need to be imposed on this process.

Open banking is supposed to increase consumer surplus, which in simple terms is the difference between the price consumers actually pay for a good or service in the market and the (higher) price they would be willing to pay. In competitive financial markets, financial institutions will keep transaction costs as low as possible and pass on consumer surplus in the form of competitive interest rates to customers. In less competitive markets, the opposite is true: financial institutions can charge additional fees and do not pass through competitive rates, thus reducing consumer surplus.[8]

To be clear, the gains in consumer surplus encompass a variety of the benefits often touted by proponents of open banking. Examples are: (i) more customized and better priced loans as a result of a

5 As mentioned above, the process of initiating transactions as well is called "write" functionality.

6 See Carstens (2018) for more.

7 To be sure, there are value-added services associated with the "write" functionality. For example, a TPP executing the spread of one's deposits across multiple banks to ensure full CDIC coverage in the low- probability event of a bank failure would reduce consumer risk.

8 There are other gains as well from open banking including increased convenience and a reduction in transaction costs, which will directly or indirectly show up in the prices consumers are charged, and therefore, in the size of the consumer surplus.

more complete data picture on respective borrowers, (ii) more real-time transaction settlements increasing convenience and reducing costs for financial customers, and (iii) lower fees for financial services as the transparency on fee structures increases.

Financial services, and in particular the Canadian banking system, are not perfectly competitive markets (see Competition Bureau 2017 and Kronick 2018 for more). Indeed, this situation is one of the main arguments driving the push to open banking. Almost by definition, then, open banking will increase consumer surplus. This becomes even more apparent when we think about the power big data confers on incumbents, who to date do not need to compensate customers for the use of this information, which they often have readily available as a by-product of intermediating financial transactions.

There are, however, a series of issues that might reduce the magnitude of the expected gain in consumer surplus from open banking.

One concern is whether TPPs end up simply recapturing above normal returns, or "rents" related to market power, from incumbents, themselves becoming dominant market players. But this is where experimentation and competition through new start-ups will help. One has to give new ideas a chance to grow and to see whether consumers value the new services being offered, especially in the context of a read-only option. And even if successful start-ups may eventually be subsumed by incumbents through corporate acquisitions, or pushed out by incumbents that offer similar services, it is hard to see that consumers will not benefit in the end from such a process.

Another concern is that benefits accrue unequally across different consumer groups. One example, as the Committee's report rightfully points out, is the potential for exacerbating the divide between rural and urban populations if differences in connectivity confer additional benefits only to more populous cities. But there are many deeper issues not discussed in the report that may be equally important and need to be considered when judging the potential success of experimentation by new start-ups.

First, open banking might force the "unbundling" of services. Not all activities performed by a financial institution, taken individually, are profitable at current prices. However, the ability of financial institutions to bundle those services with other more profitable services, enables their continued offering. If financial institutions are forced to unbundle, those activities might become more expensive, and if not provided by new entrants, be affordable only to those at the higher end of the income spectrum.

Second, a related phenomenon could be the "unpooling" of risks in financial services. Many products, from borrowing to taking out insurance, rely on pooling individual risks, often averaging or spreading the risk over a large number of customers. This aggregation is desirable for consumers, especially those individuals who are in higher-risk categories. With more data becoming available, such pooling may no longer be desirable for incumbents. While this problem is well-understood in insurance markets, it arises in financial services more generally, with open banking offering the technology to speed up the process.

