L'identité sur Internet

Briefing sur les affaires publiques de l'Internet Society

03 June 2016

Introduction

Certains pensent à leur identité numérique comme à un passeport pour Internet. En réalité, le concept d'identité sur Internet et beaucoup plus riche : nous adaptons notre identité en fonction du contexte. Par exemple, il est fort probable que nous divulguions notre « vraie » identité pour accéder aux services administratifs en ligne, alors que nous utiliserons un nom fictif ou un pseudonyme pour les medias sociaux, et que nous accéderons anonymement aux sites web publics pour des informations médicales.

Il existe cinq principaux types d'identité digitale, chacun étant utilisé dans différents contextes.

1. **Les identités électroniques.** Certains gouvernements émettent des identités électroniques à leurs citoyens pour utilisation en ligne. En certains cas, l'identité émise, ou le fournisseur d'identité, est un organisme approuvé (par ex. : un bureau de poste).

2. **Des identités basées sur un attribut.** Certaines interactions ne nécessitent pas d'identification. À la place, il suffit à la personne de posséder un attribut spécifique (par ex. : être âgé d'au moins 18 ans ou être étudiant).

3. **Les identités basées sur l'authentification.** De nombreux fournisseurs de services en ligne, tels que Facebook et Gmail, permettent aux utilisateurs l'accès à leur compte via un nom d'utilisateur et un mot de passe (aussi connus sous le nom d'« informations d'identification »). Ces identités représentent la manière dont les clients s'identifient aux fournisseurs de services et comment les fournisseurs de services authentifient ou vérifient que les utilisateurs sont ceux qu'ils prétendent être. À la différence des identités électroniques émises par le gouvernement, les identifiants de connexion peuvent être anonymes ou des pseudonymes. Les mécanismes d'authentification de seconde génération, tels que « l'authentification unique », permettent aux utilisateurs de se connecter à plusieurs services à partir d'un point d'accès.

Sur Internet, votre identité numérique n'est pas simplement un nom, c'est aussi qui vous êtes et votre clé pour des interactions enligne. Les identités numériques aident les utilisateurs à protéger leur vie privée ; à séparer les présences personnelles, sociales et professionnelles en ligne ; et à effectuer des transactions sécurisées avec des boutiques, banques, prestataires médicaux et les administrations. Les innovations axées sur l'identité peuvent encourager un secteur bancaire plus sécurisé, un commerce digital plus fiable (par ex. : signature électronique et paiement mobile) et une plus grande fiabilité du secteur des services administratifs en ligne (par ex. : déclaration de revenu et vote électroniques). Pour ces raisons, l'identité numérique est un aspect clé de nombreuses questions de la politique d'Internet, y compris la confidentialité, les objectifs en matière de protection des consommateurs, les services administratifs en ligne, le commerce numérique, et la sécurité en matière d'économie numérique. En bref, un écosystème d'identité numérique sécurisée est une composante essentielle d'un Internet sécurisé inspirant confiance.

L'Internet Society pense que les gouvernements doivent continuer à encourager le développement ouvert et l'utilisation de choix d'identité sur Internet, qu'elle soit identifiée, anonyme ou un pseudonyme. Ce dossier de politique est conçu pour aider les décideurs de politiques à comprendre les avantages de solutions d'identité en ligne pour les services, l'efficacité et la croissance économiques et l'autonomisation des citoyens.

4. **Signatures électroniques.** De nombreux pays ont adopté des lois visant à reconnaître le statut juridique des signatures électroniques. En plus d'être un moyen d'identification, les signatures électroniques peuvent avoir des répercussions telles que la confirmation ou l'acceptation d'un contrat.

5. **Les identificateurs.** Toutes les interactions en ligne impliquent d'utiliser des identifiants. Certains assurent la fonction Internet (par exemple, les adresses IP), d'autres identifient ou reconnaissent un appareil et/ou l'utilisateur (par exemple, la sécurité dans les institutions financières), et d'autres encore suivent les interactions en ligne des utilisateurs (par exemple, la publicité ciblée). Il n'existe pas de liste complète d'identificateurs : en théorie, les identificateurs sont les données qui identifient les informations relatives à un appareil et/ou un utilisateur. Les informations sur l'appareil peuvent inclurent le type d'appareil, le système d'exploitation, la version du navigateur, le navigateur, les plug-ins, etc. Les informations sur l'appareil peuvent inclurent les préférences, telles que la taille de police, les couleurs de l'écran, et le contraste, et des caractéristiques similaires.

