29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Séance plénière
Dragon : *Quand la loi rencontre la technologie*
La nanotechnologie et la protection de la vie privée (*Séance en français)*

Plenary
"*Law Meets Technology*" Dragon
Nanotechnology and Privacy
(*French Plenary*)

26 septembre/September 26
11h15 – 12h15

Série Terra Incognita, cahier de travail # 2/Terra Incognita, workbook series # 2

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Table des matières / Table of contents

Biographies

M^e Jacques Saint-Laurent—Président 2

M. Alex Türk 2

M. Hervé Fischer 3

M. Joel R. Reidenberg, Ph. D. 3

M. Bernard Sinclair-Desgagné, Ph. D. 4

Le contrôle invisible 6

Les nanotechnologies et le plan national américain de recherche et de développement pour la protection des infrastructures critiques 18

Biographies

M^e Jacques Saint-Laurent — Chair 2

Mr. Alex Türk 2

Mr. Hervé Fischer 3

Dr. Joel R. Reidenberg 3

Dr. Bernard Sinclair-Desgagné 4

Invisible Surveillance 6

Nanotechnology and the United States National Plan for Research and Development In Support of Critical Infrastructure Protection 32

Biographies

Président : M^{e} Jacques Saint-Laurent

En octobre 2004, l'Assemblée nationale du Québec a nommé, à l'unanimité, M^{e} Jacques Saint-Laurent membre et président de la Commission d'accès à l'information du Québec. Son mandat est de cinq ans. Le président est responsable de la direction et de l'administration de l'organisme québécois en charge de la protection des données personnelles dans les secteurs public et privé ainsi que de l'accès aux documents administratifs des organismes publics. À titre de juge administratif, M^{e} Saint-Laurent a rendu diverses décisions concernant des demandes de révision ou d'examen de mésentente dont la Commission doit disposer. Il a également présidé de nombreuses séances de la Commission qui ont donné lieu à des avis en matière d'accès aux documents et de protection de la vie privée. Depuis septembre 2006, M^{e} Saint-Laurent est membre du groupe de travail constitué afin de voir à la création de l'Association des autorités francophones de la protection des données personnelles. M^{e} Saint-Laurent est avocat depuis 1976. Il a été sous-ministre adjoint et Directeur de l'état civil du Québec de 2001 à 2004. Après cinq ans en pratique privée, il fut notamment directeur des Bureaux de révision paritaires à la Commission de la santé et de la sécurité du travail, directeur des affaires juridiques des ministères de la Sécurité publique puis des Ressources naturelles. De 1995 à 2001, il dirigea les 25 procureurs du contentieux du ministère de la Justice à Québec.

Conférenciers

M. Alex Türk

Alex Türk est président de la Commission nationale de l'informatique et des libertés (CNIL) depuis le 3 février 2004. Membre de la CNIL depuis 1992, il en a été le vice-président de 2002 à 2004. Dans le cadre de ses fonctions, Alex Türk a été élu président de l'autorité de contrôle Schengen (1995-1997), président de l'autorité de contrôle commune (ACC) d'Europol (2000-2002) et de l'autorité de contrôle d'Eurodac (2003). Il est actuellement vice-président du groupe de travail dit "de l'Article 29" depuis février 2007. Alex Türk a été élu sénateur du Nord en septembre 1992 (non-inscrit), puis réélu en septembre 2001. Il est

Biographies

Chair : M^{e} Jacques Saint-Laurent

In October 2004, the Quebec National Assembly unanimously appointed Jacques Saint-Laurent for a five-year term as member and Chair of the Quebec *Commission d'accès à l'information*. As Chair, Mr. Saint-Laurent is responsible for the oversight and management of the *Commission*, which is charged with the protection of personal data in the public and private sectors and with ensuring access to documents held by public agencies. As an administrative judge, Mr. Saint-Laurent has rendered a range of decisions on requests for the review and examination of disputes that fall under the Commission's jurisdiction. He has also chaired many Commission sessions, providing expert advice on access and privacy. Since September 2006, Mr. Saint-Laurent has been a member of the working group responsible for establishing the Association des autorités francophones de la protection des données personnelles, an association of Francophone data protection authorities. Mr. Saint-Laurent was called to the Quebec bar in 1976. Following five years in private practice, he held various positions including Director of the Bureaux de révision paritaires at the *Commission de la santé et de la sécurité du travail* and Director of Legal Affairs at the *Ministère de la Sécurité publique* and then at the Ministère des Ressources naturelles. From 1995 to 2001 he oversaw the 25 prosecutors at the Ministère de la Justice in Quebec City. He was Assistant Deputy Minister and Registrar of Civil Status from 2001 to 2004.

Speakers

Mr. Alex Türk

Alex Türk was elected as President of the Commission nationale de l'informatique et des libertés (CNIL) on February 3, 2004. He was initially appointed as member of the CNIL in 1992. He was the CNIL Vice-President from 2002 to 2004. In his capacity as CNIL member, Alex Türk was elected Chairman of the Schengen Joint Supervisory Authority (1995-1997), Chairman of the Europol JSA (2000-2002) and of the Supervisory Authority of Eurodac (2003). He has been vice-President of the Article 29 Working Party since February 2007. Alex Türk was elected as a member of the French Senate on September 24, 1992. He was re-

membre de la Commission des lois et membre de la Délégation pour l'Union européenne du Sénat. Il est également conseiller général du canton de Lille-centre depuis 2001. Alex Türk est également maître de conférences de droit public à l'Université de Lille II et chargé de cours à l'Institut d'études de sciences politiques et à l'Université catholique de Lille.

M. Hervé Fischer

Hervé Fischer enseigne à la Faculté des arts de l'Université du Québec à Montréal, où il a mis sur pied l'Observatoire international du numérique (www.oinm.org). M. Fischer, qui possède la double citoyenneté canadienne et française, a étudié à l'École normale supérieure de la rue d'Ulm. Il a été maître de conférence à l'Université Sorbonne‑Paris V, et il a été nommé titulaire de la chaire de la fondation Daniel Langlois en technologies numériques et en beaux‑arts à l'Université Concordia de Montréal (2000). Il est aussi responsable de la création du Media Lab du Québec, Hexagram.
Il a publié une dizaine de livres en France, au Canada et en Amérique latine, parmi lesquels :
CyberProméthée, l'instinct de pouvoir, VLB éditeur, 2003;
Les défis du cybermonde (direction), PUL, 2003;
La planète hyper, de la pensée linéaire à la pensée en arabesque, VLB éditeur, 2004;
Le déclin de l'empire hollywoodien, VLB éditeur, 2004;
Nous serons des dieux, VLB éditeur, 2006;
La société sur le divan. Éléments de mythanalyse, VLB éditeur, 2007.

M. Joel R. Reidenberg, Ph. D.

Joel R. Reidenberg est professeur de droit et ancien directeur du programme d'études supérieures en droit à la Fordham University School of Law. Il donne des cours de droit concernant la confidentialité des renseignements et la technologie de l'information, la propriété intellectuelle et le commerce international. M. Reidenberg a occupé divers postes à l'Université de Paris (Panthéon-Sorbonne et René Descartes) et aux laboratoires AT&T – recherche sur les politiques publiques. Il est expert en matière de droit et de politiques de gestion de l'information, et coauteur de livres et de monographies de premier plan sur des questions

elected in September 2001. He belongs to the Law Commission and to the EU Delegation of the Senate. He was elected as a Counselor of the Lille-centre County Council in 2001. Alex Türk, Ph.D., teaches public law at Lille II University. He is a lecturer at the Institute of Lille Political Science Institute and Catholic University.

Mr. Hervé Fischer

Hervé Fischer is a professor at the Faculty of Arts of the Université de Québec à Montréal where he established the International Digital Observatory (Observatoire international du numérique, www.oinm.org). A dual Canadian/French citizen, Mr. Fischer is a former student of the Ecole normale supérieure de la rue d'Ulm, was senior lecturer in sociology at the Sorbonne-Paris V, holder of the Daniel Langlois Chair in digital technology and fine arts at Concordia University in Montréal (2000), and responsable for establishing the Quebec media lab, Hexagram.
He has published a dozen books in France, Canada and Latin America, among them:
CyberProméthée, l'instinct de pouvoir, vlb éditeur, 2003;
Les défis du cybermonde (direction), PUL, 2003;
La planète hyper, de la pensée linéaire à la pensée en arabesque, vlb éditeur, 2004;
Le déclin de l'empire hollywoodien, vlb éditeur, 2004;
Nous serons des dieux, vlb éditeur, 2006;
La société sur le divan. Éléments de mythanalyse, vlb éditeur, 2007.

Dr. Joel R. Reidenberg

Joel R. Reidenberg is Professor of Law and a past Director of the Graduate Program in Law at Fordham University School of Law . He teaches law courses in information privacy and technology, intellectual property and international trade. Reidenberg has held appointments at the Université de Paris (Panthéon-Sorbonne and René Descartes) and at AT&T Laboratories - Public Policy Research. Reidenberg is an expert on information technology law and policy. He is co-author of leading books and monographs on international data privacy issues and Internet regulation. He has testified before the U.S. Congress on data privacy issues, consulted to both the Federal

internationales relatives à la confidentialité des données et la réglementation d'Internet. Il a témoigné sous serment devant le Congrès américain en ce qui concerne des questions de confidentialité des données, et tant la Federal Trade Commission que la Commission européenne l'ont consulté sur certaines questions liées à la protection des renseignements personnels. Avant son arrivée à Fordham, M. Reidenberg exerçait le droit à Washington D.C. et faisait partie de plusieurs groupes d'experts de l'Office of Technology Assessment. Il est titulaire d'un baccalauréat ès arts du Dartmouth College, d'un diplôme conjoint de la Columbia University et d'un diplôme d'études approfondies (DEA) en droit international économique et d'un doctorat en droit de l'Université de Paris. Il est membre des barreaux de New York et du district de Columbia.