A third, but more indirect concern, might be volatility in financial flows. Consider the possibility that households, based on advice from TPPs, shift their retail deposits to whatever financial institution is offering a higher deposit rate on that day. On the one hand, this represents an increase in consumer surplus for Canadians. However, this could also lead to financial instability, which has its own negative impact on consumer surplus. Canada was lauded during the financial crisis for having "sticky" retail deposits, i.e., deposits that are likely to stay at a particular financial institution even in times

of stress.[9] If this stickiness disappears, this creates uncertainty for bank funding models, and, therefore, financial stability.[10]

It is difficult to assess at this point which TPPs will truly add value, and how broad-based that value-added will be. The hope is that TPPs are able to use data and technology to their advantage to exploit market gaps that improve consumer choice and pricing to the broadest possible group. If TPPs are able to do that – and in a scalable way – they may push incumbents to provide similar services and products at competitive prices. The government will have to monitor whether this is occurring and at what expense. Here, the government can ensure that competitive barriers are removed for TPPs, following the maxim of experimentation. Of course, the government has then to also ensure that (i) an infrastructure is put in place that allows such experimentation to succeed and (ii) that there is a clear regulatory and liability framework in place to protect consumers.

Building an Appropriate Infrastructure

The appropriate infrastructure must be in place to ensure successful open banking implementation. The principles here are clear. As a first principle, the rules need to ensure that consumers control their data. This point is mainly a legal question and the purpose of legislation would be to transfer rights to certain aspects of freedom of contract.

Currently, the freedom of contract available to the incumbents allows them to refuse automated access to customer accounts by TPPs. The legislation would, in effect, transfer rights from individual financial institutions to TPPs (and other financial institutions), and would force the individual bank to accommodate requests for automated access to specific customer accounts at the direction of the customer. The legislation could also mandate Finance or some other government agency to establish data exchange standards, which would be used by financial institutions and TPP connected through open banking.

The second principle involves standardization – especially API solutions as discussed earlier – to ensure ease of access to data and enhanced protection in the form of cybersecurity. This can be implemented largely through proper regulation and supervision. Still, the issue of coordinating on IT standards remains. One strategy here is to task existing private-public partnerships to develop such standards. An example that comes to mind here is Payments Canada, which is already involved in developing standards for the payments landscape in Canada.

The third principle is to make sure we have a ubiquitous system in place that makes managing data access and control easy. This last point is critical, as it allows the simultaneous creation of better foundations for the future of Canada's digital economy. As we argue next, this capability involves leadership from governments, and in particular, is focused around the development of a digital ID system.

Building a proper digital ID system for Canada should be a major focus of the roadmap to open banking. While the notion of a digital ID has many different permutations, contrasting it with what could be considered the analog ID is perhaps the best way to explain it.

Think of all the cards in your wallet: licence, credit card, gym membership, etc. This is the analog system. Most of us take these cards everywhere we go, and if there are online functions, we must remember an inordinate amount of usernames and

9 See Ratnovski and Huang (2009) as an example.
10 Longworth (2020).

passwords. Moreover, when we go online we have no assurances of protection, nor do we have much say in what happens to our data, e.g., whether it gets sold to third parties.

A digital ID, on the other hand, would store your personal information online, and be uniquely yours. Essentially, a digital ID system would create a unique "online" identity for every Canadian. Not only could this ID be used to grant access to websites, automatically verifying the identity of a user, it could also be used to manage the privacy and control of the data one generates. Hence, a digital ID system would hand consumers direct control of their data.

There are different models for the development of a digital ID system. The first, which we have seen in countries such as Estonia, is a centralized system where the development of the digital ID is done by the government in isolation, and the data used to authenticate identification rests with the government. The second is based on public-private partnerships, an ecosystem of sorts, as we see for example in Sweden. In this case, users choose which information, from which sources, they want to use to authenticate who they are. They may choose to use the same information and same source for each transaction, but they have the option to differentiate.

Governments will be instrumental in helping develop the infrastructure, either as the one doing the developing or in setting the standards for the advancement of public-private partnerships that build a Canadian digital ID ecosystem.

A recent study (DIACC 2018) entitled the *Economic Impact of Digital Identity in Canada* by the Digital ID and Authentication Council of Canada (DIACC) estimated that a universal digital ID in Canada could provide $4.5 billion in value-added to small and medium enterprises. Based on estimates of the economic impact of digital ID in countries where it has been set up, typically 1 to 2 percent of GDP, puts the value to the Canadian economy at $15 billion – non-negligible to say the least.

