L’impact économique de l’identité numérique au Canada

Comprendre les avantages économiques considérables que cela peut apporter et le coût de l’inaction

L’identité numérique est essentielle pour le développement de l’économie numérique canadienne. Il s’agit d’un outil fondamental pour avoir des services numériques sécuritaires, sûrs, efficaces et accessibles. À défaut de cela, bien des problèmes que les Canadiens connaissent vont être amplifiés par l’augmentation rapide des services numériques hautement connectés. L’identité numérique de confiance va permettre aux bonnes personnes d’avoir accès aux bons services d’une manière efficace et sécuritaire. Ce livre blanc explore ces enjeux et les solutions nécessaires pour instaurer au Canada des systèmes d’identité numérique de confiance à grande échelle.

Table des matières

SYNOPSIS 3

1. QUEL RÔLE L'IDENTITÉ NUMÉRIQUE JOUE-T-ELLE DANS L'ÉCONOMIE NUMÉRIQUE? 6

2. QUI A BESOIN DE L'IDENTITÉ NUMÉRIQUE? 8

3. COMMENT L'IDENTITÉ NUMÉRIQUE SE PRATIQUE-T-ELLE AUJOURD'HUI? 9

4. QUEL IMPACT LES PROCESSUS ACTUELS ONT-ILS SUR L'ÉCONOMIE NUMÉRIQUE? 12

5. QUEL INTÉRÊT À PLUS GRANDE ÉCHELLE L'ÉCONOMIE VA-T-ELLE TIRER? 14

6. COMMENT LES PERSONNES ET LES ENTREPRISES VONT-ELLES EN BÉNÉFICIER? 17

7. QUEL EST LE RÔLE DU CITOYEN/CONSOMMATEUR? 18

8. QUEL EST LE RÔLE DU GOUVERNEMENT ET DES ENTREPRISES? 20

9. QUEL EST LE COÛT DE L'INACTION? 21

10. PAR OÙ FAUT-IL COMMENCER? 22

11. RÉFÉRENCES 24

Synopsis

L'identité numérique est essentielle pour le développement de l'économie numérique canadienne. Il s'agit d'un outil fondamental pour avoir des services numériques sécuritaires, sûrs, efficaces et accessibles. À défaut de cela, bien des problèmes que nous connaissons vont être amplifiés par l'augmentation rapide des services numériques hautement connectés. Il est essentiel, pour que l'économie canadienne puisse atteindre ce potentiel, que les consommateurs, les citoyens et les entreprises obtiennent des identités numériques de confiance qui leur permettent d'accéder à des services numériques d'une façon efficace et sécuritaire.

Gouvernements, entreprises et citoyens ont besoin de savoir qu'ils peuvent faire confiance aux renseignements numériques sur les personnes et les organisations.

Dans l'ensemble de l'économie, l'identité est fondamentale pour fournir des services :

- **Aux citoyens :** Selon une étude menée par Dashlane, un service de gestion de mots de passe, une personne a en moyenne 92 comptes enregistrés à une adresse de courriel et doit réinitialiser chaque année un mot de passe oublié pour au moins 37 de ces comptes. On s'attend à ce que d'ici 2020, le nombre de comptes qu'une seule personne pourrait avoir besoin de gérer monte à plus de 200[1]. **Le temps qu'un citoyen/client passe à réinitialiser des mots de passe oubliés dépasse 10 heures par année et, faute d'une meilleure solution, pourrait facilement excéder 25-30 heures.**

  Le citoyen/consommateur ordinaire passe en tout environ huit heures par année à créer de nouvelles sources d'identité, ou à utiliser celles qui existent, pour prouver qui il est, et pour confirmer certains éléments de son identité et qu'il a le droit d'accéder à un service. En améliorant la façon dont il peut accomplir toutes ces tâches, cela peut se traduire par une économie globale de 213 CAD par personne et de **6,1 milliards de CAD** pour toutes les personnes de plus de 19 ans[2].

- **Aux PME** : En ce qui concerne les petites et moyennes entreprises (PME), l'impact de l'identité numérique pourrait servir à améliorer des processus qui sont actuellement ardus. C'est particulièrement le cas lorsque les entreprises ont besoin de fournir une preuve d'identité entre elles.

  Étant donné que les PME comptent pour environ 30 % du PIB global du Canada[3] (450 milliards de CAD), en supposant qu'une PME ordinaire gagne ne serait-ce que 1 % d'efficacité grâce à une identité numérique de confiance, cela pourrait **ajouter 4,5 milliards de CAD à la valeur des PME**.

- **Aux institutions financières** : Au Canada, le CCIAN et les banques participantes ont déterminé qu'il y aurait moyen de faire des économies nettes de **100 millions de CAD** ou plus par institution et par année grâce aux efficacités opérationnelles obtenues en réduisant les coûts de traitement manuel et la fraude[4].

- **Pour le commerce électronique** : Le marché canadien du commerce électronique devrait voir les ventes passer de **21,7 milliards de CAD** en 2015 à **28,34 milliards de CAD** en 2018.[5] L'identité numérique de confiance est essentielle pour que le secteur continue de croître. Qu'il s'agisse du commerce électronique ou de l'économie de partage, une identité numérique robuste et fiable inspire confiance, procure une sécurité et atténue la fraude. Un atout pour les citoyens, les consommateurs et les entreprises.

- **Pour la santé** : À l'heure actuelle, des milliards de dollars sont gaspillés chaque année en temps et efforts que les professionnels de la santé consacrent pour accéder aux dossiers des patients, sans compter la frustration des patients et de leurs fournisseurs de soins de santé. **Un système sûr de validation et d'authentification de l'identité numérique pourrait permettre aux Canadiens de prouver leur identité pour accéder à des données sur la santé et consentir au partage de dossiers, ce qui réduirait grandement le temps et les coûts associés aux références**, aux demandes d'obtention de renseignements (le coût est estimé à 200 CAD par demande et il y en a des milliers chaque jour), à l'accès aux dossiers des patients pour les salles d'urgence et les visites ambulatoires, et à l'administration générale des patients.

- **Au gouvernement** : L'accès des citoyens à l'information est une priorité pour un gouvernement numérique moderne, au niveau tant fédéral que provincial. Les processus qui nécessitent une authentification et une validation de l'identité sont encore manuels, ce qui entraîne une augmentation des coûts et un accès plus lent aux services qui se répercutent directement sur les contribuables. Il est très difficile de prouver son identité et cela exige souvent une visite en personne d'au moins 30 minutes, ce qui demande du temps au préposé au comptoir comme au citoyen. En supposant que le citoyen ordinaire ne crée que deux comptes par année, à raison d'un salaire moyen de 25,88 CAD l'heure[6], on estime que cela représente **une perte de 482 millions de CAD par année**.

L'obligation de fournir des renseignements vérifiables peut varier selon les industries, mais le besoin fondamental reste le même : il faut des données fiables que le client peut fournir facilement au moment où on les lui demande, avec peu de friction, mais une sécurité et une confiance appropriées entre les parties.

Les services numériques permettent de simplifier et de rationaliser les processus manuels existants. Ils offrent également la possibilité de développer de nouveaux services perfectionnés qui tirent parti de la forte augmentation de la connectivité entre les personnes, les organisations et les appareils. Il arrive souvent que ces services ne donnent pas leur plein potentiel en raison de la friction et par manque de confiance.

De nos jours, il y a souvent une friction là où l'on fait une demande pour un service ou on y accède pour la première fois, mais cela peut se produire à bien d'autres endroits aussi. La friction est mauvaise autant pour les entreprises que pour les consommateurs/citoyens. Cela empêche d'avoir un accès légitime à des services et se répercute sur les taux de conversion. Les personnes vulnérables et défavorisées sont les plus susceptibles d'en pâtir – notamment les consommateurs/citoyens qui ont de petits budgets et des besoins en termes d'accessibilité, et les petites entreprises. Mais les effets se font sentir dans toute l'économie.

L'identité numérique que nous avons en tête est sûre, fiable et portable, et elle se sert de la technologie numérique. Elle utilise d'une manière responsable le monde hautement connecté pour procurer de la valeur aux personnes et aux entreprises, en évitant les inefficacités, les risques et la friction associés aux systèmes actuels, dont beaucoup ont été conçus avant l'Internet.

C'est le temps d'agir

C'est le moment ou jamais de s'assurer les consommateurs, les entreprises et les entités gouvernementales vont agir de concert pour atteindre l'objectif commun qui consiste à mettre en place un écosystème sécuritaire, sûr et de confiance pour l'identité numérique canadienne. Outre le potentiel de rapporter plus de 15 milliards de CAD à l'économie, cela va s'accompagner d'innombrables avantages à l'échelle de la société canadienne.

