Documents de travail de l'OCDE sur l'économie numérique No. 101

Technologies fondées sur la biométrie

OCDE

OCDE

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

10-Jun-2005

Français - Or. Anglais

DIRECTION DE LA SCIENCE, DE LA TECHNOLOGIE ET DE L'INDUSTRIE
COMITE DE LA POLITIQUE DE L'INFORMATION, DE L'INFORMATIQUE ET DES COMMUNICATIONS

Annule & remplace le même document du 24 mai 2005

Groupe de travail sur la sécurité de l'information et la vie privée

TECHNOLOGIES FONDEES SUR LA BIOMETRIE

www.oecd.org/sti/security-privacy

JT00186151

DSTI/ICCP/REG(2003)2/FINAL
Non classifié

Français - Or. Anglais

AVANT-PROPOS

Ce rapport livre un premier aperçu des avantages et des faiblesses des technologies fondées sur la biométrie. Il comprend également des informations sur les méthodologies existantes dans le domaine de la protection de la vie privée et la sécurité pour évaluer la biométrie.

Ce rapport a été préparé, avec les commentaires des pays membres, par Peter Hope-Tindall, consultant auprès de l'OCDE, sous la supervision du Secrétariat. Peter Hope-Tindall est le directeur et Architecte en Chef de la Protection de la Vie Privée (« Chief Privacy Architect ») de dataPrivacy partners.

Ce rapport a été déclassifié par le Comité de la Politique de l'Information, de l'Informatique et des Communications lors de sa 46ème session les 1-2 avril 2004. Il est publié sous la responsabilité du Secrétaire Général de l'OCDE.

TABLE DES MATIÈRES

AVANT-PROPOS 2

TABLE DES MATIÈRES 3

RÉSUMÉ 4

TECHNOLOGIES FONDÉES SUR LA BIOMÉTRIE 6

Généralités et contexte 6
Objet du présent rapport 6
Protection de la vie privée 6
Sécurité 8
Intérêt porté aux technologies fondées sur la biométrie 10
Technologies fondées sur la biométrie 11
Définitions 11
Aspects de la biométrie concernant la protection de la vie privée 13
Questions de sécurité liées à la biométrie 14
Inventaire des technologies biométriques 16
Normes sur la biométrie 43
Normes concernant la protection de la vie privée et la biométrie 44
Méthodologies et cadres régissant la mise en œuvre des technologies biométriques 44
Méthodologies assurant la protection de la vie privée et la sécurité des applications biométriques 44
Industrie de la biométrie 48
Conclusion 50

NOTES 51

REFERENCES 52

ANNEXE I – PROTECTION LÉGALE DE LA VIE PRIVÉE POUR LA BIOMÉTRIE 58

ANNEXE II – PRIVACY ARCHITECTURE AND THE PIA (texte anglais uniquement) 63

ANNEXE III – DNA-BASED TECHNOLOGIES (texte anglais uniquement) 68

ANNEXE IV – BIOMETRIC ENCRYPTION (texte anglais uniquement) 70

RÉSUMÉ

Le présent rapport constitue une introduction générale aux technologies biométriques. Il analyse également les différentes préoccupations que soulèvent ces technologies et, tout particulièrement, la protection de la vie privée et la sécurité de l'information.

Les techniques biométriques sont en plein essor et suscitent un vif intérêt dans différents domaines, tels que le secteur bancaire, l'enseignement et d'autres services publics, ainsi que dans le contexte de la sécurité des voyages. D'autres technologies biométriques permettent d'identifier des personnes sur des réseaux distants et par différents modes de communication. Durant les cinq prochaines années, l'industrie de la biométrie devrait connaître une croissance encore plus forte que celle de ces dernières années. Plusieurs normes relatives à la biométrie ont été, ou sont sur le point d'être, établies à l'appui de l'industrie et de la technologie. Certains événements survenus dans le monde et la recherche d'une solution technologique aux problèmes de sécurité ressentis par de nombreuses personnes ont accru l'intérêt porté aux technologies fondées sur la biométrie et à l'industrie de la biométrie en général.

Les applications biométriques amènent de nouveaux termes et concepts qu'il importe de bien comprendre pour pouvoir aborder ce sujet en connaissance de cause. Ce rapport présente les principales technologies biométriques, à savoir la reconnaissance des empreintes digitales, la géométrie de la main, la reconnaissance faciale, la reconnaissance de l'iris, de la rétine, de la géométrie du doigt, de la voix et la vérification dynamique de la signature. De plus, il décrit brièvement d'autres technologies biométriques moins connues telles que la géométrie de l'oreille, l'odeur corporelle, la dynamique de la frappe sur clavier et la reconnaissance de la démarche. La technologie fondée sur l'ADN, qui ne relève pas au sens strict de la biométrie, mais suscite à peu près les mêmes préoccupations que cette dernière, est traitée dans l’annexe III.

Tous les systèmes biométriques fonctionnent suivant le même principe. Ils prélèvent un échantillon biométrique, en extraient les caractéristiques ou créent un ensemble de données et effectuent une recherche fondée sur une comparaison individuelle (1 : 1) ou collective (1 : N). S'agissant de la performance des systèmes biométriques, le lecteur est averti du manque de rapports indépendants et accessibles au public sur la question et de l'importance qui doit être accordée au contexte dans l'analyse des statistiques en la matière. Plusieurs mesures de la performance sont toutefois utiles pour débattre et comparer les technologies fondées sur la biométrie et peuvent apporter une certaine objectivité au choix des technologies particulières. Les mesures de la performance abordées comprennent, notamment, le taux de faux rejets, le taux de fausses acceptations, le point d'équivalence des erreurs, l’échec à l’acquisition, l'échec à l'enrôlement. D'autres facteurs, tels que le débit, le coût, la facilité d'utilisation, l'acceptation par l'utilisateur et la transparence, jouent un rôle décisif dans le bon fonctionnement d'une application, bien qu'ils ne fassent pas partie des indicateurs principaux de la performance d'un système biométrique. Ce rapport examine certains aspects de la performance des technologies biométriques en étudiant leur adéquation à certaines applications. Il contient une synthèse détaillée assortie de plusieurs exemples d'applications existantes et projetées.

Ce rapport évoque également un certain nombre de préoccupations liées aux technologies fondées sur la biométrie, en particulier celles qui touchent à la sécurité et à la vie privée. Les trois principaux aspects liés à la vie privée se rapportent *i)* à la possibilité qu'ils se prêtent à une utilisation détournée (« *function*

creep »), *ii)* au risque que ces systèmes composent une infrastructure de surveillance et *iii)* au fait que le consentement et la transparence puissent être optionnels dans certaines mises en œuvre d'applications biométriques. S'agissant de la sécurité, ce rapport revient sur le débat récent autour des faiblesses des systèmes biométriques. Les systèmes biométriques doivent être protégés contre un certain nombre d'attaques spécifiques (usurpation ou *spoofing*, falsification ou effraction, attaques rejouées, etc.).

Afin de résoudre ces problèmes liés à la vie privée et à la sécurité, ce rapport propose aux concepteurs de systèmes d'utiliser la biométrie à bon escient pour traiter un problème de sécurité et d'incorporer des dispositifs appropriés de sauvegarde et de traitement des exceptions dans la conception générale du système.

Plusieurs moyens d'intégrer la protection de la vie privée et la sécurité dans un système biométrique sont abordés : des moyens juridiques (la législation en tant qu'outil participant à la définition d'un système biométrique), des moyens politiques (élaboration de mesures à incorporer dans les systèmes biométriques) et des moyens technologiques, tels que du matériel anti-effraction capable d'empêcher et de commander le fonctionnement d'un système biométrique. D'autres méthodes formelles telles que l'architecture de la vie privée et l'architecture de la sécurité sont également présentées. Elles visent à faire en sorte que les composantes de la protection de la vie privée et de la sécurité entrent dans la construction des systèmes. À cet égard, ce document recommande que la conception de tous les systèmes biométriques soit alignée sur les *Lignes directrices de l'OCDE sur la vie privée* et les *Lignes directrices de l'OCDE sur la sécurité*.

Ce rapport examine aussi d'autres préoccupations assez répandues concernant les technologies biométriques, telles que le risque de surestimer les capacités des systèmes biométriques et de faire reposer la sécurité entièrement sur ces systèmes, le manque de rapports indépendants et accessibles au public sur la performance de ces systèmes et le risque de recourir systématiquement aux technologies biométriques comme s'il s'agissait d'une panacée.

Enfin, ce rapport plaide en faveur du lancement d'une initiative plurinationale destinée à favoriser la recherche, le développement et la formation dans le domaine de la biométrie. De telles initiatives devraient largement tenir compte des *Lignes directrices de l'OCDE* en intégrant à la fois la protection de la vie privée et la sécurité de façon à ce que nous n'ayons pas à sacrifier l'une pour l'autre.

TECHNOLOGIES FONDÉES SUR LA BIOMÉTRIE

Généralités et contexte

Objet du présent rapport

Ce rapport livre un premier aperçu des technologies fondées sur la biométrie en analysant les avantages, les faiblesses et le champ d'application de ces différentes technologies.

Il est possible que les débats débouchent sur l'identification ou la mise au point de méthodes propres à rendre les applications des technologies fondées sur la biométrie plus respectueuses de la vie privée et plus sûres.

Le lecteur est averti du fait que les conclusions et recommandations ne doivent pas être interprétées comme s'appliquant automatiquement à toutes les circonstances.

Protection de la vie privée

De quoi s'agit-il ?

Selon les descriptions, la protection de la vie privée va du simple « droit de s'isoler » (*right to be left alone*) (Warren and Brandeis, 1890)[1] au droit qu'ont les personnes de créer et de maintenir un « espace privé » autour d'elles, tant physique que numérique, protégé des interférences des autres.

Le droit à la protection de la vie privée, se réfère généralement au droit d'accomplir les actes suivants, en restant dans les limites de la légalité :

- Ne pas divulguer des informations à caractère personnel ou choisir la personne à qui on les confiera.
- Garder l'anonymat dans le cadre de certaines activités personnelles et publiques, si nous le souhaitons (ces activités peuvent inclure l'exercice de droits publics tels que la liberté d'association ou des choix personnels, comme nos habitudes de consommation ou notre religion).
- Vivre sans être surveillé par d'autres.
- Mener des communications privées.
- Jouir d'une intimité physique et d'un espace privé.
- S'isoler, en qualité de consommateur ou de citoyen.

Éléments de la protection de la vie privée

Propriété et contrôle

Un point de vue de plus en plus admis, bien qu'il ne fasse pas l'unanimité, est que l'information appartient à la personne à laquelle elle se rapporte – ce qui appartient véritablement à la personne concernée est l'information en elle-même, pas forcément le document en papier sur lequel elle est couchée ou l'ordinateur dans lequel elle est stockée. Par conséquent, la personne concernée a le droit de déterminer qui peut accéder à l'information et quels types d'utilisation sont autorisés, ainsi que de disposer d'un mécanisme lui permettant de revoir les données et d'y apporter les corrections nécessaires.

Complexité de la protection de la vie privée

Selon les *Critères Communs pour l'évaluation de la sécurité des Technologies de l'Information* (« Critères Communs »), la protection de la vie privée repose sur trois notions : identité, associabilité et observabilité. Certains (Adams *et al.*, 2002) ont proposé d'utiliser ces trois notions pour décrire la protection de la vie privée sous la forme d'une figure tridimensionnelle et mesurer la protection de la vie privée relative d'un système ou d'une technologie donnés (Hope-Tindall, 2002a).

Lignes directrices de l'OCDE sur la vie privée

En 1980, reconnaissant l'importance de la protection des données dans les échanges internationaux, l'*Organisation de Coopération et de Développement Économiques* (OCDE) a publié des Lignes directrices sur la vie privée qui, depuis lors, servent de référence en la matière. Ces lignes directrices tendaient à harmoniser les législations nationales en matière de vie privée et, tout en soutenant les droits de l'Homme, à prévenir le blocage des flux de données internationaux. Elles traduisent un consensus sur des principes fondamentaux susceptibles d'orienter la législation ou de constituer les fondements d'un régime d'autorégulation dans les pays qui n'ont pas légiféré en la matière. Au Canada, le code type sur la protection des renseignements personnels[2] de l'Association canadienne de normalisation (CSA) est un instrument facultatif fondé sur les *Lignes directrices de l'OCDE sur la vie privée*, repris en annexe à la législation fédérale sur la vie privée[3] promulguée récemment.

Les *Lignes directrices de l'OCDE sur la vie privée* énoncent huit principes, souvent repris sous l'appellation « pratiques d'information équitables » (*fair information practices*).

Ces principes sont les suivants (OCDE, 1980) :

> **Principe de la spécification des finalités** : Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne seraient pas incompatibles avec les précédentes et qui seraient également déterminées dès lors qu'elles seraient modifiées.
>
> **Principe de la transparence** : Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel, et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.
>
> **Principe de la limitation en matière de collecte** : Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par

des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Principe de la qualité des données : Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

Principe de la responsabilité : Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Principe de la limitation de l'utilisation : Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au principe de la spécification des finalités, si ce n'est :

- Avec le consentement de la personne concernée.

- Lorsqu'une règle de droit le permet.

Principe de la participation individuelle : Toute personne physique devrait avoir le droit :

- D'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant.

- De se faire communiquer les données la concernant ; dans un délai raisonnable ; moyennant, éventuellement, une redevance modérée ; selon des modalités raisonnables ; et sous une forme qui lui soit aisément intelligible.

- D'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément à ce principe est rejetée et de pouvoir contester un tel rejet.

- De contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Principe des garanties de sécurité : Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou l'accès, la destruction, l'utilisation ou la divulgation non autorisés.

Sécurité

Rôle de la sécurité dans la protection de la vie privée

« Trop souvent, les débats partent du principe que sécurité et protection de la vie privée s'excluent mutuellement », comme l'a souligné Frank J. Cilluffo. « C'est tout simplement faux. On commet une erreur en abordant cette question en termes de « soit…soit ». Les parties prenantes devraient plutôt se pencher sur la nécessité de concilier les deux. Pour répondre au double objectif de sécurité et de protection de la vie privée, elles doivent partir de l'idée que ces deux notions vont de pair » (Cilluffo, 2000).

La nécessité d'établir un juste milieu entre la protection de la vie privée et la sécurité ne fait aucun doute. La protection de la vie privée et la protection des données personnelles sont des droits qui revêtent une importance fondamentale. Leur respect est essentiel à la protection et au soutien de la dignité humaine.

Néanmoins, des intérêts publics incontestables, précisément identifiés, peuvent justifier l'imposition de limites à la protection de la vie privée.

Les principes des *Lignes directrices de l'OCDE sur la sécurité* (OCDE, 2002) (par exemple le principe de démocratie et le principe d'éthique) et les principes des *Lignes directrices de l'OCDE sur la vie privée* (par exemple, le principe de la limitation de l'utilisation ou le principe des garanties de sécurité) tendent à faciliter l'adoption d'une démarche ménageant à la fois les objectifs de sécurité des systèmes d'information et de protection des données personnelles et de la vie privée.

Le droit souverain pour les gouvernements d'exercer leur autorité comme il convient dans des domaines clés tels que la sécurité nationale et le maintien de l'ordre public est reconnu dans les *Lignes directrices sur la sécurité* et les *Lignes directrices sur la vie privée*.

Nous proposons qu'une conception et des décisions politiques appropriées nous évitent d'avoir à choisir entre la sécurité et la protection de la vie privée. La recherche de solutions cohérentes dans le domaine de la sécurité devra tenir compte des grands enjeux économiques et sociaux.

Lignes directrices de l'OCDE sur la sécurité

De nouvelles « *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information* » ont été adoptées sous la forme d'une Recommandation du Conseil de l'OCDE, fin juillet 2002.

Sous-titrées « Vers une culture de la sécurité », les *Lignes directrices* ont été conçues avec le souci de tenir compte de notre dépendance croissante à l'égard des réseaux d'information et de l'augmentation des menaces pour la sécurité de ces réseaux. Saluant ces *Lignes directrices*, le Département d'État des États-Unis note qu'elles contribuent à « une nouvelle compréhension internationale de la nécessité de sauvegarder les systèmes d'information dont nous dépendons de plus en plus dans notre mode de vie » (Williams, 2002).

Depuis leur adoption en juillet 2002, les *Lignes directrices de l'OCDE sur la sécurité* ont servi de base à la résolution A/RES/57/239 de l'Assemblée générale des Nations Unies pour la « Création d'une culture mondiale de cybersécurité », en décembre 2002, et ont été reconnues par le Conseil des ministres de la Coopération économique Asie-Pacifique (CEAP) et par le Conseil de l'Union européenne.

Ces *Lignes directrices* sont axées sur neuf principes directeurs (OCDE, 2002) :

Sensibilisation : les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

Responsabilité : les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

Réaction : les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

Éthique : les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

Démocratie : la sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

Évaluation des risques : les parties prenantes doivent procéder à des évaluations des risques.

Conception et mise en oeuvre de la sécurité : les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

Gestion de la sécurité : les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

Réévaluation : les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

Intérêt porté aux technologies fondées sur la biométrie

Depuis peu, les technologies fondées sur la biométrie suscitent un grand intérêt pour ce qu'elles pourraient apporter à la recherche de criminels, à la lutte contre le terrorisme et comme méthode d'identification « infaillible ».

Que ces affirmations restent encore à prouver ou non, il est de plus en plus manifeste que les essais, déploiements et études de technologies biométriques s'intensifieront dans les aéroports et aux points de passage aux frontières, en vue de leur adoption dans un avenir proche :

- En 2003, 14 États membres de l'Union européenne se sont récemment dotés de cette technologie, afin de faciliter le traitement des réfugiés et des demandeurs d'asile (EC, 2003)[4].

- Le directeur de l'Association du transport aérien international (IATA) a beaucoup insisté sur la mise en place de mesures de sécurité plus strictes et plus généralisées dans les aéroports et sur les lignes aériennes, notamment à l'aide de la biométrie (Chua, 2001).

- Le 28 mai 2003, l'Organisation de l'aviation civile internationale (OACI) a adopté un projet harmonisé à l'échelle mondiale pour l'incorporation de données d'identification biométriques dans les passeports et d'autres documents de voyage lisibles à la machine (MRTD). Selon l'OACI, « L'utilisation accrue de MRTD améliorés par la biométrie permettra d'accélérer le flux des passages aux points de contrôle aux aéroports, de renforcer la sûreté de l'aviation et d'améliorer la protection contre les vols d'identité. » (OACI, 2003a)

- Aux États-Unis, la Loi sur le renforcement de la sécurité aux frontières (*Enhanced Border Security and Visa Entry Reform Act*) dispose que, à compter du 26 octobre 2004 (US House of Representatives, 2002), le Service d'immigration et de naturalisation (INS) prendra un identifiant biométrique unique, par exemple une empreinte digitale ou une image du visage, de chaque étranger entrant et sortant des États-Unis avec un visa. Par ailleurs, les États-Unis ont également étendu aux pays participants à leur programme d'exemption de visa (*Visa Waiver Program*) l'obligation d'incorporer un identifiant biométrique dans leurs documents de voyages infalsifiables nationaux, le respect de cette obligation étant une condition pour continuer de participer à ce programme (Fonseca, 2002 ; US Department of State, 2002).

Aujourd'hui, des technologies fondées sur la biométrie sont utilisées pour restreindre l'accès à des installations et systèmes d'information à haute sécurité et faciliter l'enregistrement et l'authentification des usagers en ligne.

A mesure que les innovations technologiques et le désir de se simplifier la vie amènent les hommes à interagir avec des systèmes reliés à des réseaux (comme les distributeurs automatiques de billets (DAB), les distributeurs automatiques de journaux ainsi que les services bancaires, les achats, les votes, etc. par téléphone ou par Internet), et bien que ces technologies soient loin d'avoir atteint leur maturité, les technologies fondées sur la biométrie pourraient constituer la réponse à un problème qui s'oppose sérieusement à cette évolution, à savoir la possibilité d'authentifier quelqu'un à distance.

Quelles que soient nos opinions et préférences personnelles, l'heure est venue d'envisager ces technologies comme des solutions aux problèmes présents et futurs, de déterminer leurs avantages et leurs inconvénients avec une certitude scientifique et de débattre ouvertement de leurs implications pour la sécurité et la protection de la vie privée.

Technologies fondées sur la biométrie

Définitions

Biométrie

Le terme « biométrie » vient du grec *bio* (vie) et *metron* (mesure).

> La biométrie a été définie comme : « L'exploitation automatisée de caractéristiques physiologiques ou comportementales pour déterminer ou vérifier l'identité. » (IBG, n.d.a)
>
> *Bien que le terme « automatisée » soit essentiel dans la définition d'un système biométrique (à titre d'exemple, un système de documents dont les images sont comparées manuellement n'est pas un système biométrique), il est important de noter que le terme « **assisté par un dispositif automatisé** » serait sans doute plus approprié à la définition, car, dans de nombreux cas, un système biométrique indique un degré de corrélation statistique, et non une corrélation absolue, sur base duquel un opérateur humain devra confirmer ou non l'identité. (Si certains systèmes de vérification 1 à 1 peuvent fonctionner d'une façon largement automatisée (fondée sur un seuil d'acceptation et un taux d'erreur fixé par l'opérateur), les systèmes d'identification 1 à N forcent habituellement l'administrateur du système à trouver un compromis entre le recours à un être humain pour examiner une fausse acceptation (ou un faux rejet) et l'acceptation d'un taux global d'erreur plus élevé).*

Une autre définition indique très clairement que ce champ d'étude ne concerne que les êtres humains :

> « La biométrie s'applique à des particularités ou des caractères humains uniques en leur genre et mesurables permettant de reconnaître ou de vérifier automatiquement l'identité ». (Roethenbaugh, 1998a) [*]

[*] Note de traduction : La terminologie anglo-saxonne peut paraître plus adaptée au cadre de cette définition qui renvoie à l'utilisation de technologies de l'information et de l'électronique récentes ou spécifiques, objet du présent document.

L'International Biometric Group (IBG), une entreprise bien connue d'essais et de conseils en biométrie, donne les précisions suivantes[*] quant à l'utilisation des différentes formes du mot en anglais (IBG, n.d.a):

> ***Biometric*** (nom) : une des technologies qui permettent de déterminer ou de vérifier l'identité à partir de caractéristiques comportementales ou physiologiques. Exemple : «*Finger-scanning is a commonly used biometric*». La forme plurielle est également acceptée : «*Retina-scan and iris-scan are eye-based biometrics*».
>
> ***Biometrics*** (nom) : se réfèrent à l'identification biométrique. Exemple : «*What is the future of biometrics ?* »
>
> ***Biometric*** (adjectif) : se rapporte aux technologies qui déterminent ou vérifient l'identité d'après des caractéristiques comportementales ou physiologiques. Exemple : «*Do you plan to use biometric identification or older types of identification ?* »

Système biométrique

Le terme « *Système biométrique* » peut se définir en ces termes :

Un ***système biométrique*** comprend tout le matériel, les logiciels associés, les microprogrammes (*firmware*) et les composantes de réseau nécessaires à la totalité du déroulement des processus d'enrôlement et d'appariement biométriques.

Les technologies fondées sur l'ADN relèvent-elles de la biométrie ?

Cette question revient souvent ; en fait, les technologies fondées sur l'ADN diffèrent des technologies biométriques classiques à plusieurs égards :

- Les technologies fondées sur l'ADN requièrent un échantillon matériel et non une image, une photographie ou une numérisation.
- Les ADN ne sont pas appariés en temps réel et la majeure partie des opérations ne sont pas automatisées.
- La comparaison entre les ADN ne fait pas appel à des gabarits ou à l'extraction des caractéristiques, mais se pratique sur de vrais échantillons d'ADN.