We are seeing some progress on the digital ID front in Canada. The government of Canada is using pilot projects across different departments, some in collaboration with the private sector. For example, a new airport security and screening system called Known Traveller Digital Identity, developed in collaboration with Accenture, allows travellers, in advance, to digitize travel documents and biometric information to share with authorities. Imagine then an app that can store or access such information in a secure way that only the user can control. This app collects my passport, proof of vaccinations, list of countries previously visited, and necessary biometric information. I get to the airport and all I have to do is go through the security check for luggage and the items on my person that day.

Quebec is also moving forward with a digital ID with Minister of Digital Transformation Éric Caire announcing it on June 2020, with a plan to roll it out in stages, beginning in 2021 and finishing in 2025. The plan for Quebec is to partner with the private sector in the creation of a digital ID for all Quebeckers.

User control will be key in a digital ID system, where you choose which data to share, for how long, and the way in which it can be used.[11] Under the public-private partnerships model, users do not have to attempt to manage the wide swath of data they own, i.e., the data can live where it lives, but they will be able to send pointers to the data they want to share and/or revoke.

Of course, there are technological issues to iron out in creating a digital ID system. First, ensuring security since the data stored are highly sensitive. And, second, ensuring privacy in the sense that

11 See Benay (2019) for more.

customers choose which data to share. In both instances, it will be critical for governments to step in and, at a minimum, provide a set of standards for the development of public-private partnerships, or, in a more centralized system, be ready to invest heavily given the sensitivity and sheer size of the necessary infrastructure. One particular promising avenue to explore, though not the only one, is the use of blockchain.

In previous work (see Koeppl and Kronick 2017), we discussed how a digital ID could improve the collection of taxes, the delivery of services, and issuing passports, among other things. We also highlighted how this could all be done in a safer manner on a permissioned blockchain network where the government administers and manages the blockchain, and gives permission to certain Canadians to access and use the database. Historically, and indeed still today, we often rely on trusted third parties to act as intermediaries in transactions. And we rely on these third parties to verify our identity, usually by using an analog device.

The revolutionary idea with blockchain is it can solve this problem on its own. The blockchain creates an online ledger that, once distributed among the network's participants, is tamper-proof and can verify transactions without intermediaries. Therefore, we say that blockchain is a distributed ledger among participants in a peer-to-peer network that allows one to keep records and execute contracts or agreements within the network.

In a centralized system, given the sensitivity of the data stored on any potential digital ID, we are likely looking at a permissioned blockchain where only authorized participants have direct access and/or the possibility of updating the ledger. In this type of environment, distributed networks would exist with the government – possibly through a separate, independent entity to address privacy concerns – acting as a centralized administrator.[12]

This proposition does beg the question as to whether this system gives too much access to government when it comes to your data. Some of this concern is mitigated by the fact that some of this data is government-related information anyway. For the rest, rules and regulations as to what government can access do need to be put in place with a degree of transparency that allows the public to act as judge.

Complicating a centralized system further is that much of our information comes from different levels of the public sector, as well as from the private sector. On the former, your social insurance number is issued at the federal level, your driver's licence is issued at the provincial level, and your property taxes are issued at the municipal level. Coordination will be key, and likely necessary would be new legislation that forces provinces and/or regulatory authorities to report data in a comprehensive and timely manner.

Alternatively, governments could engage more with the private sector, who are already using blockchain to build digital IDs. The breadth of interactions consumers have with different stakeholders across the private and public sphere make this an appealing alternative. Such public-private partnerships would occur along the lines of the federal government's recent partnership with Accenture, discussed above. Other potentially helpful examples of where the private sector itself has advanced the digital ID cause is SecureKey's Verified.Me, which allows you to verify your identity using personal information you agree to share from your different connections, e.g., your financial institution, with the service provider you want to transact with.