Nous devons tous œuvrer à l'unisson, en assurant une approche distinctement canadienne, pour préserver notre avenir numérique collectif, faire en sorte que la protection de la vie privée et le choix soient maintenus, et nous efforcer de protéger les plus vulnérables d'entre nous. Si nous accomplissons tout cela, nous serons en bonne voie de bâtir un environnement innovateur, hautement connecté et gratifiant qui permettra à l'économie numérique canadienne d'atteindre son plein potentiel.

Compte tenu des preuves émanant d'autres marchés et qui sont corroborées par ce que nous constatons au Canada, nous estimons d'une manière conservatrice à au moins 1 % du PIB, ou 16 milliards de CAD, la valeur potentielle que l'identité numérique de confiance apporterait à l'économie canadienne.

1. Quel rôle l'identité numérique joue-t-elle dans l'économie numérique?

L'identité numérique est essentielle pour la croissance et l'efficacité de l'économie numérique, mais la plupart des gens ignorent ce dont il s'agit.

L'absence d'une approche unifiée de l'identité numérique se répercute sur chacun d'entre nous. Pour le citoyen canadien ordinaire, les petites entreprises et les entrepreneurs, le fait de devoir prouver son identité d'une manière numérique peut prendre du temps et être ardu. Ce n'est pas évident de se souvenir des services auxquels on s'est inscrit et des mots de passe à utiliser pour y accéder, de sorte que la plupart d'entre nous ne se souviennent pas et n'ont pas de trace de tous les comptes.

Pour d'autres Canadiens, le défi est encore plus grand – ils n'ont pas assez de moyens pour prouver qui ils sont ou l'obligation d'avoir à le faire est tout simplement trop difficile. Certaines personnes se retrouvent ainsi privées de la commodité de l'accès numérique à des services essentiels comme les soins de santé, le gouvernement et les services financiers. Il s'agit souvent, hélas, des plus vulnérables de la société qui ont le plus besoin d'avoir accès à de tels services.

« Tout le monde gère de plus en plus sa vie quotidienne avec des appareils mobiles et en ligne. Nous voulons décider quand, où et comment accéder à des services, et cela nous est égal qu'ils soient fournis par le secteur public ou privé. Des identités numériques de confiance sont absolument nécessaires pour rendre cela possible. »
- CJ Ritchie, sous-ministre déléguée et dirigeante principale de l'information du gouvernement de la Colombie-Britannique

---

Les services numériques permettent de simplifier et de rationaliser les processus manuels, et de développer de nouveaux services perfectionnés qui tirent parti de l'augmentation considérable de la connectivité des personnes, des organisations et des appareils. Ces services ne donnent souvent pas leur plein potentiel en raison de la friction et du manque de confiance. Au Canada, les entreprises et les gouvernements souhaitent ardemment que les normes d'identité numérique ne se contentent pas de suivre d'autres cas de réussite à l'étranger, mais qu'elles reflètent aussi les valeurs (inclusion, transparence, confiance) auxquelles les Canadiens sont très attachés. Si nous arrivons à le faire, tout en encourageant une infrastructure sécuritaire et sûre de l'identité numérique de confiance, nous pourrons alors tirer pleinement parti des avantages de l'économie numérique.

Ce livre blanc explore l'état actuel de l'identité numérique au Canada et la façon dont nous pouvons, en agissant immédiatement, devenir un leader mondial en favorisant une économie numérique sécuritaire, sûre et de confiance – dans l'intérêt de la société, de l'économie et du Canada en tant que chef de file international.

Alors, qu'est-ce que l'identité numérique?

L'identité est une question de relations et de confiance.

Chaque organisation numérique a besoin de « connaître » ses clients avant de pouvoir interagir d'une manière significative avec eux en ligne. Mais qu'est-ce que cela signifie? Certaines entreprises sont tenues de suivre des règles strictes de « profilage du client » afin d'établir l'identité juridique des clients. D'autres peuvent ne pas être réglementées de la sorte, mais veulent quand même en savoir le plus possible sur leurs clients. Sauf que ces « relations » sont souvent à sens unique, la personne ayant très peu de visibilité ou de contrôle sur ses données personnelles.

Aujourd'hui, le consommateur/citoyen ordinaire a des relations avec des dizaines d'organisations numériques, chacune d'elles étant établie et gérée isolément des autres. Les consommateurs/citoyens sont souvent obligés de créer un compte auprès d'une organisation en ligne indépendamment que ce qu'ils veulent (autrement dit, pourquoi un client a-t-il besoin de créer un compte pour un achat ponctuel?). Ce n'est pas pratique, et c'est inefficace et peu sécuritaire. En effet, chaque client a de multiples « identités numériques » qui sont représentées par les données personnelles que chaque organisation possède sur lui et qu'il est pour ainsi dire impossible pour une personne de gérer.

Les citoyens ont donc beau avoir de multiples relations numériques, il arrive souvent qu'on ne leur fasse pas confiance et/ou qu'elles soient difficiles à gérer.

L'identité est une question de données personnelles.

Beaucoup de consommateurs/citoyens n'ont aucune idée de la quantité de données personnelles qu'ils génèrent en utilisant des services numériques, ni des multiples utilisations – bonnes et mauvaises, légales et illégales – qui en sont faites. La plupart des consommateurs/citoyens ne se rendent pas compte de la valeur de leurs données personnelles et acceptent implicitement un échange de valeur (partage de données pour accéder à des services « gratuits ») sans se demander si cet échange est équitable ou non.

Les coûts et les risques que représente pour les entreprises le fait de détenir des données personnelles deviennent de plus en plus évidents chaque fois que survient un vol de données très médiatisé. Outre les atteintes à la réputation et d'éventuelles poursuites, les autorités européennes sont en train d'instaurer des amendes punitives pour les manquements à la protection des données, ce qui va inévitablement influencer l'orientation de la législation sur la protection des données dans d'autres pays.
Les décideurs doivent se préoccuper avant tout du manque actuel de contrôle individuel sur les données personnelles.

L'identité numérique que nous avons en tête est sûre, fiable et portable, et elle se sert de la technologie numérique. Elle utilise d'une manière responsable le monde hautement connecté pour procurer de la valeur aux personnes et aux entreprises, en évitant les inefficacités, les risques et la friction associés aux systèmes actuels, dont beaucoup ont été conçus avant l'Internet.

2. Qui a besoin de l'identité numérique?

Les gouvernements et les entreprises ont besoin de savoir qu'ils peuvent faire confiance aux renseignements numériques sur les personnes et les compagnies

L'économie au complet est visée.

Beaucoup d'entreprises ont besoin d'avoir des données vérifiables sur l'identité. L'identité est essentielle, à l'échelle de l'économie, pour fournir des services, surtout dans les domaines suivants :

- **Services financiers** : De nos jours, le besoin d'avoir une identité numérique se constate avant tout dans les services réglementés, comme les services financiers. Ces derniers sont nécessaires pour effectuer de rigoureuses vérifications de « profilage du client » pour les clients qui ouvrent un compte et d'une manière périodique. Ces vérifications sont importantes pour aider à éviter le blanchiment d'argent et le financement du terrorisme, mais elles sont également chronophages, coûteuses et duplicatives. Au Canada, le CCIAN et les banques participantes ont déterminé qu'il y aurait moyen de faire des économies nettes potentielles de 100 millions de CAD ou davantage par institution et par année, grâce aux efficacités opérationnelles obtenues en réduisant les coûts de traitement manuel et la fraude[7].

- **Commerce électronique** : Une identité numérique de confiance est également nécessaire pour un large éventail de scénarios rattachés au commerce électronique où un paiement doit être effectué entre deux parties, et il faut disposer de certains moyens pour réduire le risque que des fraudeurs présentent une « personne véritable » en ligne. Cela pourrait se passer entre un consommateur et une entreprise, entre deux entreprises ou entre deux consommateurs. Les paiements dans un environnement numérique exigent une grande dose de confiance, car on ne peut pas « voir » la personne à l'autre bout de la transaction et il n'y a souvent pas de façon directe de vérifier d'une manière numérique une personne ou une organisation authentique.