M. Bernard Sinclair-Desgagné, Ph. D.

Bernard Sinclair-Desgagné est actuellement professeur titulaire de la Chaire d'Économie internationale et de gouvernance à HEC Montréal et co-titulaire de la *Chaire* « Électricité de France » de Développement durable à l'École polytechnique de Paris. Il détient un doctorat en économie managériale de l'Université Yale, et a enseigné successivement à l'INSEAD et à l'École polytechnique de Montréal avant de se joindre à HEC Montréal, en 2001. Ses principaux champs de recherche et d'expertise sont l'analyse économique des organisations, l'économie de l'environnement et la gestion du risque technologique. Ces sujets ont fait l'objet de publications dans des revues scientifiques importantes, comme *Econometrica* et *Management Science*. M. Sinclair-Desgagné a aussi travaillé comme consultant auprès de plusieurs organismes gouvernementaux. En 2004, en reconnaissance de la qualité de ses travaux scientifiques, il a été élu *Fellow* de la *European Economic Association*. En décembre 2006, il a reçu le *Prix européen de la recherche* « Finance et développement durable » pour son article intitulé « On precautionary policies », qui décrit de manière pratique les politiques de précaution.

Trade Commission and the European Commission on privacy issues, Prior to coming to Fordham, Reidenberg practiced law in Washington, DC and was a member of several Office of Technology Assessment panels. He holds an A.B. degree from Dartmouth College, a J.D. from Columbia University, and a D.E.A. droit international économique and a Ph.D in law from the Université de Paris. He is admitted to the Bars of New York and the District of Columbia.

Dr. Bernard Sinclair-Desgagné

Bernard Sinclair-Desgagné is currently the International Economics and Governance Professor at HEC Montréal and "Électricité de France" Sustainable Development Co-chair at the École Polytechnique in Paris. He holds a Ph.D. in managerial economics from Yale University and taught first at INSEAD and then at the École polytechnique de Montréal before joining HEC Montréal in 2001. His main fields of research and expertise are the economic analysis of organizations, environmental economics and technological risk management, and he has published articles on these subjects in major scientific journals such as *Econometrica* and *Management Science*. Dr. Sinclair-Desgagné has also worked as a consultant with a number of government agencies. In 2004 he was elected Fellow of the European Economic Association in recognition of his scientific work. In December 2006 he received the "Finance and Sustainability" European Research Award for his article "On Precautionary Policies," which gives a practical view of precautionary policies.

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE

TERRA INCOGNITA

PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Le contrôle invisible

Invisible Surveillance

Par/by:

Hervé Fischer

Office of the Privacy Commissioner of Canada

Commissariat à la protection de la vie privée du Canada

Le contrôle individuel instauré par la société et ses institutions publiques était traditionnellement visible et annoncé par des objets matériels, tels que barrière, guichet, poste de douane, de péage, caisse, signalisation, sonnerie d'alarme, cadran ou borne de contrôle, ou par des employés tels que : agent de police, enquêteur, contrôleur. Ses outils aussi étaient visibles et familiers : carte d'identité, passeport, ticket, badge, plaque et numéro d'immatriculation, uniforme, casquette, brassard, permis, etc. Seul le contrôle des consciences ou des âmes demeurait invisible, comme les esprits et les dieux qui y veillaient. C'est tout cet ensemble de procédés visibles qui est actuellement remplacé et exponentiellement complété par des technologies numériques de plus en plus puissantes et d'autant plus inquiétantes qu'elles deviennent invisibles.

Le panoptique numérique

C'est au philosophe anglais utilitariste Jeremy Bentham (1748 – 1832) que nous devons le « principe panoptique » – du grec : voir partout. Il l'a appliqué à un modèle de prison qu'il a inventé en 1791, et dont le bâtiment circulaire permettait à un seul gardien, situé en son centre, de contrôler visuellement d'un seul regard circulaire toutes les prisons, lesquelles devaient demeurer éclairées (1). Du fait qu'il est lui-même dans l'obscurité, et donc que les prisonniers ne le voient pas, le gardien exerce virtuellement une constante surveillance à distance, même s'il est inactif.

L'avantage évident du dispositif, du point de vue de la surveillance, outre sa rationalité architecturale et bureaucratique, est qu'il incitait les prisonniers à craindre d'être vus, et donc à s'abstenir de tout comportement interdit, même si le gardien était absent, puisque la surveillance était devenue invisible et donc virtuellement constante. Or, c'est aujourd'hui que ce concept inspiré de bonnes intentions d'économie des deniers publics, trouve son application générale la plus extensive et efficace, grâce aux technologies numériques. À une différence près, qui est considérable : celle de ses effets pervers, puisqu'il s'applique désormais de plus en plus à tous les citoyens sans distinction, comme si nous étions tous présumés coupables. C'est pour cela que je l'ai appelé le « panoptique numérique » (2).

Personal monitoring by society and its public institutions was traditionally visible and signalled by physical objects such as barriers, wickets, border crossing points, tollbooths, cash collection points, signage, alarms, checkpoints, or by employees like police officers, investigators, and ticket takers. The tools were also visible and familiar: ID cards, passports, tickets, badges, licence plates and numbers, uniforms, caps, arm bands, permits, licences, etc. Only control over people's consciences or souls remained invisible, like the spirits and the gods who watched over them. This whole set of visible procedures is currently being replaced and complemented exponentially by increasingly powerful digital technologies that are becoming more worrisome as they become less visible.

The Digital Panopticon

We owe the "panoptic principle" to English utilitarian philosopher Jeremy Bentham (1748 – 1832) – the word is from the Greek, meaning: all-seeing. He applied it to his concept of a model prison, which he invented in 1791, whose circular building made it possible for a single guard, located in the centre, to visually scan in a single circular gaze, all of the cells, which would have to remain lighted (1). Because the guard himself is in the dark, and the prisoners cannot see him, he can maintain virtually constant surveillance at a distance, even when he is inactive.

The obvious advantage of the device from the surveillance standpoint, in addition to its architectural and bureaucratic rationality, is that it led the prisoners to fear being seen, and hence to refrain from any prohibited behaviour, even if the guard was not there, because the surveillance had become invisible and thus virtually constant. Today, however, this concept, which was based on good intentions – economizing on public funds – is being extensively and effectively used widely thanks to digital technologies. There is nevertheless one major difference, and that is the nefarious effects that result from its increasingly indiscriminate use for all citizens, as if we were all presumed guilty. That is why I have called it the "digital Panopticon" (2).

I — Les paramètres fondamentaux du contrôle invisible

Avant d'aborder les usages sociaux des technologies numériques miniaturisées, leurs performances, leurs avantages et leurs risques en ce qui concerne la protection de la vie privée, nous tenterons ici d'en dégager les préoccupations paramètres spécifiques :

Nous soulignerons leur miniaturisation, leur convergence technologique, leur invisibilité, leur action à distance, leur généralisation envahissante, la vitesse en temps réel de leur efficacité (enregistrement et accès), la traçabilité et l'accumulation des données personnelles qu'elles permettent, la pérennité de ces données, leur exploitation par des moteurs de recherche et le croisement des données.

Miniaturisation

Parmi ces technologies les plus diverses, les micropuces, les dispositifs IRF ou identification par radiofréquence (RFID ou Radio Frequency Identification devices), grosses comme un grain de riz, ou même comme une tête d'épingle, deviennent de plus en plus petits, et donc faciles à dissimuler. Ils contiennent un circuit électronique microscopique. Ils peuvent même être implantés sur le corps humain (injection intradermique). Dans le domaine de la miniaturisation, depuis les effets cinématographiques de James Bond, on fait de mieux en mieux, avec des appareils photos et caméras miniaturisées dans un stylo, un téléphone cellulaire, la branche d'une paire de lunettes, un bouton de vêtement, etc. Les nanotechnologies permettent même d'ingérer dans le corps humain toute puce émettrice qui pourra être suivie à distance, et les progrès de la médecine y sont associés.

L'action à distance

Sous-cutanées, ou dissimulées dans l'emballage d'un objet, elles n'en contiennent pas moins un relais ondes courtes, voire un relais GPS, donc une mémoire capable d'être lue à distance, par exemple lors du passage entre deux bornes à l'entrée d'un édifice, ou même dans une rue, ou d'être repérée n'importe où par satellite. Ainsi, on peut retracer à la seconde près les déplacements d'un téléphone cellulaire – et donc de son usager. Dès qu'un téléphone cellulaire est activé, même s'il n'est pas utilisé pour des échanges par son

I – The Fundamental Parameters of Invisible Surveillance

Before considering the social uses of miniaturized digital technologies, along with their performance, benefits and risk with respect to privacy, we will attempt to highlight specific concerns:

We will highlight their miniaturization, technological convergence, invisibility, remote operation, widespread use, real-time speed and effectiveness (recording and access), the traceability and compilation of personal data they now make possible, the persistence of these data, their use by search engines and data linking.

Miniaturization

Among this wide variety of technologies, microchips, RFID or Radio Frequency Identification devices, which are the size of a grain of rice, or even the head of a pin, are becoming smaller and smaller and thus easier to conceal. They contain a microscopic electronic circuit. They can even be implanted on the human body (subcutaneous injection). From the early days of James Bond special effects, the world of miniaturization is doing better than ever, with miniature cameras and video cameras so small that they can be hidden in a pen, a cell phone, the temple of a pair of glasses, a shirt button, etc. Nanotechnology now makes it possible to have a human ingest a transmitting chip that can be remotely monitored, and all of the associated progress in medicine that this would allow.

Remote Operation

These devices, implanted subcutaneously or concealed in packaging, contain no less than a shortwave transmitter, or even a GPS relay, and memory that can be read remotely, for example, when going through a twin antenna gate at the entrance to a building, in the street, or even capable of being located anywhere by satellite. This means that someone using a cellular telephone can be precisely located almost to the second. Once the phone is on, even if it is not being used in conversation, it is automatically in contact with the relay towers of the communication system, and any use is monitored. This feature has already been used, like DNA samples, to demonstrate in court that a criminal was at the scene of a crime. Of course, this remote surveillance can also track the use of a bank card or a credit card, which can be used

porteur, il se met en contact automatiquement avec les tours relais qui en assurent l'efficacité communicationnelle, mais qui enregistrent en même temps toute prise en charge. Cela a déjà permis de démontrer en cour la présence d'un criminel sur le lieu du crime, comme le ferait un échantillon d'ADN. Bien entendu, cette télésurveillance peut exploiter tout aussi bien l'utilisation d'une carte bancaire ou de crédit, qui fonctionne par connexions Internet avec le serveur d'une banque, et garder la mémoire du lieu et du temps.