Par conséquent, l'appariement des ADN ***ne*** relève ***pas*** de la biométrie au sens strict, ***pas plus*** que l'observation des empreintes digitales en médecine légale traditionnelle.

Ces distinctions mises à part, nous pensons que les technologies fondées sur l'ADN doivent être débattues parallèlement à d'autres technologies biométriques, dans la mesure où elles servent à déterminer ou à vérifier l'identité à partir de caractéristiques physiologiques. Au-delà de la définition, la plupart des observateurs estiment que les technologies fondées sur l'ADN sont analogues aux autres technologies biométriques et peuvent remplir les mêmes fonctions que ces dernières. Les technologies fondées sur l'ADN ont des implications politiques semblables, quoique beaucoup plus lourdes, à celles des autres technologies biométriques.

---

[*] Note de traduction : les termes et les exemples sont conservés en anglais. En français, on trouve les termes suivants : le nom commun « biométrie » qui se rapporte au champ d'étude (ex. : « Quel est le futur de la biométrie ?») et l'adjectif « biométrique » qui se rapporte aux technologies de ce domaine (ex. : « un identifiant biométrique, les technologies biométriques »).

Bien que les technologies fondées sur l'ADN ne constituent pas l'objet principal de ce rapport, l'annexe III fournit une description succincte et une analyse de ces technologies.

Aspects de la biométrie concernant la protection de la vie privée

La biométrie, à l'instar de toutes les technologies, est définie par son usage. Les technologies biométriques ne sont, en elles-mêmes, ni nécessairement préjudiciables ni nécessairement favorables à la protection de la vie privée. L'application de ces technologies soulève néanmoins plusieurs *problèmes* de protection de la vie privée particuliers.

« Détournement d'usage » (Function creep)

Le détournement d'usage est l'expression utilisée pour décrire le détournement d'un processus ou système, par lequel les données collectées pour une utilisation spécifique servent ensuite un autre objectif involontaire ou non autorisé.

Du point de vue des principes régissant la protection de la vie privée, un tel détournement pourrait être considéré comme contraire au « principe de la spécification des finalités » ; puisqu'il équivaut à l'utilisation, la rétention ou la divulgation ultérieures de données sans le consentement de la personne et incompatibles avec le type d'utilisation spécifié au moment de leur collecte.

Prenons l'exemple du système d'un service d'aide sociale qui impose une capture de l'empreinte des doigts au moment de l'inscription. Supposons que ce service se soit engagé auprès de l'allocataire inscrit à n'utiliser cette capture qu'à la ***seule*** fin de vérifier que ce dernier ***ne*** touche ***pas*** deux fois les prestations sociales (cumul d'avantages). Si la capture sert ensuite un autre objectif (par exemple une utilisation non décrite dans l'engagement initial), alors il s'agit d'un cas de détournement de type «function creep».

Infrastructure de surveillance/identificateur unique

Ce que certains craignent le plus est que la biométrie devienne un instrument de surveillance et de contrôle social. Sans doute parce qu'elle incarne la forme ultime d'identification personnelle, la biométrie peut être considérée comme facilitant tous les aspects inquiétants et déshumanisants d'une société d'information – une société dans laquelle une somme d'informations personnelles jamais égalée auparavant peut être recueillie et exploitée de façon systématique. Le risque existe effectivement que l'authentification biométrique devienne la forme par défaut de l'authentification et de l'identification humaines, même dans des situations où une méthode moins intrusive suffirait, simplement parce qu'une empreinte biométrique peut être prise de tout le monde et aussitôt utilisée. Un instrument d'identification biométrique facilite considérablement la surveillance fondée sur l'exploitation de données (ou « dataveillance »). « Là où toutes les transactions électroniques exigent une authentification électronique, ceux qui ont accès aux données de la transaction ont aussi un portrait détaillé de la personne » (O'Connor, 1998). Un risque inhérent à une telle utilisation de la biométrie serait que les identifiants biométriques soient utilisés pour relier des données transactionnelles à l'insu de la personne concernée, et à fortiori sans son consentement.

Comme l'a fait remarquer M. George Tomko, un expert en protection de la vie privée et concepteur de systèmes biométriques, « la biométrie, si elle est utilisée telle qu'elle est commercialisée actuellement par [la plupart] des fournisseurs (où le gabarit biométrique est utilisé comme moyen d'identification ou de vérification), portera atteinte à la vie privée et mettra en péril nos libertés. En deux mots, la biométrie fondée sur un gabarit ne respecte pas la vie privée. Chaque fois que la vérification ou l'identification reposent sur la comparaison avec un gabarit stocké, cela crée des conditions qui, au fil du temps,

compromettront la vie privée – que ce soit du fait d'une entreprise ou des pouvoirs publics, notamment lorsqu'il faudra faire face à la prochaine situation de crise nationale ». (Tomko, 2002)

Consentement/transparence

Certaines technologies biométriques peuvent être utilisées sans le consentement ou la participation active de la personne, et même à son insu.

Les casinos (Curran, 2001) ont déjà recours à la reconnaissance faciale pour détecter la présence de tricheurs et de personnes interdites de jeu. Le Royaume-Uni automatise le processus de reconnaissance des criminels dans certaines rues urbaines, en combinant la vidéosurveillance en circuit fermé à la reconnaissance faciale (Lack, 1999 ; Townsend and Harris, 2003). AC Nielsen, une société d'études de marché, a breveté un système qui identifie par reconnaissance faciale les personnes qui font leurs emplettes, afin de cerner leurs habitudes d'achats.[5] Dans chacun de ces cas, la personne peut ignorer qu'elle est observée à l'aide d'une technologie de reconnaissance faciale.

La reconnaissance de l'iris peut déjà se pratiquer à bonne distance (45 à 70 cm) de la personne. Avec les progrès technologiques, il est très vraisemblable que l'iris pourra être balayé à des distances encore plus grandes et sans que la personne observée ne s'implique d'une quelconque manière.

Sur le plan de la protection de la vie privée, ces situations risquent d'enfreindre les principes de limitation en matière de collecte, de transparence et de spécification des finalités.

Établissement du profil de l'ADN

L'un des plus grands risques liés à l'identification fondée sur l'ADN est sans doute que les informations rassemblées sur l'ADN à des fins d'identification soient utilisées à d'autres fins via un détournement de type *function creep*. Grâce à la recherche sur le génome humain, l'établissement du profil de l'ADN permet de tirer certaines conclusions relatives à la santé du porteur de l'ADN. Si un système d'identité fondé sur l'ADN est créé à grande échelle, il y a fort à parier que de fortes pressions seront exercées par les utilisateurs potentiels de cette information (compagnies d'assurance, institutions financières, chercheurs) pour pouvoir accéder au profil de l'ADN, afin d'effectuer des analyses de risques et des recherches.

Questions de sécurité liées à la biométrie

En matière de sécurité, la vérification revêt trois formes : « quelque chose que nous connaissons » (comme un mot de passe ou un numéro d'identification personnelle – NIP) ; « quelque chose que nous possédons » (comme une carte à puce ou un badge) ; et « quelque chose que nous sommes » (comme une empreinte biométrique).

Alors que les mots de passe et les badges peuvent être utilisés frauduleusement par d'autres, nos attributs biométriques sont difficiles à transférer à une autre personne (sans intervention chirurgicale). A condition d'être employée de façon adéquate et responsable, la biométrie est susceptible de conférer un degré élevé de sécurité à un système donné, en particulier lorsqu'elle est associée à l'une des deux ou aux deux autres formes de vérification. Ces formes « multimodales » d'authentification (mot de passe combiné à un badge, badge combiné à la biométrie, et même la combinaison d'un mot de passe, d'un badge et de la biométrie) sont susceptibles d'accroître considérablement la sécurité et la protection de la vie privée.

La biométrie comporte toutefois plusieurs risques pour la sécurité qui doivent être pris en compte lors de la mise en place de tout système biométrique. Il a été démontré que les systèmes biométriques peuvent être vulnérables à différents types d'attaques.

Certaines attaques nécessitent un accès physique et logique au système biométrique et au capteur,[6] (Soutar, n.d.) un autre type d'attaque se sert d'une impression à haute définition d'une image de l'iris (Thalheim, Krissler and Ziegler, 2002), un autre encore utilise tout simplement un bonbon en gélatine pour faciliter l'usurpation de l'identité d'une autre personne (Matsumoto *et al.*, 2002). Il convient de doter l'architecture des systèmes biométriques de protections spécifiques capables de les protéger contre ces failles de sécurité. Un dispositif permettant de vérifier que l'élément scanné est bien vivant (*liveness checking* également appelé mesure «*antispoof*») employé dans un scanner biométrique et dans le système associé peut élever sensiblement le degré de sécurité.

De par leur nature statique, les technologies biométriques sont aussi vulnérables à une attaque « rejouée » (*replay attack*). La réponse à une question telle que « quelles sont les caractéristiques de votre index droit ? » ou « quel est l'aspect de votre visage ? » est toujours identique. C'est pourquoi les concepteurs ou les exploitants des systèmes biométriques devraient s'assurer que les processus d'extraction biométrique ou de génération d'un gabarit procèdent toujours d'un nombre aléatoire qui transforme l'extraction en un événement unique et sûr. Cette protection empêcherait quiconque de réintroduire subrepticement dans un système biométrique un échantillon ou un gabarit biométrique obtenu précédemment.

Il importe de se rappeler que les technologies fondées sur la biométrie ne représentent que l'une des composantes d'un système global de sécurité ou d'identification. Il faut toujours créer des systèmes de secours et de traitement des exceptions appropriés faisant appel à des technologies complémentaires et supplémentaires, de telle sorte que notre dépendance à l'égard de la biométrie soit correctement dosée par rapport au profil global de menace du système et tienne compte des limites de la technologie. Il est important de s'assurer que les conséquences pour la sécurité de rejets erronés par un système pour des raisons accidentelles (problème de voix, cicatrice sur un doigt, pansement, etc.) ou à cause d'un simple dysfonctionnement du système sont correctement prises en compte. On peut dire qu'une sur-utilisation des technologies biométriques pour des transactions de faible enjeu ou à faible risque devrait faire l'objet d'une conception prudente.

On pourrait être tenté de croire ou espérer que la mise en œuvre de systèmes biométriques permet de réduire les traitements et les procédures manuels et de secours. Or, il n'en est rien : les procédures de secours et les traitements redondants sont encore plus importants dans le contexte d'un système biométrique et devraient être spécifiquement prévues dans la conception du système.

Même pourvues de dispositifs de protection intégrés dans leur architecture, certaines technologies fondées sur la biométrie nécessiteront certainement une supervision humaine ou vidéo de la collecte de l'échantillon biométrique pour se prémunir contre certaines attaques (utilisant par exemple un doigt différent ou le moulage, en plâtre ou en gélatine, d'un doigt sur un scanner digital, ou la présentation d'une image numérique d'un visage ou d'un iris, etc.) ou des tentatives de destruction ou d'altération du scanner biométrique par des utilisateurs.

Il importe également de s'assurer que les données ne puissent être « volées » ou « s'échapper » d'un système biométrique, au niveau du détecteur ou de la base de données. Des échantillons biométriques (images) et des gabarits ou des jeux de données caractéristiques représentant les échantillons pourraient être utilisés pour dérober une identité ou commettre une attaque par usurpation d'identité.

Les systèmes biométriques multimodaux (associant plusieurs techniques biométriques – par exemple la reconnaissance des doigts combinée à celle de l'iris ou la reconnaissance faciale combinée à la géométrie de la main) sont susceptibles d'offrir un degré de sécurité et de fiabilité plus élevé. Ces systèmes peuvent utiliser une seule technologie biométrique par défaut (par exemple la reconnaissance faciale) pour les transactions quotidiennes et deux technologies biométriques pour les transactions spéciales ou ayant une valeur plus élevée, lorsqu'une plus grande fiabilité est exigée. En diminuant le nombre d'interactions biométriques, il est possible de réduire les chances que les données soient «volées» ou «s'échappent» d'un système, tout en améliorant la souplesse et la fiabilité.

Inventaire des technologies biométriques

Introduction

La section suivante décrit le fonctionnement général d'un système biométrique. Elle énumère les principales technologies biométriques et fournit des exemples d'application des systèmes et d'activités de recherche. Les passages relatifs à la fiabilité et à la performance des technologies biométriques s'appuient sur les résultats d'essais de produits biométriques réalisés par le *Communications Electronics Security Group* (CESG) au Royaume-Uni (Mansfield *et al.*, 2001), d'essais comparatifs d'appareils de reconnaissance faciale proposés par divers fournisseurs (*Face Recognition Vendor Test*),[7] du concours de vérification d'empreintes digitales édition 2002 (*Fingerprint Verification Competition*)[8] et sur des informations communiquées par les fournisseurs. Les observations sur la facilité d'emploi et l'acceptation par l'utilisateur s'appuient sur l'expérience acquise par l'auteur avec l'exploitation de systèmes biométriques, sur des entretiens avec d'autres personnes travaillant dans cette industrie et sur l'évaluation de la performance des technologies biométriques menée par Sandia Labs en 1991 (Holmes, Wright and Maxwell, 1991).

Avertissement

Les sources susmentionnées ont été choisies pour leur facilité d'accès et non pas parce que l'auteur les considère particulièrement exactes ou pertinentes à l'égard d'une application ou d'une installation particulières. Les protocoles d'essai employés dans les sources susmentionnées ne sont pas nécessairement applicables à toutes les applications.

Fiabilité

Comme nous l'avons signalé plus haut, les observations concernant la fiabilité ont été synthétisées à partir des documents (accessibles à tous) susmentionnés sur la performance des technologies biométriques. L'auteur a tenté d'estimer en gros une mesure unique de la fiabilité fondée sur des mesures du taux de faux rejets, du taux de fausses acceptations, du point d'équivalence des erreurs et des taux pour d'autres erreurs (échec à l'enrôlement, échec à l'acquisition).

Facilité d'emploi

La facilité d'emploi se réfère à la facilité avec laquelle une personne peut interagir avec un système biométrique pendant qu'elle est identifiée ou authentifiée par ce système. Cette mesure est surtout objective et dépend du type de dispositif utilisé pour capturer l'échantillon biométrique (caméra, scanner, etc.). Les applications en service peuvent avoir à trouver une sorte de compromis entre la facilité d'emploi et la fiabilité. La facilité d'emploi est évaluée d'après les expériences personnelles de l'auteur avec ces technologies, des entretiens avec des collègues et un passage en revue de documents de référence (sources précitées et OACI, 2003b).

Acceptation par l'utilisateur

L'acceptation par l'utilisateur reflète l'ampleur des inquiétudes et des objections que l'utilisation d'une technologie biométrique donnée tend à susciter. Dans certains pays, la reconnaissance faciale est mal acceptée parce que les visages des femmes sont généralement couverts ; dans d'autres pays, la reconnaissance des doigts a des connotations de criminalité. Cette mesure, très subjective, varie d'une personne à l'autre et d'un pays à l'autre, suivant le régime de protection des données en vigueur, le contexte culturel et les attentes personnelles des utilisateurs. L'acceptation est évaluée d'après les expériences personnelles de l'auteur avec ces technologies, des entretiens avec des collègues et un passage en revue des documents de référence susmentionnés. Cette évaluation pourra évoluer dans le temps et donc être différente à l'avenir. De par sa nature propre au contexte et subjective, cette notion d'acceptation par l'utilisateur est susceptible d'intervenir lors de la mise en oeuvre d'une application biométrique en complexifiant les aspects sociaux et politiques. Ce point pourrait motiver la création d'une réglementation dans ce domaine.

Stabilité

La stabilité est définie par la constance d'une caractéristique biométrique au cours du développement normal et du vieillissement d'une personne. En principe, plus une caractéristique est stable, moins il est nécessaire de mettre à jour les données personnelles ou de réenregistrer la personne.

Transparence

La transparence se réfère à la mesure dans laquelle il est nécessaire que la personne concernée sache qu'elle fait l'objet d'une capture biométrique pour que le système de capture fonctionne. Certaines technologies biométriques (reconnaissance faciale, certaines formes de reconnaissance de l'iris, reconnaissance de la démarche, etc.) autorisent la capture à l'insu ou sans le consentement de la personne concernée. La transparence donne une indication de la capacité d'une technologie donnée d'opérer à l'insu des personnes. Certains projets, tels que le projet d'identification à distance des personnes conduit par DARPA, font volontairement appel à des technologies biométriques capables de fonctionner à l'insu des personnes.[9]

Fonctionnement d'un système biométrique

Le flux d'informations dans un système biométrique peut être résumé par les étapes suivantes :

- Prélèvement d'un échantillon biométrique.
- Extraction des données biométriques.
- Création d'un gabarit biométrique ou d'un ensemble de données caractéristiques décrivant les échantillons.
- Comparaison avec un gabarit biométrique ou un ensemble de données caractéristiques.

Le processus d'extraction des caractéristiques et de création d'un gabarit ou d'un ensemble de données caractéristiques est irréversible. Il est impossible de recréer un échantillon biométrique brut (tel que l'image d'un visage, d'un iris, d'une rétine ou d'un doigt) à partir d'un gabarit ou d'un ensemble de données caractéristiques. Jusqu'à présent, la plupart des systèmes biométriques ne peuvent interopérer qu'en utilisant l'échantillon biométrique brut. Lorsque l'échantillon biométrique est détruit après la capture (peut-être pour accroître le niveau de protection de la vie privée d'un système donné), l'interopérabilité reste donc limitée. A l'avenir, la normalisation des gabarits biométriques pourrait permettre aux systèmes d'interopérer avec ces gabarits, comme ils peuvent le faire actuellement avec les échantillons biométriques bruts. Bien qu'il faille toujours encourager la normalisation, il faut être conscient que tant que

l'interopérabilité **et** la protection de la vie privée ne sont pas garantis, il y a lieu de faire un compromis direct entre l'interopérabilité et la protection de la vie privée conférée *de facto* par la non interopérabilité (ce compromis s'appliquera de la même manière à la rétention d'échantillons biométriques bruts et de gabarits biométriques). *Note : en fait, ce peut être l'intention du concepteur du système qui, en vertu du « principe de la spécification des finalités », prévient toute interface avec d'autres systèmes.*

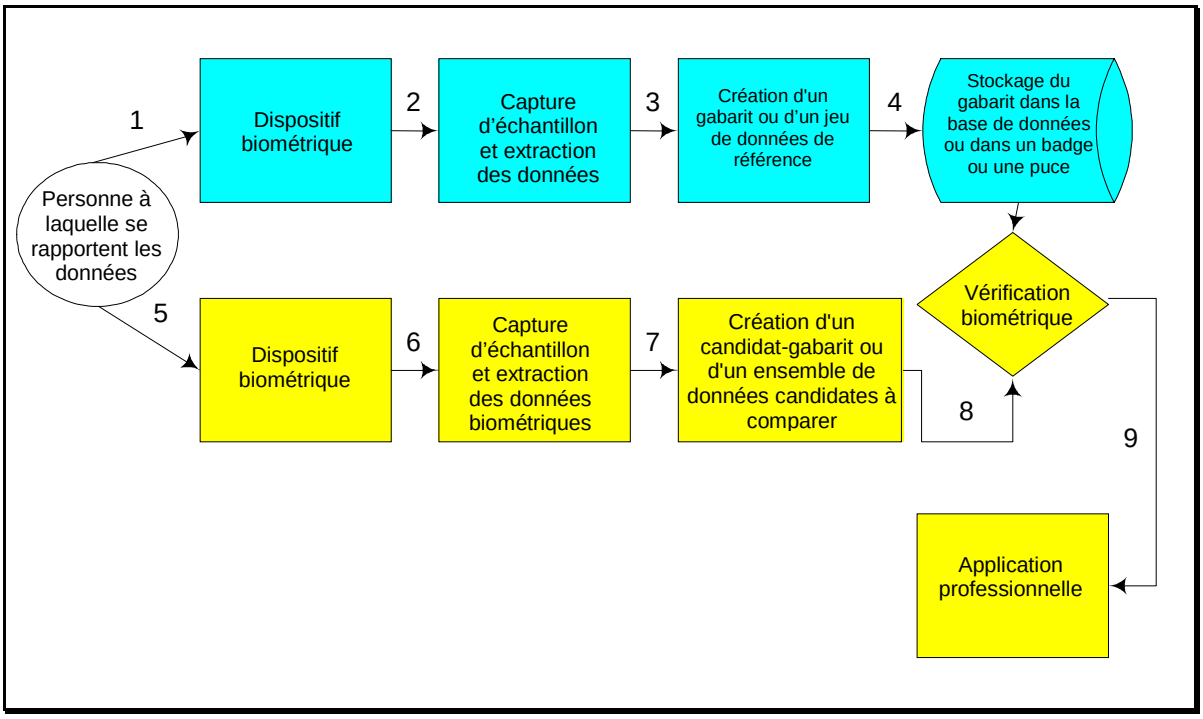
Les systèmes biométriques effectuent deux types de comparaison :

- Un à plusieurs (1 : N, comparaison aussi dénommée « recherche, identification ou reconnaissance biométrique ») : les recherches «un à plusieurs » visent à établir l'identité sur la seule base d'informations biométriques. La comparaison « un à plusieurs » répond à la question : « Qui suis-je? ». Les systèmes capables d'effectuer ce type de comparaison doivent inclure une base de données centrale renfermant tous les gabarits biométriques enregistrés par le système. Cette base de données est utilisée pour effectuer les recherches « un à plusieurs ».

- Un à un (1 : 1, comparaison aussi dénommée « vérification, appariement ou authentification biométriques ») : la confirmation de la validité d'une identité déclarée par la comparaison entre un gabarit de vérification et un gabarit d'enrôlement. La vérification implique une déclaration d'identité. La comparaison «un à un» répond à la question : « Suis-je effectivement la personne que je déclare être ? ». Aucune base de données centrale n'est **nécessaire** dans les systèmes pratiquant une vérification, si la comparaison s'effectue sur un gabarit stocké dans un dispositif en possession de la personne dont l'identité est vérifiée.

La figure 1 décrit les éléments fondamentaux d'un système biométrique.

Figure 1. Conception d'un système biométrique



Note : Le processus d'enrôlement biométrique est illustré en gris foncé et le processus de vérification ou de recherche biométrique en gris clair.

Processus d'enrôlement

Durant l'enrôlement, la personne utilise un dispositif biométrique *(1)* (par exemple un lecteur d'empreintes digitales) pour fournir un échantillon biométrique *(2)*. Le système biométrique extrait les informations décrivant les caractéristiques de l'échantillon biométrique. Passé ce stade, l'échantillon biométrique original (par exemple une image du doigt) peut être éliminé de façon à respecter la vie privée (comme nous l'avons évoqué plus haut, cette élimination limitera l'interopérabilité du système biométrique). L'information sur les caractéristiques biométriques est ensuite convertie *(3)* au format « gabarit » ou « jeu de données ». Ce gabarit ou ce jeu de données sur les caractéristiques est ensuite stocké *(4)* dans une base de données biométriques centralisée ou, dans un système distribué, sur un dispositif en possession de l'utilisateur (carte à puce ou à bande magnétique).