- **Santé** : À l'heure actuelle, des milliards de dollars sont gaspillés chaque année en temps et efforts par les professionnels de la santé pour accéder aux dossiers des patients, une source de frustration pour les patients et leurs fournisseurs de soins. Les dossiers de santé électroniques sont éparpillés entre de multiples systèmes exclusifs qui ne communiquent souvent pas entre eux. C'est essentiel de vérifier l'accès approprié aux données et de ne partager que les renseignements nécessaires avec le destinataire voulu après avoir obtenu le consentement explicite du patient afin de protéger les renseignements sensibles nécessaires pendant le traitement médical. Ces inefficacités peuvent mener à une duplication des tests de laboratoire et de diagnostic, faire perdre du temps à attendre le transfert physique des dossiers médicaux des patients entre les fournisseurs de soins de santé, et entraîner une utilisation inefficace des ressources des urgences[8]. Un système sûr de validation et d'authentification de l'identité numérique permettrait aux Canadiens de prouver leur identité afin d'accéder à des données sur la santé et de consentir au partage de dossiers, ce qui réduirait considérablement le temps et les coûts associés aux références, aux demandes de divulgation des renseignements (environ 200 CAD par demande, à raison de milliers de demandes par jour), à l'accès aux dossiers des patients pour l'urgence et les visites ambulatoires, ainsi que l'administration générale des patients.

- **Gouvernement** : Au niveau fédéral et provincial, il est prioritaire pour un gouvernement numérique moderne de rendre l'information accessible aux citoyens. Les processus qui nécessitent une authentification et une validation de l'identité sont encore manuels, ce qui entraîne une augmentation des coûts et un accès plus lent aux services qui se répercutent directement sur les contribuables. Il est très difficile de prouver son identité et cela exige souvent une visite en personne d'au moins 30 minutes, ce qui demande du temps au préposé au comptoir comme au citoyen. En supposant que le citoyen ordinaire ne crée que deux comptes par année, à raison d'un salaire moyen de 25,88 CAD l'heure[9], on estime que cela représente une perte de 482 millions de CAD par année. Des défis se posent aussi aux petites entreprises qui doivent interagir avec des services locaux et des ministères provinciaux et fédéraux. Selon le secteur, elles doivent remplir différentes exigences, notamment pour l'enregistrement, l'obtention de licences et de permis, et les inspections, des démarches qui sont toutes principalement manuelles à l'heure actuelle.

Outre ces domaines essentiels, l'identité numérique est déjà utilisée et va gagner en importance dans des industries comme le commerce de détail pour confirmer l'adresse ou l'âge, le travail pour vérifier les antécédents ou les emplois, l'éducation pour valider les diplômes et l'assurance pour prévenir la fraude.

Les exigences en ce qui concerne les renseignements vérifiables peuvent varier selon les secteurs, mais le besoin fondamental demeure le même : avoir des données fiables qui peuvent être facilement fournies par le client au moment où elles sont requises, avec peu de friction, mais une sûreté et une confiance appropriées entre les parties.

3. Comment l'identité numérique se pratique-t-elle aujourd'hui?

Aujourd'hui, l'identité se pratique souvent mal.

Problèmes de base

Aujourd'hui, pratiquement tous les services en ligne comportent certains éléments reliés à l'identité personnelle. Mais les approches adoptées posent souvent des problèmes au niveau de la fiabilité, de la sécurité et de l'utilisation.

Au niveau vraiment de base, un témoin placé sur un navigateur permet à un site web de stocker une référence unique à la personne ainsi que des renseignements personnels. Cela permet au site web de détecter et de suivre l'utilisateur au fil des multiples interactions avec des sites web. Souvent, la personne n'a pas conscience des données qui sont stockées et de la façon dont elles sont utilisées.

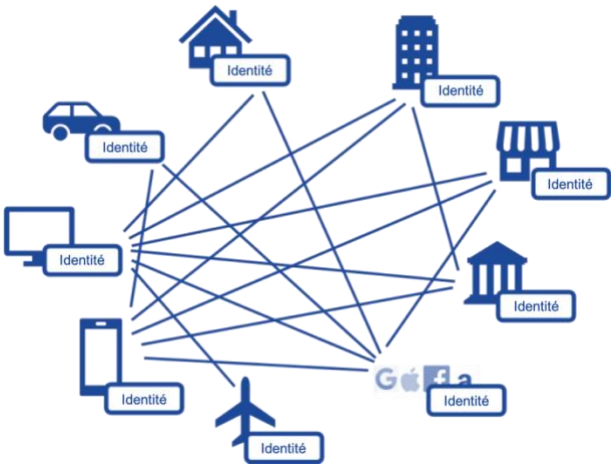


Figure 1 : L'identité numérique aujourd'hui – en silos et fragmentée

De nombreux services numériques exigent la création d'une « identité » spécifique au service. Cela oblige les clients à gérer de multiples comptes, ce qui prend du temps et coûte cher aux entreprises aussi.

Selon une étude menée par le service de gestion de mots de passe Dashlane, une personne ordinaire a 92 comptes enregistrés à une adresse de courriel et elle doit réinitialiser chaque année le mot de passe d'au moins 37 comptes. On s'attend à ce que d'ici 2020, le nombre de comptes qu'une seule personne pourrait avoir besoin de gérer dépasse les 200[10]. Le temps qu'un citoyen/client passe à réinitialiser des mots de passe oubliés dépasse 10 heures par année et, faute d'une meilleure solution, il pourrait facilement excéder 25-30 heures.

En ce qui concerne un employé d'entreprise, ce problème prend encore plus d'ampleur lorsqu'il est question des applications internes et outils commerciaux. LastPass, un autre service de gestion de mots de passe, s'est penché sur la gestion des mots de passe au travail. Il a constaté qu'un employé doit, en moyenne, taper des justificatifs pour s'authentifier sur des sites web et des applications **154 fois par mois**. Une chose est sûre : la saisie des mots de passe fait (encore) partie du rituel quotidien. Si un employé ordinaire stocke **191 connexions dans sa voûte**, il semble que les mots de passe ne sont pas tous utilisés tout le temps. Les données montrent aussi qu'**il faut en moyenne 14 secondes pour taper un mot de passe**. Cela représente **une moyenne d'environ 36 minutes gaspillées par mois** pour une activité qui n'apporte aucune valeur à l'entreprise[11].

En extrapolant ces données à l'ensemble de la main-d'œuvre canadienne, on constate que cette simple tâche coûte à elle seule près de 300 millions de CAD par mois et plus de 3,5 milliards de CAD par année.[12] Outre l'acte qui consiste à taper des mots de passe, on estime à 40 CAD par incident le coût administratif moyen dans les centres téléphoniques pour gérer et administrer les mots de passe égarés, oubliés ou volés[13]. En prenant un incident par année par travailleur canadien, cela représente pour les 18,65 millions de travailleurs canadiens 746 millions de CAD dépensés chaque année rien qu'en services de gestion de mots de passe et heures productives perdues. Ces deux exemples représentent à eux seuls des économies potentielles de plus de 4 milliards de CAD par année.

Duplication en pure perte

En plus de gaspiller le temps des utilisateurs avec des activités comme des mots de passe oubliés, il y a une duplication considérable des efforts de la part des entreprises pour vérifier les données d'identité des consommateurs/citoyens. C'est tout particulièrement le cas des procédures d'accueil et de profilage du client

que les institutions financières utilisent lors de l'ouverture des comptes. À cela s'ajoute la maintenance constante de ces renseignements tout au long de la vie du compte du client. Une étude menée par Thompson Reuters a montré que les coûts et la complexité du profilage du client augmentent, et que même si les coûts moyens des sociétés financières pour remplir leurs obligations s'élèvent à 60 millions USD, certaines dépensent jusqu'à 500 millions USD pour la conformité du profilage du client et la diligence raisonnable envers le client.[14] Étant donné que le profilage du client comporte souvent des processus similaires d'une institution à l'autre, ce coût pourrait être rationalisé avec une solution numérique appropriée et permettrait par la même occasion de réduire le risque de vol d'identité.

ÉTUDE DE CAS 1 – OUVERTURE D'UN RESTAURANT

Emma, 42 ans, est propriétaire d'une petite chaîne de restaurants marchant bien à Fredericton, au Nouveau-Brunswick, depuis cinq ans. Ses enseignes ayant rapporté des revenus excédentaires suffisants, elle a décidé d'ouvrir deux nouveaux établissements pour étendre ses activités à d'autres villes.

Sans l'identité numérique
Emma fait des recherches sur les licences, permis et documents d'enregistrement commerciaux dont elle a besoin pour ouvrir deux nouveaux restaurants. Découragée par la complexité du processus, elle renonce à réunir tous les formulaires qu'elle doit remplir.