How does this all relate to open banking? Above, we discussed the fact that safety and privacy of

12 For example, the privacy commissioner's office could be tasked with administering such a system. Of course, this does not get around issues such as provincial identification and record keeping being subsumed within such a federal entity.

consumer data, plus consumer-controlled access to this data, were a necessity in a read-only open banking world. A blockchain could be leveraged to build a smart contract platform where consumers can give access to their data to particular TPPs. This would put rules around what data can be accessed by a TPP. This data could be stored anywhere. On the blockchain for the digital ID system. On a private database. On a commercial platform. Of course, such a technology is not easy to build, but holds great promise for our digital future.

The development of a digital ID system only furthers the need to ensure privacy rules are firmly in place ex ante, and well understood by all. Here, developing a framework and infrastructure for open banking can be the catalyst to get us to the finish line.

Other jurisdictions have created new frameworks for privacy in the digital era, including the EU's General Data Protection Regulation. Canada has recently moved on this front as well, with the release by the federal government of the Digital Charter. There are 10 principles that define the Charter, including around Safety and Security: "Canadians will be able to rely on the integrity, authenticity, and security of the services they use and should feel safe online" (Baer and Newman 2019), as well as Control and Consent: "Canadians will have control over what data they are sharing, who is using their personal data and for what purposes, and know that their privacy is being protected" (ibid).

The Digital Charter is not law, and will require the government to amend current legislation, including the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which governs the use of personal data by businesses in Canada. The federal government has released a proposal to modernize PIPEDA, which will focus on four areas, including enhancing individuals' control, and enhancing enforcement and oversight so there are meaningful penalties if businesses break the law.[13]

We note two critical missing elements from the proposed changes to PIPEDA, announced by the government in May 2019: first, a clear dispute resolution mechanism when wrong data is shared, wrong advice is given, and/or consumers have been discriminated against; and second, a clear liability framework (Senate 2019 and Finance 2020). These issues should be rectified immediately.

The Digital Charter, alongside updates to PIPEDA, are critical to successful implementation of a digital ID system, which will ensure the benefits of open banking are realized without some of these well-known risks. Once again, the idea of a smart contract between the entity that stores the data, the TPP, and the consumer is compelling. It puts the consumer in charge, controlling TPP access to their data, independent of who stores the data. We would welcome the teaming up of government with tech companies working on such an implementation.

Protecting Consumers

The final part of our roadmap refers to the regulatory controls needed to protect consumers in an environment of market experimentation. As just described, we presume that regulation will go hand-in-hand with the development of the necessary infrastructure, including a digital ID system.

The big issues center around regulatory requirements for market conduct and consumer protection. Such regulation is absolutely crucial for open banking under controlled experimentation. If TPPs are giving you advice on where to deposit and/or invest your money, or where to take out a loan, we need oversight to ensure financial customers are not taken advantage of, and they have

13 See Baer and Newman (2019) for more.

recourse in a clear liability framework if they are. This is complicated in Canada with its complex web of regulatory bodies governing the financial services sector. For constitutional reasons, these regulatory bodies are fragmented at both the functional and geographical level.

In the case of deposit-taking institutions, oversight responsibility at the federal level is shared by the Office of the Superintendent of Financial Institutions (OSFI) and the Financial Consumer Agency of Canada (FCAC). OSFI is the federal regulator responsible for prudential regulation of federally chartered deposit institutions like our Big Five banks. FCAC is the federal regulator tasked with ensuring financial institutions are compliant with consumer protection laws. Moreover, they have the ability to apply penalties to financial institutions for non-compliance. They are also tasked with promoting financial literacy in Canada. At the provincial level, deposit-taking institutions such as credit unions and *caisses populaires* are regulated by provincial financial regulators, both in terms of prudential and market conduct/consumer protection.