Processus de vérification ou de recherche

Lors de la recherche ou de la vérification, la personne *(5)* utilise un dispositif biométrique pour fournir un échantillon biométrique *(6)*. Le système biométrique extrait les informations décrivant les caractéristiques de l'échantillon biométrique. Passé ce stade, l'échantillon biométrique original peut aussi être éliminé d'une façon protégeant la vie privée. Les caractéristiques biométriques sont ensuite converties au format « gabarit » ou « jeu de données » *(7)* ; ce gabarit ou cet ensemble de données serviront à effectuer la recherche ou la vérification. Le gabarit ou le jeu de données est ensuite soumis *(8)* au moteur de vérification biométrique. Dans le cas d'une recherche, le candidat est comparé à tous les échantillons biométriques stockés dans le système, générant de zéro à beaucoup d'appariements possibles. S'agissant d'une vérification, la comparaison 1 à 1 du candidat avec son identité supposée ne peut produire que deux résultats : la confirmation ou l'infirmation. Généralement, une interconnexion *(9)* avec un logiciel applicatif professionnel est utilisée pour traiter le résultat du système biométrique.

Méthode scientifique/essai biométrique

> « Le véritable objectif de la méthode scientifique est de nous permettre de vérifier que la nature ne nous a pas fait croire que nous connaissions quelque chose qu'en fait nous ignorons »
>
> - Robert M. Pirsig, *Zen and the Art of Motorcycle Maintenance.*

Lorsque nous envisageons les nouvelles technologies, il importe particulièrement de s'assurer que les connaissances scientifiques qui sous-tendent chaque technologie résistent à un examen approfondi ***et*** qu'elles étayent ce que nous pensons qu'elles étayent. Il existe un malentendu général entre les gouvernements et le grand public au sujet des capacités et de la fiabilité des technologies biométriques (McMilan, 2002).

Dans un exposé récent, Jim Wayman, directeur du Biometric Test Center de l'Université de l'État de San José (États-Unis), concluait que « le battage fait autour de la biométrie est correct sur le plan factuel, mais risque de donner une impression pas forcément exacte » (Wayman, 2002). L'envolée de la valeur boursière de certaines entreprises spécialisées dans le domaine de la biométrie (le cours de Visionic, par exemple, a triplé depuis le 11 septembre 2001 [*Business Week*, 2002]) tend à confirmer que le public attend une solution biométrique miracle depuis l'attaque du World Trade Center. Exploitant cette veine d'intérêt du public, certains fournisseurs ont même commencé à vanter leurs produits respectifs en les présentant comme une solution au crime et au terrorisme, dès le lendemain de la tragédie du 11 septembre 2001 (AcSys Biometrics, Corp. et Nexus Group International Inc., 2001).

Dans un document sur la reconnaissance faciale, Roger Clarke de l'Australian Privacy Foundation a déclaré : « la technologie et les produits qui l'utilisent, n'ont pas été suffisamment testés par des laboratoires indépendants. La performance des installations actuelles n'a pas fait l'objet d'une évaluation

critique par des experts indépendants et, bien que très peu d'essais aient été pratiqués, leurs résultats ont généralement été occultés » (Clarke, 2003). Roger Clarke nous met en garde sur le fait que « la rareté des informations donne à penser que le fonctionnement des technologies est désastreux » (Clarke, 2003).

Une multitude de paramètres permettent de mesurer la performance d'un système biométrique. Certains paramètres mesurent directement le fonctionnement du système tandis que d'autres sont déduits de ces mesures. Malheureusement, il n'existe pas de paramètre unique établissant la performance d'un système dans toutes les circonstances et dans tous les environnements. Il faut analyser plusieurs paramètres pour déterminer les points forts et les faiblesses de chaque technologie et de chaque fournisseur pour une application donnée. La sélection et l'interprétation des paramètres de mesure particuliers représentent un exercice délicat exigeant un haut niveau de compétence.

Il convient aussi de noter que les caractéristiques propres à chaque application (par exemple la taille de la population, la technologie biométrique choisie, l'environnement, les modalités de l'identification et de l'authentification) influencent sensiblement les résultats de la mesure de la performance. La validité des essais visant à établir la performance d'un système est optimale lorsque les applications sont testées en conditions réelles.

Mesures de la performance de la biométrie

Chaque technologie biométrique recourt à une méthode différente pour attribuer une « note » à la corrélation biométrique (le degré de similitude entre l'échantillon biométrique du candidat et un échantillon biométrique prélevé précédemment) ; la note obtenue par l'échantillon biométrique du candidat doit dépasser une valeur de seuil déterminée pour que ledit échantillon soit déclaré « correspondant ». Comme nous l'avons noté précédemment, cette corrélation est une fonction statistique dépendant du type de technologie biométrique, du matériel et du logiciel, de l'algorithme et des réglages opérationnels du système. Une même corrélation peut être ou ne pas être bonne suivant le contexte.

Taux de faux rejets (*False Reject Rate*)

Le taux de faux rejets indique dans quelle mesure un système biométrique donné ne réussit pas à apparier des échantillons provenant du même utilisateur (rejet d'un utilisateur légitime).

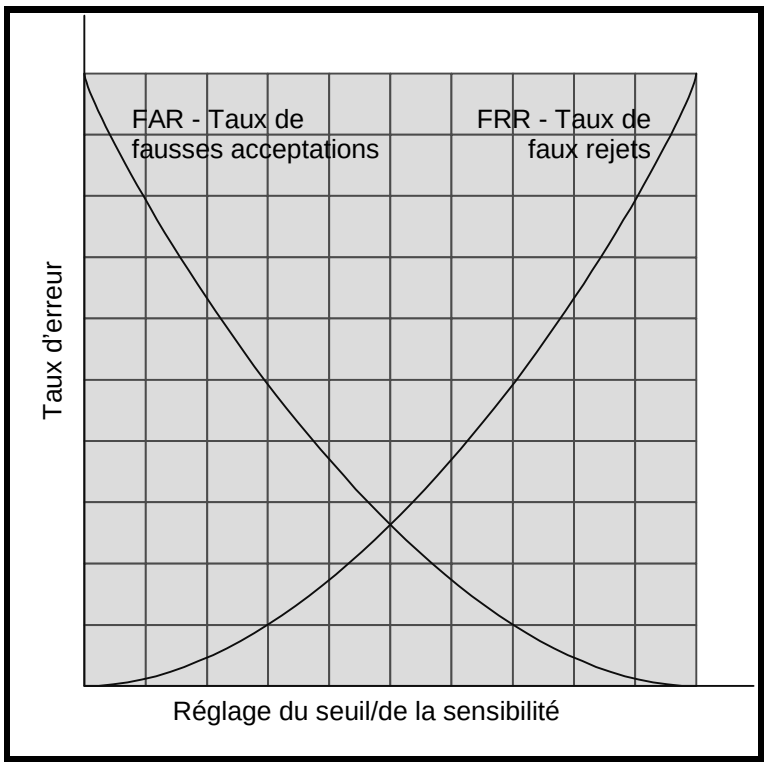
Taux de fausses acceptations (*False Acceptance Rate*)

Le taux de fausses acceptations indique dans quelle mesure un système biométrique donné apparie des échantillons ne provenant pas du même utilisateur (confusion d'un imposteur avec un utilisateur légitime).

Point d'équivalence des erreurs

Le point d'équivalence des erreurs, ou taux d'exactitude croisée, est déterminé par le point d'intersection entre la courbe du taux de fausses acceptations et la courbe du taux de faux rejets. En général, la valeur de l'exactitude croisée augmente parallèlement à l'exactitude inhérente d'une technologie biométrique (taux d'erreur plus faible au point d'intersection). Un exemple de courbes d'erreurs croisées est reproduit à la figure 2.

Figure 2. Courbe du point d'équivalence des erreurs dans un système biométrique

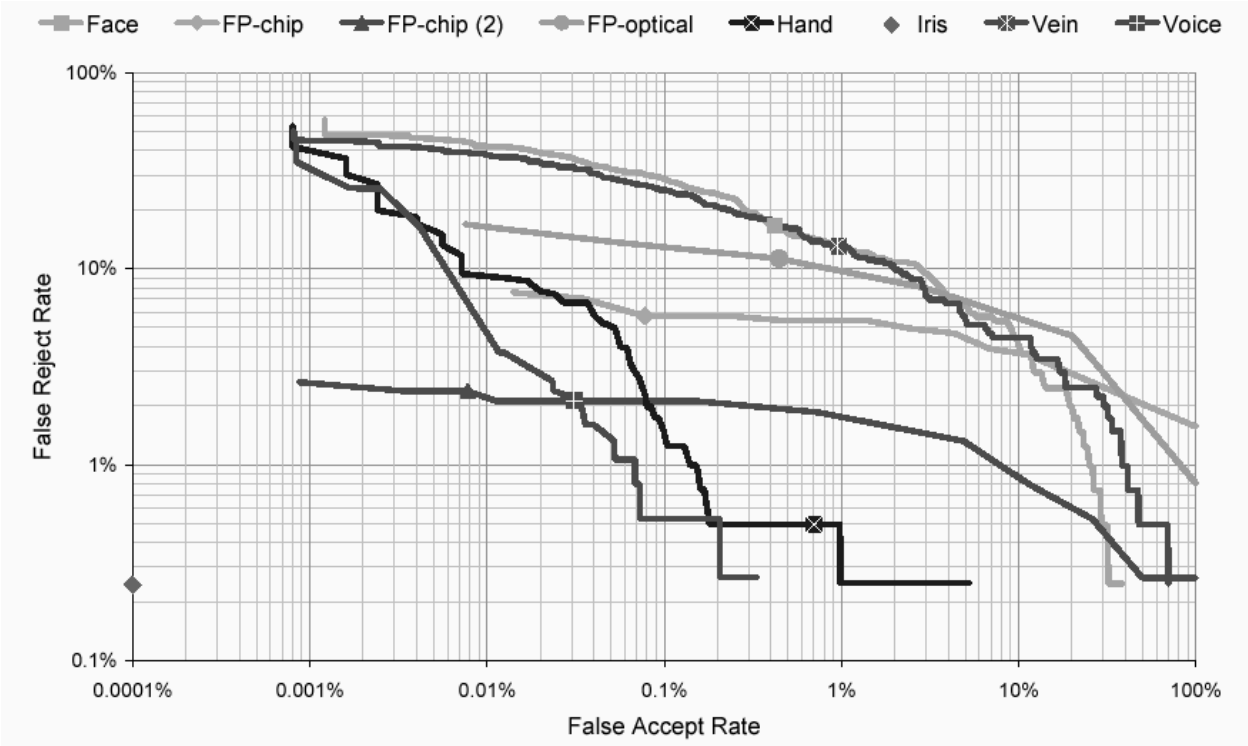


Source: Mansfield, T. *et al.* (2001), "Biometric Product Testing Final Report", CESG report, 19 mars, www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, consulté le 20 avril 2004.

Équilibre des erreurs dans un système biométrique

Comme le montre la figure 3, pour toutes les technologies biométriques (à l'exception de la reconnaissance de l'iris, où les valeurs de l'erreur et de l'exactitude sont préétablies) le réglage des caractéristiques de la performance s'effectue sur une large gamme de valeurs d'erreur. Le concepteur du système et son administrateur peuvent régler la performance en fonction du rôle du système (si le système est destiné à contrôler l'accès ou à empêcher un double enrôlement) et du degré auquel le traitement des exceptions est tolérable (le traitement des fausses acceptations et des faux rejets).

Figure 3. Exemple de courbe d'équilibre des erreurs de plusieurs systèmes biométriques



Légende :
Face : Visage – FP chip : empreinte digitale (puce) – FP-chip (2) : empreinte digitale (puce-2) - FP-Optical : empreinte digitale (optique) – Hand : main - Iris : iris - Vein : veine – Voice : voix.
False Reject Rate : Taux de faux rejets. False Accept Rate : Taux de fausses acceptations.

Note :Ce graphique est extrait de l'évaluation réalisée par le *Communications Electronics Security Group* (CESG) en 2000, sur un nombre limité de participants : il n'est reproduit ici qu'à titre d'exemple ; la performance réelle de chaque technologie biométrique varie suivant le contexte.

Source: Mansfield, T. *et al.* (2001), "Biometric Product Testing Final Report", CESG report, 19 mars, www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, consulté le 20 avril 2004.

Autres mesures de la performance

Échec à l'acquisition

Le taux d'échec à l'acquisition indique la proportion de cas où un système biométrique ne parvient pas à capturer ou à obtenir une image de qualité suffisante. Par exemple, un système incapable de prendre l'image d'un visage sur certains fonds ou de saisir l'empreinte d'un doigt blessé qui porte une cicatrice ou un pansement masquant les caractéristiques du doigt.

Échec à l'enrôlement

Le taux d'échecs à l'enrôlement indique la proportion de personnes pour lesquelles le système est incapable d'extraire suffisamment de caractéristiques et de produire plusieurs gabarits similaires. C'est le cas lorsque le système s'applique à une caractéristique biométrique inexistante (par exemple une capture de l'empreinte digitale pour un utilisateur qui n'a pas de doigts), lorsqu'il est incapable de produire une image

de qualité suffisante lors de l'enrôlement ou de reproduire les caractéristiques biométriques à l'identique. En raison d'une certaine anomalie génétique, les doigts de certaines personnes ne présentent pas suffisamment de détails et de caractéristiques pour l'élaboration d'un gabarit biométrique. Les personnes âgées donnent souvent lieu à des échecs à l'enrôlement, l'élasticité et l'épaisseur de la peau se modifiant avec l'âge.

Débit

Le débit mesure le rythme auquel l'identification et l'authentification biométriques peuvent être effectuées. Ce paramètre comprend deux composantes : la durée de l'acquisition et de l'extraction et la durée de la recherche et de l'appariement. Dans les systèmes biométriques à très grande échelle, qui traitent une immense population, le débit est un facteur risquant de compromettre le bon fonctionnement du système.

Coût du système

Le coût d'un système inclut non seulement le coût du matériel et des logiciels, mais également les frais de fonctionnement et les coûts associés aux erreurs de fonctionnement. Si un système d'identification 1 : N est réglé de façon à réduire au minimum les faux rejets, il est probable que son taux de fausses acceptations augmentera (le système pourrait vous prendre pour quelqu'un d'autre), ce qui nécessitera un suivi manuel. De même, si un système de vérification 1 : 1 est réglé de façon à réduire au minimum les fausses acceptations (quelqu'un se faisant passer pour vous), il est probable que son taux de faux rejets augmentera (rejet d'un utilisateur légitime), rendant ainsi nécessaire une intervention manuelle ou un traitement des exceptions. Le choix du réglage du système se répercutera toujours sur le coût.

Technologies biométriques fondées sur des caractéristiques physiologiques

Les technologies biométriques fondées sur des caractères physiologiques s'appuient sur des données et des mesures directement effectuées sur une partie du corps humain.

Comme nous l'avons évoqué plus haut, la possibilité pour la personne concernée d'exprimer clairement son consentement risque d'être d'autant plus limitée que l'échantillon biométrique peut être prélevé à son insu (par exemple : avec la reconnaissance du doigt, la personne peut exprimer son consentement clairement en plaçant un doigt sur le scanner ; avec la reconnaissance de la rétine, la personne peut donner son consentement en regardant dans le scanner de la rétine, etc.).

Il est important de noter en parcourant l'inventaire des technologies biométriques fondées sur des caractéristiques physiologiques, que, dans toute la mesure du possible, notre préférence va toujours aux processus de collecte d'un échantillon biométrique permettant à l'utilisateur de manifester clairement son consentement.

Reconnaissance de l'empreinte digitale

Fonctionnement

On sait depuis longtemps que, de par leur caractère unique, les sillons de l'empreinte digitale (et d'autres parties du corps) peuvent servir à identifier les personnes. Dans les années 1890, un système de classification destiné à faciliter la recherche d'empreintes digitales dans un stock d'empreintes a vu le jour. Bien qu'elle ait donné lieu à d'abondantes recherches par la suite, la discipline de l'identification par les empreintes digitales remonte à plus d'un siècle.

Ce système est fondé sur la reconnaissance de certains types de traits, dont les principaux sont les arcs, les boucles et les tourbillons. Chaque doigt présente au moins un trait principal. Les traits mineurs (ou minuties), quant à eux, sont formés par la position des extrémités et des bifurcations des sillons. Chaque doigt porte entre 50 et 200 traits mineurs, ce qui fournit un grand nombre de données pour l'extraction des caractères. La dimension des gabarits créés à partir des minuties est généralement comprise entre 250 et 700 octets (voir figure 4).

Figure 4. Traits d'une empreinte digitale

La plupart des instruments biométriques exploitent les minuties d'une façon ou d'une autre. Ceux qui n'utilisent pas les minuties apparient des dessins en extrapolant des données à partir d'une série de sillons particulière. Ensuite, la vérification consiste à localiser un segment de la même zone que celle qui a été sélectionnée lors de l'enrôlement et à le comparer. L'utilisation de plusieurs sillons réduit la dépendance à l'égard des minuties dont les points tendent à s'user au fil du temps. Les gabarits créés pour l'appariement des dessins sont généralement, mais pas toujours, deux à trois fois plus gros que les gabarits tirés des minuties (900 – 1 200 octets).

Fiabilité

Cette technique offre une fiabilité élevée, et peut même être très fiable, si on le souhaite : il suffit d'augmenter le nombre de doigts soumis aux processus d'enrôlement et d'appariement. Elle se prête à un grand nombre d'applications grâce à la souplesse d'ajustement de la performance et de la configuration. Les systèmes sont généralement réglés de façon à tolérer un taux de faux positifs élevé aux dépens du taux de faux négatifs, mais cela dépend des applications. Les fabricants affirment que le taux d'erreur de leurs appareils est faible, mais en présence d'une très vaste population, il faudra probablement recourir à une méthode d'élimination ou faire porter la reconnaissance sur plusieurs doigts pour maintenir une performance acceptable.

Facilité d'emploi

Au signal, l'utilisateur place son doigt sur un petit lecteur à balayage optique ou capacitif. Ce lecteur est monté dans un périphérique, souris, clavier ou carte PCMCIA à usage spécial. L'utilisateur doit généralement maintenir son doigt en place une à deux secondes, durant lesquelles s'opèrent la capture de l'échantillon et l'extraction des données. La facilité d'emploi de la reconnaissance d'empreinte digitale est qualifiée d'élevée.

Acceptation par l'utilisateur

S'il est courant et accepté dans certaines parties du monde, la reconnaissance d'empreinte digitale continue à être perçu de façon quelque peu négative, à cause de son association avec l'étude des empreintes digitales en criminologie. L'acceptation par l'utilisateur est qualifiée de moyenne à faible.

Stabilité

Les sillons et le dessin de notre empreinte digitale sont stables au cours du temps. Ils peuvent cependant être abîmés par une forte usure ou des blessures et il arrive que les empreintes digitales des personnes âgées soient difficiles à différencier (les traits sont difficiles à extraire à cause de la finesse de la peau). Malgré ces problèmes, la stabilité est qualifiée d'élevée.

Exemples d'applications existantes

Gouvernements/immigration

- L'Union européenne (UE) a récemment mis en ligne son système Eurodac, cette grande base de données centralisée sur les empreintes digitales permettra à tous les États membres de comparer les empreintes digitales des demandeurs d'asile à celles déjà enregistrées par les autres pays de l'UE. S'il s'avère qu'une personne a déjà présenté une demande d'asile dans un autre pays de l'Union, elle devra représenter sa demande dans ce même pays (EC, 2003).[10]

- Nombre d'États relèvent les empreintes digitales des nouveaux demandeurs de prestations sociales ou de personnes sollicitant l'aide d'autres programmes. Ceci protège contre une fraude consistant à toucher plusieurs fois l'aide sociale en s'inscrivant sous plusieurs noms différents. 900 000 personnes ont été enrôlées dans un tel système par l'État de New York.

Enseignement

- En Pennsylvanie la cantine d'une école pratique la reconnaissance d'empreinte digitale (*eSchool News*, 2001).

- De même que la bibliothèque d'une école au Minnesota (*eSchool News*, 2000).

Authentification en ligne/sur un réseau

- Des scanners conçus pour les doigts commencent à être incorporés dans des composants d'ordinateurs personnels pour authentifier les utilisateurs. Hewlett-Packard a introduit récemment un Assistant numérique personnel muni d'un capteur biométrique pour la reconnaissance d'empreinte digitale qui permet de restreindre l'accès aux seuls utilisateurs autorisés (Hamilton, 2003).

- D'autres fabricants, comme Acer Inc., le géant asiatique de l'informatique, et International Business Machines Corp. (IBM) ont incorporé des unités de reconnaissance d'empreintes digitales dans leurs ordinateurs portables.

- Targus Inc., premier fabricant d'accessoires pour ordinateurs, vend actuellement un lecteur d'empreintes digitales sur carte PC, le «DEFCON Authenticator» – destiné aux ordinateurs portables et un lecteur monté dans une sorte de petit périphérique appelé « pod » qui peut se connecter à tout ordinateur via un port USB.

Géométrie de la main

Fonctionnement

La géométrie de la main est à l'heure actuelle l'une des technologies biométriques les plus utilisées et les plus adaptées au contrôle de l'accès, du temps et de la présence. Contrairement à des technologies biométriques plus spéciales et moins courantes, des dispositifs utilisant la reconnaissance de la main équipent efficacement des milliers de lieux de travail, d'universités, d'immeubles d'habitation et d'aéroports – tous les endroits exigeant un moyen d'authentification raisonnablement exact et non intrusif. La nature de cette technologie est telle que la plupart des projets sont appliqués à une échelle relativement petite et ne comprennent que quelques lecteurs, mais certains projets en comptent néanmoins des dizaines.

Cette technologie utilise une image tridimensionnelle de la main et mesure la forme, la largeur et la longueur des doigts et des articulations. L'utilisateur pose la main désignée sur le lecteur, en plaçant ses doigts sur des marques. La caméra prend une image de la face supérieure de la main, qui fournit des informations sur la longueur et la largeur, ainsi qu'une image latérale qui donne un profil d'épaisseur (voir figure 5). Le gabarit ainsi produit n'excède pas la dizaine d'octets.

Figure 5. Scanner de la géométrie de la main

Source: Wilson, Bill (1992). "Hand Geometry Boasts Simplicity, Convenience", *Access Control*, mars, reprint, p. 1.

Fiabilité

Cette technologie peut offrir une fiabilité élevée, si on le souhaite. Elle se prête à un grand nombre d'applications grâce à la souplesse d'ajustement de la performance et de la configuration. La géométrie de la main convient mieux aux vérifications 1 :1.

Facilité d'emploi

L'utilisateur pose sa main, paume vers le bas, sur un scanner métallique (illustré ci-dessus) en plaçant ses doigts entre des marques en relief. Ces marques assurent une position correcte de la main. La facilité d'utilisation de la géométrie de la main est qualifiée d'élevée.

Acceptation par l'utilisateur

L'acceptation par l'utilisateur de la géométrie de la main est qualifiée de moyenne à élevée.

Stabilité

La stabilité de cette technologie est qualifiée de moyenne à élevée. La forme et les caractéristiques de la main évoluent lentement au cours de la vie.

Exemples d'applications existantes

Gouvernement/immigration

- L'application la plus connue par un organisme public est sans doute celle du Système de traitement accéléré des passagers par le service d'immigration et de naturalisation des États-Unis (INSPASS). Jusqu'à sa suspension récente,[11] l'INSPASS permettait aux voyageurs effectuant des trajets fréquents d'éviter les longues files d'attente devant les guichets de l'immigration, dans les aéroports internationaux de Los Angeles, Miami, Newark (New Jersey), New York City, Washington, San Francisco, Toronto et Vancouver. Après s'être fait enregistrer par le service, les passagers autorisés recevaient une carte à bande magnétique sur laquelle étaient encodées les informations tirées du balayage de leur main. Au lieu de devoir se présenter au personnel de contrôle des passeports, les voyageurs bénéficiant d'INSPASS glissaient leur carte, posaient leur main et passaient directement au portail des douanes. INSPASS traitait plus de 60 000 personnes.
- Le gouvernement mexicain applique un dispositif de contrôle de la présence au Ministère de la réforme foncière utilisant la géométrie de la main. Ce système couvre six sites séparés et est relié au système de registre du personnel.