Principales considérations

Il existe des considérations en matière de confidentialité et de cas d'utilisation spécifiques de chacune des identités numériques principales.

- **Les identités électroniques.** Pour recevoir une identité électronique provenant du gouvernement, les citoyens doivent généralement confirmer leur identité en présentant un passeport émis par le gouvernement, une carte d'identité, ou une autre forme d'identification émise par le gouvernement. Par conséquent, les deux types d'identité sont liés. En général, les identités électroniques émises par le gouvernement ont pour fonction principale les services gouvernementaux (par exemple, les déclarations d'impôts et la demande de prestations). Les usages secondaires concernent habituellement des services nécessitant un degré de certitude élevé ou l'assurance que la personne est qui il ou elle prétend être (par exemple, les dossiers bancaires et médicaux). Les identités électroniques émises par le gouvernement ont la plupart du temps des fonctions multiples, telles que l'identification, l'authentification à deux facteurs pour accéder à des services en ligne (par exemple, les services de gouvernement virtuel). Elles peuvent servir d'informations électroniques prouvant la possession d'un passeport pour accéder à des données personnelles, et de signature électronique juridiquement valable.

- **Des identités basées sur un attribut.** Même si un attribut (par exemple, l'âge) pourrait ne pas indiquer l'identité réelle d'un individu, une combinaison d'attributs rendrait cela possible (par exemple, la date de naissance, le code postal et le sexe).

- **Les identités basées sur l'authentification.** Pour diverses raisons, les mécanismes d'authentification ne nécessitant qu'un nom d'utilisateur et un mot de passe ne sont certainement pas sécurisés. Souvent, le nom d'utilisateur est une adresse e-mail ou un autre identifiant évident (par exemple, un nom ou un surnom) ; les gens réutilisent fréquemment les mots de passe ou utilisent des mots de passe faciles à deviner (par exemple, 12345) ; et lorsque les utilisateurs

oublient leurs mots de passe, les sites les réinitialisent généralement en utilisant l'adresse e-mail enregistrée dans le profil, ce qui rend le compte encore plus vulnérable. Aujourd'hui, de nombreux fournisseurs de services proposent une protection de contrôle d'accès supplémentaire via l'authentification à deux facteurs. Ce type d'authentification nécessite de combiner quelque chose que l'utilisateur reçoit (par exemple, un code à usage unique expirant envoyé au téléphone intelligent de l'utilisateur) et quelque chose que l'utilisateur connaît (par exemple, le nom d'utilisateur ou le mot de passe). Les mécanismes d'authentification unique offrent aux utilisateurs une plus grande commodité, mais peuvent les amener à faire le suivi des services connectés.

Notez que même si les utilisateurs choisissent des identifiants de connexion pseudonymes, le contenu de leurs comptes (par exemple, le texte de l'email ou les photos) peut révéler leur véritable identité.

- **Signatures électroniques.** Les signatures électroniques peuvent avoir deux fonctions : confirmer qu'un utilisateur assume le contenu d'un document et confirmer l'auteur du message. La reconnaissance juridique transfrontalière des signatures électroniques est essentielle pour un commerce international efficace.

- **Les identificateurs.** Les identificateurs peuvent servir à identifier un appareil ou un utilisateur[1] spécifique ou suivre un appareil ou les interactions en ligne de l'utilisateur de l'appareil. Certains identificateurs peuvent être remarqués facilement (par exemple, les fonctionnalités du navigateur), d'autres sont délibérément placés dans un appareil pour faciliter le suivi (par exemple, les cookies). Les identificateurs peuvent être regroupés, reliés et utilisés pour déterminer les connexions.

Difficultés

La confidentialité est l'un des plus gros challenges pour ce qui est de l'identité numérique. On ne peut plus affirmer que « Sur Internet, personne ne sait que vous êtes un chien » pour citer la célèbre bande dessinée de *The New Yorker* (1993). Malgré les innombrables manières dont les identités numériques sécurisées et vérifiables sont utilisées, la majorité des utilisateurs d'Internet est aujourd'hui plus facile à identifier qu'avant. Dans de nombreux cas, bien que l'identité réelle d'un utilisateur ne puisse pas être connue immédiatement, elle peut être déduite par une personne ayant suffisamment accès soit à ses données soit à ses attributs (par exemples, les amis sur Facebook, les données de géolocalisation, le temps Internet et les dates).