So, already we see a potential problem. We have argued that since open banking will be read-only, TPPs are not accepting deposits, or issuing credit, so their aggregation of transaction data and advice based on that data falls under concerns of consumer protection. However, if they are aggregating data from a consumer with accounts at a Big Five bank and a credit union, and then providing advice, who is in charge of regulating that TPP? Coordination between the FCAC and provincial financial commissions will, therefore, be critical to implementing open banking in a fashion that protects consumers. While the Committee was clear on the need for a liability framework, and mentioned that there are a number of complex questions around the provinces and territories, details were scarce. The Senate report was similarly scarce on details, though did state clearly that the federal government, provinces and territories should "work together to modernize and harmonize their respective laws and standards in order that an open banking framework be inclusive and enable the participation of credit unions, *caisses populaires* and other provincially and territorially regulated financial institutions."

But this isn't the only problem. Let's move beyond bank data aggregation and advice, and think of open banking as open financial services, bringing in another subsector of financial services: insurance. There are potentially two big issues. First, banks are currently prohibited from sharing customer data directly or indirectly with insurance companies/agents/brokers. Under open banking, how would this sharing work if a Fintech who specializes in finding the highest savings account interest rate, also provides advice on insurance products? Second, in the case of insurance, OSFI again is the federal prudential regulator, however the provinces are in charge of licensing insurers operating within their jurisdictions, as well as dealing with issues of business conduct and consumer concerns. What if a TPP wants access to data from a big life insurer operating across different provinces? Are all provincial regulators supervising the TPP in this case? Do we need a passport system like with securities regulation?

There is no single body that regulates Fintechs in Canada. They are, instead, governed by existing regulation, including, for example, PIPEDA and anti-money laundering laws. However, it is unclear that these laws are sufficient to protect consumers once Fintechs have access to the types of data they might under open banking.

A possible approach would be to bring Fintechs into the umbrella of securities regulation. After all, they aggregate and intermediate information to give financial services advice. But once again with securities regulation, each province maintains its own provincial securities commission, in charge of supervising securities dealers. Notwithstanding, a passport system already exists whereby participants are allowed to do business in any other province.

The notable exception is Ontario, meaning other provinces have agreed to recognize Ontario-headquartered participants, but Ontario is not required to do the same. Of course, the creation of the Capital Markets Regulatory Authority is meant to bring all the securities commissions under one regulatory roof. As of writing, a little over half of the provinces and territories have signed on, with Alberta and Quebec notably standing out as holdouts. Again, the question becomes who regulates a TPP engaging in securities advice spanning multiple provincial jurisdictions.

Many securities regulators have already gained experience with Fintechs over the last few years using their sandbox approach. It is clear that we should harness this experience and use it for controlled experimentation. This experience could be the road to implementation for some of the Senate committee's recommendation that would "allow new third-party providers to safely test and develop open banking technology that meet any relevant open banking standards" (Senate 2019). One could think about further amending this approach by requiring TPPs "to carry professional indemnity insurance or provide some other comparable guarantee" as required in the report of the Department of Finance (Finance 2019).

On the issue of enforcement writ-large for open banking, we believe the Department of Finance should follow the UK in the following two regards (ibid):

1. "Implement a complaints handling process in the event of breaches to the open banking standards;
2. Create an Open Banking Service Desk to receive complaints and a Complaints Resolution Committee for disputes."

We would add one final recommendation on penalties, coming from the Senate report, with respect to Australia's customer data right, which goes beyond just financial data, but crucially includes the possibility of "criminal sanctions for non-compliance with the consent provisions."

Conclusion

In this *Commentary*, we have provided a roadmap for implementing open banking along three key themes:

- how to generate value for consumers;
- how to build a secure infrastructure for data sharing; and
- how to improve the regulatory framework to protect consumers.

On value for consumers, the guiding principle should be constrained market experimentation. TPPs should be allowed to start offering their services to consumers in a controlled environment where policymakers take into account potential risks that not all consumers may benefit from open banking.