Enseignement

- L'Université de Géorgie a choisi cette technologie pour contrôler l'accès à la cafétéria des étudiants. Lorsqu'ils se rendent à la cafétéria, les étudiants doivent d'abord glisser leur carte d'identité dans un lecteur et faire vérifier leurs mains avant de pouvoir entrer au restaurant (Zunkel, 1994).
- Une école primaire américaine identifie les personnes venant chercher les enfants grâce à cette technologie. Toutes les personnes autorisées par les parents peuvent participer au système. Quiconque vient chercher un enfant à l'école doit d'abord poser sa main sur un lecteur qui en relève la géométrie (IR Recognition Systems, 1998).
- A Toronto, au Canada, un club de tennis et de remise en forme[12] vérifie l'identité de ses 12 000 membres à l'aide de la géométrie de la main.

Secteur privé

- Dans l'Ontario, au Canada, les centrales nucléaires sont équipées de cette technologie (Milroy, 1998).
- Aux États-Unis, des scanners de la géométrie de la main vérifient l'identité aux entrées principales de plus de la moitié des centrales nucléaires (findBIOMETRICS.com, n.d.).

Autres

- Aux jeux olympiques d'Atlanta (été 1996), la géométrie de la main a permis d'identifier et d'assurer la sécurité de quelque 150 000 athlètes, accompagnateurs et autres participants (Tomko, 1996). Intégré au système de sécurité du Village olympique, ce dispositif a couvert des millions de transactions en un temps minimum (findBIOMETRICS.com, n.d.).

- Le Bureau fédéral des prisons des États-Unis utilise la géométrie de la main pour suivre les mouvements des détenus, du personnel et des visiteurs à l'intérieur des prisons. Toutes les personnes qui pénètrent dans l'enceinte doivent faire balayer leur main. L'information est introduite dans une base de données et la personne reçoit une carte à bande magnétique qu'elle portera sur elle en permanence. Les détenus ne peuvent accéder à des endroits tels que la cafétéria, l'hôpital et les salles de loisirs sans leur carte (Chua, 2001).

Reconnaissance faciale

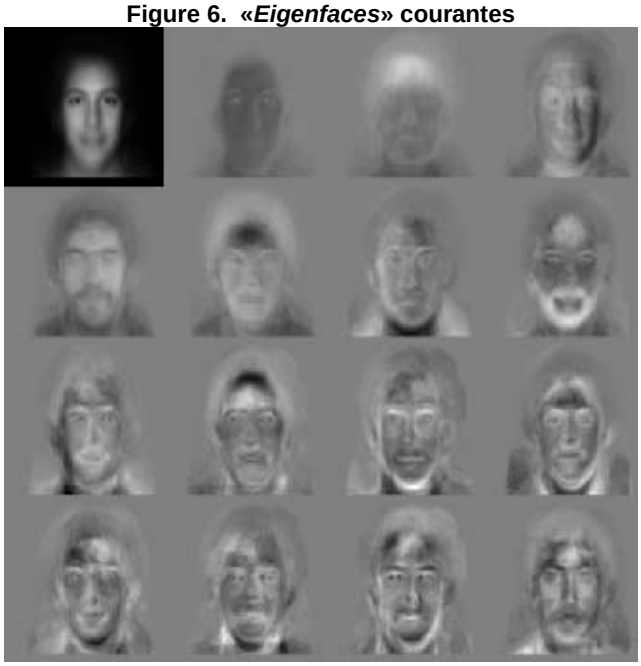
Fonctionnement

L'enregistrement dure généralement 20 à 30 secondes durant lesquelles l'appareil prend plusieurs images du visage. Idéalement, ce dernier sera pris sous différents angles et avec différentes expressions pour accroître la précision de l'appariement. Après l'enregistrement, le système extrait les caractéristiques distinctives (ou produit des images globales de référence), afin de créer un gabarit. Ce dernier est beaucoup moins lourd que l'image dont il provient, les portraits totalisent 20 à 40 kilo-octets, tandis que les gabarits exigent entre 100 et 3 500 octets. Les modèles plus petits sont normalement destinés aux comparaisons 1 : N (1 à beaucoup).

Suivant son fournisseur, l'instrument exploite l'une des quatre méthodes principales d'identification et de vérification des personnes, à savoir les *eigenfaces*, l'analyse des caractéristiques, le réseau neuronal et le traitement automatique du visage.

Eigenface: que l'on peut traduire par «notre propre visage» est une technologie brevetée par le Massachusetts Institute of Technology (*MIT*, 2002), qui utilise des images bidimensionnelles globales reproduisant les caractères distinctifs d'un portrait dans une échelle de gris. Les autres méthodes de reconnaissance faciale reposent souvent sur des variantes de l'*eigenface* (voir figure 6).

Figure 6. «*Eigenfaces*» courantes



Source: MIT (2002), "Photobook/Eigenfaces Demo", http://vismod.media.mit.edu/vismod/demos/facerec/basic.html, consulté le 20 avril 2004.

L'*analyse des caractéristiques* représente peut-être la technologie de reconnaissance faciale la plus répandue. Cette technologie, apparentée à l' *eigenface*, supporte mieux les modifications de l'apparence du visage (passage du sourire à la moue, par exemple). Identix, l'une des principales entreprises de reconnaissance faciale, utilise l'analyse locale des traits.[13] Il s'agit d'une technique mathématique mise au point par les cofondateurs de Visionics Corporation, qui repose sur la constatation que tous les portraits (en l'occurrence, toujours des schémas complexes) peuvent être synthétisés à partir d'un « ensemble irréductible de blocs de construction », en quelque sorte, des blocs de construction du visage comparables à des atomes. L'analyse locale des traits exploite des dizaines de traits de différentes régions du visage et tient compte de la localisation relative de ces traits. L'identification et la vérification se fondent sur les types et l'agencement des blocs de construction qui représentent les traits extraits.

L'analyse locale des traits résiste aux variations de luminosité, de teint de la peau, de port de lunettes, d'expression et de coiffure, ainsi qu'aux variations d'inclinaison (jusqu'à 35 degrés dans toutes les directions).[14]

Réseau neuronal : Cette technologie compare les traits des deux visages (le visage enrôlé et le visage à vérifier) afin d'établir s'ils coïncident ou non. Le réseau neuronal détermine la similitude des traits globaux uniques des visages enrôlés et du visage à vérifier à l'aide d'un algorithme, en exploitant au mieux le portrait. Lors d'un appariement incorrect, l'algorithme modifie la pondération attribuée à certaines caractéristiques du visage. En théorie, cette méthode accroît la capacité d'identifier des visages dans des conditions difficiles.

Traitement automatique du visage : Il s'agit d'une technologie plus rudimentaire utilisant des distances et des rapports de distances entre des caractéristiques faciles à saisir, tels que les yeux, la pointe du nez et les commissures des lèvres. Si, dans l'ensemble, il n'est pas aussi résistant que *l'eigenface*, l'analyse des caractéristiques ou le réseau neuronal, le traitement automatique du visage peut s'avérer plus efficace dans des situations où le visage est pris de face sous une faible lumière.

Fiabilité

Cette technologie est susceptible d'offrir un degré de fiabilité élevé si on le souhaite, mais en réalité, la performance du système est plus souvent mesurée d'après par le nombre de faux positifs ou doubles appariements qu'une application donnée peut tolérer. Les essais effectués sur des systèmes de reconnaissance faciale montrent que ces derniers peuvent difficilement avoir une bonne performance avec des taux d'erreur acceptables.

Facilité d'emploi

L'utilisateur se place face à la caméra, celle-ci étant installée de préférence près du visage. Dans certaines situations, l'utilisateur devra modifier légèrement l'aspect de son visage pour autoriser une acquisition biométrique correcte. La facilité d'emploi de la reconnaissance faciale est qualifiée de moyenne à élevée.

Acceptation par l'utilisateur

L'acceptation par l'utilisateur de cette technologie est qualifiée d'élevée, étant donné le caractère non invasif de la capture biométrique.

Stabilité

La stabilité de la reconnaissance faciale est qualifiée de moyenne à faible. Certains systèmes de reconnaissance faciale sont plus aptes que d'autres à résister aux modifications du visage qui s'opèrent tout au long de la vie.

Exemples d'applications existantes

Gouvernement/immigration

- Selon un article paru récemment dans la presse britannique : « …des caméras de surveillance seront capables de zoomer sur les visages des conducteurs entrant dans la zone située à la périphérie de Londres où la circulation se trouve ralentie à cause des embouteillages, et ce dans le cadre d'une opération complexe, surnommée « anneau d'acier », autour de la capitale ». L'article indique que le nouveau système de reconnaissance faciale vise à protéger la ville d'une attaque terroriste : les visages filmés par des centaines de caméras sont comparés à des portraits de différents suspects stockés dans les bases de données de la police et des services secrets. Les experts britanniques en défense affirment que le nouveau système « …pourrait intercepter un camion ou une voiture piégés, censés figurer en première ligne des desseins d'Al Quaida en Grande-Bretagne » (Townsend and Harris, 2003).

- Le Ministère japonais du territoire, des infrastructures et des transports conduit un essai consistant à associer des puces à circuit intégré sans contact à la reconnaissance faciale ***et*** à la reconnaissance de l'iris, en vue de réduire le temps d'attente aux guichets d'enregistrement dans les aéroports japonais (Miyake, 2002).

- SmartGate, un système de reconnaissance faciale qui vérifie les photos d'identité des passeports est appliqué à titre expérimental par le Service des douanes australiennes depuis l'été 2002 (Australian Justice and Customs, 2002).

- Depuis les événements du 11 septembre, l'application de la reconnaissance faciale à l'identification des terroristes et d'autres criminels soulève un intérêt considérable.[15]

Secteur bancaire

- Aux États-Unis, certaines banques et stations services et certains commerces de proximité font appel à cette technologie pour identifier et enregistrer les transactions effectuées par chèque (*Biometric Technology Today*, 1998). Un système américain de distributeurs automatiques de billets prend une image biométrique chaque fois qu'un client encaisse un chèque. Le client doit au préalable être enregistré par le système, mais il n'a pas besoin de posséder un compte bancaire ni un permis de conduire. Pour encaisser un chèque, les clients encodent leur numéro de sécurité sociale. Cette information, combinée à l'empreinte biométrique enregistre en temps réel et de façon permanente la transaction (*Biometric Digest*, 1998).

- Les banques allemandes utilisent la reconnaissance faciale pour offrir à leurs clients un service de retrait de coffres-forts accessible 24 heures sur 24 et fonctionnant sans personnel. Les clients demandent leur coffre à un guichet automatique équipé d'une caméra vidéo. La caméra saisit et traite le portrait du client. Le logiciel du système vérifie l'identité de la personne et s'assure qu'elle est habilitée à retirer le coffre. Si la personne y est autorisée, le coffre est extrait par des robots et remis à son propriétaire grâce à un système de délivrance automatique (Burnell, 1997).

Voyages et loisirs

- Une entreprise malaisienne met à profit cette technologie pour créer un système de sécurité destiné aux aéroports qui suit les bagages des passagers en les associant à une image de leur visage. Ce système n'autorise le chargement des bagages dans l'avion qu'au moment où leurs propriétaires embarquent (Belsize, 1997).

- Certains casinos identifient des joueurs suspects à l'aide de la reconnaissance faciale. Une caméra de surveillance prend une image du visage de l'individu et la compare à une base de données de photos numérisées de tricheurs connus.

Authentification en ligne/sur un réseau

- Certaines applications remplacent les mots de passe ouvrant l'accès à un ordinateur. Leur principal avantage est que la reconnaissance faciale permet d'opérer les mains libres. La caméra étant fixée à l'écran de l'ordinateur, il suffit que l'utilisateur regarde l'écran pour que son identité soit vérifiée. Il est possible de couper l'accès à des informations sensibles dès que l'utilisateur quitte le champ de vision de la caméra.

Autres

- En janvier 2000, la police de Tampa, en Floride, a mené l'un des plus grands essais de reconnaissance faciale lors du championnat de football «SuperBowl XXXV» à Tampa Bay (Bonsor, n.d.).

Reconnaissance de l'iris

Fonctionnement

La reconnaissance de l'iris met à profit les caractéristiques uniques de l'iris humain pour vérifier l'identité d'une personne. L'iris est la portion pigmentée (généralement dans les tons bruns ou bleus) de l'œil qui encercle la pupille.

Chaque iris présente une trame complexe et à ce point unique que, chez une même personne, la trame de l'iris droit est complètement différente de celle de l'iris gauche. Le système a été qualifié d'infaillible (Golgotha, 1999), la reproduction artificielle de l'iris étant pratiquement impossible en raison de ses propriétés et du nombre de caractéristiques mesurables. L'iris est stable tout au long de la vie et n'est généralement pas atteint par l'usure, ni par des blessures (l'utilisateur ayant tout intérêt à le protéger). Les lentilles de contact ordinaires n'interfèrent pas avec le fonctionnement de l'appareil et les entreprises spécialisées prétendent (RYCOM Inc., n.d.) que les lentilles de couleur n’interfèrent pas non plus bien qu’il y ait peu de recherches indépendantes sur ce sujet. La technologie de la reconnaissance de l’iris implique l’utilisation d’une caméra à haute résolution et d’une source de lumière pour prendre une image numérique de l'iris. L'iris étant normalement visible à environ 85 %, (le reste est recouvert par les paupières), aucune opération intrusive n'est nécessaire. Ce type de technologie biométrique se prête aussi bien aux vérifications 1 : 1 qu'à la reconnaissance 1 : N (Roethenbaugh, 1998b).

Le gabarit généré par la reconnaissance de l'iris exige environ 500 octets de mémoire.

Fiabilité

Contrairement à d'autres technologies biométriques, la reconnaissance de l'iris accuse un taux d'erreur extrêmement faible sur toute la gamme de configurations du système. Sa fiabilité est qualifiée de très élevée.

Facilité d'emploi

L'utilisateur se place à proximité du dispositif d'acquisition (caméra périphérique ou montée sur un mur) et centre son œil sur le dispositif de façon à ce que le reflet de l'œil soit visible. L'utilisateur se place à une distance variant entre 10 et 70 cm, suivant le type de caméra. La capture et l'extraction des caractéristiques sont quasi immédiates. La reconnaissance de l'iris finira par devenir très facile à utiliser, mais pour l'heure il figure encore parmi les technologies biométriques les plus complexes. Sa facilité d'emploi est qualifiée de moyenne à faible.

Acceptation par l'utilisateur

L'acceptation de cette technologie par l'utilisateur est qualifiée de moyenne à élevée, compte tenu de son caractère non intrusif. A mesure que les progrès technologiques autoriseront de plus grandes distances, la reconnaissance de l'iris sera sans doute encore mieux acceptée.

Stabilité

Les iris sont très stables tout au long de la vie. La stabilité de cette technologie est qualifiée d'élevée.

Exemples d'applications existantes

Gouvernement

- CANPASS (Système canadien des services voyageurs) – Air : Cette initiative prise conjointement par l'Agence des douanes et du revenu du Canada (ADRC) et par Citoyenneté et Immigration Canada facilitera et sécurisera l'entrée au Canada des voyageurs aériens préalablement approuvés et ne présentant pas de risque particulier. Ce programme d'enregistrement facultatif fait appel à la reconnaissance de l'iris pour confirmer l'identité des passagers.[16]

Secteur bancaire

- Certains fabricants de distributeurs automatiques de billets remplacent les mots de passe ou les numéros d'identification personnels par la reconnaissance de l'iris. En mai 1999, la Bank United of Texas est devenue la première banque des États-Unis à appliquer la reconnaissance de l'iris aux guichets automatiques.

- Cette technologie est déjà adoptée par plus d'une dizaine de banques à l'extérieur des Etats-Unis (*Mercury News*, 1999).

- A Toronto, la Banque Royale du Canada et la Banque Canadienne Impériale de Commerce ont mis à l'essai un distributeur automatique de billets équipé de dispositif de reconnaissance de l'iris (Bonier, n.d.).

Enseignement

- Aux États-Unis, une chaîne de taekwondo utilise la reconnaissance de l'iris pour accélérer les procédures quotidiennes d'inscription sur le registre à l'entrée et de traitement de l'information. Avant d'entrer dans une classe, les étudiants doivent toujours fixer la caméra durant une seconde afin que leur identité soit vérifiée (Iridian Technologies, Inc. n.d.).

Voyages

- L'aéroport d'Amsterdam-Schiphol déclare obtenir de bons résultats avec un système de sécurité biométrique qui combine la reconnaissance de l'iris à une carte spéciale, permettant ainsi aux passagers d'éviter le contrôle traditionnel des passeports (CNN, 2000). Les passagers qui prennent fréquemment l'avion peuvent s'inscrire au « Privium Club », qui utilise un logiciel et du matériel mis au point par Schiphol, les autorités aéroportuaires et le service de l'immigration (Chua, 2001). Les données décrivant l'iris des membres sont encodées sur la puce d'une carte d'identification. Le passager peut franchir très rapidement le contrôle des passeports et l'enregistrement en regardant dans un scanner. Ce système est également utilisé pour le personnel de l'aéroport dans les zones sûres.

- Un système biométrique de reconnaissance de l'iris, conçu par EDS, est à l'essai à l'aéroport israélien Ben Gourion (Delaney and Prada, 2002).

- Le Ministère japonais du territoire, de l'infrastructure et des transports conduit un essai en associant des puces (à circuit intégré) sans contact à la reconnaissance faciale *et* à la reconnaissance de l'iris, en vue de réduire le temps d'attente à l'enregistrement dans les aéroports japonais (Miyake, 2002).

Reconnaissance de la rétine

Fonctionnement

La reconnaissance de la rétine permet d'observer les ramifications vasculaires qui tapissent le fond de l'œil (surface interne antérieure). Comme il n'existe pas deux rétines identiques (même chez de vrais jumeaux), ces ramifications vasculaires permettent d'identifier une personne.

Les capteurs de fond rétinien balayant la rétine envoient un faisceau lumineux dans le globe oculaire et enregistrent la disposition des veines dans l'œil. Eu égard au caractère intrusif du prélèvement d'un échantillon biométrique et à la nécessité de la participation active et consentante de l'utilisateur, certaines personnes considèrent que la reconnaissance de la rétine respecte mieux la vie privée que la reconnaissance de l'iris (Pigg, 2002).

Les gabarits issus de la reconnaissance de la rétine comptent une centaine d'octets.

Fiabilité

La fiabilité est qualifiée de très élevée.

Facilité d'emploi

L'utilisateur dirige son regard vers une petite ouverture aménagée dans un dispositif installé sur une table ou sur un mur. Il doit garder la tête parfaitement immobile pendant qu'il fixe une lumière verte émise

par le dispositif. La capture et l'extraction prennent généralement 6 à 10 secondes. La reconnaissance de la rétine est également l'une des technologies biométriques les plus complexes. Sa facilité d'emploi est qualifiée de faible.

Acceptation par l'utilisateur

L'acceptation de la reconnaissance de la rétine par l'utilisateur est qualifiée de faible. Certains utilisateurs se demandent si le balayage de l'intérieur de l'œil par un faisceau lumineux ne risque pas d'avoir des répercussions sur leur santé. D'après le rapport des laboratoires Sandia, la reconnaissance de la rétine suscite la réaction la plus négative de toutes les technologies biométriques. L' « identification de la rétine, qui implique le passage d'un rayon infrarouge à travers la pupille, soulève des inquiétudes chez les utilisateurs… » (Holmes, Wright and Maxwell, 1991).

Stabilité

La rétine est très stable tout au long de la vie. La stabilité de cette technologie biométrique est qualifiée d'élevée.

Exemples d'applications existantes

Autres

- Compte tenu de son coût élevé et du fait qu'il est perçu comme intrusif, la reconnaissance de la rétine est peu utilisé en dehors de certaines applications spécialisées exigeant une haute sécurité et d'applications concernant la sûreté nationale.

Géométrie des doigts

Fonctionnement

Cette technologie obéit aux mêmes principes que la géométrie de la main, mais n'utilise qu'un ou deux doigts. On mesure les caractéristiques uniques des doigts, telles que leur largeur, leur longueur, leur épaisseur et la taille des articulations.

Les systèmes appliquant la géométrie des doigts peuvent servir à la vérification 1 : 1 ou à l'identification 1 : N. Le principal avantage de ces systèmes réside dans leur rapidité et leur capacité de traiter un « haut débit d'utilisateurs » (Roethenbaugh, 1998b). Un fabricant déclare que son système confirme l'identité en une seconde (Biome Partners, Inc., 1999). Les systèmes fondés sur la géométrie des doigts sont considérés comme très durables et capables de bien s'adapter aux conditions extérieures (Roethenbaugh, 1999). Par exemple, Disney World, aux Etats-Unis, utilise la géométrie tridimensionnelle de deux doigts pour vérifier l'identité des détenteurs de laissez-passer d'une saison (James, 1997).

Fiabilité

La fiabilité est qualifiée de moyenne. Ne convient pas aux applications 1 : N.

Facilité d'emploi

A l'instar de la géométrie de la main, cette technologie requiert un scanner spécialement conçu pour la main sur lequel l'utilisateur pose son doigt ou comportant un trou dans lequel l'utilisateur glisse son doigt. La facilité d'emploi de cette technologie est qualifiée d'élevée.

Acceptation par l'utilisateur

L'acceptation de cette technologie par l'utilisateur est qualifiée de moyenne à élevée, en raison du caractère non intrusif de la capture biométrique. Certains systèmes avec lesquels l'utilisateur doit enfoncer complètement son doigt dans un trou peuvent soulever plus de résistances chez les utilisateurs.

Stabilité

La stabilité de la géométrie du doigt est qualifiée de moyenne à élevée. La forme et la géométrie des doigts peuvent se modifier lentement au cours de la vie.

Technologies biométriques fondées sur le comportement

Reconnaissance vocale

Fonctionnement

La technologie fondée sur la reconnaissance vocale utilise les aspects individuels de la voix pour vérifier l'identité des personnes. La reconnaissance vocale peut faire appel à n'importe quel dispositif de captage audio composé de téléphones ou de microphones avec ou sans fil. La performance des systèmes de reconnaissance vocale est susceptible de varier suivant la qualité du signal audio et la différence entre l'appareil d'enregistrement et l'appareil vérificateur, de sorte que la capture s'effectue normalement avec l'appareil censé servir à la vérification ultérieure.

Lors de l'enregistrement, la personne est invitée à sélectionner une expression ou à répéter une séquence de nombres. Les expressions sélectionnées doivent durer environ 1 à 3 secondes (les expressions très courtes ne renferment pas suffisamment de données sur l'identité et les expressions trop longues en contiennent trop, ce qui, dans les deux cas, diminue l'exactitude). On demande généralement à l'utilisateur de répéter plusieurs fois l'expression ou le nombre, si bien que le processus d’enrôlement est un peu plus long que pour les autres technologies biométriques. Le gabarit courant en reconnaissance vocale exige 4 000 à 10 000 octets.

Du point de vue technique, la reconnaissance vocale relève à la fois de la biométrie physiologique et de la biométrie comportementale, car la voix est en grande partie déterminée par la morphologie de la gorge et du larynx, bien qu'elle puisse être modulée par le locuteur.