Convergence

Cette miniaturisation peut se conjuguer avec des équipements lourds à distance, avec lesquels ils sont en relais, capables d'enregistrer et d'accumuler les signaux recueillis et de les traiter. Les systèmes sans fil et Bluetooth permettent de déchiffrer le contenu d'un ordinateur ou d'un téléphone cellulaire par ondes courtes à distance, dans une voiture stationnée devant le siège social d'une entreprise ou la maison d'une personne. Il faut donc avoir conscience que ces technologies miniaturisées, déjà forts puissantes en elles-mêmes, peuvent être mises en réseau sans fil avec toutes les technologies numériques les plus puissantes et les plus avancées.

Invisibilité

On conjugue ainsi la puissance et l'invisibilité. Nous oublions facilement, de ce fait, que nous sommes sans cesse sous télésurveillance. Nous oublions les témoins (cookies) qui sont installés dans nos ordinateurs dès la sortie d'usine et ceux qui nous sont envoyés à notre insu par les serveurs Internet, capables de lire nos disques durs et de transmettre, modifier, voire détruire (virus) les contenus à distance. Et c'est sans compter les logiciels espions qu'envoient par Internet des compagnies ou des curieux, pour connaître nos navigations Internet, lire nos fichiers, contrôler leurs chargements légitimes ou illégitimes. Se brancher à l'Internet, c'est désormais prendre le risque d'installer chez soi, un espion puissant à notre insu, au cœur même de nos communications professionnelles et privées.

De même, nous ne voyons pas les dispositifs en réseau qui peuvent balayer (scanner) tous nos messages par télécopieur, Internet, téléphone. Ils sont « dans l'air numérique ». Les satellites de

through an Internet connection with a bank server, which records the place and time.

Convergence

Miniaturization can be linked by relay to remote computers that can record and store the signals that are captured and then process them. Wireless and Bluetooth systems can decrypt the contents of a computer or a cellular telephone remotely by shortwave, whether from a car parked in front of a company's head office or an individual's home. It is therefore important to be aware that these miniaturized technologies, which are already very powerful on their own, can be networked wirelessly with all of the most powerful and advanced digital technologies available.

Invisibility

Power and invisibility are being coordinated in this way. This makes it easy for us to forget that we are continually being monitored remotely. We forget about the cookies installed in our computers from the moment they leave the factory, along with those sent without our knowledge by Internet servers, which can read our hard disks and malicious software such as keystroke loggers and viruses that can transmit, modify or even destroy the contents of our hard disks remotely. Not to mention spyware, sent by companies or curious people to find out where we are navigating on the Internet, or to read our files, and monitor any legitimate or illegitimate downloads and uploads. Connecting to the Internet now means taking the risk of installing a powerful spy in your home, one at the very centre of our professional and private communications.

Similarly, we cannot see the networked devices that can scan all our fax, Internet and telephone messages. They are "in the digital ether." Completely invisible surveillance satellites can now monitor any activity here on Earth that is likely to be of interest, on a scale of only a few metres. We don't pay any special attention to discreet Webcams located in cities, on subway or bus routes, at shopping centres, along highways, all of which can record what we do and transmit it to remote surveillance centres, and which are also linked to databases and search engines capable of facial recognition, detecting atypical behaviour, and immediately reporting it to an alerting system.

surveillance – parfaitement invisibles – peuvent lire désormais au sol toute activité susceptible d'intérêt à une échelle de quelques mètres. Nous ne remarquons pas davantage les Webcams discrètes en milieu urbain, dans les réseaux de transport en commun, dans les centres commerciaux, sur les autoroutes, capables de capter nos faits et gestes et de les transmettre dans des centres de télésurveillance, mais qui sont aussi en relation avec des banques de données et des moteurs de recherche susceptibles de faire de la reconnaissance de visage, de déchiffrer des comportements atypiques et de les signaler immédiatement à un système d'alerte.

Invasion

Leur miniaturisation, comme leur invisibilité et leur polyvalence, favorisent de plus en plus leur usage dans tous les domaines des activités humaines, qu'il s'agisse, comme pour les codes-barres dont ils tendent à prendre la relève, de l'identification d'objets de consommation courante (ils sont à l'essai dans les centres commerciaux), ou de nous-mêmes, citoyens de l'âge numérique, puisqu'on tend à utiliser de plus en plus ces technologies sur nos documents d'identité, nos cartes de crédit, nos dossiers médicaux, nos objets personnels (voiture, téléphone, carte de transports en commun, de péage, professionnelles, badges, etc. Leur coût de revient est de plus en plus bas, et leur efficacité pour la gestion légitime de notre monde d'objets de consommation contamine les domaines beaucoup plus sensibles qui relèvent de la protection, elle aussi tout à fait légitime, de notre vie privée.

Vitesse et temps réel d'enregistrement et d'accès

À une époque de plus en plus soumise aux valeurs de l'efficacité, donc de la vitesse et de la gestion en temps réel, les technologies numériques répondent à nos attentes les plus folles. Des centres de surveillance à distance peuvent non seulement recevoir constamment toutes ces informations que leur livrent les dispositifs invisibles de télésurveillance, mais aussi les traiter, les classer, les croiser et les afficher en quelques secondes sur les écrans de télésurveillance. La vitesse et la puissance des serveurs avec lesquels ils sont en communication doublent tous les dix-huit mois, selon la loi de

Invasion

Miniaturization, together with invisibility and versatility, is increasing their use in virtually every area of human endeavour, whether, as for bar codes, which they are replacing, to be used to identify consumer products (they are being tested in shopping centres), or on us, the citizens of the digital age, because there is a trend towards increased use of these technologies for our ID documents, credit cards, medical records and personal items (car, telephone, public transit travel card, toll road card, business cards, badges, etc.).

The production cost is dropping rapidly, and their efficiency in legitimate uses for managing our world of consumer items is contaminating areas that are much more sensitive, such as the protection of our privacy, which is equally legitimate.

Speed and Real-Time Recording and Access

In an era that is increasingly driven by the values of efficiency, and hence speed and real-time management, digital technologies meet our wildest expectations. Remote surveillance centres can not only continually receive all the information delivered to them by invisible remote surveillance devices, but can also process it, classify it, cross-tabulate it and display it within a few seconds on remote surveillance monitors. The speed and power of the servers to which they are linked doubles every 18 months, according to Moore's Law. Google can scan billions of Web pages in a few tenths of a second. Allow me to recount the following anecdote I heard: an immigration employee at an American border crossing decided to check the name of a traveller not only in his police databases, but also via Google; he found that the traveller had admitted in a book to having used drugs. He had the person arrested, questioned, detained and turned away!

Traceability

RFIDs, the remote surveillance of messages and people by scanners, Webcams, or satellite GPSs, are all convergent devices that are very powerful because of their links to databases. They can be used not only to capture signals and information, but can also closely monitor the movements of these signals. In the agri-food industry (whether the source is a sick animal, the cold chain*, or a terrorist's cellular telephone), this traceability can be extremely useful. When ordinary citizens are

Moore. On voit que Google est capable de balayer (scanner) des milliards de pages Web en quelques dixièmes de seconde. On m'a raconté l'anecdote suivante : un employé de l'immigration aux douanes américaines a eu l'idée de vérifier le nom d'un voyageur non seulement sur ses bases de données policières, mais aussi sur Google; et y découvrant que ce voyageur avait dans un livre témoigné de son usage de drogues, il l'a fait arrêter, interroger, détenir, puis renvoyer!

Traçabilité

Les IRF (RFID), la télésurveillance des messages et des personnes par balayage (scan), par webcaméras, les GPS par satellite, sont des dispositifs convergents dotés d'une grande puissance, celle des serveurs. Ils peuvent non seulement capter des signaux et des informations, mais ils permettent aussi de suivre à la trace les déplacements de ces signaux. Dans l'industrie agroalimentaire (qu'il s'agisse de l'origine d'un animal malade, de la chaîne du froid, ou du téléphone cellulaire d'un terroriste), cette traçabilité peut être d'un grand intérêt. Lorsqu'il s'agit des citoyens, de graves questions se posent. Lorsque l'on indexe ou taggue (métadonnées invisibles) une information pour que les moteurs de recherche la retrouvent rapidement sur le Web et identifient pour nous le livre, la bibliothèque, l'année, l'auteur, etc., on développe un Web sémantique d'une grande valeur pour la recherche et l'information. Lorsque l'on taggue les chercheurs eux-mêmes, en indexant leur profil selon leurs habitudes de navigation, on peut certes les aider à trouver plus précisément et plus rapidement ce qui les intéresse. Mais on crée aussi ainsi ce que j'ai appelé l' « Hyperweb » (3), c'est-à-dire des hyper usagers au sujet desquels on accumule des informations qui sont liées à leur hyper communauté sémantique virtuelle, et qui deviennent exploitables dans le forage des données (data mining) du marketing commercial, ou pour toute chasse aux sorcières. Google pratique déjà cette méthode de l'Hyperweb, tout comme Amazon.com qui enregistre les achats de livres de ses clients, ce qui lui permet d'informer d'autres clients (B et C) qui ont acheté quelques-uns des livres que le client A s'est procuré, des autres livres qu'il a également acheté à cette occasion.

involved, some serious questions need to be asked. When information is indexed or tagged (invisible metadata) so that search engines can rapidly find it on the Web and tell us about the book, the library, the year, the author, etc. for this information, we have a semantic Web that is extremely valuable for research and information. When the researchers themselves are tagged by indexing their profiles on the basis of their browsing habits, then it is true that this makes it possible to more accurately and more quickly find what is of interest to them. But doing this also creates what I have called the "hyperweb"(3), that is to say hyperusers about whom data are stored and linked to their virtual semantic hypercommunity, and which then can be used in datamining by commercial marketers, or even for witch hunts. Google is also using this hyperweb method, as is Amazon.com, which records its customers' book purchases, and is thus able to make suggestions to other customers (B and C) who may have bought one or two of the same books as customer A, and tells them about other books that customer A has also purchased.