Principes directeurs

Voici les principes directeurs que les gouvernements et les citoyens doivent prendre en compte :

- **Les individus devraient avoir la possibilité d'utiliser des identités numériques pseudonymes et anonymes, selon le contexte et les personnes avec qui ils**

1 See Panopticlick, an Electronic Frontier Foundation research project on the uniqueness of browsers, https://panopticlick.eff.org/.

interagissent. Les individus devraient avoir accès à des identités numériques fiables, sûres, prenant en compte le respect de la vie privée dès la conception lors des transactions en ligne, particulièrement celles contenant des données sensibles (par exemple, les données médicales et financières) ou tout contenu privé. Fondamentalement, ce sont les caractéristiques qui favoriseront un environnement de consommation sécurisé, fiable et protecteur.

- **Il n'est pas nécessaire que les identités numériques soient émises par le gouvernement pour être fiables.** Cependant, les gouvernements devraient envisager de proposer une identification électronique pour un accès plus sécurisé aux services du gouvernement virtuel et aux transactions commerciales (par exemple, les transactions bancaires) qui nécessitent un niveau d'authentification élevé. Ceci contribuerait à la sécurité des transactions de chaque partie.

Les gouvernements ayant déjà émis l'identification électronique (fournisseurs d'identité) devraient prendre les mesures suivantes :

- Examiner la(les) forme(s) d'identité électronique la(les) plus appropriée(s) aux usages envisagés ; et identifier les problèmes économiques, sociaux, ou d'autres obstacles qui pourraient empêcher leur déploiement ou utilisation.

- Veiller à ce que leur système d'identité électronique soit techniquement interopérable et juridiquement compatible avec les systèmes d'identité déployés par d'autres gouvernements, afin que leurs identités électroniques puissent être utilisées lors des transactions internationales.

- Empêcher le gouvernement et d'autres parties qui l'utilisent de suivre l'utilisation d'identité électronique entre les services et les institutions, à moins que cela ne soit absolument nécessaire. Une bonne pratique de confidentialité et de sécurité consiste à mettre en quarantaine l'utilisation des identités numériques et des données utilisées pour y accéder.

- Recueillir et utiliser uniquement les données nécessaires pendant tout le cycle de vie de l'identité électronique. Appliquer le principe de minimisation des données de cette manière augmente la confiance des consommateurs ainsi que le choix.

- Rendre les identités électroniques révocables en cas de besoin (par exemple, en cas de compromis).

- Procéder à une analyse approfondie des risques et des avantages avant d'envisager d'utiliser des données biométriques à des fins d'identités électroniques. En cas de compromis, les données biométriques sont irrévocables (par exemple, on ne peut pas changer son empreinte digitale). Pour cette raison, il faudrait éviter cela, à moins que ce ne soit absolument nécessaire.

Les gouvernements devraient veiller à ce que les citoyens à qui ils n'ont pas émis d'identités électroniques ne soient pas exclus des services gouvernementaux.

Conclusion

Une identité numérique efficace favorise des échanges sécurisés sur Internet. Pour cette raison, il est essentiel que les gouvernements (1) continuent d'encourager le développement ouvert et l'utilisation des nouvelles technologies pour exprimer son identité sur Internet, qu'elles soient identifiées, des pseudonymes, ou anonymes ; et (2) s'abstenir de toute activité pouvant freiner l'innovation ou le progrès économique et social, telle qu'exiger un niveau d'identification requis pour accéder à Internet ou aux médias sociaux.

Ressources supplémentaires

L'Internet Society a publié plusieurs articles et du contenu supplémentaire en rapport avec cette question. Ils sont disponibles en libre accès sur le site Web de l'Internet Society.

- Comprendre votre identité en ligne : aperçu sur l'identité, 2011, http://www.internetsociety.org/understanding-your-online-identity-overview-identity

- Comprendre votre identité en ligne : protection de votre confidentialité, 2012, http://www.internetsociety.org/understanding-your-online-identity-protecting-your-privacy-0

- R. Wilton, *Avez-vous choisi un fournisseur d'identité récemment ?*, 2014, http://www.internetsociety.org/doc/have-you-chosen-identity-provider-lately

Vous trouverez en ligne plus d'informations sur l'identité numérique en ligne.

- *Gestion de l'identité numérique : favoriser l'innovation et la confiance dans l'économie Internet* , Organisation de Coopération et de Développement Économiques, 2011, http://www.oecd.org /sti/interneteconomy/49338380.pdf

- E. Birrell and F.B. Schneider, "Federated Identity Management Systems: A Privacy-Based Characterization," *Security & Privacy, IEEE,* vol. 11, no. 5, septembre-octobre 2013, pp. 36–48, https://www.cs.cornell.edu/fbs/publications/idMgmt.SP.pdf