La vérification 1 : 1 est l'application qui convient le mieux. Cette technologie est facile à utiliser et ne requiert aucune connaissance particulière de la part de l'utilisateur. Lorsqu'en 1997, une banque canadienne a mené une enquête auprès de ses clients sur l'acceptabilité de diverses technologies biométriques, seule la reconnaissance vocale n'a pas été rejetée (Baker, 1997).

Fiabilité

La fiabilité est qualifiée de moyenne. Cette technologie ne se prête généralement pas à des applications 1 : N. Les changements de voix dus à une maladie peuvent parfois poser un problème.

Facilité d'emploi

L'utilisateur récite une expression dans un microphone ou un téléphone lorsqu'il est invité à le faire. La facilité d'emploi de la reconnaissance vocale est qualifiée d'élevée.

Acceptation par l'utilisateur

L'acceptation de la reconnaissance vocale par l'utilisateur est qualifiée d'élevée.

Stabilité

La stabilité de la reconnaissance vocale est qualifiée de moyenne à faible, la voix ayant tendance à changer au cours du temps.

Exemples d'applications existantes

Gouvernement/immigration

- La reconnaissance vocale est mise en œuvre dans des solutions d'accès physique dans le contexte du passage des frontières (Jackson, 1997).

Secteur bancaire

- On intègre la reconnaissance vocale à des systèmes destinés à sécuriser des opérations bancaires et commerciales en ligne (PR Newswire, 1999a).

Authentification en ligne/sur réseau

- En mai 1999, le « Home Shopping Network » avait annoncé avoir vendu plus de 5 000 ordinateurs personnels équipés de systèmes de vérification du locuteur depuis la mi-avril (PR Newswire, 1999b).

Autres

- Un fabricant d'automobiles européen a même étudié la possibilité d'incorporer la vérification du locuteur dans ses systèmes de contact (Cole, 1995).

Vérification dynamique de la signature

Fonctionnement

Cette technologie biométrique comportementale analyse la façon dont une personne signe. La biométrie de la signature est souvent appelée « vérification dynamique de la signature ». Cette technologie accorde autant d'importance à la façon dont une personne signe qu'au tracé statique de la signature proprement dite. A titre d'exemple, l'angle d'inclinaison du stylo sur le papier, le temps requis pour signer, la vitesse et l'accélération de la calligraphie, la pression exercée et le nombre de fois que le stylo décolle du papier sont des caractéristiques comportementales (Rosen, 1990) propres à chaque personne qui peuvent toutes être mesurées et analysées. La vérification dynamique de la signature n'étant pas fondée sur une image statique, la contrefaçon est jugée difficile.

Les données relatives à la signature peuvent être enregistrées à l'aide d'un stylo lecteur ou d'une tablette graphique ou des deux. Le stylo renferme des capteurs, de même que la tablette où les capteurs sont enrobés dans la surface sur laquelle on écrit ; ces capteurs détectent les caractéristiques propres à la façon de signer de chacun. Une autre variation a vu le jour récemment : l'émission acoustique. Celle-ci mesure le son émis lorsqu'une personne signe sur une feuille de papier (*Association for Biometrics and*

International Computer Security Association, 1998). Les gabarits employés pour la vérification dynamique de la signature totalisent environ 1 500 octets.

Fiabilité

La fiabilité est qualifiée de moyenne. Cette technologie ne se prête généralement pas aux applications 1 : N. Tout comme la géométrie de la main, la vérification dynamique de la signature ne permet pas d'apparier un gabarit avec son correspondant si celui-ci se trouve dans une grande base de données.

Facilité d'emploi

Au signal, l'utilisateur signe sur un dispositif de capture électronique. La facilité d'emploi de la vérification dynamique de la signature est qualifiée d'élevée, c'est l'une des technologies biométriques les plus faciles à utiliser.

Acceptation par l'utilisateur

L'acceptation de la vérification dynamique de la signature est qualifiée de moyenne à élevée.

Stabilité

La stabilité de cette technologie est qualifiée de moyenne à faible, notre signature ayant tendance à évoluer au fil du temps.

Exemples d'applications existantes

Banques

- La Chase Manhattan Bank a mis à l'essai la vérification dynamique de la signature pour identifier des clients représentant une entreprise avant une transaction.

Secteur privé

- En Amérique, plusieurs hôpitaux, pharmacies et compagnies d'assurances utilisent cette technologie biométrique pour authentifier des documents électroniques.

Autres technologies biométriques

Les technologies exposées ci-après sont encore, à notre avis, à un stade trop expérimental ou inabouti pour pouvoir être considérées comme prêtes à être appliquées. Elles sont abordées ici pour donner une idée au lecteur des voies sur lesquelles s'engage la recherche.

Géométrie de l'oreille

Fonctionnement

La forme de l'oreille externe, des lobes et la structure du cartilage représentent un champ moins connu de la biométrie physiologique (*Association for Biometrics and International Computer Security Association*, 1998). Apparemment la police est capable de relever les empreintes des oreilles laissées par les criminels lorsqu'ils écoutent aux portes et aux fenêtres. Cette technologie a été utilisée aux Pays-Bas (*The Toronto Star*, 1995) pour obtenir des condamnations. Une entreprise française met au point

l'«octophone», un appareil biométrique ressemblant à un téléphone qui capte des images de l'oreille (McMurchie, 1999).

Mesure de l'odeur corporelle

Fonctionnement

Cette technologie analyse l'odeur du corps humain ; un dispositif capte l'odeur émise par certaines parties du corps peu intimes telles que le dos de la main, le bras ou le cou. L'odeur particulière de chaque être humain est composée par des substances chimiques qui sont extraites par le système et classées sur un gabarit (Roethenbaugh, 1998b). L'Université de Cambridge aurait mis au point un «nez électronique» capable d'identifier les personnes d'après leur odeur corporelle (Spinney, 1994).

Dynamique de la frappe sur clavier

Fonctionnement

La dynamique de la frappe repose sur l'idée que la façon de dactylographier, en particulier son rythme, permet de distinguer les personnes. La dynamique de la frappe relève de la biométrie comportementale et évolue au fil du temps, à mesure que les utilisateurs apprennent à dactylographier et acquièrent leur propre manière de frapper les touches. Aux États-Unis, la *National Science Foundation et le National Bureau of Standards* ont mené des études qui ont démontré qu'aucune manière de frapper n'est identique à une autre (Miller, 1987). Cette technologie donne les meilleurs résultats avec les personnes qui peuvent taper sans regarder leur clavier. Néanmoins, l'état de santé et la fatigue des utilisateurs peuvent affecter le rythme de la frappe (Roethenbaugh, 1998b).

Récemment, la création de logiciels permettant de contrôler l'accès aux ordinateurs et à Internet a ravivé l'intérêt porté à cette technologie. Un système établit des profils individuels d'après la façon dont les utilisateurs entrent leur mot de passe, en tenant compte de facteurs tels que la dimension de la main, la vitesse de frappe, et la durée pendant laquelle les touches sont maintenues enfoncées (Nelson, 1998). Cette technologie pourrait être utilisée avec n'importe quel clavier : « des claviers d'ordinateurs aux téléphones en passant par les claviers des distributeurs automatiques de billets » (Net Nanny, 1998). Naguère, l'application de la dynamique de la frappe était limitée, notamment par la différence entre les claviers.

Reconnaissance de la démarche

Fonctionnement

Plusieurs universités mènent des recherches[17] sur la reconnaissance automatique des personnes d'après leur ***démarche***, ou leur propre façon de se déplacer. Lorsqu'une personne marche, plusieurs parties de son corps – les jambes, l'articulation des genoux, les bras, les coudes, etc. – décrivent un mouvement particulier qui se répète. Une caméra vidéo saisit ces points en mouvement et les envoie à un ordinateur qui les analyse. L'ordinateur enregistre la séquence de mouvements et établit des relations mathématiques pour chaque point afin de créer la « signature » de la démarche dont il a besoin pour reconnaître chaque personne.

Une bourse DARPA du gouvernement des États-Unis soutient cette recherche à l'appui du projet « Identification des personnes à distance ». [18] « Contrairement aux visages et aux iris, la démarche de quelqu'un peut être repérée à grande distance à l'aide d'une caméra à faible résolution et observée ainsi d'à peu près n'importe quel angle. Elle est aussi très difficile à déguiser » (*New Scientist*, 1999). Les premières applications qui viennent à l'esprit sont la défense d'un périmètre autour des ambassades et des installations militaires.

Tableau récapitulatif des technologies biométriques

Le tableau 1 offre une récapitulation générale de certaines technologies biométriques. Ce tableau est très subjectif et approximatif. Les éléments montrés sont susceptibles de varier beaucoup suivant le contexte, l'utilisation, l'algorithme, etc. Étant donné que certaines technologies biométriques sont plus matures que d'autres et que les systèmes biométriques dépendent beaucoup du contexte, les résultats réels varieront suivant la technologie choisie, l'application visée et la taille de la population enregistrée. Il faudrait aussi tenir compte d'autres facteurs, tels que la durée de la capture et de la recherche (qui sortent du cadre de ce rapport) pour interpréter correctement ce tableau récapitulatif.

Tableau 1. Tableau récapitulatif des technologies biométriques

Technologie biométrique	Fiabilité	Facilité d'emploi	Acceptation par l'utilisateur	Stabilité	Coût	Transparence[1]	Applications courantes	Convient aux comparaisons	
								1 : 1	1 : N
Reconnaissance de l'empreinte digitale	Élevée ou très élevée	Élevée	Moyenne à faible	Élevée	* à ***	Visible	Autorisation des voyageurs, permis de conduire, aide sociale	oui	oui
Géométrie de la main	Élevée	Élevée	Moyenne à élevée	Moyenne à élevée	***	Visible	Contrôle d'accès, autorisation des voyageurs, soins de jour	oui	non
Reconnaissance faciale	Moyenne à élevée[2]	Moyenne à élevée	Élevée	Moyenne à faible	***	Dissimulé	Casinos, autorisation des voyageurs	oui	potentielle-ment[3]
Reconnaissance de l'iris	Très élevée	Moyenne à faible	Moyenne à élevée	Élevée	*****	Dissimulé	Prisons, contrôle d'accès, autorisation des voyageurs	oui	oui
Reconnaissance de la rétine	Très élevée	Faible	Faible	Élevée	****	Visible	Contrôle d'accès, autorisation des voyageurs	oui	oui
Géométrie du doigt	Moyenne	Élevée	Moyenne à élevée	Moyenne à élevée	***	Visible	Contrôle d'accès, détenteurs de tickets d'entrée aux parcs d'attraction	oui	non
Reconnaissance vocale	Moyenne	Élevée	Élevée	Moyenne à faible	*	Dissimulé	Applications à basse sécurité, authentification par téléphone	oui	non
Vérification dynamique de la signature	Moyenne	Élevée	Moyenne à élevée	Moyenne à faible	**	Visible	Applications à basse sécurité, applications à signature existante	oui	non

Notes :

1. La transparence désigne la mesure dans laquelle un système peut être exploité à l'insu des personnes concernées. Les systèmes visibles ne peuvent prélever un échantillon biométrique à l'insu de la personne concernée, contrairement aux systèmes dissimulés.

2. La reconnaissance faciale pourrait théoriquement être fort exacte (comme le suggère l'essai récent de reconnaissance faciale mené dans des conditions contrôlées – *Facial Recognition Vendor Test*), mais des projets pilotes récents et des essais en conditions réelles ont fait apparaître des taux d'erreurs beaucoup plus élevés et montré qu'il était très difficile d'obtenir des résultats exacts avec ces systèmes.

3. Ibid.

Source : Author

Discussion

Un passage en revue des données non confidentielles sur la performance des technologies biométriques et les résultats d'essais de technologies biométriques publiés dans la presse donne à penser que la biométrie « n'est pas encore mûre ». Autrement dit, si les technologies biométriques semblent donner de bons résultats dans des applications de type 1 : N de taille limitée (et même dans certaines applications plus vastes de type 1 : 1), elles ne sont pas encore suffisamment précises, fiables et commodes pour pouvoir être appliquées dans des systèmes d'identification couvrant une population très nombreuse. Même si certains médias et rapports anecdotiques ont fournit des indices de succès concernant des mises en œuvres à grande échelle, les données de tierces parties confirmant ces succès et fournissant des informations importantes sur le contexte de la mise en œuvre (performance, précision et traitement des exceptions) se laissent encore attendre.

Mais il ne faudrait pas pour autant écarter complètement ces technologies. En effet, si elles sont utilisées à bon escient, les technologies biométriques nous permettent de résoudre des problèmes nouveaux et ***à la fois*** de renforcer la sécurité ***et*** de protéger la vie privée. Par exemple, le concepteur d'un système peut utiliser une technologie biométrique pour garantir la participation physique d'une personne à une transaction électronique ou à une rencontre en face à face. Ce type de conception a récemment été envisagé dans un projet auquel l'auteur du présent rapport a participé. Il s'agissait de stocker des informations sur une carte à puce qui serait remise à la personne concernée. Seule la présence physique de la personne concernée (confirmée par la collecte d'un échantillon biométrique) permettrait à la carte à puce de déverrouiller le système, ou autoriserait l'accès à la base de données ou sa mise à jour. Ce type d'utilisation stratégique des technologies biométriques pourrait à la fois protéger la personne concernée contre une usurpation d'identité (augmentation de la sécurité) et prévenir l'utilisation à mauvais escient des bases de données contenant des informations personnelles (amélioration de la protection de la vie privée).

Le grand public (et hélas aussi quelques fournisseurs) croit à tort qu'une personne peut être formellement identifiée par un système biométrique. Nous devons nous rappeler qu'un système, ***quel qu'il soit***, peut tout au plus indiquer un degré de corrélation et, (selon la taille de la population) avec les comparaisons 1 : N, rechercher un nombre de candidats susceptibles de correspondre à l'utilisateur, du fait qu'ils dépassent le seuil de similitude fixé.

Michael Thieme, le directeur des projets spéciaux à *l'International Biometric Group* (New York) expose clairement les limites de cette technologie :

> « La reconnaissance faciale livre une PROBABILITÉ que deux images correspondent à la même personne. Ni le logiciel de reconnaissance faciale, ni aucune autre technologie biométrique, ne peuvent établir avec certitude que deux personnes incarnent réellement une seule et même personne.
>
> Le fait de recourir à la reconnaissance faciale ou à n'importe quelle autre technologie biométrique pour obtenir une détermination irréfutable est contraire aux principes fondamentaux de la technologie biométrique. » (Thieme, 2003)

En optant pour les systèmes d'authentification 1 : 1 plutôt que pour les systèmes d'identification 1 : N, on maîtrise plus facilement le taux d'erreur et la performance d'une technologie biométrique donnée et, par conséquent, les chances de réussite de l'application.

Recommandations

Les essais biométriques, les projets pilotes et la mise en oeuvre de systèmes nous livrent un certain nombre d'enseignements d'application générale. A l'intérieur des limites et des contraintes de tout projet particulier, les concepteurs et administrateurs de systèmes devraient :

- Communiquer de façon transparente et honnête pour chaque projet de système.
- Superviser de façon appropriée les personnes interagissant avec les systèmes biométriques.
- S'assurer que des dispositifs de secours et de traitement des exceptions adéquats sont bien en place.
- S'assurer que les fonctions connexes (enregistrement, admissibilité au programme) étayent et améliorent la sécurité et la protection de la vie privée d'un système biométrique et ne permettent pas, par exemple, l'usurpation d'identité par l'utilisation d'un identifiant biométrique valide.
- Préférer au départ des systèmes petits ou moyens, bien ciblés et internes, avant d'envisager des systèmes à grande échelle couvrant une population très nombreuse. Cela facilite la résolution des problèmes de performance et permet de perfectionner le système en tirant les leçons de l'expérience, à mesure que la technologie mûrit.
- Envisager, si possible, de recourir à des systèmes pilotes et à des essais afin de recueillir des données sur la performance de la technologie dans des conditions réelles, avant d'appliquer le système à grande échelle.
- Réduire au minimum les atteintes à la vie privée et accroître l'exactitude de la technologie biométrique en privilégiant les systèmes d'authentification 1 : 1 par rapport aux systèmes d'identification 1 : N.
- S'assurer que la technologie biométrique constitue une solution appropriée au problème à traiter, en comparaison avec une méthode d'authentification plus classique. Tenir compte de l'acceptation par l'utilisateur et respecter les sensibilités culturelles.
- Chaque fois qu'il est possible de le faire, développer des systèmes où l'enrôlement est facultatif (*opt-in*).
- Collecter les échantillons biométriques de façon transparente pour l'utilisateur et avec son consentement.
- Si possible, permettre à l'utilisateur de conserver lui-même le gabarit biométrique (peut-être sur une carte à puce ou un badge) et ***ne pas*** stocker le gabarit biométrique dans un système central.

Problèmes

L'auteur a recensé les problèmes suivants en ce qui concerne les technologies fondées sur la biométrie :

- Le rejet ou l'acceptation d'un individu par un système biométrique peut être établit à tort. Les systèmes commettent des erreurs et peuvent manquer de rigueur au stade de l'enrôlement pour vérifier correctement l'identité d'une personne.
- Les évaluations indépendantes de la performance des technologies biométriques sont peu nombreuses.

- S'agissant des systèmes biométriques appliqués à une très grande population, toutes les mesures de la performance sont extrapolées, si bien qu'elles comportent un risque d'erreur élevé.

- Il faut éviter de créer une sous-classe de personnes non authentifiables par une technologie biométrique du fait que ces personnes sont l'objet d'erreurs de type « échec à l'enrôlement » ou « échec à l'acquisition ».

- L'attitude de certains fournisseurs de technologies biométriques qui se sont empressés d'offrir des « solutions » juste après le 11 septembre 2001 a des relents d'opportunisme.

- Les solutions fondées sur la biométrie risquent d'apparaître comme une panacée technologique aux yeux du grand public, qui tend à surestimer leur fiabilité et leur champ d'application et risque d'assimiler à tort la technologie à une protection contre le terrorisme.

- Le risque qu'un système biométrique présente une défaillance à grande échelle est élevé (un système dont la performance est inacceptable et qui nécessite un puissant dispositif de traitement des exceptions).

Normes sur la biométrie

Afin d'accroître l'interopérabilité entre systèmes biométriques, plusieurs organisations établissent des normes.

- Normes générales relatives à la biométrie :

  - Le *National Institute for Standards and Technology* (NIST) des États-Unis a défini le « format biométrique commun d'échange de fichiers » (*Common Biometric Exchange File Format* – CBEFF), comme un « ensemble commun d'éléments de données assurant la compatibilité entre différentes technologies biométriques et favorisant l'interopérabilité des programmes et systèmes d'applications biométriques en permettant l'échange de données biométriques ».[19]

  - L'Organisation pour le développement de normes d'information structurées (OASIS) élabore le langage XCBF (un format biométrique commun XML), une représentation XML des formats CBEFF.[20]

  - Le consortium BioAPI a défini une interface de programmation d'applications (API), afin de faciliter la tâche des programmeurs lorsqu'ils installent un logiciel destiné à un système biométrique.[21]

- L'Organisation de l'aviation civile internationale (OACI) et l'ISO/IEC étudient la nécessité d'établir des normes sur la biométrie appliquées au domaine des voyages :

  - Le Sous-comité électrotechnique international/Comité technique mixte (IEC JTC[22]) de l'ISO sur l'informatique a :

    - Un sous-comité 17 sur les cartes et l'identification personnelle.[23]

    - Un sous-comité 27 sur les techniques de sécurité.

- Un sous-comité 37 sur la biométrie.[24] Le groupe spécial 6 nous intéresse tout particulièrement puisqu'il étudie les questions, notamment sociétales, liées à la biométrie (en particulier la protection de la vie privée).

- Le Groupe consultatif technique sur les documents de voyage lisibles à la machine (*Technical Advisory Group on Machine Readable Travel Documents* - TAG/MRTD) de l'OACI a révisé le document 9303 afin d'y « inclure la confirmation assistée par une machine de l'identité du détenteur légitime d'un document de voyage lisible à la machine ». Cette révision prévoit l'inclusion d'une empreinte biométrique interopérable dans le monde entier dans un document de voyage lisible à la machine. [25]

Normes concernant la protection de la vie privée et la biométrie

L'OACI et l'ISO ont tenté de tenir compte de la question de la protection de la vie privée en élaborant leurs normes, mais, à notre avis, leurs efforts bien intentionnés n'ont pas tout à fait porté leurs fruits. Il est probable que cela résulte en grande partie du fait que la protection de la vie privée ait été présentée comme une question d'acceptation par le public au lieu de l'envisager comme une question objective de conception des systèmes et de gouvernance. L'opinion publique et l'acceptation d'un système par la population sont utiles dans la mesure où elles nous signalent que quelque chose ne va pas, mais l'acceptation par le public ***ne peut*** régler tous les problèmes de protection de la vie privée d'une initiative ou d'une norme proposées.

Méthodologies et cadres régissant la mise en œuvre des technologies biométriques

Comme cela a été indiqué en introduction, nous espérons que le débat alimenté par le présent document permettra d'élaborer un cadre pour la mise en oeuvre des technologies fondées sur la biométrie propre à améliorer la protection de la vie privée et la sécurité.

Plusieurs approches permettant de garantir qu'un système donné respecte les exigences en matière de protection de la vie privée et/ou de sécurité sont présentées ci-dessous pour discussion dans l'espoir que cet exposé encourage les initiatives dans ce domaine.

Méthodologies assurant la protection de la vie privée et la sécurité des applications biométriques

Moyens réglementaires – recourir à la loi pour assurer la protection de la vie privée et la sécurité

Certaines juridictions ont prévu des sanctions pénales générales ou spécifiques pour garantir la sécurité des systèmes biométriques et proscrire des actes permettant de se soustraire aux contrôles de sécurité.

Plusieurs juridictions ont aussi proposé ou promulgué une loi spécifique pour la protection de la vie privée dans le contexte de l'utilisation de la biométrie. Suivant les cas, cette loi peut se substituer ou s'ajouter à la législation générale relative à la protection de la vie privée. L'annexe I contient deux exemples provenant d'Amérique du Nord.

Moyens politiques – respect de la sécurité et de la vie privée

Il est souvent fait appel à des mesures politiques pour garantir la protection de la vie privée et la sécurité.

L'Évaluation de l'Impact sur la Vie Privée (EIVP ou *Privacy Impact Assessment - PIA*) et les audits de protection de la vie privée permettent de s'assurer que les mesures régissant la protection de la vie privée sont respectées et qu'elles offrent effectivement un niveau donné de protection. Si ces dispositifs sont courants dans le secteur public, ils commencent tout juste à faire leur apparition dans le secteur privé.

L'évaluation des menaces et des risques contre la sécurité et les audits de sécurité sont les outils utilisés traditionnellement pour vérifier si les mesures de sécurité sont appliquées et si elles sont appropriées.

Les critères communs offrent un cadre souple et formel pouvant être utilisé pour vérifier qu'un système ou produit informatique donné répond effectivement au profil de sécurité annoncé. L'adaptation du système des critères communs aux profils de protection de la vie privée est en cours (Adams *et al.*, 2002).