Avec l'identité numérique
Emma se connecte au portail gouvernemental numérique sécurisé de Service New Brunswick (SNB). Elle gère déjà ses permis et licences commerciaux existants, de sorte qu'elle connaît les formalités et est à l'aise. Elle peut facilement entamer le processus pour inscrire ses nouvelles enseignes en ligne, car elle est guidée tout au long de la démarche pour valider les renseignements sur les endroits proposés, les permis et licences pertinents pour son type de restaurants, et les autres exigences à remplir. Comme SNB peut vérifier si Emma est une vraie personne qui est propriétaire d'une entreprise, il y a moins de problèmes pour avoir l'assurance que sa demande commerciale est légitime. Après avoir rempli ses demandes et en attendant qu'elles soient approuvées, Emma reçoit une invitation à consulter le système de soumission d'un fournisseur d'équipement de restaurant où elle peut spécifier le genre d'équipement de cuisine qu'il lui faut pour les nouveaux établissements. Elle soumet une demande de devis et reçoit en l'espace de quelques heures les réponses de 10 fournisseurs reconnus comme des entreprises légitimes en activité au Nouveau-Brunswick. Après avoir examiné les devis, elle arrête son choix sur un fournisseur le lendemain, envoie sa commande et planifie les livraisons.

Au-delà des services financiers et du profilage du client, le principe des données sur l'identité du client qui sont reproduites dans de nombreux services numériques est couramment accepté dans l'économie numérique d'aujourd'hui. Quand une personne ou une entreprise veut créer un nouveau compte en ligne ou partager certaines de ses données avec des fournisseurs, une bonne partie de ses données d'identité sont souvent nécessaires pour établir un nouveau compte, bien que ces mêmes données existent dans de nombreux d'autres endroits. Même lorsque les données sont partagées entre des entreprises, cela est rarement fait d'une manière qui respecte la vie privée du client. Cette duplication pose aussi un problème lorsque les renseignements du client changent (nom légal par suite d'un mariage, changement d'adresse en cas de déménagement, changement de numéro de téléphone, etc.) et qu'ils doivent être mis à jour dans chacun des comptes créés en ligne.

Le client est le produit

Le modèle de gestion des services Internet gratuits est basé sur la création d'un « profil » de l'utilisateur, qui est une forme d'identité. Ce profil est compilé à partir de toutes les données qui peuvent être recueillies sur l'utilisateur, notamment des données saisies explicitement ainsi que des données contextuelles et d'utilisation qui peuvent être agrégées. Elles servent à cibler l'utilisateur avec de la publicité, laquelle est ensuite une source de revenus pour ces entreprises.

Il y a bien des raisons pour lesquelles cette approche n'est pas souhaitable du point de vue de l'identité, notamment les préoccupations à propos de la confidentialité des données et du contrôle des renseignements personnels (données de géolocalisation, renseignements permettant d'identifier les personnes, etc.). Ce modèle ne laisse au client que peu de contrôle sur ses propres données une fois qu'il pénètre l'écosystème. Outre le respect de la vie privée, la sécurité et le contrôle, il y a aussi la crainte que les données fournies par un utilisateur puissent ou non être entièrement exactes. Les réseaux sociaux incitent d'une manière inhérente les personnes à partager des renseignements essentiellement véridiques, ou même légèrement biaisés. Cela engendre là encore des problèmes reliés à la qualité des données et à la capacité de faire confiance aux données validées. Les entreprises préfèrent souvent faire confiance à des données qui peuvent être vérifiées avec un grand niveau de certitude et validées par une source indépendante afin de réduire le niveau de risque en menant n'importe quel nombre de transactions.

Même si les personnes sont généralement disposées à partager des renseignements personnels en échange de services de valeur, les sondages montrent que la façon dont les données personnelles sont utilisées suscite un malaise grandissant. Selon une étude menée par la société de télécommunications Orange, 78 % des consommateurs/citoyens trouvent difficile de faire confiance à la façon dont les entreprises utilisent ces données[15].

4. Quel impact les processus actuels ont-ils sur l'économie numérique?

Les lacunes actuelles de l'identité numérique entraînent des risques inacceptables pour les personnes et les entreprises, et entravent la croissance de l'économie numérique.

Vols de données

Lorsque des données personnelles sont recueillies, stockées ou traitées, les incidents de sécurité peuvent sérieusement menacer la protection de la vie privée. Ils engendrent également d'importants coûts pour les utilisateurs. Selon Privacy Rights Clearinghouse[16], le nombre d'incidents relevés est d'environ 45 par année, tandis que le nombre total de dossiers volés est de plus en plus fonction des vols de données à grande échelle, c.-à-d. des vols de données impliquant plus de 10 millions de dossiers. Depuis 2005, plus de 6 000 entreprises et organisations ont signalé des vols. Rien qu'en 2015, par exemple, près de 165 millions de dossiers contenant des numéros de sécurité sociale [des États-Unis] ont été compromis dans 338 vols, selon l'Identity Theft Resource Center.[17]

Le vol de données de Home Depot en 2014 (56 millions de cartes de crédit et de débit) a coûté à l'entreprise 263 millions de USD en dépenses d'atténuation, soit environ 4,70 USD par dossier perdu. Le vol de données de Target en 2013 (40 millions de cartes de crédit et de débit et 70 millions de dossiers de clients non titulaires de cartes) a coûté à l'entreprise 291 millions de USD en dépenses d'atténuation, soit environ 2,65 USD par dossier[18]. Ces exemples, parmi bien d'autres survenus au cours de la dernière décennie, ont sapé la confiance des consommateurs dans l'économie numérique. Cela a amené de nombreux consommateurs/citoyens à hésiter à partager des renseignements en ligne, à plus forte raison des données d'identité sensibles qui pourraient, selon eux, être perdues, volées ou partagées d'une manière non autorisée et sans leur consentement.

Appropriation de comptes

Du fait de ces vols de données très médiatisés, une nouvelle série de problèmes a commencé à prendre forme au-delà des simples achats avec des cartes de crédit frauduleuses. C'est particulièrement le cas lorsque des renseignements permettant une identification plus personnelle ont été volés, les cybercriminels ayant passé plus de temps à essayer de voler l'identité et de s'approprier frauduleusement des comptes. Contrairement aux données des cartes de crédit qui peuvent être facilement changées par la banque émettrice en cas de vol, les données sur l'identité, comme l'adresse résidentielle ou le numéro d'assurance sociale d'une personne, ne sont pas faciles à remplacer.

L'industrie de la sécurité axe ses efforts sur la prévention des vols, tandis que les criminels s'attachent à extraire de la valeur des données volées. De même qu'une entreprise établit le profil d'un client, les criminels essaient de créer un dossier numérique complet des victimes potentielles. Pour les personnes qui ont une valeur nette élevée, de tels profils peuvent rapporter une prime pouvant atteindre plus de 450 USD sur le web noir[19]. Avec ces données, un cybercriminel peut éventuellement ouvrir de nouveaux comptes financiers ou accéder à des fonds dans des comptes existants en usurpant l'identité du client.

Évolution des risques de fraude

La fraude ne se borne plus à attraper des criminels qui utilisent de véritables cartes de crédit volées. Les vols de données ont permis à des criminels agissant sur le web noir d'avoir accès à des milliers voire des millions de comptes financiers et données d'identité personnelles volés. De ce fait, la fraude prend à présent de nombreuses formes. La fraude aux centres téléphoniques est devenue un problème plus médiatisé après le lancement en septembre 2014 d'Apple Pay. Il y a eu aussitôt une augmentation de la fraude aux centres téléphoniques, car les cybercriminels ont compris qu'ils pouvaient créer des comptes en utilisant les données de cartes de crédit volées.

Selon Pindrop Security, un appel sur 2 900 adressé en 2015 aux centres téléphoniques des grandes banques était frauduleux[20]. En 2016, cette proportion était davantage de l'ordre d'un appel sur 2 000. Parmi les banques régionales, on parle davantage d'un appel sur 700. Les criminels utilisent des techniques d'appropriation de comptes pour amener socialement les agents des centres téléphoniques à prendre le contrôle des comptes clients, établir de nouvelles marges de crédit et transférer de l'argent.

La fraude d'identité synthétique est un autre type de fraude qui se manifeste régulièrement. Elle diffère du vol d'identité traditionnel par le fait que l'auteur crée de nouvelles identités synthétiques au lieu de voler des identités existantes. Le processus consiste à voler tout d'abord de véritables numéros de sécurité sociale qui ne sont pas activement utilisés — c'est le cas des enfants et des personnes âgées qui utilisent peu, voire pas du tout de crédit — puis à créer des identités en ajoutant de fausses adresses. Ces voleurs, qui mettent au point un stratagème de longue haleine qui peut prendre des années à rapporter, bâtissent lentement une cote de crédit pour ces nouvelles identités, en interagissant avec les banques au moyen de téléphones prépayés provisoires dont ils se débarrassent à un moment donné. Ils finissent par accumuler des dettes de 20 000 USD ou davantage sur un nombre incalculable de comptes, puis disparaissent sans laisser de trace[21].

5. Quel intérêt à plus grande échelle l'économie va-t-elle tirer?

Les avantages économiques seront considérables.