Data Storage and Continuity

Needless to say, the current practice, one that is difficult to prevent and even desirable in the case of medical records, is to keep records accessible well beyond the four, five or six years that data banks are often authorized to keep the data they collect about citizens going about their various activities. The trails we leave behind us in all of our consumer behaviour (credit cards), as taxpayers, at border crossings, etc., build up and can stick to us like a criminal record. It is important to remain aware of the fact that the digitized archiving of data does not pose the same challenges in terms of space as the paper records of the STASI, and such data can be accessed the very moment people want to see it.

II – Interesting Social Uses

No one can deny the convenience and efficiency of electronic money, or of the smart cards that increasingly allow us to pay for a subway trip, a bus trip or even to travel on a toll road. The cookies in our computers also greatly speed up the time it takes to display our usual files and Web sites.

We are not questioning the need for restricted ac-

Accumulation et pérennité des données

On aura compris que bien au-delà des quatre, cinq ou six années souvent autorisées de conservation des banques de données où s'accumulent les informations glanées sur chaque citoyen dans ses diverses activités, il est courant et difficile d'empêcher, voire souhaitable dans le cas de dossiers médicaux, de rendre des dossiers accessibles. La trace que nous laissons dans tous nos comportements de consommateur (cartes de crédit), de contribuable, aux postes d'immigration, etc., s'accumule et peut rester collée à nous comme un casier judiciaire. Il faut être conscient que l'archivage numérisé des informations ne pose pas les mêmes défis d'encombrement que les dossiers de papier de la STASI et qu'ils sont toujours accessibles à la seconde quand on le veut.

II - Des usages sociaux intéressants

Nul ne niera la commodité et l'efficacité de l'argent électronique pour chacun de nous, ni des cartes à puce qui nous permettront de plus en plus de franchir les tourniquets du métro, les postes de péage sur les autoroutes ou de monter dans les autobus. Les témoins (cookies) dans nos ordinateurs nous font aussi gagner beaucoup de temps pour afficher nos dossiers ou sites Web habituels.

Les exigences de sécurité dans les zones à accès restreint, celles entourant la protection contre les terroristes, aussi bien que des voleurs avec nos systèmes de détection de mouvement ne sont pas en cause. Mais ces dispositifs nous poussent à ne pas avoir une opinion tranchée sur les technologies qui, comme toujours, ne sont ni bonnes, ni mauvaises en soi. C'est l'usage que nous en faisons qui est bon ou mauvais et qui, de ce fait, doit attirer l'attention du législateur.

Depuis quelques années – 2002 ou 2004, selon les sources –, plus de 2 000 personnes portaient des puces VeriChip, qui utilisent l'IRF (RFID), permettant la lecture de leur dossier médical et dont le coût serait très modeste : environ 250 $ CAN. On aurait commencé à tester l'usage de cette puce intradermique en Europe pour divers usages, notamment comme carte de débit bancaire. De même, au Mexique, quelque 160 personnes seraient ainsi fichées à l'aide d'une puce intradermique permettant le contrôle de

cess to secure areas, protection from terrorists, or even protection from thieves through the use of motion detectors. But these devices tend to get us accustomed to certain technologies which, as is usually the case, are neither good nor bad in themselves. It is how we use them that can be good or bad, and that is what should retain the attention of lawmakers.

For a few years now, – 2002 or 2004, depending on the sources – over 2,000 people have been carrying VeriChips, which use RFID, that can provide the contents of their medical record at a very modest cost of approximately C$250. Subcutaneous chips are being tested in Europe for a variety of purposes, including as debit cards. Similarly, in Mexico, close to 160 people have been indexed with a subcutaneous chip that allows them access to high security areas.

Implanting a subcutaneous chip with GPS can protect people (4). By this I mean people whose safety is in danger (illness, children, celebrities in places where there is a high risk of kidnapping, soldiers in battlefields). It can also become an electronic leash for prisoners on parole. This Digital Angel, the name used by a U.S. manufacturer, can protect our safety in many ways.

Technological progress should therefore not be rejected wholesale. But the subject of our concerns lies in the potential abuses, which can become widespread, and that is what we are going to discuss.

III - The Pernicious Effects of Invisibility

More and more people are pointing to the dangers of a digital Wild West, an area of extremely rapid technological development that attracts investors looking for quick profits, and willing to use research funding for legitimate purposes, such as those we listed above, but who also use them for much less desirable activities. And it needs to be pointed out that the current lack of legislation promotes these misuses. There are no laws yet that would be able to provide a framework to mitigate the pernicious effects of these technologies. Worse still, the current paranoia over threats of terrorism, particularly in the United States, is encouraging public funding for such research and its excessive use by antiterrorism institutions that have statutory exemptions from any laws that might exist, and encourages tolerance that is as

l'accès à des zones sous haute sécurité.

L'implantation d'une puce intradermique avec GPS peut protéger des personnes (4). On pense à la sécurité de personnes en danger (malades, enfants, personnalités dans des zones comportant un risque d'enlèvement, soldats sur les champs de bataille). Cela peut devenir aussi une véritable laisse électronique pour les prisonniers en semi-liberté. Ce Digital Angel – cet ange numérique, selon le nom d'un fabricant américain – peut avoir de multiples usages pour notre sécurité.

On ne peut donc rejeter en bloc ces progrès technologiques. Mais l'objet de nos préoccupations se situe plutôt dans les abus qui risquent de plus en plus d'en résulter, voire de se généraliser, et c'est ce que nous allons aborder.

III - Effets pervers de l'invisibilité

De plus en plus nombreux sont ceux qui soulignent le danger d'un Farwest numérique, d'une zone de développement technologique extrêmement rapide, attirant des investisseurs en quête de profits rapides et utilisant des recherches financées pour des objectifs légitimes, tels que ceux énumérés précédemment, mais qui en détournent la puissance dans des activités beaucoup moins recommandables. Et il faut noter que le manque actuel de législation favorise ces dérives. Il n'existe pas encore de lois qui permettraient d'encadrer les effets pervers de ces technologies. Pire, la paranoïa actuelle qui résulte, notamment aux États-Unis, des menaces terroristes, favorise le financement public de ces recherches et l'usage abusif de ces dernières par les institutions de lutte antiterroriste qui bénéficient de lois d'exception ou d'une tolérance aussi discrète que dangereuse du point de vue de la démocratie.

Ainsi, on pourra se méfier du vote électronique, qui pourrait très bien, du point de vue technologique, laisser une trace nominale du choix politique des électeurs. Chacun sait que les compagnies d'assurances aimeraient avoir accès à nos dossiers de santé ou d'infractions sur la route. La crainte légitime des usurpations d'identité, de l'accès illégal aux banques de données personnelles, du vol d'argent électronique, incite à développer des contrôles électroniques de plus en plus sophistiqués. C'est le jeu de l'alarme et du voleur qui se répète et

discreet as it is dangerous from the standpoint of democracy.

Electronic voting is another case in point, because it would be very easy from a technological standpoint to keep track of how voters vote. Everyone knows that insurance companies would like to have access to our health records and our traffic violations. The fear of identify theft, illegal access to personal databases, electronic theft of money, because it is illegal, encourages the development of increasingly sophisticated electronic controls. It is cops and robbers all over again, taken to the next level.

We can only hope that there will never be a STASI again – a naive hope, perhaps – because a STASI that has access to current digital technology would be a fearsome octopus indeed. It needs to be clearly stated that the current status of the fight against terrorism encourages some very dangerous abuses. We are delighted to learn that intelligence services have been able to succeed, partly as a result of their surveillance of personal messages, the Internet and cellular telephones, or perhaps even through the use of Webcams, and have been able to prevent disasters. But we also know that mistakes and abuses are increasingly possible, indeed more frequent.

Likewise, indexing of our consumer profiles – the invisible trail that we leave everywhere behind us when we make online purchases or store purchases using credit cards – promotes datamining techniques over which we have no control. We have no access to these databanks, we can't see them, we don't know whether they exist, or where, and yet we are surprised when we receive mail or e-mail that appears to be so closely targeted to our "lifestyle". We have no protection from these invisible watchers and recorders of our private behaviour.

IV - Recommendations

To Deal With the Complexity of the Phenomenon

In view of all these probable and likely even more widespread threats and misuses of technology, democracies are clearly still powerless, and even accomplices. Not only is the law evolving more slowly than digital technologies, but our consciences are even slower. Legislating in these

s'amplifie.

Et il faut espérer qu'il n'y aura plus jamais de STASI – un espoir qui peut sembler très naïf, car si la STASI était dotée des technologies numériques actuelles, elle serait devenue une terrible pieuvre. Or, disons-le clairement, la situation actuelle de lutte contre le terrorisme favorise des dérives très dangereuses. On se réjouit d'apprendre que les services de renseignement ont réussi, notamment grâce à la surveillance des messages personnels, de l'Internet et des téléphones cellulaires, ou grâce à des webcaméras, à empêcher des catastrophes. Mais on sait aussi que les bavures et les abus sont de plus en plus possibles, voire nombreux.

De même, l'indexation de nos profils de consommateurs – la trace invisible que nous laissons partout par nos achats en ligne ou dans les magasins avec nos cartes de crédit – favorise des techniques de forage de données (data mining) que nous ne contrôlons pas. Nous n'avons pas accès à ces banques de données, nous ne les voyons pas, nous ne savons pas si elles existent, ni où, et nous nous étonnons de recevoir par la poste ou par courriel des publicités sur mesure, en fonction de notre « style de vie ». Nous n'avons pas de recours contre ces surveillants et enregistreurs invisibles de nos comportements privés.

IV - Recommandations

Face à la complexité du phénomène

Face à tous ces dangers, à ces dérives probables et même de plus en plus répandues, les démocraties sont manifestement encore impuissantes, voire complices. Non seulement le droit évolue moins vite que les technologies numériques, mais nos consciences aussi sont plus lentes. Légiférer dans ces domaines suscite souvent des craintes inhibitrices. On souligne l'importance de ne pas freiner le développement technologique, ni économique. On souligne que lorsque la loi sera promulguée, la nature du problème sera déjà modifiée par les avancées technologiques. On craint les effets pervers d'une législation dysfonctionnelle par rapport aux technologies, voire qui aurait elle-même des conséquences négatives imprévisibles, du fait que tout est nouveau dans ces domaines et tout change tout le temps.

areas often raises fears that cause inhibitions. People argue that it is important not to slow down technological and economic development. People say that by the time laws have been passed, the nature of the problem will have already been altered by technological advances. We fear the pernicious influence of dysfunctional legislation on technologies, claiming that it could even have unforeseeable negative impacts because everything is new in these areas and everything is constantly changing.