Moyens technologiques – intégrer des dispositifs de sécurité et de protection de la vie privée au système

Protections physiques visant à garantir la sécurité et la protection de la vie privée

Matériel anti-effraction

De nombreux systèmes sont équipés d'une protection physique destinée à accroître leur niveau de sécurité et ce type de protection est bien accepté. Les banques établissent très souvent des spécifications précises pour les protections équipant les claviers numériques et les distributeurs automatiques de billets. Les systèmes visant à assurer la sécurité nationale sont presque toujours munis de dispositifs physiques de cryptage anti-effraction et auto-destructifs (Schneier, 1996). Et comme l'a souligné un expert en sécurité : « Jusqu'à présent, la *National Security Agency* (NSA) des États-Unis a toujours refusé d'utiliser des logiciels pour crypter des informations confidentielles. C'est trop facile de pirater le logiciel… et de provoquer toutes sortes de failles difficiles à détecter dans le système de cryptage » (Smith, 1998).

Ce matériel anti-effraction est conçu pour qu'un technicien ou un programmeur ne puissent pas ***facilement***, ni ***efficacement*** briser les protections de sécurité d'un système donné.

Une démarche analogue peut être appliquée pour assurer la protection de la vie privée dans des systèmes biométriques. En deux mots, il est possible d'assujettir un système biométrique à certaines règles en utilisant des composants matériels spécifiques.

Ces règles concrétiseraient des mesures spécifiques de protection de la vie privée et des règles de fonctionnement du système.

Avec un tel système, il deviendrait impossible à un concepteur de logiciels de contourner les mesures de protection de la vie privée. On confèrerait ainsi le « sens du bien et du mal » à certaines pièces physiques du mécanisme – le mécanisme saurait quand il peut autoriser le système biométrique à fonctionner (en contrôlant le lien vers une identité, par exemple) ou lui interdire de fonctionner. Ces pièces physiques anti-effraction utiliseraient des primitives cryptographiques sécurisées par des clés physiques qui seraient inconnues du concepteur et de l'opérateur du système, et d'ailleurs de n'importe qui d'autre (cela peut se faire à l'aide de modules sécurisés d'injection de clé confiés à des tierces parties).

Comme nous l'avons noté plus haut, il existe déjà un modèle très courant, dans le monde de la sécurité, qui fonctionne de la façon suivante : les distributeurs automatiques de billets et les claviers numériques sont équipés de pièces physiques anti-effraction du même type qui communiquent avec des pièces physiques anti-effraction connectées sur les ordinateurs centraux de la banque. Le mécanisme physique « sait » si une transaction qui débute est légitime. La clé est d'abord chargée dans le dispositif physique anti-effraction par injection sécurisée et peut ensuite être réinjectée sans que l'opérateur « sache » en quoi elle consiste.

L'une des manières d'appliquer ce dispositif de sécurité pourrait consister à utiliser des « jetons de confiance » (*trusted token*): un petit ordinateur logé dans un boîtier anti-effraction serait placé dans le scanner biométrique, tandis qu'un autre « jeton de confiance » serait installé dans le serveur central du système biométrique. Ces deux pièces matérielles se « feraient mutuellement confiance » et ne feraient confiance à rien d'autre. Le jeton central refuserait de divulguer une identité à moins que la demande n'émane de son partenaire placé dans le scanner. Ainsi, il deviendrait impossible d'utiliser un système biométrique sans le consentement de la personne concernée (avec, par exemple, une empreinte digitale latente) (Borking, 1996). [26]

(Les « jetons de confiance » sont des ordinateurs non spécialisés, faciles à configurer et à sécuriser. La logique, qui requiert un cryptage puissant et une demande émise par le scanner correspondant, est « gravée » dans le « jeton de confiance ». Toute tentative d'ingénierie inverse ou de reprogrammation du « jeton de confiance » le détruira.)

Protecteur d'identité

John Borking de l'autorité de protection des données des Pays-Bas (*Registratiekamer*) a écrit abondamment au sujet du protecteur d'identité, un composant capable d'accroître la protection de la vie privée en limitant la circulation d'informations relatives à l'identité au sein d'un système complexe. Ce composant matériel spécialisé dans l'identité est comparable à la composante abstraite de « désidentification » de l'architecture de protection de la vie privée (voir plus bas).

STEP – Technologie de sécurité permettant la protection de la vie privée

Les technologies de sécurité permettant la protection de la vie privée (*Security Technology Enabling Privacy*) (Cavoukian, 2002) ont vu le jour à l'initiative de la Commissaire à l'information et à la protection de la vie privée de l'Ontario. Ainsi qu'elle le note dans son rapport :

> « Jusqu'à présent, la protection de la vie privée et la sécurité étaient considérées comme des forces opposées s'annulant mutuellement. Une telle conception implique nécessairement un équilibre dans lequel chaque antagoniste perd autant de poids que l'autre en gagne. Dans le paradigme de la théorie du jeu, plus on gagne sur un tableau, plus on perd sur l'autre, de sorte que la somme est toujours nulle. Mais le niveau de sécurité auquel aspire le grand public est tel que cette logique de «perdre et gagner» menace considérablement la vie privée. Si le débat qui a pris naissance après le 11 septembre 2001 reste bloqué dans ce dilemme, il risque de s'en prendre au fondement même de la vie privée et de la remettre en question.
>
> C'est pourquoi, nous devons sortir de ce paradigme. Le présent rapport explique pourquoi il n'y a pas de raison inhérente pour laquelle l'amélioration de la sécurité doit se faire aux dépens de la vie privée. Si nous parvenons à recadrer le débat, en remettant en question l'hypothèse de départ, à savoir qu'il faut sacrifier la protection de la vie privée à la cause de la sécurité, alors nous pourrons prendre les mesures nécessaires pour améliorer les deux. Il est possible de revoir la conception de nombreuses technologies de sécurité afin de réduire au minimum ou de supprimer

> celles de leurs caractéristiques qui portent atteinte à la vie privée tout en maintenant leur niveau d'efficacité élevé. Si nous remplaçons l'hypothèse de départ par une nouvelle hypothèse, à savoir que protection de la vie privée et sécurité représentent deux facettes complémentaires d'un tout indivisible (et non deux pôles opposés), nous serons alors en mesure de concevoir des technologies qui assurent la sécurité publique sans porter atteinte à la vie privée » (Cavoukian, 2002).

Outre le cryptage biométrique, le rapport sur les technologies de sécurité permettant la protection de la vie privée illustre celles-ci par l'exemple suivant :

> « Les technologies d'examen des passagers au scanner sont très courantes dans tous les aéroports, où elles servent à détecter une menace éventuelle contre la sécurité. Néanmoins, la reconnaissance peut constituer une intrusion dans l'intimité physique des passagers. Des chercheurs du Département de l'énergie des États-Unis ont mis au point une nouvelle technologie grâce à laquelle le scanner assure une plus grande sécurité tout en respectant la vie privée. Le *Pacific Northwest National Laboratory* du Département de l'énergie a conçu une technologie de reconnaissance faisant appel à l'imagerie holographique en trois dimensions, qui se limite à révéler des objets cachés sous les vêtements des passagers des lignes aériennes, au lieu de dévoiler la totalité de leur corps. Le « Personal Security Scanner » détecte non seulement les armes métalliques, mais aussi celles faites en plastique ou en céramique, ce qui lui confère un avantage sur les systèmes de surveillance qui n'utilisent que des détecteurs de métaux. Le scanner émet des ondes radio inoffensives à très haute fréquence et relativement longues qui peuvent pénétrer les vêtements. Les concepteurs ont réglé le problème posé par le fait que l'opérateur du scanner pouvait voir des parties dévêtues des corps des passagers, en reprogrammant le système de façon à ce qu'il n'affiche que les objets dissimulés et non l'image de la personne. Le « Personal Security Scanner » offre un excellent exemple de technologie conçue et utilisée de façon à répondre aux exigences de sécurité tout en réduisant au minimum l'intrusion dans l'intimité des personnes » (Cavoukian, 2002).

Architecture de la sécurité et de la protection de la vie privée

Architecture de la sécurité

Les concepteurs de systèmes appliquent souvent une méthode structurée, dénommée « architecture de la sécurité » pour intégrer effectivement la sécurité à la conception d'un système donné. Fondée sur l'évaluation des menaces pour la sécurité et sur une politique de sécurité, l'architecture de la sécurité permet de concevoir un système en atténuant les risques et en élevant la sécurité globale du système.

Les piliers de l'architecture de la sécurité sont l'authentification, le contrôle de l'accès, la confidentialité des données, l'intégrité des données et la non-répudiation.[27]

Architecture de la protection de la vie privée

Une démarche analogue peut s'appliquer à la protection de la vie privée et au développement d'une architecture de la protection de la vie privée (Hope-Tindall, 2002b). L'architecture de la protection de la vie privée obéit à une démarche structurée, reposant sur une évaluation de l’impact sur la vie privée et sur une politique de protection de la vie privée, qui permet de concevoir un système en atténuant les risques et en élevant la protection de la vie privée globale du système.

Généralement, une démarche d’architecture de protection de la vie privée passe par l’étude des différentes options ou modèles de conception du système, et, après analyse, la sélection de l'option ou du

modèle qui correspond à l'application professionnelle visée avec le plus faible impact sur la vie privée. Il est bien entendu nécessaire de mener en parallèle une évaluation de l'impact sur la vie privée afin de faciliter la création de l'architecture de la vie privée.

Conformément aux principes de limitation en matière de collecte des données et de qualité des données des *Lignes directrices de l'OCDE sur la vie privée*, l'architecture de la vie privée vise à réduire la quantité d'informations sur l'identité dans une transaction au minimum nécessaire qu'implique l'objectif pour lequel les données personnelles sont recueillies. L'architecture de la vie privée conjugue la technologie, la politique, la surveillance et la gouvernance dans une conception unique du système, en vue de préserver et d'accroître la protection de la vie privée. L'annexe II offre une analyse des composants constitutifs de l'architecture de la vie privée et de la position de l'architecture de la vie privée en général.

Un élément essentiel de la conception (l'emplacement physique du gabarit biométrique) pourrait être étudié dans une architecture globale de la vie privée. Par exemple, le stockage du gabarit biométrique sur une carte à puce au lieu d'une base de données centralisée pourrait résoudre en partie bon nombre de problèmes de protection de la vie privée associés aux systèmes biométriques, à condition que la carte à puce et le système biométrique soient protégés de façon appropriée (par exemple en limitant l'accès au moyen d'un lecteur autorisé et d'un code d'identification personnelle). La carte à puce peut voyager avec la personne concernée, celle qui, en définitive, peut donner son consentement puisqu'elle exerce la garde de sa propre empreinte biométrique. Le système de filière accélérée mis en place par l'aéroport de Schiphol (Pays-Bas) pour les voyageurs qui prennent fréquemment l'avion illustre ce qui précède (CNN, 2000 ; Chua, 2001). D'autre part, Bioscrypt, une entreprise canadienne, a commencé à commercialiser un produit spécialement conçu pour mettre à profit cette architecture décentralisée (Smart Card Alliance, 2002). Il est possible d'accroître encore la protection de la vie privée en intégrant judicieusement à la conception d'un système biométrique les technologies d'infrastructure à clé publique (ICP ou *Public Key Infrastructure - PKI*), de réseau privé virtuel et d'autres technologies de sécurité.

Industrie de la biométrie

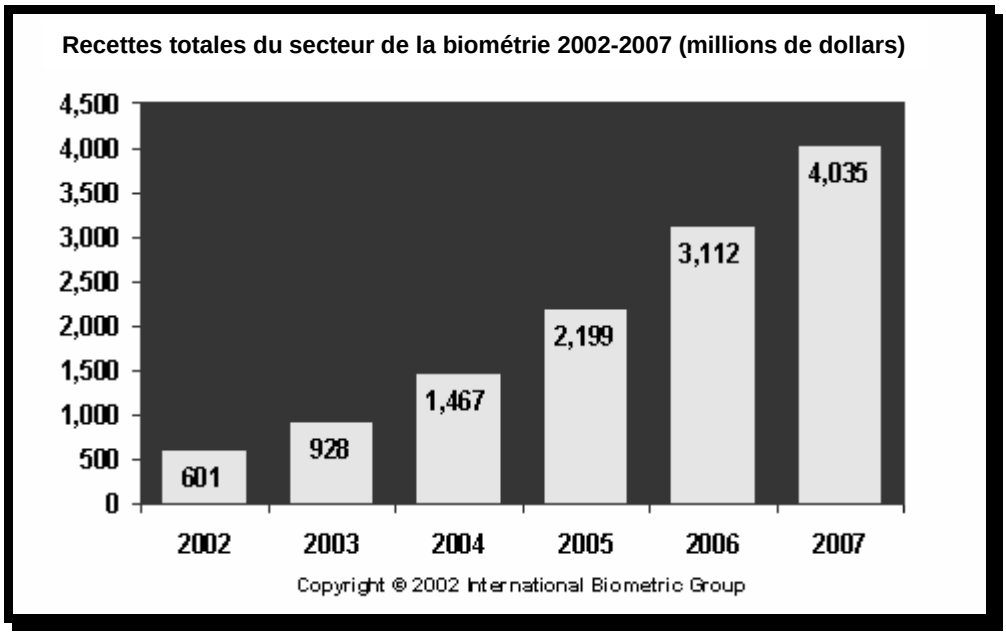
Même avant le regain d'intérêt pour les technologies biométriques suscité par les événements du 11 septembre 2001, l'industrie de la biométrie s'attendait à une hausse sensible de ses recettes à court terme. Cette prévision n'a été revue à la hausse que lorsque les fournisseurs, les pouvoirs publics et les citoyens ont commencé à voir dans les technologies biométriques une solution générale aux problèmes de sécurité rencontrés par de nombreux pays et organisations.

D'après le rapport exhaustif et très sérieux publié par l'International Biometric Group, *Biometric Market Report 2003-2007*, les recettes de ce secteur devraient dépasser USD 4 milliards d'ici à 2007, grâce au déploiement à grande échelle de systèmes biométriques dans le secteur public, à l'émergence de modèles de revenus transactionnels et à l'adoption et à l'utilisation de formats de données et d'infrastructures biométriques normalisés (voir figure 7).

Eu égard aux perspectives d'expansion du marché de la biométrie et aux résultats financiers de nombreuses entreprises de biométrie, l'auteur estime que l'industrie de la biométrie n'a pas besoin à l'heure actuelle d'un soutien extérieur supplémentaire pour enregistrer une croissance sensible. Néanmoins, la réussite, la facilité d'utilisation et l'acceptation par le public de diverses initiatives biométriques ainsi que les progrès scientifiques intéressant la biométrie (fiabilité, performance, sécurité et niveau de protection de la vie privée des systèmes) dépendront de la coopération entre fabricants, clients, groupes industriels, voire utilisateurs, des systèmes biométriques.

Il existe divers groupes industriels et associations ; certains pays ont déjà créé des services chargés de coordonner l'adoption et la mise en œuvre de technologies biométriques au sein de leur gouvernement, d'autres ont aussi ouvert des centres d'essais et d'évaluation et instauré des mécanismes permettant de rendre compte de l'efficacité et l'applicabilité des technologies biométriques. L'Union européenne appuie aussi BIOVISION (« une feuille de route pour la biométrie en Europe : 2003-2010 »), un projet visant à favoriser une utilisation sûre, ergonomique, socialement acceptable et éthique de la biométrie en Europe.

Figure 7. Projection de croissance du marché des technologies biométriques



Source: IBG (2002), *IBG Biometric Market Report 2003-2007*.

Ces initiatives sont certainement utiles, cependant l'auteur estime qu'il serait également opportun d'entamer un effort de recherche global et international en biométrie. Cet effort pourrait encourager de futures recherches consacrées à des technologies d'identification et d'authentification éthiques et permettre le développement et l'encouragement de modèles propres à accroître la sécurité, l'ergonomie, la transparence technologique et le respect de la vie privée pour ces technologies. De plus, cet effort pourrait favoriser l'élaboration d'une procédure d'essai transparente et indépendante pour les technologies biométriques, qui garantirait aux fournisseurs, aux clients et aux utilisateurs des mesures précises et pertinentes de la performance des systèmes prises dans des conditions réelles.

L'auteur de ce rapport pense qu'il est nécessaire de mieux informer les utilisateurs et le public en général de ces systèmes, en battant en brèche certains mythes et idées fausses à propos des technologies fondées sur la biométrie et l'ADN. Dans ce domaine, une initiative internationale est éminemment souhaitable à bien plus d'un titre. Il conviendrait également d'informer les fournisseurs et leurs clients sur les dispositifs de sécurité et de protection de la vie privée intégrables à ces systèmes, pour qu'ils en saisissent les avantages potentiels et le caractère impératif sur le plan commercial. De fait, si on ne s'attelle pas à ces questions de sécurité et de protection de la vie privée, les inquiétudes des utilisateurs finaux risquent fort de limiter le développement des technologies biométriques et l'acceptation de leur mise en oeuvre. L'avenir ne s'améliorera que si nous évaluons honnêtement le *statu quo*, les problèmes et les débouchés actuels, et si nous encourageons ***tous*** le développement de la meilleure technologie pour l'avenir de la meilleure façon qui soit.

Conclusion

Nous sommes déjà à l'ère des technologies fondées sur la biométrie. Il est nécessaire que nous comprenions leurs limites, leurs avantages et leurs risques respectifs. Nous devons recenser et classer les applications potentielles, afin de nous assurer que la technologie est appropriée, efficace par rapport à son coût et fiable.

De notre volonté d'incorporer des contrôles réglementaires ***et*** politiques ***et*** technologiques à ces systèmes et technologies dépendra la mesure dans laquelle ces systèmes et technologies amélioreront notre qualité de vie, nous la facilitant et la rendant plus sûre, ou, au contraire, menaceront notre liberté par une surveillance et un contrôle réels ou potentiels.

Nous ne devrions pas avoir à choisir entre sécurité et protection de la vie privée. En agissant de manière responsable et au prix d'un effort soutenu, non seulement nous pouvons, mais nous ***devons*** avoir les deux. A cet effet, il est impératif que nous soutenions et favorisions le développement de technologies, techniques et méthodes élevant le niveau de sécurité et de protection de la vie privée.

NOTES

1. L'expression “right to be left alone” avait été forgée par le juge Cooley plusieurs années avant.
2. Norme nationale du Canada intitulée « Code type sur la protection des renseignements personnels » CAN/CSA-Q830-96.
3. Annexe 1 – *Loi sur la protection des renseignements personnels et des documents électroniques* – Lois et règlements codifiés du Canada 2000, c. 5 (ci-après LPRPDE).
4. Pour plus de détails, voir : http://europa.eu.int/comm/justice_home/doc_centre/asylum/fingerprints/doc_asylum_fingerprints_en.htm et aussi http://europa.eu.int/comm/justice_home/news/information_dossiers/news_eurodac_whatis_en.htm consulté le 20 avril 2004.
5. Market research method and system for collecting retail store and shopper market research data, Assignee : A.C. Nielsen Company, United States Patent Number : 5331544, 19 juillet 1994.
6. Par exemple, Hill-climbing attack.
7. “The Facial Recognition Vendor Test – 2000” et “The Facial Recognition Vendor Test – 2002”, www.frvt.org, consulté le 20 avril 2004
8. “The Fingerprint Verification Competition – 2002”, http://bias.csr.unibo.it/fvc2002, consulté le 20 avril 2004
9. Voir http://infowar.net/tia/www.darpa.mil/iao/HID.htm, consulté le 20 avril 2004
10. Voir note 4.
11. A la suite des événements du 11 septembre 2001.
12. Mayfair Lakeshore Racquet & Fitness Club, www.cbc.ca/consumers/market/files/home/biometrics/dayinlife.html, consulté le 20 avril 2004
13. Voir www.identix.com/newsroom/lfa.html, consulté le 20 avril 2004
14. Voir note 13.
15. Par exemple, voir http://faculty.darden.virginia.edu/smithr/Biometrics.doc, consulté le 20 avril 2004
16. Pour plus d’informations, voir www.cbsa-asfc.gc.ca/travel/canpass/menu-e.html, consulté le 20 avril 2004
17. Par exemple, voir www.isis.ecs.soton.ac.uk/image/gait/, consulté le 20 avril 2004
18. Pour plus d’informations, voir www.gait.ecs.soton.ac.uk, consulté le 20 avril 2004
19. « Fondé en 1901, le NIST est une agence fédérale sans fonction réglementaire relevant de l'administration technologique du Département du commerce des États-Unis. Le rôle du NIST consiste à établir et à promouvoir le mesurage, la normalisation et des technologies, afin d'élever la productivité, de faciliter les échanges et d'améliorer la qualité de la vie ». Pour plus d’informations, voir www.itl.nist.gov/div895/isis/bc/cbeff, consulté le 20 avril 2004
20. « Un groupement de fournisseurs et d'utilisateurs désirant rédiger des directives pour l'interopérabilité des produits compatibles avec le langage SGML (langage standard généralisé de balisage) a fondé SGML Open, en 1993, et l'a rebaptisée OASIS en 1998 pour refléter l'élargissement du champ de ses activités techniques, englobant notamment le langage XML (langage extensible de balisage) et d'autres normes connexes ». www.oasis-open.org/committees/xcbf/, consulté le 20 avril 2004
21. Le consortium bioAPI, lancé en avril 1998, regroupe différents acteurs dans le domaine de la biométrie. www.bioapi.org, consulté le 20 avril 2004
22. Voir : www.jtc1.org, consulté le 20 avril 2004
23. Voir : www.sc17.com, consulté le 20 avril 2004 pour plus d’informations
24. Voir : www.jtc1.org/Navigation.asp?Area=Structure&Mode=Browse&CommLevel=SC&SubComm=ISO%2FIECJTC1SC00037&x=8&y=10, consulté le 20 avril 2004
25. www.icao.int/icao/en/atb/fal/mrtd/biometric_tech.htm, consulté le 20 avril 2004
26. Voir aussi articles dans le *Schwerpunktheft “Digitales geld”, Datenschutz und Datensicherheit*, 7, 1997.
27. ISO7498-2 Security Architecture reference.

REFERENCES

AcSys Biometrics Corp. and Nexus Group International Inc. (2001) "AcSys Biometrics Management Group Available For Comment", Media Advisory, 12 septembre, www2.cdn-news.com/scripts/ccn-release.pl?/2001/09/12/091201-7118-e.html, consulté le 20 avril 2004.

Adams, Dawn *et al*. (2002), "IBM Domus ITSL", exposé devant le groupe de travail PETTEP – San Francisco (12e conférence, Computer Freedom and Privacy - CFP 2002), 16 avril 2002.

Association for Biometrics and International Computer Security Association (1998), "1998 Glossary of Biometric Terms", révisé 1999 version disponible à www.afb.org.uk/docs/glossary.htm, consulté le 20 avril 2004.

Australian Justice and Customs (2002), "Passport Verification World First", 26 août, www.law.gov.au/www/justiceministerHome.nsf/Web+Pages/ED7C05CFE3763380CA256C220003EEEE?OpenDocument, consulté le 20 avril 2004.

Baker, Geoff (1997), "Newest Form of ATM Security Catches Eye of Banking Industry," *Ottawa Citizen*, 3 juillet, p. C1.

Belsize, Laurent (1997) "Coming Soon: ATMs That Recognise Your Eyes", *Christian Science Monitor*, 2 décembre.

Biome Partners, Inc. (1999), "New 3D Finger Geometry Biometrics for OEM's and Systems Integrators", communiqué de presse, 15 janvier.

Biometric Digest (1998), "Mr. Payroll Corp.'s Machine Makes Military Base Debut", juin, p. 3, www.biodigest.com/BiometricDigest/BackIssues/199806.pdf, consulté le 20 avril 2004.

Biometric Technology Today (1998), Vol. 6, No. 5, septembre, pp. 6, 8.

Bonier, Paul (n.d.), "Up Close and Personal: Biometrically Identifying Bank Customers Eye to Eye is an Invasion of Privacy," *Kitchener-Waterloo Record*, p. A11.