Nous sommes fermement convaincus que les avantages collectifs de la mise en place de normes d'identité numérique et de systèmes d'identité pouvant fournir des renseignements vérifiés apporteront de nombreux avantages qualitatifs et quantitatifs à l'économie canadienne. Il est difficile de prédire exactement quelle valeur sera générée et quelles économies seront réalisées, mais les perspectives qui suivent montrent l'impact économique potentiel.

Quantification des avantages économiques potentiels pour le Canada

Les avantages économiques potentiels pour l'économie canadienne pourraient être réalisés grâce à une série d'effets de dominos obtenus au moyen de solutions d'identité numérique convenablement mises en place, comme l'introduction d'efficacités où l'assurance de l'identité est difficile à établir et onéreuse, la réduction de la fraude reliée à l'identité, et l'ouverture de nouvelles possibilités procurant de la valeur aux personnes et aux entreprises.

Pour quantifier l'intérêt potentiel, nous tenons compte de ce qu'il en coûte actuellement pour assurer l'identité de 36,7 millions de citoyens, dont 28,8 millions sont âgés de 19 ans et plus[22], et du 1,17 million d'entreprises qui sont des employeurs[23] (en excluant les entreprises « autonomes).

Personnes
En ce qui concerne les personnes, nous savons qu'il y a beaucoup de tâches quotidiennes qui sont tout bonnement plus difficiles faute d'avoir en place les bons outils numériques. Dans le contexte inefficace actuel, on peut supposer que le citoyen/consommateur ordinaire passe en tout environ 8 heures par année à créer de nouvelles sources d'identité ou à en utiliser qui existent déjà pour prouver qui il est, et pour confirmer certains éléments de son identité et le fait qu'il a le droit d'accéder à un service. En améliorant la façon d'accomplir toutes ces tâches, cela peut se traduire par une économie globale de 213 CAD par personne et de 6,1 milliards de CAD pour l'ensemble des personnes âgées de plus de 19 abs[24].

Entreprises
En ce qui concerne les petites et moyennes entreprises, l'impact de l'identité numérique pourrait servir à améliorer des processus qui sont ardus à l'heure actuelle. C'est particulièrement le cas lorsque les entreprises doivent fournir une preuve d'identité à une autre entreprise, par exemple pour essayer d'avoir accès à des produits ou des services financiers pour développer leurs activités, tenter de trouver et d'acheter des marchandises auprès de fournisseurs, effectuer des transactions depuis

des endroits géographiques éloignés et valider la propriété bénéficiaire de l'entreprise.

Étant donné que les PME comptent pour environ 30 % du PIB global du Canada[25] (450 milliards de CAD) et en supposant qu'une PME ordinaire pourrait gagner seulement 1 % d'efficacité en ayant accès à une identité numérique de confiance, cela représente une valeur ajoutée potentielle de 4,5 milliards de CAD pour les PME.

Avantage économique réel réalisé en Estonie et en Inde

Il existe certains pays où une forme d'identité numérique efficace et efficiente est une réalité et a procuré un avantage économique considérable. L'identité sécuritaire et authentifiée est un « droit de naissance » pour chaque Estonien : avant même qu'un nouveau-né n'arrive à la maison, l'hôpital a déjà délivré un certificat de naissance numérique et l'assurance maladie est automatiquement effective. Tous les habitants du petit État balte ont à partir de 15 ans une carte d'identité électronique dont ils se servent pour obtenir des soins de santé, utiliser les services bancaires électroniques, faire des achats en ligne, signer des contrats numériques, crypter le courriel, se procurer des billets de tram et bien d'autres choses. L'État estonien offre en tout 600 services électroniques à ses citoyens et 2 400 aux entreprises[26]. En plus de faciliter le quotidien des Estoniens, l'Estonie affirme que ses systèmes en ligne ajoutent 2 % par année à son PIB[27] et que l'utilisation de signatures électroniques dans le pays permet d'économiser chaque année 2 % du PIB du pays, l'équivalent du budget de la défense de l'Estonie[28].

Ces dernières années, l'Inde a fait, grâce à son programme Aadhaar couronné de succès, des progrès remarquables pour enregistrer ses habitants et leur attribuer une identité numérique, beaucoup d'Indiens n'ayant pas auparavant de pièces d'identité officielles. Aadhaar est exploité par l'Unique Identification Authority of India (UIDAI). Il s'agit d'un programme permanent; l'inscription se poursuit et des efforts sont déployés pour « implanter » les numéros Aadhaar dans les bases de données de divers programmes de prestations sociales[29], dossiers fiscaux, systèmes RH de la fonction publique, registres d'entreprises, etc. Plus d'un milliard d'Indiens ont été inscrits[30], un véritable exploit à tous points de vue.

La Banque mondiale estime que l'initiative Aadhaar permet **au gouvernement indien d'économiser environ 1 milliard de USD par année en évitant la corruption**, en plus de souligner que les technologies numériques favorisent l'inclusion, l'efficacité et l'innovation.

Avantage économique potentiel en Australie et au Royaume-Uni

Outre les avantages déjà obtenus avec les systèmes d'identité numérique existants, de nombreux pays ont mené des études pour déterminer la valeur que des solutions d'identité numérique pourraient éventuellement procurer à leurs économies. Selon une étude conjointe de l'Australia Post et du Boston Consulting Group, « la valeur potentielle d'une solution d'identité numérique pour l'Australie **permettrait d'économiser jusqu'à 11 milliards de AUD en réduisant le coût des services et de la fraude, et en améliorant l'expérience client**[31] ». Ces 11 milliards de AUD représentent environ 1 % du PIB australien.

Une étude conjointe de l'Open Identity Exchange (OIX) et de Ctrl-Shift sur la taille et le potentiel du marché britannique pour l'assurance de l'identité a également montré une valeur potentielle considérable. Selon le rapport, **les coûts totaux de l'assurance de l'identité pour les organisations, qui sont actuellement de 1,65 milliards de £ [2,86 milliards de CAD], pourraient passer à moins de 150 millions de £ [260 millions de CAD]** au cours de la prochaine décennie à mesure que de nouveaux processus basés sur les principes de « création unique et utilisations multiples » sont implantés. Cela va favoriser davantage le virage vers les transactions en ligne[32]. Il n'y a pas un « dossier » unique prépondérant pour la prestation ou l'achat de services d'assurance de l'identité. Les structures de coûts et mesures incitatives de chaque partie sont différentes, ce qui crée des millions de « minidossiers » différents. Mais globalement, le marché des attributs vérifiés et les services qu'ils permettent d'offrir seront fondamentaux et essentiels pour l'économie des renseignements personnels du 21e siècle. [33]

ÉTUDE DE CAS 2 – ACCESSIBILITÉ

Thomas est un jeune diplômé universitaire de 23 ans dont la mobilité réduite l'empêche de signer des documents imprimés. Il aimerait louer son premier appartement maintenant qu'il a fini ses études et a arrêté ses trois premiers choix.

Sans l'identité numérique
Thomas communique avec les gestionnaires de chaque appartement pour fixer une date de visite pour chaque appartement. Après avoir vu les trois, il fait son choix et appelle un ami pour l'aider à remplir le lendemain le contrat de location et les documents de vérification des antécédents. Après avoir envoyé les documents, il reçoit un appel du propriétaire disant que quelqu'un d'autre a déjà déposé les documents et signé un contrat pour louer l'appartement. Thomas doit se rabattre sur son deuxième choix dans un autre quartier et, comme il n'a pas sur tout de suite que son premier choix n'était pas disponible, il ne peut pas emménager avant deux autres semaines. Il doit aussi envoyer un chèque au propriétaire qui n'offre pas la possibilité de faire des transferts électroniques ou des prélèvements mensuels automatiques.

Avec l'identité numérique
Thomas communique avec les gestionnaires de chaque appartement pour fixer une date de visite pour chaque appartement. Après avoir vu les trois, il fait son choix et se sert de son téléphone mobile pour ouvrir un lien que le gestionnaire de propriété lui a envoyé pour remplir le contrat de location et effectuer la vérification des antécédents en ligne. Thomas peut remplir automatiquement tous ses renseignements personnels pour la demande grâce à son identité numérique de confiance et faire sa demande dans les heures qui suivent la visite du dernier appartement. Le gestionnaire de propriété l'appelle le lendemain matin pour lui dire que sa demande a été approuvée et il peut emménager d'ici une semaine.
Comme son compte bancaire est relié à son identité numérique, le dépôt de sécurité et le premier mois de loyer seront envoyés au gestionnaire de propriété la veille de son emménagement, et son loyer sera prélevé automatiquement du même compte tous les mois.