Lawmakers and members of Parliament cannot also be information technology specialists, and they generally need to rely on experts who may even disagree among themselves. That is what is happening with control nanotechnologies, just as it has happened with stem cells in medicine. Should research be allowed? How? Should it be prohibited when there are obvious advantages and growing international competition?

One essential fact needs to be mentioned here. If we want to control these surveillance technologies, there will have to be not only a legislative framework, but also leading-edge technological research in order to be able to put into practice what we decide to do. Maintaining control over the uses to which digital technologies are put is reminiscent of the myth of Sisyphus. The task always needs to be started over again, because technologies change, methods are developed to sidestep prohibitions, and algorithms are altered as well. Not only is it impossible for legislation to be written as quickly as pages of programming, but it also cannot guess what technology will be invented tomorrow morning and implemented by afternoon.

As for citizen's control (or social watch) it is paradoxically more and more difficult to effect because of the complexity and invisibility of digital technologies, and yet it is also perhaps the most effective form of control. There are all kinds of people who are developing freeware, who invent wiki software, who exchange information in virtual communities, and who come up with ideas for sites like Youtube and Myspace, which amounts to grassroots democracy. There are misuses, but also a genuine digital democracy, within which abuse by police, humanitarian scandals and financial wrongdoing all have more trouble hiding than in the past. Information is becoming democratized, and circulating more freely than ever before, thanks to digital technology.

Les législateurs, les députés ne peuvent être des spécialistes en informatique et doivent s'en remettre chaque fois à des experts, eux-mêmes éventuellement en désaccord entre eux. Il en est des nanotechnologies de contrôle comme des cellules souches en médecine. Autoriser la recherche? L'usage? L'interdire alors qu'il y a aussi des avantages évidents et une compétition internationale incessante?

Un fait fondamental doit être souligné ici. Si l'on veut exercer son emprise sur ces technologies de contrôle, il va falloir non seulement un encadrement législatif, mais aussi de la recherche technologique de pointe pour être capable de mettre en pratique ce qu'on décide. Le contrôle des usages des technologies numériques évoque le mythe du rocher de Sisyphe. La tâche est toujours à recommencer, car les technologies changent, apprennent à éviter les interdits, changent d'algorithmes. Et non seulement le droit ne peut pas s'écrire aussi vite que les pages de programmation, mais il ne peut non plus deviner ce que la technologie va inventer demain matin et mettre en œuvre demain après-midi.

Quant au contrôle citoyen lui-même, il est paradoxalement tout à la fois de plus en plus difficile par rapport à la complexité et à l'invisibilité des technologies numériques, et peut-être le plus efficace. Car on ne compte pas le nombre de ceux qui développent du logiciel libre, qui inventent des logiciels Wiki, qui échangent des informations dans des communautés virtuelles, qui proposent des sites Youtube ou Myspace de participation à la démocratie de base. Il existe des effets pervers, mais aussi une véritable démocratie numérique de base, à laquelle les abus policiers, les scandales humanitaires, financiers n'échappent plus autant que jadis. L'information se démocratise grâce au numérique et circule de plus en plus de manière irrépressible.

Les ébauches législatives

Bien des lois, dans divers pays, sans traiter ici des services secrets de renseignement qui ont toujours des statuts d'exception, tendent à contrôler et même à garantir la transparence de ces dispositifs, dont tout citoyen, que ce soit sur son lieu de travail, dans ses rapports avec les administrations, incluant le service d'ordre public, et dans ses communications privées, doit être légalement clairement informé. Nous apprenons à légiférer, sinon dans le détail technologique

Legislative Drafts

Many statutes in various countries are attempting to control and even guarantee the transparency of these devices, about which all citizens, whether at work, in their dealings with government including the police (but excluding the secret intelligence services that always have exception status), and in their private communications, must legally be kept clearly informed. We are learning to legislate, if not in terms of changing technological details, then at least on the principles involved, which remain stable. For example, the European Union and the Government of California have drawn up legislation (see appendices).

Some non-profit organizations are also actively combating the spread of these miniaturized surveillance technologies. One major example is CASPIAN, about which a great deal of documentation has been appended.

It is impossible in this working paper to put forward specific legislative recommendations.

An Urgent Debate for Canada

It is also high time here in Canada, in a country that legitimately boasts about being an advanced democracy, that we do some serious collective thinking about, and establish legislative principles that could provide a framework for, the public and commercial uses to which we can put these unavoidable and exponentially growing technologies.

Endnotes

* A "cold chain" is a temperature-controlled supply chain. Cold chains are common in the food and pharmaceutical industries.

(1) www.fr.wikipedia.org/wiki/Jeremy_Bentham

(2) Hervé Fischer, Etc. review, Montreal - July, 2005, http://www.c2so.ens-lsh.fr/IMG/pdf/7-COMMINT-_Herve_Fischer.pdf

(3) Hervé Fischer, Observatoire international du numérique (blogue)

(4) Kevin Warwick, the English researcher, implants chips near the brain and has been conducting some remarkable experiments. See his site: www.kevin-warwick.com

changeant, du moins sur des principes qui demeurent stables. Ainsi, l'Union européenne ou le gouvernement de Californie, parmi d'autres, ont entrepris de légiférer (voir les annexes).

Certains organismes sans but lucratif militent activement contre la généralisation de ces technologies miniaturisées de contrôle. C'est le cas notamment de CASPIAN, à propos duquel on trouvera en annexe une abondante documentation.

Il est impensable de proposer dans ce document de travail des recommandations législatives précises.

Un débat urgent pour le Canada

Il est grand temps ici aussi, au Canada, un pays qui se vante légitimement d'être une démocratie avancée, de consacrer un vaste effort de réflexion collective et de mettre en place des principes législatifs capables d'encadrer les usages, tant publics que commerciaux, de ces technologies désormais incontournables et en développement exponentiel.

Notes de bas de page

(1) www.fr.wikipedia.org/wiki/Jeremy_Bentham

(2) Hervé Fischer, revue Etc. Montréal - Juillet, 2005, www.c2so.ens-lsh.fr/IMG/pdf/7-COMMINT-_Herve_Fischer.pdf

(3) Hervé Fischer, Observatoire international du numérique (blogue)

(4) Kevin Warwick, chercheur anglais, s'implante des puces près du cerveau et se livre à des expériences étonnantes à cet égard. Voir son site : www.kevin-warwick.com
On pourra aussi lire Mario Tessier, Extropiens et transhumanistes, revue Solaris, No161. hiver 2007, Montréal (p114-131) et consulter quelques sites sur les tendances à transformer l'être humain en être numérique ou bionique ou en cyberborg :
Institute for Ethics and Emerging Technologies: www.ieet.org
Technoliberation.net
Future Hi Blog: www.futurehi.net
Cyborg Democracy www.cyborgdemocracy.net
Better Humans www.betterhumans.com

Also useful is Mario Tessier's Extropiens et transhumanistes, in the journal Solaris, No. 161. Winter 2007, Montreal (pp. 114-131) or consult a number of sites about trends in the transformation of human beings into digital or bionic beings, also called cyborgs:
Institute for Ethics and Emerging Technologies: www.ieet.org
Technoliberation.net
Future Hi Blog: www.futurehi.net
Cyborg Democracy www.cyborgdemocracy.net
Better Humans www.betterhumans.com

We also recommend a number of essential general works:
- Francis Fukuyama, Our Posthuman Future, Consequences of the Biotechnology Revolution, Farrar, Straus, and Giroux, 2002.
- Michael Chorost, Rebuilt: How Becoming Part Computer Made Me More Human, Boston, Houghton Mifflin, 2005
- Jérôme Goffette, Naissance de l'anthropotechnie: De la médecine au modelage de l'humain, Paris, Librairie philosophique Vrin (Pour demain), 2006.
- Dominique Babin, PH1, Manuel d'usage et d'entretien du post-humain, Paris, Flammarion, 2004
- David Brin: The Transparent Society, Perseus Press, 1998
- Dr. Katherine Albrecht and Liz McIntyre, Spychips. Penguin/Plume (October 2006).
http://www.spychips.com/book/booksales.html

On recommandera aussi quelques livres de base:

- Francis Fukuyama, La Fin de l'homme; les conséquences de la révolution biotechnique, Paris, Gallimard, 2002.
- Michael Chorost, Rebuilt : How Becoming Part Computer Made Me More Human, Boston, Houghton Mifflin, 2005
- Jérôme Goffette, Naissance de l'anthropotechnie: De la médecine au modelage de l'humain, Paris, Librairie philosophique Vrin (Pour demain), 2006.
- Dominique Babin, PH1, Manuel d'usage et d'entretien du posthumain, Paris, Flammarion, 2004
- David Brin: The Transparent Society, Perseus Press, 1998
- Dr. Katherine Albrecht et Liz McIntyre, Spychips. Penguin/Plume (October 2006). http://www.spychips.com/book/booksales.html

29E CONFÉRENCE INTERNATIONALE DES COMMISSAIRES
À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE

LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE
TERRA INCOGNITA
PRIVACY HORIZONS

29TH INTERNATIONAL CONFERENCE OF
DATA PROTECTION AND PRIVACY COMMISSIONERS

Les nanotechnologies et le plan national américain de recherche et de développement pour la protection des infrastructures critiques

Nanotechnology and the United States National Plan for Research and Development In Support of Critical Infrastructure Protection

Par/by:

Lisa Madelon Campbell

Publié dans / Published in
Canadian Journal of Law and Technology
Vol. 5, no3
Novembre 2006 / November 2006

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Afin de prévoir et d'anticiper les menaces à la sécurité nationale, les gouvernements en général, celui des États-Unis en particulier consacrent des ressources importantes à l'élaboration de systèmes technologiques qui permettent de collecter de l'information sur les gens. Depuis les cinq dernières années, le gouvernement américain recueille de l'information sur les personnes qui traversent ses frontières, à partir de diverses sources, notamment les postes frontaliers, les organes d'exécution de la loi et ceux d'immigration. Jusqu'à tout récemment, il semblait impossible pour le gouvernement américain de réaliser des analyses utiles à partir des données recueillies. En raison du volume et de la complexité de ces informations, il semblait impossible de réaliser des analyses permettant d'agir de manière préventive. Cependant, les progrès technologiques réalisés en informatique laissent supposer qu'il sera éventuellement non seulement possible de recueillir et de traiter des quantités considérables de données, mais également de le faire en temps réel, ce qui permettra aux organes d'exécution de la loi d'agir de manière préventive comme jamais auparavant.