Bonsor, Kevin (n.d.), "How Facial Recognition Systems Work", http://computer.howstuffworks.com/facial-recognition.htm/printable, consulté le 20 avril 2004.

Borking, John, (1996) "Der Identity Protector" and "Einsatz datenschutzfreundlicher technologien in der Praxis", *Datenschutz und Datensicherheit*, 11, pp. 636-640; 654-658.

Burnell, John (1997), "Identifying the Biometric Opportunity: Biometric Technology is Now an Affordable Tool for Many Users and Applications Beyond Security", *Automatic ID News*.

Business Week (2002), "Why Visionics Is Flying Higher", 14 janvier, www.businessweek.com/magazine/content/02_02/c3765101.htm#B3765105, consulté le 20 avril 2004.

Cavoukian, Ann (2002), "Security Technology Enabling Privacy (STEPs): Time for a Paradigm Shift", Information and Privacy Commissioner/Ontario, juin, www.ipc.on.ca/scripts/index_.asp?action=31&P_ID=13289&N_ID=1&PT_ID=11351&U_ID=0, consulté le 20 avril 2004.

Chua, June (2001), "Biometrics: The Future of Security", *CBC News Online*, septembre, www.cbc.ca/news/indepth/background/wtc_biometrics.html, consulté le 20 avril 2004.

Cilluffo, Frank J. (2000) "Cyber Attack: The National Protection Plan and its Privacy Implications", déclaration by M. Cilluffo, Deputy Director, Organised Crime Project Director, Task Force on Information Warfare and Information Assurance, Center for Strategic and International Studies adressée au Sénat des Etats-Unis, 1 février.

Clarke, Roger (2003), "SmartGate: A Face Recognition Trial at Sydney Airport", Australian National University, Department of Computer Science, 26 août, mise à jour le 7 février 2004, www.anu.edu.au/people/Roger.Clarke/DV/SmartGate.html, consulté le 20 avril 2004.

CNN (Cable News Network) (2000), "Schipol Backs Eye Scan Security", CNN.com/WORLD, 27 mars, www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/, consulté le 20 avril 2004.

Cole, George (1995), "Giving Voice to Security" *Financial Times*, 15 septembre.

Cooley, Thomas M. (1888), *Cooley on Torts 29*, 2nd edition.

Curran, John (2001), "Casinos Using Facial Surveillance", Associated Press, 26 février, www.crimelynx.com/casino.html, consulté le 20 avril 2004.

Delaney, Kevin and Paulo Prada (2002), "In Security, the Eyes Tell All: IBM and Dutch Airport to Sell State-of-the-Art Iris-Scanning System", *Wall Street Journal Europe*, 28 avril, www.biometricgroup.com/in_the_news/wsj_europe.html, consulté le 20 avril 2004.

EC (European Commission), (2003), "European Fingerprint ID System Will Track Asylum Seekers", communiqué de presse, The European Commission: Representation in the United Kingdom, 14 janvier, www.cec.org.uk/press/pr/pr03/pr0302.htm, consulté le 20 avril 2004.

eSchool News (2000), ""Best Practices – Technology: This Minnesota High School Gives Fingerprint Scanning a Whorl"", *eSchool News Online*, 1 septembre, www.eschoolnews.com/news/showStory.cfm?ArticleID=1277, consulté le 20 avril 2004.

eSchool News (2001), "Fingerprint Technology Speeds School Lunch Lines", *eSchool News Online*, 29 janvier, www.eschoolnews.com/news/showStory.cfm?ArticleID=2146, consulté le 20 avril 2004.

findBIOMETRICS.com (n.d.), "Hand Geometry – Now and in the Future", www.findbiometrics.com/Pages/hand_finger%20articles/hand_2.html, consulté le 20 avril 2004.

Fonseca, Brian (2002), "Airports Look to Biometrics for Security: Integrated Facial Recognition, Digitally Protected Passports on the Way", *InfoWorld*, 1 mars, www.infoworld.com/article/02/03/01/020301hnbiometrics_1.html, consulté le 20 avril 2004.

Golgotha, Guy (1999), "Bar Codes for the Body Make it to the Market: Biometrics May Alter Consumer Landscape", *Washington Post*, 21 juin, p. A1.

Hamilton, Tyler (2003), "Finger on the Future", *The Toronto Star*, 17 mai.

Holmes, J., L. Wright et R. Maxwell (1991), "A Performance Evaluation of Biometric Identification Devices", Sandia Report, Sandia National Laboratories, SAND91-0276/UC-906, juin, http://infoserve.sandia.gov/cgi-bin/techlib/access-control.pl/1991/910276.pdf, consulté le 20 avril 2004.

Hope-Tindall, Peter (2002a), "Privacy Impact Assessment – Obligation or Opportunity: The Choice is Ours!", presenté au CSE ITS Conference, Ottawa, Ontario, 16 mai, www.enterpriseprivacy.com/cseits2002/ITS%20Material.pdf, consulté le 20 avril 2004 (voir également Annexe II).

Hope-Tindall, Peter (2002b), "Privacy Architecture", présenté à Showcase Ontario 2002, 10 septembre, www.enterpriseprivacy.com/Corp2002/2000-09-10Arch_files/frame.htm, consulté le 20 avril 2004.

IBG (International Biometric Group) (n.d.a), "How is 'Biometrics' Defined?" www.biometricgroup.com/reports/ public/reports/biometric_definition.html, consulté le 20 avril 2004.

IR Recognition Systems (1998), "A Show of Hands Keeps School Children Safe," communiqué de presse, 16 novembre, www.handreader.com/news/pressreleases/1998_archives/981116.htm, consulté le 20 avril 2004.

Iridian Technologies, Inc. (n.d.), "Spring Technologies and Johan Rhea Tae Kwon Do Launch New Technology that Enhances Customer Service," communiqué de presse (pour plus d'information sur Iridian, voir www.iriscan.com, consulté le 20 avril 2004).

Jackson, William (1997), "Digital Video Patrols Border: INS Inspectors in Montana Use Surveillance Equipment at Canadian Line, *Government Computer News*, 15 décembre, www.gcn.com/archives/ gcn/1997/December15/comm.htm, consulté le 20 avril 2004.

James, Frank (1997), "Body Scans Could Make ID Process Truly Personal", *Chicago Tribune*, 4 juin, cité dans John D. Woodward, "Biometrics: Privacy's Foe or Privacy's Friend?", Proceedings of the IEEE, Vol. 85. No. 9, septembre, p. 1483.

Lack, Bob (1999), "Development of Facial Recognition Technologies in CCTV Systems," *SourceUK.net*, 25 octobre, www.sourceuk.net/indexf.html?00624, consulté le 20 avril 2004.

Mansfield, T. *et al.* (2001), "Biometric Product Testing Final Report", CESG report, 19 mars, www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf, consulté le 20 avril 2004.

Matsumoto, T. *et al.* (2002), "Impact of Artificial Gummy Fingers on Fingerprint Systems", Proceedings of the International Society for Optical Engineering, *Optical Security and Counterfeit Deterrence Techniques IV*, Vol. 4677.

McMilan, Robert (2002), "The Myth of Airport Biometrics", *Wired News*, 9 août, www.wired.com/ news/conflict/0,2100,54418,00.html?tw=wn_story_related, consulté le 20 avril 2004.

McMurchie, Laura Lyne (1999), "Identifying Risks in Biometrics Use", *Computing Canada*, 12 février, p. 12, www.findarticles.com/cf_dls/m0CGC/6_25/53880053/p1/article.jhtml, consulté le 20 avril 2004.

Mercury News (1999), "Bank Will ID its Customers by Pattern of Eye's Iris," 13 mai.

Miller, Benjamin L. (1987), "Biometrics: Getting Computers to Identify People," *Canadian Datasystems*, Vol. 19, No. 11, novembre, p. 65.

Milroy, Susannah (1998), "Biometric Identification and Access Control Go Hand-In- Hand", *SP&I News*, avril.

MIT (Massachusetts Institute of Technology) (2002), "Photobook/Eigenfaces Demo", http://vismod.media.mit.edu/vismod/demos/facerec/basic.html, consulté le 20 avril 2004.

Miyake, Kuriko (2002), "Japan to Test Biometrics for Airport Check-in", IDG News Service, Tokyo Bureau, 6 novembre, security.itworld.com/4360/021106japanbio/page_1.html, consulté le 20 avril 2004.

Nelson, Matthew (1998), "Net Nanny Finds New Keys to Security: Let Your Fingers Do the Walking to a New Form of Password Protection", *InfoWorld Electric*, 9 octobre, www.pcworld.com/news/article/0,aid,8361,00.asp, consulté le 20 avril 2004.

Net Nanny (1998), "Net Nanny Releases Much Anticipated Alpha Version of BioPassword®, its Patented Keystroke Dynamics Security Solution", communiqué de presse, 26 août, www.netnanny.com/press/press_980826.htm, consulté le 20 avril 2004.

New Scientist (1999), "Tripped Up: Watch How You Walk, You May Incriminate Yourself", 4 décembre.

OACI (Organisation de l'aviation civile internationale), (2003a), "ICAO Recommendation", www.icao.int/mrtd/biometrics/recommendation.cfm, consulté le 20 avril 2004.

OACI (2003b), "Biometric Deployment of Machine Readable Travel Documents", ICAO TAG MRTD/NTWG Technical Report, Version 1.9, 19 mai, www.icao.int/mrtd/download/documents/Biometrics%20deployment%20of%20Machine%20Readable%20Travel%20Documents.pdf, consulté le 20 avril 2004.

O'Connor, Sean (1998) "Collected, Tagged, and Archived: Legal Issues in the Burgeoning Use of Biometrics for Personal Identification", *Stanford Technology Law Review*, STLR Working Paper, http://stlr.stanford.edu/stlr/Working_Papers/98_O_Connor_1/index.htm, consulté le 20 avril 2004.

OCDE (2002), *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité*, OCDE, Paris, www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html, consulté le 20 avril 2004.

OCDE (1980), *Lignes directrices sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, OCDE, Paris, 1980, www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html, consulté le 20 avril 2004.

Pigg, Susan (2002), "Iris-Recognition Device to be Demonstrated: Technology Could Speed Path of Frequent Fliers", *The Toronto Star*, 24 septembre, www.hope-tindall.com/peter/2002_sep_24.htm, consulté le 20 avril 2004.

PR Newswire (1999a), "SAFLINK Develops Way to Secure Internet Banking/Brokerage Account Balances, Bill Payment, and Funds Transfer Using Biometrics", 24 juin, www.findarticles.com/cf_dls/m4PRN/1999_June_24/54981904/p1/article.jhtml, consulté le 20 avril 2004.

PR Newswire (1999b), "Home Shopping Network and SAFLINK Corporation Ship Biometric Security to 5,000 Families", 11 mai, http://www.findarticles.com/cf_dls/m4PRN/1999_May_11/54597538/p1/article.jhtml, consulté le 20 avril 2004.

Roethenbaugh, Gary (1998a), "An Introduction to Biometrics and General History", *Biometrics Explained*, Section 1.

Roethenbaugh, Gary (1998b), "Technology Overview", *Biometrics Explained*, Section 3.

Roethenbaugh, Gary (1999), "Types of Biometric", *ICSA Biometrics Buyer's Guide*, Chapter 4.

Rosen, Jerome (1990), "Biometric Systems Open the Door", *Mechanical Engineering*, Vol. 112, No. 11, novembre, p. 59.

RYCOM Inc. (n.d.), "Frequently Asked Questions (FAQs) About Iris Recognition", www.rycom.ca/solutions/security/iridian/media_faq.htm#9, consulté le 20 avril 2004.

Schneier, Bruce (1996), *Applied Cryptography*, John Wiley & Sons, Inc., pp. 223-224.

Smart Card Alliance (2002), "Bioscrypt On Board with HID's iCLASS(TM) for Access Control", Industry News, 14 mai, www.smartcardalliance.org/industry_news/industry_news_item.cfm?itemID=346, consulté le 20 avril 2004.

Smith, Rick (1998), "Re: military encryption ?", Usenet posting to comp.security.misc, Secure Computing Corporation, 20 octobre 1998, http://groups.google.com/groups?oi=djq&selm=an_403329809, consulté le 20 avril 2004.

Soutar, Colin (n.d.), "Biometric System Security", Bioscrypt Inc., www.bioscrypt.com/assets/security_soutar.pdf, consulté le 20 avril 2004.

Spinney, Laura (1994), "Crooks Smelly Armpits Give the Game Away", *New Scientist*, 14 septembre, p. 10.

Thalheim, Lisa, Jan Krissler, and Peter-Michael Ziegler (2002), "Body Check: Biometric Access Protection Devices and their Programs Put to the Test", *c't*, www.heise.de/ct/english/02/11/114/, consulté le 20 avril 2004.

The Toronto Star (1995), "Pinched by the Ear", 6 juillet, p. 43.

Thieme, Michael (2003), "Was It Really Saddam on TV Last Night?", posting to The Biometric Consortium's Discussion List BIOMETRICS@PEACH.EASE.LSOFT.COM, 20 mars.

Tomko, George (1996), "Biometric Encryption – New Developments in Biometrics", presentation au 18eme International Privacy and Data Conference, Ottawa, 19 septembre, www.privcom.gc.ca/speech/ archive/02_05_a_960918_01_e.asp, consulté le 20 avril 2004.

Tomko, George (2002), "The Fundamental Problem with Template-based Biometrics", presentation lors de la 12e Conférence : Computers, Freedom and Privacy, San Francisco, 16 avril.

Townsend, Mark et Paul Harris (2003), "Security Role for Traffic Cameras", *The Observer*, 9 février, http://observer.guardian.co.uk/politics/story/0,6903,892001,00.html, consulté le 20 avril 2004.

US Department of State, "Enhanced Border Security and Visa Entry Reform Act: Questions and Answers", Office of the Spokesman, 9 mai, www.state.gov/r/pa/prs/ps/2002/10049.htm, consulté le 20 avril 2004.

US House of Representatives (2002), "Enhanced Border Security and Visa Entry Reform Act of 2002", United States H.R. 3525, www.unitedstatesvisas.gov/pdfs/Enhanced_Border_SecurityandVisa_Entry.pdf, consulté le 20 avril 2004.

Warren and Brandeis (1890), "The Right to Privacy", 4 *Harvard Law Review* 4, 193.

Wayman, J. (2002), "Biometric Authentication Technologies: Hype Meets the Test Results", présentation lors de la 11e USENIX Security Symposium, San Francisco, 5-9 août, www.usenix.org/events/sec02/wayman.pdf, consulté le 20 avril 2004.

Williams, Martyn (2002), "OECD Publishes Cybersecurity Guidelines", *ComputerWorld*, IDG News Service, 8 août, www.computerworld.com/governmenttopics/government/policy/story/0,10801,73297,00.html, consulté le 20 avril 2004.

Zunkel, Richard (1994), "Palm Reading for Protection," *Security Management*, novembre, pp. 89-90.

ANNEXE I – PROTECTION LÉGALE DE LA VIE PRIVÉE POUR LA BIOMÉTRIE

Loi sur le programme Ontario au travail. Loi de l'Ontario 1997, chapitre 25, annexe A.[1]

"Renseignements biométriques" (*Biometric information*) signifie information dérivée des caractéristiques uniques d'un individu ce qui n'inclut ni l'image photographique, ni l'image d'une signature.

Renseignements biométriques

75. (1) Si la présente loi ou les règlements autorisent quiconque à recueillir ou à utiliser des renseignements personnels, des renseignements biométriques ne peuvent être recueillis ou utilisés qu'aux fins suivantes :

1. Veiller à ce qu'un particulier ne soit inscrit qu'une seule fois à titre d'auteur de demande, de bénéficiaire, de conjoint, de partenaire de même sexe ou d'adulte à charge.
2. Authentifier l'identité d'un particulier qui prétend avoir droit à une aide.
3. Permettre à un particulier de recevoir une aide fournie par l'intermédiaire d'une institution financière ou d'un autre fournisseur autorisé et d'en accuser réception.
4. Permettre à un auteur de demande, à un bénéficiaire, à un conjoint, à un partenaire de même sexe ou à un adulte à charge d'obtenir l'accès à des renseignements personnels.
5. Permettre à un particulier de faire une déclaration par un moyen électronique, notamment vocal, à toute fin autorisée aux termes de la présente loi.
6. Comparer des données conformément à une entente conclue en vertu de l'article 71 ou 72 afin de vérifier l'admissibilité à une aide ou à des prestations. 1997, chap. 25, annexe A, par. 75 (1); 1999, chap. 6, par. 50 (7).

(2) Les renseignements biométriques peuvent être recueillis aux termes de la présente loi qu'auprès du particulier auquel ils se rapportent, que conformément à une entente visée à la disposition 6 du paragraphe (1) ou que conformément à l'article 73.

(3) Les renseignements biométriques ne doivent pas être divulgués à un tiers sauf si la divulgation est faite conformément :

a) soit à une ordonnance d'un tribunal ou à un mandat;

b) soit à une entente conclue en vertu de l'article 71 ou 72 afin de vérifier l'admissibilité à un régime de prestations sociales, y compris un régime de prestations sociales visé par la Loi de l'impôt sur le revenu ou la Loi de l'impôt sur le revenu (Canada);

c) soit à l'article 73.

1 www.e-laws.gov.on.ca/DBLaws/Statutes/English/97o25a_e.htm, consulté le 20 avril 2004.

(4) Les renseignements biométriques à recueillir auprès du particulier auquel ils se rapportent doivent être recueillis ouvertement et directement auprès de celui-ci.

(5) L'administrateur veille à ce que seules les personnes qui ont besoin de renseignements biométriques afin d'exercer leurs fonctions aux termes de la présente loi puissent y avoir accès et puissent les utiliser et que ceux-ci ne soient pas utilisés comme identificateur unique de dossiers ou identificateur commun de dossiers personnels, sauf selon ce qui est autorisé aux termes du paragraphe (1).

(6) L'administrateur veille à ce que les renseignements biométriques recueillis aux termes de la présente loi soient codés sans délai après leur collecte, que les renseignements biométriques originaux soient détruits après l'encodage et que les renseignements biométriques codés ne soient stockés ou transmis que sous une forme codée et qu'ils soient détruits de la façon prescrite.

(7) Ni le directeur ni l'administrateur ne doivent mettre en place un système qui permet de reconstituer l'échantillon biométrique original à partir de renseignements biométriques codés ou de le conserver, ou qui en permet la comparaison avec une copie ou une reproduction de renseignements biométriques qui n'ont pas été obtenus directement du particulier.

(8) Les seuls renseignements personnels qui peuvent être conservés avec les renseignements biométriques concernant un particulier sont le nom, l'adresse, la date de naissance et le sexe du particulier.

(9) Pour l'application de l'article 67 de la Loi sur l'accès à l'information et la protection de la vie privée et de l'article 53 de la Loi sur l'accès à l'information municipale et la protection de la vie privée, le paragraphe (3) est une disposition ayant trait au caractère confidentiel qui l'emporte sur ces lois. 1997, chap. 25, annexe A, par. 75 (2) à (9).

Biometric Identifier Privacy Act – State of New Jersey[1]

ASSEMBLY, No. 2448
STATE OF NEW JERSEY
210th LEGISLATURE

INTRODUCED JUNE 13, 2002

Sponsored by:
Assemblywoman JOAN M. QUIGLEY
District 32 (Bergen and Hudson)

(texte anglais uniquement)

An Act concerning biometric identifiers and supplementing Title 2A of the New Jersey Statutes.

Be It Enacted *by the Senate and General Assembly of the State of New Jersey:*

1. This act shall be known and may be cited as the "Biometric Identifier Privacy Act."

2. As used in this act:

   "Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of a hand or a face geometry.

   "Governmental entity" means the State, any agency, authority, or employee thereof, or any political subdivision of the State, including but not limited to any county, municipality, or school district, or any agency, authority, or employee thereof.

3. a. Notwithstanding any other provision of law to the contrary, no person shall obtain a biometric identifier of an individual, for the purpose of commercial advantage, without authorisation of the individual.

   b. A person who possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier to another person unless:

   (1) The individual consents to the sale, lease or disclosure.

   (2) The sale, lease or disclosure completes a financial transaction requested or authorised by the individual.

   (3) The sale, lease or disclosure is required or permitted by federal or State law. Or

   (4) The sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose.

   c. A person who possesses a biometric identifier of an individual shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects other confidential information.

1 www.njleg.state.nj.us/2002/Bills/A2500/2448_I1.HTM, consulté le 20 avril 2004.

d. A person aggrieved by a violation of this section may bring an action in the Superior Court to enjoin further violation and to recover for the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.

e. Any person who violates any provision of this section shall be liable for a civil penalty of not more than USD 25,000 for each violation. Any such penalty shall be enforced and collected in accordance with "The Penalty Enforcement Law of 1999," P.L.1999, c.274 (C.2A:58-10 et seq.). Any action to collect or enforce any such penalty shall be brought in the Superior Court by the Attorney General or county prosecutor.

4. a. A governmental entity that possesses a biometric identifier of an individual shall not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(1) The individual consents to the sale, lease or disclosure.

(2) The sale, lease or disclosure is required or permitted by a federal or State law. Or

(3) The sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose.

b. A governmental entity that possesses a biometric identifier of an individual shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental entity stores, transmits, and protects other confidential information.

c. A governmental entity that possesses a biometric identifier of an individual shall establish a reasonable procedure under which an individual is entitled to have the governmental entity correct information about the individual that is possessed by the governmental entity and that is incorrect. The procedure shall not unduly burden an individual using the procedure.

d. A person aggrieved by a violation of this section may bring an action in the Superior Court, to enjoin further violation and to recover the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.

e. Information compiled pursuant to this section shall not be subject to disclosure pursuant to P.L.1963, c. 73 (C.47:1A-1 et seq.) as amended and supplemented.

5. This act shall take effect immediately.

STATEMENT

This bill, the "Biometric Identifier Privacy Act," provides guidelines for the use and distribution of biometric identifiers and establishes civil penalties for the misuse of the information.

A biometric identifier is a retina or iris scan, fingerprint, voiceprint, or record of a hand or a face geometry. Biometrics technology is a non-invasive method of using computer technology to provide automatic identification or identity verification or authentication of individuals. The technology acquires an image of a physical feature which is then applied to the algorithm to produce a "template." This "template" is then encrypted for data transmission and storage. This stored "template" can then be stored and compared against the live "template" when necessary. This technology is being used for criminal identification as well as in airport security systems, border clearances and for transaction verifications in internet businesses. It is the sponsor's intent to protect the users of this technology by insuring that this data is not obtained, disclosed, misused or released without an individual's authorisation.

Under the provisions of the bill a person cannot obtain another individual's biometric identifier information, for the purpose of commercial advantage, without authorisation from that individual. The bill prohibits a person who possesses a biometric identifier of another individual from selling, leasing, or otherwise disclosing this information unless: the individual consents to the sale, lease or disclosure; the sale, lease or disclosure completes a financial transaction requested or authorised by the individual; the sale, lease or disclosure is required or permitted by federal or State law; or the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose. A person who possesses a biometric identifier of an individual would be required to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which that person stores, transmits, and protects other confidential information. The bill provides that any person who violates the provisions of the act would be liable for a civil penalty of not more than USD 25,000 for each violation. The Attorney General or county prosecutor would bring the action to collect or enforce the penalty in Superior Court. Furthermore, the bill provides that any person who has been aggrieved by a violation of the act may bring an action in the Superior Court, to enjoin further violation and to recover the actual damage sustained by reasons of such violation, including costs and reasonable attorneys fees.