Faire du Canada un chef de file numérique

En adoptant l'identité numérique et en collaborant avec les entreprises et le gouvernement, le Canada a la possibilité de devenir un chef de file numérique qui peut favoriser un environnement propice aux entreprises en démarrage, aux petites entreprises et à l'innovation. Le Canada peut, en ayant des systèmes plus efficaces pour mettre sur pied et exploiter une entreprise, avoir un meilleur accès à des services financiers et faciliter l'accès à des renseignements vérifiables, permettre aux entreprises de croître selon des façons qui n'étaient pas possibles avant.

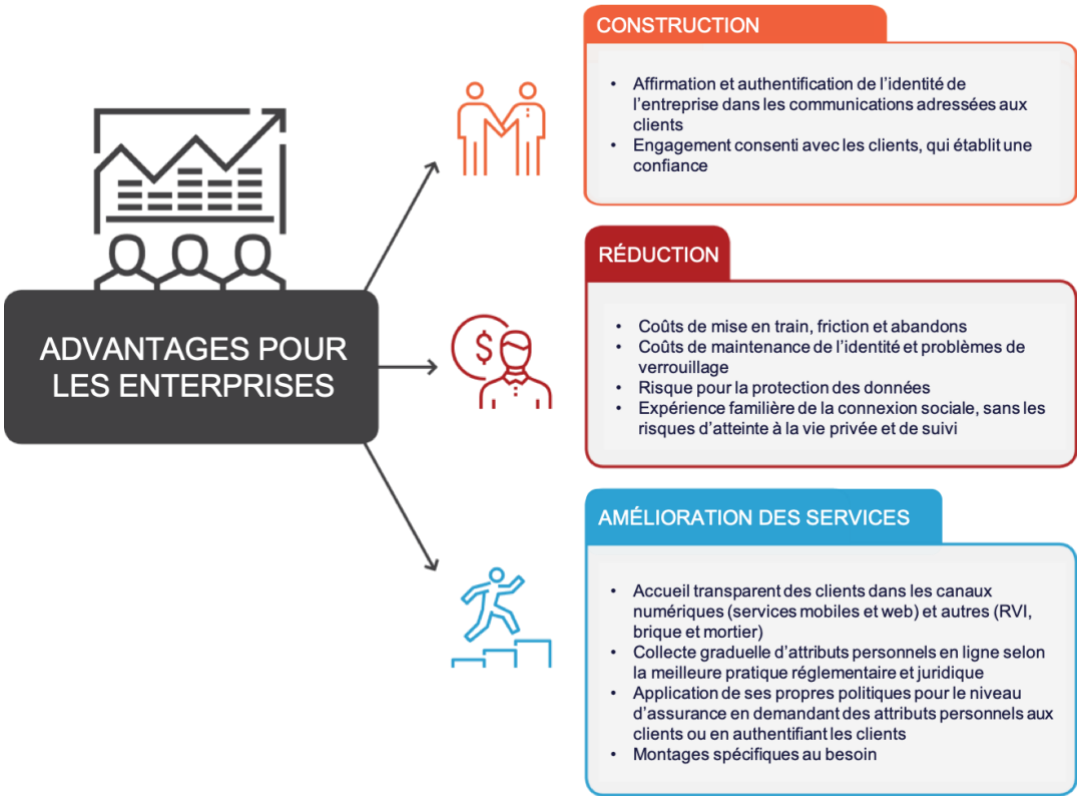
En plus d'encourager l'essor commercial au pays, le Canada pourrait jouer au niveau international un rôle de premier plan similaire à celui que l'Estonie a endossé pour promouvoir sa propre solution d'identité numérique. En plus d'avoir des processus numériques efficaces pour ses habitants, le pays a autorisé des investissements de l'étranger en Estonie. Cela s'est fait en instaurant un processus de création d'entreprises entièrement numérique (assujetti à une vérification des antécédents) et en exportant des capacités de détermination de l'identité dans des pays similaires (p. ex. Azerbaïdjan)[34].

Compte tenu des preuves émanant d'autres marchés et qui sont corroborées par ce que nous constatons au Canada, nous estimons d'une manière conservatrice à au moins 1 % du PIB, ou 15 milliards de CAD, la valeur potentielle que l'identité numérique de confiance apporterait à l'économie canadienne.

6. Comment les personnes et les entreprises vont-elles en bénéficier?

Les avantages pour les personnes et les entreprises sont réels.

Les personnes et les entreprises vont bénéficier de l'identité numérique de confiance. Nous avons discuté des ratés actuels de l'identité, des risques qui se posent si nous continuons à utiliser des processus d'identité disjoints et des avantages quantitatifs potentiels pour l'économie. Nous exposons ci-dessous certains avantages spécifiques et tangibles envisagés pour améliorer le quotidien de tous les Canadiens.



7. Quel est le rôle du citoyen/consommateur?

Il faut mettre le citoyen/consommateur au centre pour corriger les lacunes actuelles de l'identité numérique

Prise en charge des données
Cela ne suffit plus que les organisations considèrent comme « siennes » les données des clients. Cette façon de penser a amené les entreprises à stocker d'énormes quantités de données qui, comme nous l'avons vu avec les vols de données et tentatives d'appropriation de comptes de grande envergure, finissent rarement bien pour les clients. En mettant les consommateurs/citoyens, et leur identité, au centre de l'écosystème, cela peut permettre aux organisations de se concentrer sur leurs activités essentielles au lieu de passer du temps à bâtir leur propre infrastructure d'identité ou à recueillir des données sur le consommateur/citoyen qui existent déjà ailleurs.

Ce problème répandu dans l'environnement numérique d'aujourd'hui peut être atténué en utilisant par exemple une affirmation vérifiable où, au lieu que les données d'identité réelles circulent parmi de multiples parties, le consommateur/citoyen peut recevoir un outil qui lui permet de vérifier d'une manière indépendante les données demandées (par l'intermédiaire d'une tierce partie connue et de confiance). Par exemple, si l'âge est nécessaire pour déterminer l'admissibilité à accéder à un service, le citoyen peut utiliser un service d'identité numérique pour prouver, par le biais d'une relation existante avec une tierce partie, qu'il a l'âge requis.

Relier les points

Dans le monde numérique hautement connecté, c'est le citoyen/consommateur qui est le mieux placé pour relier entre elles les diverses parties de sa vie, notamment celles de sa vie numérique. En fournissant aux citoyens/consommateurs les outils nécessaires pour gérer leurs données et relations, ils peuvent devenir le point de contrôle menant à une approche qui est plus efficace et qui protège mieux la vie privée.

Il en va autrement de la façon dont nous utilisons l'identité dans le monde physique actuel (c.-à-d. présenter un permis de conduire ou un passeport pour avoir accès à un service), car les données sur l'identité ne sont pas conservées; elles sont simplement utilisées pour les besoins du moment. Ce même principe peut s'appliquer aussi aux solutions numériques et est de plus en plus considéré comme une façon de réduire la quantité de données personnelles qui prolifèrent dans les systèmes d'organisations disparates.

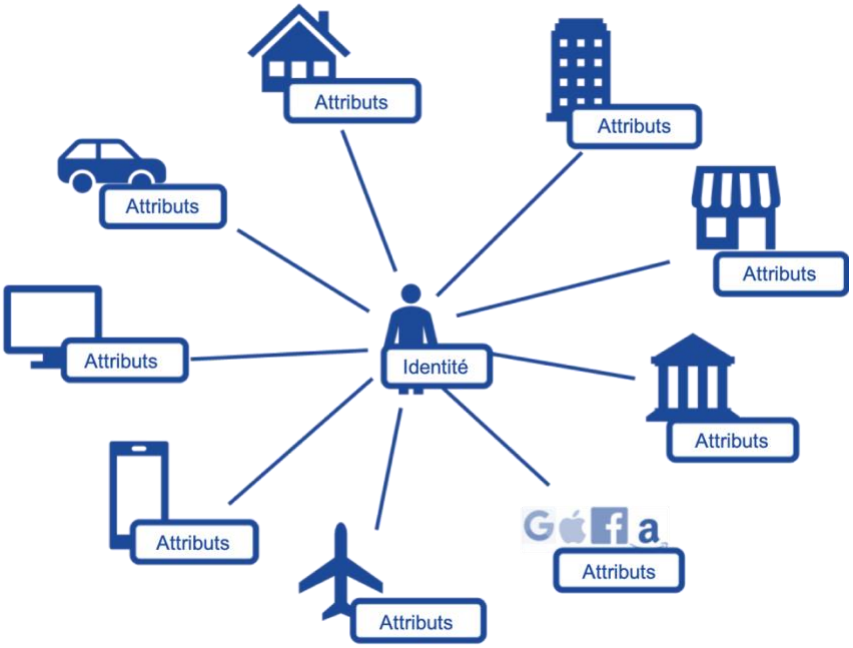


Figure 2 : Identité numérique de confiance – mettre le client au centre

L'habilitation instaure de la confiance

Le fait d'habiliter le citoyen/consommateur va augmenter la confiance dans les services en ligne. Si les citoyens/consommateurs ont une transparence et un contrôle sur leur vie numérique, ils seront plus disposés à partager des données sur l'identité pour activer des services numériques. Le fait d'utiliser des techniques pour réduire la quantité de données garantit que celles-ci sont recueillies uniquement dans un but précis, et avec le consentement de l'utilisateur, les entreprises numériques et les organisations gouvernementales peuvent montrer par leurs actes qu'elles ont spécifiquement l'intention de conserver les données des clients d'une manière sécuritaire, sûre et confidentielle.