Ce document présente les voies par lesquelles les nanotechnologies pourraient révolutionner l'industrie informatique et les incidences de ces développements sur la collecte, le traitement et la diffusion d'information qu'effectue le gouvernement américain à des fins de sécurité nationale sur les individus. Dans un article précédent[1], nous avions examiné l'utilisation croissante des données biométriques (ou physiologiques) par les gouvernements afin d'identifier des individus. L'un des problèmes étudiés dans ce document est que, même si les gouvernements réussissent à recueillir de grandes quantités d'information sur des personnes, ils ne disposent pas encore des moyens qui leur permettent de traiter et d'analyser cette information à des fins utiles. Les progrès réalisés dans le domaine des nanotechnologies pourraient changer la donne.

Il est également question d'intéresser le public à l'élaboration des nanotechnologies émergentes pour des raisons de respect de la vie privée et du dossier médical en particulier, ainsi qu'au fait que la communauté scientifique reconnaît que le succès d'une nouvelle technologie dépend en grande partie de son acceptation par l'ensemble de la communauté.

Les nanotechnologies

Afin de bien comprendre la manière dont les nanotechnologies modifieront à jamais les méthodes de calcul, il importe d'examiner leur fondement scientifique d'abord. De façon générale, les scientifiques savent qu'à l'échelle de l'infiniment petit, il existe des capacités informatiques qui dépassent de loin les capacités de traitement et de stockage des ordinateurs actuels. Comme nous le verrons plus loin, des nanotechnologies conjuguant la biologie et la technologie utilisent des cellules organiques pour créer des dispositifs de calcul qui permettent d'emmagasiner et de traiter des quantités d'information beaucoup plus considérables que celles gérées par les ordinateurs actuels.

Le principe sous-jacent des nanotechnologies a d'abord été décrit en Grèce antique par Démocrite d'Abdère (vers 460 à 370 avant Jésus-Christ) qui affirmait que toute matière était composée d'atomes distincts et minuscules. D'ailleurs, le mot grec « nano » signifie « nain »[2]. Le nanomètre correspond à un milliardième de mètre et les nanotechnologies comprennent l'analyse et la manipulation de quantités de matière dont les dimensions varient de 1 à 100 nanomètres.[3]

À la fin des années 50, le physicien Richard Feynman (Prix Nobel) évoquait l'idée de réorganiser les atomes à des fins de stockage d'information.[4] Trente ans plus tard, on assistait à la naissance des nanotechnologies avec la publication de l'ouvrage de K. Eric Drexler intitulé « *Engins de création : L'avènement des nanotechnologies* ».[5] Drexler y décrit des dispositifs qui permettraient aux atomes de se lier entre eux de manière à créer une multitude de configurations stables qu'il a appelées « assembleurs ». Il décrit ensuite un processus de fabrication moléculaire complexe qui deviendrait possible grâce à l'utilisation de ces assembleurs.[6] Voici sa description :

> La nature nous montre que les molécules peuvent se comporter comme des machines, parce que les choses vivantes ont justement recours à une telle

> machinerie. Les enzymes sont des machines moléculaires qui fabriquent, brisent et réorganisent les liens entre les molécules. Les muscles sont commandés par des machines moléculaires qui déplacent les fibres les unes par rapport aux autres. L'ADN sert de système de stockage de données, transmettant des instructions numériques à des machines moléculaires, les ribosomes, qui fabriquent des molécules de protéines. Et ce sont ces protéines de molécules qui, à leur tour, constituent la majeure partie de la machinerie moléculaire que nous venons de décrire.[7]

Les nanotechnologies fonctionnent à une échelle infiniment petite. L'échelle atomique et moléculaire, de l'ordre du centième de nanomètre, correspond à 1/100 000 du diamètre d'un cheveu humain.[8] La taille des protéines et des brins d'ADN (acide désoxyribonucléique) est habituellement de 5 à 200 nm, alors que celle des cellules sanguines se situe entre 5 000 et 10 000 nm. Les nanotechnologies ne se résument pas à une science à l'échelle microscopique; elles comprennent la fabrication de matériaux et l'élaboration de procédés dont les aspects chimiques et biologiques diffèrent des procédés de fabrication tels que nous les connaissons.[9]

Les nanotechnologies utilisent des procédés de fabrication complètement différents des procédés classiques, se servant davantage de la biologie comme modèle, ainsi que des atomes et des molécules, pour créer des structures haut de gamme permettant de réaliser des opérations extrêmement complexes.[10] Les nanotechnologies sont déjà appliquées à un certain nombre de domaines; c'est le cas notamment de l'utilisation du dioxyde de titane comme ingrédient transparent dans la crème solaire (on ne peut pas le voir lorsqu'on l'applique sur la peau) ainsi que des mémoires informatiques rapides et de petites tailles.[11]

L'industrie des nanotechnologies

À ce jour, plus de vingt pays possèdent des programmes de nanotechnologie et l'investissement collectif annuel mondial est estimé à quatre (4) milliards de dollars.[12] Les responsables américains comparent l'incidence socio‑économique probable des nanotechnologies à celle de la révolution industrielle. En 2004, les retombées financières mondiales des nanotechnologies ont été estimées à environ 20 à 50 milliards de dollars en revenus.[13] De tous les pays asiatiques, le Japon est le plus gros consommateur de nanotechnologies et les sommes consacrées à ce domaine au cours de l'exercice financier de 2003 se sont élevées à 13 milliards de dollars, ce qui représente des investissements dépassant ceux des américains.[14] Dans le financement et la réglementation des nanotechnologies, l'Union européenne suit un chemin différent de celui des États-Unis et du Japon, en mettant davantage l'accent sur les retombées sociales potentielles.[15]

Au cours des six dernières années, les sommes consacrées aux nanotechnologies aux Etats-Unis ont presque triplé et le budget de 2007 consacre près de 1,3 milliard de dollars à la recherche et au développement des nanotechnologies.[16] Le gouvernement américain est de loin le plus gros investisseur en nanotechnologies aux États‑Unis.[17] Comme l'a fait observer le directeur de l'*Office of Science and Technology Policy,* « les investissements en recherche et développement dans le domaine des sciences et des technologies nanométriques sont essentiels pour respecter les trois objectifs du président : gagner la guerre contre le terrorisme, assurer la sécurité intérieure et renforcer l'économie ».[18] En d'autres termes, le gouvernement fédéral cherche à exploiter le potentiel des nanotechnologies à des fins d'économie et de sécurité nationale.[19]

L'informatique moléculaire rendue possible

Le domaine de l'informatique a évolué considérablement au cours des trente dernières années et une notion appelée *Loi de Moore,* ou le doublement de la densité d'intégration à chaque année et demie, s'est développée avec l'accroissement des capacités informatiques des dispositifs utilisés

actuellement. Plus simplement, la puissance informatique que l'on achète avec 1 000 $ double tous les deux ans.[20] La taille et le coût ont été réduits au fil du temps. Ainsi, un transistor qui valait un dollar en 1968 coûtait à peine un dix millième de cent en 2002.[21]

Toutefois, les limites physiques des puces d'ordinateur à semi-conducteur classiques seront bientôt atteintes; il est impossible de fabriquer des puces plus petites tout en conservant la même capacité informatique. Pour cette raison, l'électronique moléculaire ou l'informatique au niveau cellulaire deviendra le prochain enjeu. Les nanotechnologies accroîtront la performance de la mémoire électronique et des systèmes intelligents intégrés et ce, à moindre coût. Par exemple, une société basée à Vancouver (Canada) est en train de fabriquer un ordinateur quantique doté de puces miniatures qui auront une capacité de calcul supérieure à celle de tous les ordinateurs rassemblés construits à ce jour.[22]

Plusieurs sociétés œuvrant dans le domaine de l'informatique sont actuellement en train de mettre au point des puces-mémoires, basées sur la technologie des nanotubes de carbone, qui augmenteraient considérablement les capacités de stockage des dispositifs mobiles.[23] Pour fabriquer des nanotubes de carbone, on utilise des cylindres extrêmement fins constitués de petites feuilles de graphite dont le diamètre est de quelques nanomètres. Leur petite taille et leur grande conductivité en font des composantes idéales pour les dispositifs électroniques.[24] Ces nouvelles technologies délaissent les procédés classiques qui utilisent des transistors en silicium et réorganisent plutôt les molécules et les atomes, le carbone et d'autres matières de manière à les utiliser comme s'il s'agissait de transistors, de câbles et de processeurs qui seront beaucoup plus puissants que les ordinateurs que nous utilisons aujourd'hui.[25]

En 2003, des scientifiques israéliens ont annoncé qu'ils avaient créé une machine programmable utilisant l'informatique moléculaire qui était 100 000 fois plus rapide que l 'ordinateur personnel le plus rapide. N'utilisant qu'une simple molécule d'ADN comme logiciel et des enzymes comme matériel, cette machine peut réaliser des opérations de calcul à partir des réactions chimiques produites lorsque ces composantes sont regroupées.[26] Bien que de nombreuses applications soient en cours d'élaboration, on utilise déjà certains nanomatériaux ou nanotechnologies. Par exemple, la capacité de stockage dans la plupart des ordinateurs peut maintenant être augmentée grâce à des couches nanométriques constituées de matériaux magnétiques.[27]

La taille réduite et la capacité de calcul accrue de ces matériaux ont également des effets sur la manière dont les ordinateurs sont utilisés. Les dispositifs qui sont utilisés pour accéder au *World Wide Web* sont de plus en plus petits et différenciés, de sorte qu'ils pourront bientôt être intégrés de manière subtile et non envahissante dans notre environnement. Ces dispositifs informatiques peuvent aujourd'hui capter des informations concernant le monde physique dans lequel ils se trouvent, y compris des images, des sons et des changements de température et de résonance électromagnétique.[28] On les a décrits comme étant « un système nerveux numérique réceptif au monde matériel » :[29]