In addition, the bill prohibits any governmental entity which possesses a biometric identifier of an individual from selling, leasing, or otherwise disclosing the biometric identifier to another person unless: the individual consents to the sale, lease or disclosure; the sale, lease or disclosure is required or permitted by a federal or State law; or the sale, lease or disclosure is made by or to a law enforcement agency for a law enforcement purpose. A governmental entity that possesses a biometric identifier of an individual would be required to store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the governmental entity stores, transmits, and protects its other confidential information. The bill also requires the governmental entity to establish a reasonable procedure under which an individual is entitled to have the governmental entity correct information about the individual that is possessed by the governmental entity and that is incorrect. The procedure cannot be unduly burdensome.

ANNEXE II – PRIVACY ARCHITECTURE AND THE PIA
(texte anglais uniquement)

Privacy Impact Assessment – Obligation or Opportunity: The Choice is Ours!

Peter Hope-Tindall

Prepared for CSE ITS Conference – Ottawa, Ontario – May 16th, 2002

The Privacy Impact Assessment (PIA) has become the favoured tool for the identification of privacy risks in proposed government and private sector initiatives. Indeed, in Canada, federal and provincial funding requirements mandate the production of some form of a PIA before work begins on a new technology, program or initiative. This has, unfortunately, reinforced a 'compliance mentality' view of the PIA as yet another hurdle to be overcome in the already cumbersome project and funding process.

Usually, at the funding submission or project approval stage, work has not progressed beyond the contextual and conceptual layers of system design, and in some cases certain elements in the contextual and conceptual layers will remain incomplete or subject to change.

The risk associated with producing a thorough PIA at project initiation time, is that the further down the design layers we travel (i.e. the closer to implementation) the less relevant the PIA may become; in fact, once enumerated in the PIA, risk factors may be thought of as 'documented and dealt with' even though an obvious correction or change exists either in policy or within a specific architecture layer which could mitigate the problem.

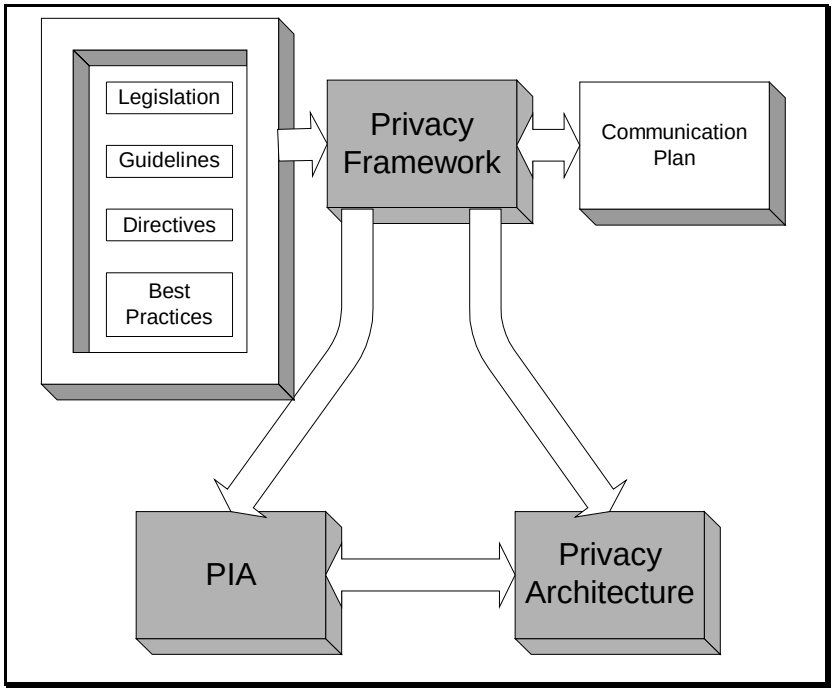
There is a substantial risk that a PIA may become an apology for the privacy shortcomings of a contemplated system and not an article for correction and change of the identified problems.

While it is important to document and evidence the due diligence in support of the quest for privacy, all too often, the main purpose of the PIA is to communicate the privacy risks to other parties (frequently, ***only*** the Privacy Commissioner) and to sit on a shelf gathering dust; a paperweight in which we can take solace – knowing that we have complied with the requirement to produce a PIA.

The author believes that another model exists, one in which the PIA can attain its lofty goals, one in which the PIA can be transformed from an apology into an authoritative text, from an obligation into an opportunity.

The author proposes a privacy triumvirate, a three-headed creature that addresses legislation, policy and technology. These components are 'Privacy Framework', our old friend the Privacy Impact Assessment 'PIA' and 'Privacy Architecture'.

Figure 1a. **The 'three-headed privacy creature'**



The Privacy Framework contains many of the introductory and general provisions that appear in a traditional PIA. Usually, the context and metrics used for a traditional PIA are somewhat abstract. They consist of legislation, guidelines and directives, and in the case of the private sector, corporate policies and mission statements. It is simplistic and ineffective to suggest that a common application and equal weighting of these metrics will fit all new technologies, programs or services. This approach is somewhat arbitrary in that it is a measurement 'in a vacuum' against the same standard for all projects.

Instead, the author believes that these inputs should be used to synthesise a unique 'Privacy Framework' from among these various privacy imperatives. The customised Framework will allow the PIA and the Privacy Architecture to emphasise the important over the less important, to allow measurements and decisions to be made in the proper context and to facilitate solutions to problems instead of focusing on merely documenting issues.

The Privacy Framework allows for a customisation of the privacy drivers, tailored to fit the risk profile and specifics of a given project. This recognises that while for many projects the drivers will be identical (and by no means are we advocating an opportunistic 'situational ethics' view of privacy; moving the goal posts so the team can score) in some cases unique features of the program or technology will raise unique issues. Examples such as smart cards and projects utilizing biometrics easily come to mind.

Best practices from other jurisdictions and an environmental scan of technology issues or solutions related to the initiative can be placed in the Privacy Framework, a placeholder for reference material for the steps below.

If properly constructed the Privacy Framework will serve as a kind of 'Privacy Constitution' for the PIA and Privacy Architecture, it will justify them and serve as an introduction to both of these other components. An additional benefit is realised, in that a comprehensive document is available for early submission with project funding requests and approval; and for early review by the Privacy Commissioner or oversight body. The importance of this demonstration of early good faith should not be underestimated.

Once the Privacy Framework has been crafted, it can be used to deliver consistent messaging and communications to all stakeholder groups, ***not just the Privacy Commissioner***. It can clearly communicate the privacy priorities and emphasis that a government or institution places on a given initiative. In many cases, it is this lack of effective communication that ultimately dooms a project in the face of a cynical public or vocal opposition from opposition groups.

The PIA allows us to fully explore the policy and non-technical elements of a proposed system as well as document the impact of technical design elements woven into the Privacy Architecture. The component contains the bulk of what most could consider a traditional PIA; a detailed review of the proposed system or project and a data flow and an impact analysis. Operating in support of the Privacy Framework it responds with policy changes; administrative controls; and recommendations for new legislation and directives. Many issues which are identified will be handed to the Privacy Architecture for solution.

It is important that the PIA be both active and responsive. Active in that opportunities for the introduction of privacy enhancing policies (which will tend to introduce elements of consent and individual control) are sought out; responsive in that compensating policy and legislative changes are introduced in response to issues raised during design, from the Privacy Architecture, and from difficulties encountered during implementation.

The Privacy Architecture allows us to truly build 'privacy into the design'. Operating in support of the Privacy Framework (as does the PIA) it responds with architecture improvements instead of policy changes; with technological controls instead of administrative controls; with hardware instead of laws and directives.

At the appropriate stage, as an addition to the communication plan, the Privacy Architecture allows us to communicate to external privacy stakeholder groups (*e.g.* the Privacy Commissioner, oversight and certification bodies) examples of our focus on the importance of privacy at the design stage.

More importantly however, the bringing together of all technical privacy components in a single book within the Privacy Architecture is an opportunity to allow technical problems identified in the PIA to be overcome and to allow technical problems identified in other architecture areas (Security, Network, Application, Technical) to be overcome. There may also be policy or other issues identified within the Privacy Architecture that will be passed back to the PIA for a policy or other non-technical solution.

It is important that the Privacy Architecture be both active and responsive. Active in that opportunities for the introduction of privacy enhancing components (which will tend to introduce elements of consent and individual control) are sought out; responsive in that compensating technical components are introduced in response to issues raised during design, from the PIA, and from fundamental policy decisions.

The reader should be cautioned that the PIA and Privacy Architecture will never be 'fully completed'. They will approach completion as the project is implemented, but the necessary steps of follow-up review and audit will remain ongoing for the duration of the project or system lifetime. Indeed, it is not uncommon for privacy issues in system design and policy review to arise only ***after*** a live system is up and running; the privacy regime employed ***must*** be flexible enough to allow a response in this situation.

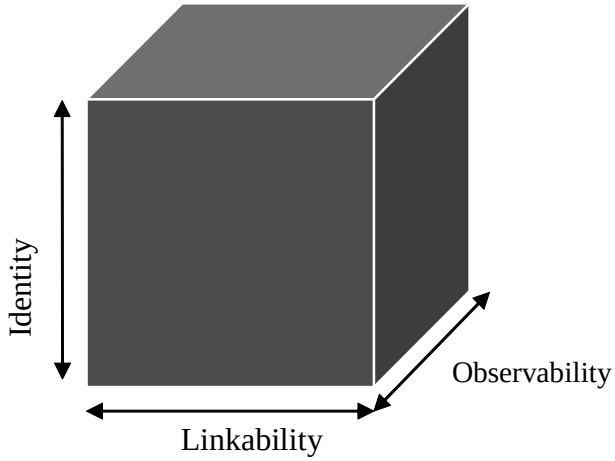
Metrics – How do we measure success?

With the PIA and the Privacy Architecture focused on finding solutions instead of documenting issues, we must now be able to measure the privacy impact of each possible solution somewhat objectively; to allow us to choose one solution over another.

The author proposes a three dimensional privacy metric to allow this measurement to be made somewhat, although not completely objectively.

The three dimensions are Identity, Linkability and Observability:

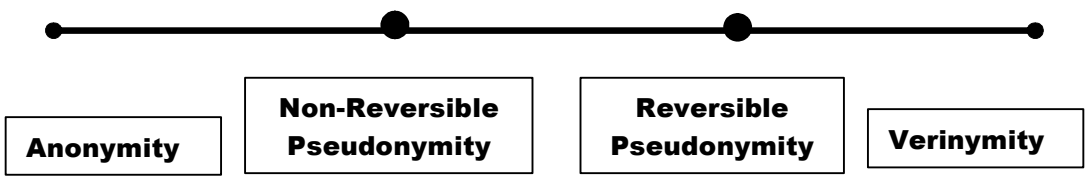
Figure 2a. **Three dimensions privacy measurement**



Identity (or nymity)

Measures the degree to which information is personally identifiable.
The Identity measurement takes place on a continuum, from full anonymity (the state of being without name) to full verinymity (being truly named).

Figure 3a. **Identity measurement**



The goal of the Privacy Architect and the PIA author is always to decrease the amounts of identity in a given system. A minimalist design approach should be employed and if identity data is not required, it should be intentionally removed from the architectural equation. Many tools employing reversible and non-reversible pseudonymity are available for this purpose. These identity tools are among the primary tools used by the workmen and workwomen known as 'Privacy Architects'.

Linkability

Measures the degree to which data elements are linked to each other. (Identity measurement can be thought of as the degree to which data elements are linkable to the verinym or true name of the data subject).

The requirements for unlinkability are intended to protect the user against the use of profiling of operations. For example, when a telephone smart card is employed with a unique number, the telephone company can determine the behavior of the user of this telephone card. Hiding the relationship between different invocations of a service or access of a resource will prevent this kind of information gathering.

Unlinkability requires that different operations cannot be related. This relationship can take several forms. For example, the user associated with the operation, or the terminal which initiated the action, or the time the action was executed.

The primary solution to linkability is generally the token-based approach, with an awareness of other factors [(time, location, message contents (which we refer to as observability)] which could also tend to allow transactions to be linked. In addition, approaches such as message padding and 'salting' are employed to prevent data matches.

Observability:

Measures the degree to which identity or linkability may be impacted from the use of a system.

These three metrics cannot provide an abstract measurement (unless some external reference standard is developed) however; they allow us to make a relative measurement comparing one solution to another. In all cases, the goal for the Privacy Architect and the PIA author is to minimise identity, minimise linkability and minimise observability.

While no system design or project implementation can be perfect, we believe that a balanced approach such as that advocated above will allow a government or institution to not only realise the best, most privacy protective solution for their proposed system; but will easily ***demonstrate*** that they delivered the ***very best possible*** solution.

Our approach of emphasising solutions over issues, while accepting that some issues may unfortunately remain unresolved, is clearly preferred to a process that simply documents and leaves all issues unresolved.

The key to a successful and privacy enhancing implementation is the recognition that three crucial areas need to be addressed; legislation, policy and technology.

ANNEXE III – DNA-BASED TECHNOLOGIES
(texte anglais uniquement)

DNA

DNA identification

DNA or deoxyribonucleic acid, is perhaps thought of as the ultimate identifier. At the heart of DNA identification is the human genome itself. Each person carries a unique genetic code, a sequence of over 3 billion nucleic acid base pairs – adenine (A), cytosine (C), guanine (G), and thymidine (T).

Every cell of a human body contains its own copy of that person's complete genetic code, determined at conception – a code that is different for every person on the planet, (with the exception of identical twins). Unlike fingerprints, there's no way to change a person's DNA by surgery or by cutting off the person's hands.

Today, this testing has three primary uses:

Paternity and sibling testing (verification of genetic provenance).
Identification of blood, semen and tissue samples left at crime scenes.
Identification of human remains.

Yet, while DNA identification appears powerful, and in fact is very effective at ***excluding*** an individual from a given match, the system suffers from a fundamental flaw. The problem is that, unlike fingerprints, not everybody's DNA is unique; as noted above – identical twins, by definition, share the same genetic pattern. And identical twins (also known as monozygotic twins) are fairly common; Identical twins happen in about 1 of every 250 births.[1] The incidence of identical twin pregnancies is very similar for all races and age groups. Adopting DNA as a sole identification system would instantly create millions of potential false matches.

Over the past decade, DNA identification has also worked its way into thousands of court cases. The test is thought to be ideal for crimes where no fingerprints are found, and needs only tiny amounts of genetic information for success. Even so, further research and scientific verification is needed to ensure that DNA identification is as accurate as commonly perceived by the average person. Some have suggested that a PIN or password could be used to differentiate between two identical twins; the belief among security experts is that this solution is not appropriate, as it relies too heavily upon the agreement and participation of the individuals involved. Two identical twins in collusion could easily defeat such a system. However, other biometrics could be used to successfully differentiate identical twins, or those that

1 Ventura, Stephanie *et al.* (1999), "Births: Final data for 1999", National Vital Statistics Reports, Vol. 49, No. 1, Centers for Disease Control and Prevention, www.cdc.gov/nchs/data/nvsr/nvsr49/nvsr49_01.pdf, consulté le 20 avril 2004.

because of coincidence or family genetic make-up have similar DNA (iris patterns for example are different between identical twins and in fact between the two eyes of a given individual).[1]

Existing applications

Many jurisdictions have forensic identification databases containing DNA samples. Some jurisdictions also have mandatory procedures to deposit the DNA of convicted criminals into their DNA database for matching against DNA material recovered from unsolved crimes. Supporters of these systems note that DNA identification is vital in the solution of some cases.[2]

An extremely large DNA identification databank has been constructed by the US Department of Defense (DoD). The purpose of the Department of Defense DNA Registry is to identify the remains of lost soldiers. As of 2001, the Registry's Specimen Repository had an estimated 3.5 million DNA specimens.

According to a written statement about the repository that appeared on the DoD's Web site:

> The blood is placed on special cards with the service member's Social Security number, date of birth, and branch of service designated on the front side of the card. On the reverse side of the bloodstain card are a fingerprint, a bar code, and signature attesting to the validity of the sample. Ultimately, the bloodstain card is stored in a vacuum-sealed barrier bag and frozen at -20 degrees Celsius, in the Specimen Repository. The oral swab (buccal scraping) is fixed in isopropanol and stored at room temperature. Great care is taken to prevent the possibility of error from sample switching or mislabeling.[3]

Many other DNA storage systems exist, but are not presently being used for identification purposes. These include research databases, blood banks and tissue storage facilities. In spite of the fact that these systems are not ***primarily*** identification systems, care should be taken in the design, architecture and policy development of these systems since the potential exists for new technology to allow these DNA samples to be used to profile and identify individuals.

1 Daugman, J and Downing, C (2001) "Epigenetic randomness, complexity, and singularity of human iris patterns." Proceedings of the Royal Society, B, 268, Biological Sciences, pp 1737 – 1740.

2 *The Toronto Star* (2003), "DNA links sex attacks", 20 February.

3 US DOD - Armed Forces DNA Identification Laboratory.

ANNEXE IV – BIOMETRIC ENCRYPTION
(texte anglais uniquement)

Biometric encryption[1]

As indicated earlier in this paper,[2] some consider ***any*** use of template based biometrics to be potentially privacy invasive. A potential (although not commercially available) solution to the creation of a unique identifier lies in a technology known as 'Biometric Encryption'. In biometric encryption the biometric is used as a key to encrypt and decrypt, but no copy of the biometric sample or template is retained.

Dr. Tomko coined the term 'biometric encryption', in conjunction with a number of US patents that were issued to Dr. Tomko and his various co-inventors between 1994 and 2000.[3] To quote from a presentation supplied to the author directly by Dr. Tomko:

> "The prevailing biometric model, based on retention of the biometric template, is not the only option available. Biometric technology can also be designed as a liberating technology, with the potential to actually enhance privacy, and also, in the process, advance the security associated with public safety. The key is to make the biometric, such as your finger print, the actual encryption key – your own private key, which is never stored anywhere, other than on your finger – that's where it belongs, from a privacy perspective. I call this biometric encryption.
>
> In biometric encryption, you can use the biometric to encrypt a PIN, a password, or an alphanumeric string, for numerous applications – to gain access to computers, bank machines, to enter buildings, etc. The PINs can be 100s of digits in length; the length doesn't matter because you don't need to remember it. And most importantly, all one has to store in a database is the biometrically encrypted PIN or password, not your biometric template."

To understand how biometric encryption works, we first need to look at the functioning of a traditional biometric system. In a traditional biometric system, a template or set of features, or an image is extracted from a biometric sample and stored somewhere in a database. This storage could be in a centralised database or it could be a distributed storage medium such as a smart card. During identification and verification, a comparison is performed between the live person and the stored biometric template.

With biometric encryption we do not store any form of biometric whatsoever, no biometric sample is stored; no biometric template is stored. Instead the biometric sample or template is used as a symmetric encryption and decryption key to cryptographically transform some other piece of information.

---

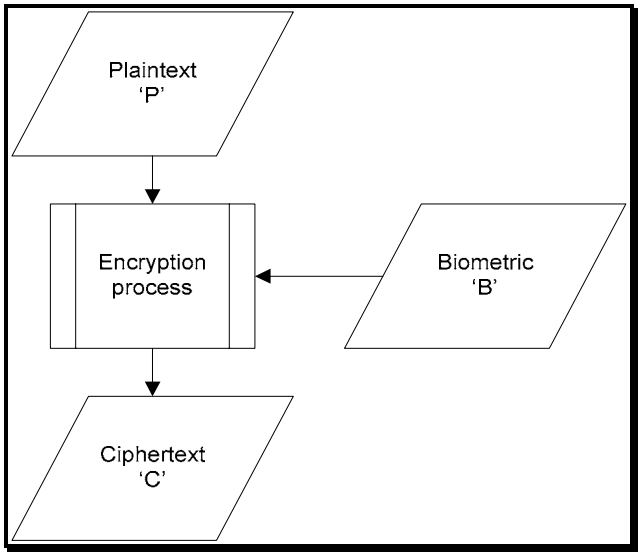
1 There is a pending trademark application on behalf of Bioscrypt Inc. for the term *Biometric Encryption*. (http://strategis.ic.gc.ca/SSG/0806/trdp080643600e.html, consulté le 20 avril 2004).

2 See Tomko, 2002.

3 The US Patents' numbers directly relevant to biometric encryption are: 5,541,994; 5,680,460; 5,712,912; 5,737,420; 5,740,276; 5,832,091.

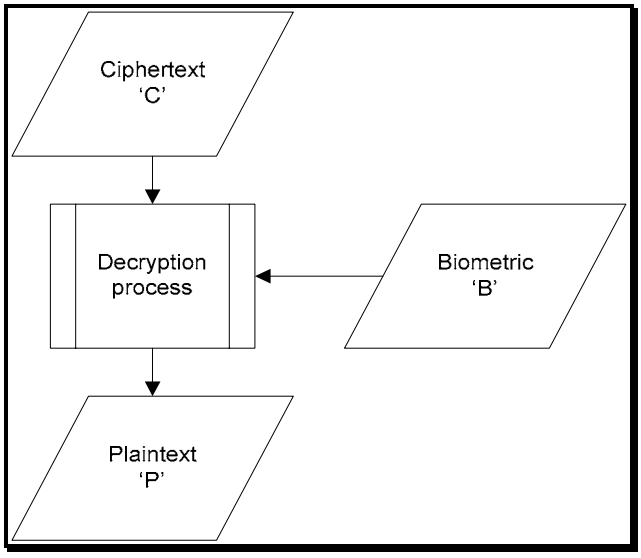
When a user enrols, his biometric is used to encrypt a piece of information (it could be any piece of information, an account number, a text string or a credential of some kind). If we call this piece of information 'P', then plaintext 'P' will be transformed into ciphertext 'C' using the biometric 'B'. This ciphertext is now stored in the biometric encryption system (see Figure 1b). Note, after the encryption process the biometric 'B' is deleted and is ***not stored*** anywhere.

Figure 1b. **Biometric encryption enrolment**



When a user identifies or verifies, his biometric is used to decrypt the ciphertext that was stored during enrolment. Ciphertext 'C' will be transformed into plaintext 'P' using the biometric 'B' (see Figure 2b).

Figure 2b. **Biometric encryption verification**



The correct user is the ***only person*** who possesses the correct key (his or her biometric) and will be the ***only person*** who can correctly complete the decryption process.

It is challenging to implement this encryption and decryption step, given that each biometric sample or template is distinct for each extraction. We need, what some have referred to as, 'fuzzy encryption' and 'fuzzy decryption'. Interestingly, a solution may be found in technology used to fight spam. 'Nilsimsa Signatures'[1] are fuzzy signatures used to recognise message content as spam, they are able to disregard small changes in text that are statistically insignificant (since spammers will tend to attempt to disguise there messages once they recognised by making changes to the message content). In the same way Nilsimsa signatures may allow us to recognise a biometric which is slightly different each time the user interacts with a system.

Ultimately, biometric encryption does present us with both a key management benefit and a key management problem. While a user can never lose or forget his key (since it literally lives on his body) neither can he effectively 'revoke' a key should it become compromised. This very practical challenge remains to be addressed in the design of biometric encryption.

While biometric encryption would seem to offer a solution to the majority of privacy concerns related to biometric-based technology, it is not, unfortunately, readily available to deploy today.

A number of companies hold patents and have prototype technology and systems based on these patents, but the author is not aware of any ongoing research to bring these systems to market.

1 Voir *Vipul's Razor*, www.brics.dk/~engberg/usr_local_doc/razor-agents-shr-2.36/README, consulté le 20 avril 2004.