8. Quel est le rôle du gouvernement et des entreprises?

Il faut aussi, pour régler les lacunes de l'identité numérique actuelle, que les gouvernements, les entreprises et l'industrie collaborent ensemble.

La collaboration est essentielle pour réussir.

Une organisation ne peut régler cela à elle seule – toutes les parties de l'économie numérique dépendent de l'identité numérique qui se traduit par une multitude de parties prenantes potentielles et de besoins différents. Mais étant donné l'urgence de donner aux clients le contrôle de leurs identités numériques, chaque partie prenante ne peut plus se contenter de cheminer seule. Les organisations de tous genres, du secteur public et privé, doivent collaborer pour établir des normes et créer des écosystèmes.

L'identité des personnes et des entreprises est nécessaire sous une forme quelconque dans presque toutes les industries. Cette omniprésence signifie que des solutions auront inévitablement un impact considérable sur l'ensemble de l'économie.

ÉTUDE DE CASE 3 – SERVICES FINANCIERS

James est un directeur des ventes de 45 ans et le père de deux adolescents. Son réfrigérateur est tombé soudainement en panne et le technicien qui est passé a décrété qu'il doit être remplacé. James est sur le point de partir en voyage d'affaires, de sorte qu'il manque de temps et doit trouver rapidement un autre réfrigérateur en son absence.

Sans l'identité numérique
En se rendant à l'aéroport, James appelle son marchand d'électroménagers local pour voir s'il peut avoir exactement le même modèle de réfrigérateur. Comme l'associé à qui il parle n'est pas sûr d'en avoir en stock, il promet de rappeler James bientôt. Entre-temps, James doit prendre son vol et, pendant qu'il est dans les airs, l'associé lui laisse un message dans sa boîte vocale pour dire qu'il n'a pas le même modèle, mais d'autres semblables qui devraient avoir les mêmes dimensions. James décide que c'est très compliqué et choisit d'attendre son retour pour aller en personne chez le marchand et voir ce qu'il y a de disponible.

Avec l'identité numérique
En se rendant à l'aéroport, James appelle son marchand d'électroménagers local pour voir s'il peut avoir exactement le même modèle de réfrigérateur. Le marchand a les renseignements sur son achat précédent et détermine qu'il n'a plus le même modèle. Il présente à James trois options qui ont les mêmes dimensions, avec les caractéristiques et des photos de chacune. Après que James a confirmé son choix, le marchand demande son consentement pour voir s'il y a des solutions de financement. James accepte et un processus transparent intervient pour trouver la meilleure offre disponible compte tenu de son historique financier (auquel le marchand n'a pas accès, mais qui sert à trouver un jumelage potentiel avec une institution financière). James choisit la meilleure option pour étaler ses paiements, le marchand est payé instantanément et le réfrigérateur est livré à la maison avant que James revienne de son voyage d'affaires.

Pourquoi les initiatives liées à l'identité numérique ont échoué par le passé

Les initiatives en matière d'identité numérique menées par le passé ont souvent eu de la difficulté à gagner en envergure et en masse critique. Il arrive souvent que les consommateurs/citoyens ne saisissent pas pleinement la valeur de l'identité (et des données personnelles). Les entreprises ont tendance à se concentrer sur l'avantage concurrentiel que confère le fait de « posséder » l'identité du client, en omettant de voir l'avantage économique plus important de la collaboration. Il y a souvent des questions de responsabilité qui empêchent d'éventuels fournisseurs d'identité numérique de faire le saut. Lorsqu'on met ensemble tous ces problèmes, il est difficile de faire une proposition qui séduit à la fois le fournisseur et l'utilisateur de l'identité numérique.

Mais ces difficultés ne sont pas insurmontables. Les initiatives BankID menées dans les pays nordiques montrent que l'identité numérique peut fonctionner. Dans ces pays, les banques ont collaboré pour fournir des systèmes d'identité numérique qui ont été adoptés depuis par le gouvernement afin de donner accès à de nombreux services bancaires en ligne et services gouvernementaux numériques. Les clients peuvent utiliser leur BankID pour fournir les renseignements sur leur identité d'une manière numérique ou signer d'une façon sécuritaire des documents numériques pour louer une voiture ou un appartement, s'inscrire à l'université, demander un prêt étudiant, obtenir un permis de conduire ou vérifier des dossiers de santé. Tout cela peut à présent être fait plus simplement et sans avoir recours à des processus manuels qui, autrefois, prenaient souvent beaucoup de jours ou de semaines.

Rôle du CCIAN

Le CCIAN est un consortium neutre, mené par l'industrie, de leaders des secteurs public et privé, qui a pour vocation de développer un cadre canadien d'identification et d'authentification numériques pour assurer la participation entière et sécuritaire du Canada à l'économie numérique mondiale. Les membres du CCIAN incluent des représentants des gouvernements fédéral et provinciaux, ainsi que des chefs de file du secteur privé.

Le CCIAN a pour objectif de procurer aux Canadiens des occasions sociétales et économiques en fournissant le cadre voulu pour développer un écosystème d'identification et d'authentification numériques robuste, sûre et évolutif qui protège davantage la vie privée, et qui va abaisser les coûts des gouvernements, des consommateurs/citoyens et des entreprises tout en améliorant la prestation des services et en contribuant à la croissance du PIB. En cultivant des solutions d'identité axées sur les utilisateurs, et en faisant en sorte que ces outils soient adoptés par de grandes organisations, nous allons améliorer la sécurité et la protection de la vie privée des utilisateurs; incorporer des processus de preuve et d'authentification de l'identité numérique établis par le CCIAN et le National Institute of Standards and Technology (NIST);[35] réduire les coûts et les risques du fonctionnement numérique pour les entreprises et les gouvernements au Canada; et décupler l'innovation canadienne, ce qui va créer des milliers d'emplois.

9. Quel est le coût de l'inaction?

Le Canada ne peut pas se le permettre.

Si nous ne nous attachons pas à faire de l'identité numérique une priorité pour le Canada, nous allons perdre de nombreuses occasions, notamment le potentiel de croissance dans l'économie numérique, en plus de courir le risque d'être devancés par d'autres nations développées qui traitent cela comme une plus grande priorité, et que des géants de l'Internet comme Google, Facebook et Amazon prennent une place encore plus importante dans la vie du citoyen/consommateur.

D’autres pays qui ont déjà des solutions d’identité en place ont commencé à chercher des façons de déborder de leurs frontières en jouant un rôle de premier plan pour promouvoir l’identité numérique et en se servant de leurs propres expériences comme modèle pour de nouvelles initiatives. Dans certains cas, cela pourrait générer des revenus en permettant à d’autres pays de tirer parti des solutions, plateformes ou infrastructures existantes.

Étant donné que les plus grands fournisseurs de services Internet sont déjà bien placés pour être des chefs de file de l’identité numérique dans le monde entier, ces services ne sont pas encore aussi fiables du point de vue des risques (en raison de la faible assurance des données). Par ailleurs, nous n’avons pas encore vu la portée de ce qu’ils peuvent accomplir et ne savons pas si, en admettant qu’ils en aient la possibilité, ils vont chercher encore à consolider leur contrôle des clients pour renforcer et approfondir leurs relations avec les consommateurs/citoyens.

Avantages de développer l’économique numérique du Canada

Outre les avantages quantifiables, la croissance de l’économie numérique du Canada présente d’autres avantages qualitatifs découlant d’une meilleure identité numérique. L’accès amélioré et simplifié à des services d’identité vérifiables peut éventuellement engendrer de nouvelles opportunités pour ceux qui sont actuellement exclus, notamment les chômeurs, les immigrants, les aînés et les personnes vulnérables. Ces groupes ont tous tendance à avoir plus de difficulté à valider leur identité ou à participer à l’économie de la même façon que d’autres. Le fait d’offrir de nouvelles possibilités pour avoir une validation de l’identité plus efficace, simplifiée et sécuritaire donne l’occasion de les intégrer dans l’économie, et facilite l’accès à des emplois, des services gouvernementaux, des prestations et bien d’autres services.