> Ce à quoi nous pouvons désormais nous attendre, ce sont des réseaux d'éléments de calcul miniaturisés, interconnectés et sans fil, ayant des capacités de détection, de traitement et de commande, qui seront intégrés dans le monde physique. Cette boucle d'asservissement — données de détection, traitement et réponse – peut s'appliquer sans intervention humaine directe et sans délai.[30]

La mise au point des nanocapteurs, lesquels permettent une surveillance exacte et instantanée de certains événements mettant en cause des agents de guerre chimique, est en cours.[31] Les capteurs seront bientôt intégrés dans une grande diversité de matériaux; c'est le cas notamment des capteurs de gaz intégrés dans les moteurs de véhicule et les détecteurs de produits chimiques dans les réseaux d'eau potable.[32] Certains disent que cela permettra le développement de ce qu'on appelle « l'informatique diffuse », où le principal dispositif de communication sera une version perfectionnée des ordinateurs portatifs que nous connaissons aujourd'hui. Ces dispositifs plus évolués seraient des téléphones, et donneraient accès au *World Wide Web* ainsi qu'à différents réseaux et bases de

données. Le principal empêchement au développement de cette technologie est le défi que pose l'alimentation électrique des dispositifs – les piles au lithium habituellement utilisées dans les téléphones cellulaires et les ordinateurs portatifs ne sont plus assez puissantes pour alimenter des dispositifs qui accompliraient plusieurs fonctions additionnelles.[33]

Bien que les gouvernements aient des intérêts évidents dans l'informatique diffuse pour des raisons d'efficacité et d'économie d'échelle, il est fort probable qu'elle se développe de manière autonome, de la même manière que le *World Wide Web* s'est développé suite à la demande des particuliers d'obtenir davantage d'information concernant les environnements dans lesquels ils fonctionnent.[34] À mesure que les nanotechnologies rendront possible la fabrication de dispositifs informatiques de plus en plus petits qui auront des capacités de calcul encore plus grandes que leurs prédécesseurs de plus grande taille, il sera plus économique et plus efficace de recueillir, stocker, traiter et diffuser de grandes quantités d'information. Cela aura inévitablement des incidences sur la protection de la vie privée et la sécurité des personnes.[35]

Initiative nationale de nanotechnologie des États-Unis

Le gouvernement fédéral des États-Unis investit depuis longtemps dans le développement de technologies à valeur ajoutée, particulièrement depuis la Deuxième Guerre mondiale.[36] Le développement des ordinateurs modernes résulte en grande partie des projets de recherche militaire financés par le gouvernement durant la Deuxième Guerre mondiale.[37]

En 2003, le gouvernement américain a sanctionné la « *21st Century Nanotechnology Research and Development Act* » (« la Loi »)[38] qui a pour objectif principal de développer des utilisations commerciales pour les nanotechnologies. La Loi prévoit près de cinq milliards de dollars en financement entre 2004 et 2008 dans le cadre de l'Initiative nationale de nanotechnologie (« INN »), projet regroupant les programmes de neuf organismes fédéraux, y compris le *National Science Foundation,* la NASA (*National Aeronautics and Space Administration)* et le ministère de la sécurité intérieure. L'administration fédérale décrit l'INN comme étant une priorité en matière de recherche et de développement au sein de plusieurs organismes et remarque que les dépenses fédérales dans le domaine ont augmenté de 83 % au cours des deux dernières années[39] et devraient atteindre 1 milliard de dollars au total au cours de l'exercice financier de 2005.[40]

L'un des principaux objectifs de l'INN est de financer des travaux de recherche et le développement qui amélioreront la sécurité nationale aux États-Unis.[41] L'INN laisse entrevoir un « avenir dans lequel la capacité de comprendre et de contrôler la matière à l'échelle nanométrique mènera à une révolution technologique et industrielle »[42] et, en ce sens, l'INN s'engage à favoriser la découverte, l'élaboration et le déploiement des nanotechnologies, entre autres afin de promouvoir la sécurité nationale.

On considère que la défense nationale et la sécurité sont des domaines qui se recoupent. Dans la poursuite de cet objectif, l'INN travaille à l'élaboration de « systèmes efficaces et capables de générer des fonctions de commande, de contrôle, de communication, de surveillance, de reconnaissance et d'information ».[43] Bien que 14 ministères et organismes participent dans une certaine mesure à l'élaboration des nanotechnologies aux fins de défense nationale et de sécurité, ces enjeux, comme on peut s'y attendre, sont prioritaires pour les ministères de la Sécurité intérieure et de la Défense.[44]

Le ministère de la Sécurité intérieure a également mis sur pied le *Cyber Security research and development Center*. Le centre est l'organisation chargée de répartir le financement du ministère en matière de recherche et de développement dans le domaine de la sécurité informatique.[45] Les ministères de la Sécurité intérieure et de la Défense participent à l'élaboration de systèmes nanotechnologiques qui augmenteront la vitesse des ordinateurs et permettront l'élaboration de mémoire stable et de mémoire d'expansion dans le domaine de la surveillance et des communications.[46] Des 23 organismes fédéraux qui participent à l'INN, 11 disposent de budgets en recherche et développement pour les nanotechnologies.

Grâce au financement complet ou partiel de l'INN, des capteurs nanoélectromécaniques permettant de détecter et de déterminer la nature des molécules constituant un agent de guerre chimique ont déjà été mis au point. Sur le plan informatique, le financement de l'INN a aidé à développer des prototypes de dispositifs de stockage des données basés sur l'électronique moléculaire et possédant une densité d'enregistrement des centaines de fois supérieure à celle des dispositifs commerciaux actuellement disponibles sur le marché.[47]

Plan national

Le *National Plan for Research and Development in Support of Critical Infrastructure Protection,*[48] (« le Plan ») publié en 2004 par le bureau de l'exécutif (l'« *Executive Office »)* du président, l'*Office of Science and Technology Policy* et le *Science and Technology Directorate of the Department of Homeland Security* du ministère de la Sécurité intérieure, établit le lien entre le gouvernement, l'industrie privée et les citoyens. Dans le Plan, on explique que les infrastructures critiques ne sont pas seulement des bâtiments et des structures; elles comptent des personnes et du matériel, ainsi que des systèmes informatiques qui travaillent de concert à des processus qui sont fortement interdépendants.[49]

Le Plan expose l'un des objectifs principaux de la protection des infrastructures critiques : intégrer les systèmes de surveillance et la collecte des données, l'analyse et la production de rapports. Les auteurs du Plan espèrent que cela fournira une « capacité de sensibilisation aux situations en temps réel » permettant d'obtenir une « vision commune nationale ». On y explique que « le cœur du système sera un réseau de capteurs intelligents, autonomes et autoréparables qui permettra une surveillance continue des opérations et le transfert de l'information. »[50]

Les auteurs du Plan prévoient que cela sera possible si les prévisions actuelles concernant le développement des ordinateurs se réalisent. Plutôt que de se fier aux câbles et à l'électricité, les ordinateurs de l'avenir seront basés sur des processus biologiques qui utilisent des molécules et des échanges chimiques. Les ordinateurs quantiques pourraient transmettre de l'information grâce à la rotation magnétique (ou spin) de l'électron, ce qui leur permettrait d'effectuer des tâches beaucoup plus complexes que celles effectuées par les ordinateurs actuels.[51]

Les transformations dans le domaine de l'informatique arrivent à temps pour les législateurs américains, parce que, selon les auteurs du Plan, « des quantités importantes de données seront traitées et analysées afin de filtrer les signaux de fond en vue de détecter des anomalies ou des modèles répétitifs ». Toutes ces données seront examinées en rapport avec l'information reçue en provenance de différents capteurs et seront par la suite analysées afin de déterminer leur utilité éventuelle auprès des organes d'exécution de la loi et du renseignement.[52]

Il est difficile de prévoir l'évolution des choses. Cependant, il est précisé dans le Plan que :

> La détection de l'intention comprend l'examen, la combinaison d'observations, d'actions, de liens et d'antécédents historiques afin de déterminer avec précision si une personne, un groupe, ou une série d'événements sont susceptibles de mener à des événements terroristes.[53]

Les services du renseignement et les organes responsables de l'exécution de la loi peuvent être aidés à cet égard par l'utilisation de « capteurs psychologiques ou physiologiques » qui pourraient révéler l'état d'esprit d'un individu.[54] Selon le Plan :

> Les systèmes intelligents comporteront de nombreux types de capteurs, des capacités de communication qui leur permettront de « parler » les uns avec les autres et des capacités de calcul qui leur permettront de réaliser des analyses, de comparer des données et des analyses et d'apprendre en fonction des analyses et de l'expérience passée. Pour être déployés à grande échelle, ces capteurs intelligents

> doivent être disponibles à faible coût, durables, précis, capables de s'autoétalonner et de s'adapter à l'environnement. Les capteurs et les systèmes de capteurs devront être « programmés » afin d'être sensibles à la menace, de pouvoir s'autoconfigurer et de s'autoréparer. Ils pourraient être branchés à des câbles ou sans fil, ou une combinaison des deux – mais ils devront être sécurisés sur le plan de l'information.[55]

Ces systèmes de pointe comprendront des « réseaux intelligents » qui communiqueront les uns avec les autres et organiseront les tâches de manière à collaborer entre eux et à s'ajuster eux-mêmes afin de répondre aux situations qui évoluent.[56] Le Plan reconnaît la nécessité d'intégrer aux systèmes de modélisation informatique autant de mesures biométriques que possible, afin de renforcer la précision des systèmes d'identification et d'authentification.[57]

Ces efforts de recherche et de développement sont orientés vers ce que le Plan décrit comme étant « un contrôle situationnel dynamique », c'est-à-dire un plan quelque peu ambitieux visant à recueillir de grandes quantités de données auprès des personnes, des objets et des capteurs, à analyser ces données puis à déterminer les mesures ou l'attitude à prendre de manière à contrôler le résultat d'une situation donnée :