On building a secure infrastructure for data sharing, consumers need to gain control over the data they generate. Technology needs to be standardized and improved so that consumers can manage data access in a ubiquitous, secure, and easy way. Key steps are clear legislation for data privacy, a digital ID system, and a clear liability framework regarding data sharing and usage.

On regulatory framework and consumer protection, Canada's regulatory framework needs to be brought into the age of Fintech. This will involve a new framework for handling consumer complaints from TPPs and a concerted effort by the federal government and the provinces to streamline financial regulation across jurisdictions and integrate such regulation across different areas.

While we feel cautiously optimistic that open banking will ultimately benefit Canadian households and businesses, we see the danger of missed opportunities.

The development of a modern digital ID system and an overhaul of privacy laws are clearly pressing issues where open banking may very well provide a push in the right direction.

Our considerations and recommendations may also help move open banking along, but are unlikely

to solve the regulatory fragmentation problem writ-large, a problem that hampers innovation in the financial services sector more generally (Omran and Kronick 2019). Therefore, open banking will very likely have to stay narrow at first in reach and the types of activities allowed. In the long run, for open banking to become an unequivocal success, Canada will require a fundamental and extensive overhaul of its regulatory framework. Open banking may very well be the catalyst to achieve such change. If not, Canada is unlikely to realize the same benefits from Fintech that other countries like the UK and Australia are likely to enjoy.

REFERENCES

Baer, Aaron, and Sarah Newman. 2019. "Canada's New Digital Charter and what this Means for PIPEDA." The Spotlight – Tech, Privacy, and IP Law Blog. 13 June. https://www.airdberlis.com/insights/blogs/thespotlight/post/ts-item/canada-s-new-digital-charter-and-what-this-means-for-pipeda.

Benay, Alex. 2019. "Canada needs to assert its digital identity." *The Globe and Mail*. 3 October. https://www.theglobeandmail.com/business/commentary/article-canada-needs-to-assert-its-digital-identity/.

Bradshaw, James. 2020. "Canadian financial institutions join data exchange to speed up development of open banking." *The Globe and Mail*. 29 July. https://www.theglobeandmail.com/business/article-canadian-financial-institutions-join-data-exchange-to-speed-up/.

Carstens, Augustin. 2018. "Big tech in finance and new challenges for public policy." Bank for International Settlements. FT Banking Summit Keynote Address. 4 December. https://www.bis.org/speeches/sp181205.pdf.

Competition Bureau. 2017. *Technology-led Innovation in the Canadian Financial Services Sector – A Market Study. Ottawa*. December. https://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/vwapj/FinTech-MarketStudy-December2017-Eng.pdf/$FILE/FinTech-MarketStudy-December2017-Eng.pdf.

Department of Finance. 2019. *A Review into the Merits of Open Banking*. Consulting with Canadians. https://www.fin.gc.ca/activty/consult/2019/ob-bo/pdf/obbo-report-rapport-eng.pdf.

Department of Finance. 2020. *Consumer-directed Finance: the Future of Financial Services*. Consulting with Canadians. https://www.canada.ca/en/department-finance/programs/consultations/2019/open-banking/report.html#_ftnref6.

Digital ID and Authentication Council of Canada. 2018. *Economic Impact of Digital Identity in Canada*. https://diacc.ca/wp-content/uploads/2018/05/Economic-Impact-of-Digital-Identity-DIACC-v2.pdf.

Kronick, Jeremy. 2018. *Productivity and the Financial Sector – What's Missing?* Commentary 508. Toronto: C.D. Howe Institute. May. https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Commentary_508.pdf.

Kronick, Jeremy, and Nikki Hui. 2018. "The Path to Open Banking in Canada." C.D. Howe Institute Intelligence Memo. 13 November. https://www.cdhowe.org/intelligence-memos/kronick-hui-path-open-banking-canada.

Longworth, David. 2020. *The Era of Digital Financial Innovation: Lessons from Economic History on Regulation*. Commentary 568. Toronto: C.D. Howe Institute. March. https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Commentary%20568.pdf.