Outre un meilleur accès aux personnes sous-desservies, l’identité numérique offre la possibilité de faire des gains de productivité à grande échelle dans de vastes segments de population et d’entreprises. Selon un rapport de l’OCDE, « la transformation numérique récente des activités économiques a donné lieu à quatre principales tendances innovatrices : 1) la mesure améliorée et en temps réel des activités commerciales; 2) des expériences commerciales accélérées et plus abordables; 3) un partage d’idées à plus grande échelle et simplifié; et 4) la capacité de reproduire les innovations d’une façon plus rapide et plus fidèle (croissance).[36]”

La sécurité et l’application de la loi comportent aussi des avantages sociétaux dont il faut tenir compte. Même si elle ne se fait pas « en ligne », la vérification de l’identité en personne peut s’effectuer d’une manière numérique. Si une solution d’identité est conçue de manière à empêcher une surveillance indésirable, cela peut être une occasion d’offrir quelque chose qui fournit un service public en étant plus exact, en réduisant les possibilités d’identité fautive ou d’accusations erronées, et en procurant aux responsables de la sécurité publique des outils pour mener leurs activités avec plus d’efficacité.

10. Par où faut-il commencer?

Le CCIAN et le cadre de confiance pancanadien

Le CCIAN s’est engagé d’une approche fondée sur la collaboration pour développer un cadre de confiance pancanadien[37] qui va établir des lignes directrices pour les fournisseurs de services d’identité numérique des secteurs privé et public. Pour que le Canada participe pleinement à la transformation numérique et à l’économie numérique mondiale, il faut concevoir des solutions d’identité numérique qui soient fiables, sûres, évolutives et pratiques, et qui protègent davantage la vie privée. Les solutions fabriquées au Canada reflètent et incorporent les principes, intérêts commerciaux et modèles techniques canadiens, et sont conformes aux règlements canadiens. Le

cadre de confiance pancanadien soutient la mise en place d'un écosystème canadien de l'identité numérique qui est innovateur et sûr, et qui protège la vie privée.

D'importants progrès ont été accomplis, mais cette initiative doit être accélérée pour que les entreprises et les consommateurs/citoyens du Canada puissent avoir une attente de base quant à la façon dont les initiatives reliées à l'identité numérique peuvent s'avérer concluantes au Canada. La priorité accordée à l'identité numérique doit venir en tête du programme des décideurs, des politiciens et des chefs d'entreprise. Il faut, pour tirer parti des avantages et que l'impact sur l'économie se fasse pleinement sentir, qu'une politique sur l'identité numérique au niveau du gouvernement et le développement de solutions d'identité numérique soient une priorité importante pour tous les intervenants.

C'est le temps d'agir

C'est le moment ou jamais de s'assurer que les consommateurs, les entreprises et les entités gouvernementales vont agir de concert pour atteindre l'objectif commun qui consiste à mettre en place un écosystème sécuritaire, sûre et de confiance pour l'identité numérique canadienne.

Outre le potentiel de rapporter plus de 15 milliards de CAD à l'économie, cela va s'accompagner d'innombrables avantages pour tous les pans de la société canadienne. Tout le monde, depuis un capitaine de navire en Colombie-Britannique à un serveur de restaurant à Toronto et à un enseignant du Nouveau-Brunswick, va bénéficier de l'obtention de ce droit pour le Canada.

Nous devons tous œuvrer à l'unisson, tout en assurant une approche distinctement canadienne, pour préserver notre avenir numérique collectif, faire en sorte que la protection de la vie privée et le choix soient maintenus, et nous efforcer de protéger les plus vulnérables d'entre nous. Si nous accomplissons tout cela, nous serons en bonne voie de bâtir un environnement innovateur, hautement connecté et gratifiant pour que l'économie numérique canadienne donne tout son potentiel.

Références

[1] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
[2] 8 heures par année x salaire horaire moyen de 26,68 CAD = 266,80 CAD par personne par année x 28,8 M de travailleurs canadiens
= CAD $6.1B, (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/dsbbcan-fra.htm, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-fra.htm)
[3] https://www.ic.gc.ca/eic/site/061.nsf/fra/h_03018.html#toc-09
[4] CAD 225 per user (https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/
18 M de travailleurs – Statistique Canada : http://www.statcan.gc.ca/pub/91-550-x/2008001/part-partie1-fra.htm
600 heures - ID Alerts : http://www.idalerts.ca/identity-theft-statistics/
5.68M - Canadian Underwriter : http://www.canadianunderwriter.ca/insurance/canada-second-expensive-country-data- breaches-ibm-ponemon-institute-study-1004115487/
[5] https://www.statista.com/statistics/289741/canada-retail-e-commerce-sales/
[6] Statistique Canada : (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-fra.htm)
[7] [225] 225 CAD par utilisateur (https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/) 18 M de travailleurs – Statistique Canada : http://www.statcan.gc.ca/pub/91-550-x/2008001/part-partie1-fra.htm
600 heures - ID Alerts : http://www.idalerts.ca/identity-theft-statistics/
5,68 M - Canadian Underwriter : http://www.canadianunderwriter.ca/insurance/canada-second-expensive-country-data- breaches-ibm-ponemon-institute-study-1004115487/
[8] Canada Health Infoway, Connected Health Information in Canada: A Benefits Evaluation Study, https://www.infoway-inforoute.ca/fr/component/edocman/ressources/rapports/evaluation-des-avantages/3514-etude-d-evaluation-des-avantages-de-l-information-de-sante-connectee-au-canada?Itemid=189
[9] Statistique Canada : (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-fra.htm)
[10] https://blog.dashlane.com/infographic-online-overload-its-worse-than-you-thought/
[11] https://blog.lastpass.com/2017/11/lastpass-reveals-8-truths-about-passwords-in-the-new-password-expose.html/
[12] 36 minutes par mois x 18,65 millions de travailleurs canadiens x salaire horaire moyen de 26,68 CAD, (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/dsbbcan-fra.htm, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-fra.htm)
[13] https://www.secureidnews.com/news-item/passwords-the-bane-of-enterprise-security/
[14] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html
[15] http://reports.weforum.org/rethinking-personal-data/
[16] http://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en
[17] https://www.pcworld.com/article/3075539/security/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html
[18] http://www.digitaltransactions.net/news/story/Expenses-From-the-Home-Depot-and-Target-Data-Breaches-Surpass-_500-Million
[19] https://www.pcworld.com/article/3075539/security/all-about-your-fullz-and-how-hackers-turn-your-personal-data-into-dollars.html
[20] https://www.pindrop.com/resources/download/report/2017-call-center-fraud-report
[21] https://www.forbes.com/sites/alanmcintyre/2018/02/07/the-battle-against-synthetic-identity-fraud-is-just-beginning/#5b0238664ca0
[22] Statistique Canada, tableau CANSIM 051-0001
[23] https://www.ic.gc.ca/eic/site/061.nsf/fra/h_03018.html
[24] 8 heures par année x salaire horaire moyen de 26,68 CAD = 266,80 CAD par personne par année x 28,8 M de travailleurs canadiens
= 6,1 G CAD, (http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/dsbbcan-fra.htm, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/labr69a-fra.htm)
[25] https://www.ic.gc.ca/eic/site/061.nsf/fra/h_03018.html#toc-09
[26] https://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge
[27] http://fortune.com/2017/04/27/estonia-digital-life-tech-startups/
[28] https://www.gemalto.com/govt/customer-cases/estonia-eid
[29] http://economictimes.indiatimes.com/news/economy/policy/indias-first-national-social-security-platform-to-be-developed-by-deity/articleshow/52301300.cms?from=mdr
[30] http://www.business-standard.com/article/current-affairs/aadhaar-crosses-1-billion-mark-says-prasad-116040401147_1.html
[31] https://auspostenterprise.com.au/content/dam/corp/ent-gov/documents/digital-identity-white-paper.pdf

[32] https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/ (p. 4)
[33] https://www.ctrl-shift.co.uk/insights/2014/06/09/economics-of-identity/ (p. 5)

[34] https://cyber.ee/en/referentsid-ja-kogemused/referents/national-electronic-id-solution-for-the-government-of-the-republic-of-azerbaijan/
[35] https://pages.nist.gov/800-63-3/sp800-63-3.html
[36] OECD (2017) – Going Digital: Making the Transformation Work for Growth and Well-Being https://www.oecd.org/mcm/documents/C-MIN-2017-4%20EN.pdf
[37] https://diacc.ca/2016/08/11/pctf-overview/