Omran, Farah, and Jeremy Kronick. 2019. *Productivity and the Financial Services Sector – How to Achieve New Heights*. Commentary 555. Toronto: C.D. Howe Institute. October. https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Commentary%20555.pdf.

Ratnovski, Lev., and Rocco Huang 2009. "Why are Canadian Banks More Resilient." IMF Working Paper 09/152. July. https://www.imf.org/external/pubs/ft/wp/2009/wp09152.pdf.

Senate of Canada. 2019. *Open Banking: What it Means for You. Standing Senate Committee on Banking, Trade, and Commerce*. https://sencanada.ca/en/info-page/parl-42-1/banc-open-banking/.

NOTES:

NOTES:

NOTES:

Recent C.D. Howe Institute Publications

September 2020	Klassen, Kenneth J., and Nick Pantaleo. "Assessing the Canada Revenue Agency: Evidence on Tax Auditors' Incentives and Assessments." C.D. Howe Institute E-Brief.
August 2020	Koeppl, Thorsten V., and Jeremy Kronick. *"Going Direct": Not a New Tool, But an Old Pitfall for the Bank of Canada.* C.D. Howe Institute Commentary 578.
August 2020	Robson, William B.P., and Farah Omran. *The ABCs of Fiscal Accountability: Grading Canada's Senior Governments, 2020.* C.D. Howe Institute Commentary 577.
July 2020	Richards, John. *Student Performance in PISA 2018: Nettlesome Questions for Canada.* C.D. Howe Institute Commentary 576.
July 2020	Mysicka, Robert, Lucas Cutler, and Tingting Zhang. *Licence to Capture: The Cost Consequences to Consumers of Occupational Regulation in Canada.* C.D. Howe Institute Commentary 575.
July 2020	Robson, William B.P. *Quirks and Fixes: Accounting for Broader Public-Sector Pension Plans in Canada.* C.D. Howe Institute Commentary 574.
July 2020	Manucha, Ryan. *Internal Trade in Focus: Ten Ways to Improve the Canadian Free Trade Agreement.* C.D. Howe Institute Commentary 573.
June 2020	Ciuriak, Dan. *The Trade and Economic Impact of the CUSMA: Making Sense of the Alternative Estimates.* C.D. Howe Institute Working Paper.
June 2020	Gros, Barry. "Room to Thrive: Why Principles-based Standards Make Sense for Regulating Contingent Pension Plans." C.D. Howe Institute E-Brief.
June 2020	Mahboubi, Parisa, and Mariam Ragab. *Lifting Lives: The Problems with Ontario's Social Assistance Programs and How to Reform Them.* C.D. Howe Institute Commentary 572.
May 2020	Richards, John. "No Easy Answers: Insights into Community Well-being among First Nations." C.D. Howe Institute E-Brief.
May 2020	Baldwin, Bob. *The Shifting Ground of Pension Design: Reflections on Risks and Reporting.* C.D. Howe Institute Commentary 571.

Support the Institute

For more information on supporting the C.D. Howe Institute's vital policy work, through charitable giving or membership, please go to www.cdhowe.org or call 416-865-1904. Learn more about the Institute's activities and how to make a donation at the same time. You will receive a tax receipt for your gift.

A Reputation for Independent, Nonpartisan Research

The C.D. Howe Institute's reputation for independent, reasoned and relevant public policy research of the highest quality is its chief asset, and underpins the credibility and effectiveness of its work. Independence and nonpartisanship are core Institute values that inform its approach to research, guide the actions of its professional staff and limit the types of financial contributions that the Institute will accept.

For our full Independence and Nonpartisanship Policy go to www.cdhowe.org.



C.D. HOWE
INSTITUTE

67 Yonge Street, Suite 300,
Toronto, Ontario
M5E 1J8

Canadian Publication Mail Sales
Product Agreement #40008848