> Le contrôle dynamique est la capacité d'intégrer les flux de données multiples recueillis auprès des personnes, des objets, des détecteurs et de divers systèmes de données, comme les données relatives au suivi du fret, les manifestes de passagers des compagnies aériennes, les registres d'Interpol, du FBI et de la police locale, ainsi que l'information financière, etc., et d'agir sur ces paramètres.[58]

La conclusion du Plan fait brièvement mention de la nécessité de protéger les droits individuels et le droit à la vie privée. Les auteurs laissent entrevoir qu'il sera important de comprendre les répercussions de l'élaboration de vastes bases de données qui contiennent de l'information sur les citoyens qui vivent aux États-Unis et ailleurs dans le monde.[59]

Répercussions de l'utilisation des nanotechnologies par le gouvernement dans le domaine de la surveillance

Même si les progrès nanotechnologiques font de ces nouvelles capacités informatiques une réalité, il subsiste quelques défis à relever. Le gouvernement américain est déjà en train de mettre en œuvre, à titre de priorité en matière de recherche et de développement, des systèmes de surveillance à base de données multiples qui fourniront des renseignements au personnel d'exécution de la loi. Le programme américain intitulé *Visitor and Immigrant Status Indicator Technology Program* du ministère de la Sécurité intérieure sur les entrées et les sorties du pays, recueillera de grandes quantités de renseignements sur les personnes qui traversent les frontières. Parmi ces renseignements, mentionnons le nom et le genre, des renseignements biométriques, la citoyenneté, le lieu de résidence et l'adresse complète pendant le séjour au pays.[60]

Les auteurs du Plan national émettent cependant une réserve : « La majorité de ces systèmes continueront de contenir des technologies anciennes pour lesquelles les interfaces pourraient être les plus efficaces pour améliorer la sécurité. Ces anciens systèmes ne sont pas toujours capables d'effectuer une intégration ou une collaboration intelligentes ».[61] Cela fait allusion au fait qu'un grand nombre et une variété de bases de données ont été mises au point dans le cadre d'initiatives d'exécution de la loi au cours des vingt dernières années. Un grand nombre d'entre elles utilisent des technologies incompatibles et recueillent des données basées sur des ensembles de règles différents, ce qui fait qu'elles ne puissent pas être combinées en une base de données unique dans laquelle on pourrait effectuer des recherches.

La volonté du gouvernement de recueillir de vastes quantités d'information peut refléter le fait que la connaissance du profil des individus (c'est-à-dire ce que l'on recherche essentiellement) est inefficace

si l'on tient compte seulement des caractéristiques de base comme la race, par exemple. La race à elle seule ne permet pas de prévoir le comportement humain; par conséquent, le fait de placer une confiance excessive dans ce paramètre peut mener les agences d'exécution de la loi à commettre des erreurs et à mettre sous enquête des personnes innocentes.[62] Les politiques gouvernementales relatives au profilage racial des arabes, des musulmans, des sikhs et des personnes originaires d'Asie du Sud établis aux États-Unis depuis 2001 n'ont pas réussi à permettre la détection d'activités terroristes importantes contre les États-Unis, ce qui laisse supposer que la race à elle seule ne permet pas de prévoir des comportements violents.[63] Comme l'affirment de nombreux observateurs, la notion de « terroriste » qui s'est développée dans la culture politique des États-Unis est un ensemble complexe qui comprend la race, la nationalité et la religion. Elle pourrait mener à supposer que des membres de certains groupes soient plus susceptibles de commettre des actes de violence que d'autres.[64]

De même, bien que la présence de plus en plus grande de l'informatique diffuse rende plus facile la localisation et le suivi des personnes,[65] le lieu géographique à lui seul n'est pas un indicateur fiable du comportement à venir. Alors, quel type d'information le gouvernement essaie-t-il de recueillir? Le plus grand nombre possible, semble-t-il. Les personnes qui souhaitent traverser la frontière des États-Unis devront fournir des renseignements biologiques intimes les concernant, et cette information sera stockée et utilisée en vue de les identifier pendant leurs déplacements à l'intérieur des États-Unis. Cette information sera comparée à l'information obtenue auprès des organes d'exécution de la loi, des postes frontaliers et des autorités responsables de l'immigration.

L'une des raisons importantes justifiant les investissements du gouvernement américain dans les nanotechnologies est de recueillir de l'information et d'éviter des actions qui pourraient constituer une menace à la sécurité nationale. Cependant, comme l'ont démontré des catastrophes récentes, le gouvernement, lorsqu'il agit seul, est souvent incapable de réagir rapidement et de manière appropriée. Comme certains l'ont remarqué, la prise de décision au XXIe siècle et le pouvoir qui l'accompagne sont décentralisés.[66] Les entités privées sont présentes verticalement et horizontalement à presque tous les paliers de gouvernance et participent même aux affaires les plus délicates du pays, comme celles concernant le domaine militaire.[67] Par exemple, il existe un comité créé par le *Directorate for Science and Technology of the Department of Homeland Security* du ministère de la Sécurité intérieure. L'une des missions de cette direction est d'améliorer les capacités techniques des opérations ministérielles.[68] Un autre organisme au sein du ministère, le *Homeland Security Science and Technology Advisory Committee,* identifie des domaines de recherche qui sont potentiellement importants pour la sécurité des États-Unis. Afin de combler les besoins des chercheurs en matière de financement et les besoins du gouvernement en matière de recherche sur une puissance informatique accrue, ce comité comprend vingt scientifiques qui ne sont pas des employés du gouvernement et qui ont servi dans des domaines pertinents comme l'ingénierie et l'intervention en cas d'urgence.[69]

Participation du public aux nanotechnologies émergentes

En plus des répercussions que pourraient avoir les nanotechnologies sur la protection de la vie privée, on dénombre des répercussions concrètes en matière de santé et d'environnement. De plus, l'opinion de la communauté scientifique en regard de l'engagement public a évolué au cours des dernières années. Il est de plus en plus prouvé que consulter et faire participer le public à l'élaboration des technologie émergentes favorise leur acceptation et la gestion adéquate des risques. Les critiques estiment que malgré d'importantes sommes consacrées à la recherche et au développement en nanotechnologie, il n'y en a pas assez allouées à la gestion du risque et à la recherche sur les effets des nanotechnologies sur la santé et l'environnement.[70]

Les universitaires recommandent une méthode « postnormale » pour inclure le public dans le développement des technologies émergentes. Ils estiment que la participation du public et la création de mécanismes de rétroaction permettront d'accroître la base de connaissances et d'identifier les valeurs importantes et les domaines possibles de conflit.[71] Une telle participation du public transforme les

citoyens en une forme de « communauté élargie des pairs » qui aidera à évaluer les technologies émergentes.[72]

La méthode appelée « conférence de concertation » est un concept danois qui permet de créer des politiques concernant les questions hautement techniques, par le biais du Conseil des technologies (organisme administratif du gouvernement). Le Congrès des États-Unis a employé une méthode semblable lorsqu'il a créé les « conseils » de citoyens sur la politique en matière de nanotechnologie.[73] Cependant, pour être efficace, la méthode ne doit pas se limiter à une simple étude sur les groupes cibles, comme on en retrouve en marketing. Il faut créer une boucle de rétroaction qui tient compte des préoccupations et qui modifie la méthode en fonction de ces préoccupations, afin de forger la crédibilité et de réduire les risques au minimum.

L'un des problèmes avec la participation du public est l'utilisation d'une terminologie hautement technique et complexe – comme dans le cas des brevets, les termes et les notions de nanotechnologie diffèrent considérablement de ce que le grand public connaît. Cependant, comme certains auteurs l'ont fait remarquer, il est essentiel que les scientifiques communiquent avec d'autres représentants du public et qu'ils participent aux politiques découlant des technologies émergentes. S'ils ne le font pas, la science deviendra déstabilisée et trop politisée.[74]

Plusieurs observateurs des progrès en nanotechnologie mentionnent l'exemple de l'expérience européenne avec les aliments modifiés génétiquement : les scientifiques ont omis de tenir compte de la méfiance du grand public en regard de cette technologie et des conséquences financières dévastatrices que cela aurait sur l'industrie.[75] L'industrie privée, les chercheurs et le gouvernement en sont venus à se rendre compte de l'importance d'informer le public sur les technologies émergentes de manière transparente et de tenir compte des préoccupations du public.[76]

Les progrès en nanotechnologie sont semblables à ceux réalisés dans le domaine de la recherche sur les cellules souches, en ce sens qu'elles sont nouvelles, hautement scientifiques et qu'elles ont des implications sociales et politiques énormes. Dans les deux cas, les processus législatifs n'ont pas progressé au même rythme que les percées scientifiques.[77] La difficulté des interactions entre les législateurs et le public est facilement concevable en raison de la nature hautement technique des applications de nanotechnologie. Le même problème a été observé par ceux qui se sont dépêchés à présenter des demandes de brevets pour de nouvelles applications de nanotechnologie. Il est difficile pour ceux qui ne sont pas familiers avec les nanotechnologies d'imaginer ces nouveaux concepts et, encore plus, de les comprendre afin de prendre des décisions éclairées concernant leur utilisation. Considérons, par exemple, un brevet présenté à l'université Cornell en 2004, portant sur le « piégeage entropique et les tamis moléculaires », procédé au cours duquel on utilise les réactions d'une matière à des stimuli électriques afin de faciliter le passage vers le bas des molécules de plus grande taille, alors que les molécules de plus petite taille ne passent pas. En effet, à l'échelle nanométrique, les molécules se comportent de manière contraire à ce à quoi l'on s'attendrait normalement.[78]

À l'automne 2005, la *United States National Science Foundation* a fourni 20 millions de dollars à un réseau éducatif de vulgarisation des nanotechnologies qui mettra sur pied des expositions et des programmes d'éducation du public dans les musées scientifiques. Un autre 14 millions a été consacré aux universités afin qu'elles puissent réaliser de la recherche sur les implications sociales des progrès en nanotechnologie. En outre, le « *Societal Dimensions Program Component Area* » de l'INN prévoit consacrer 43 millions de dollars en 2006 à l'éducation et à la recherche sur les implications sociales des nanotechnologies, y compris les préoccupations concernant la vie privée qui pourraient découler de l'utilisation des capteurs employés dans les nanotechnologies.[79]

Cela pourrait être une indication que le gouvernement tire parti de ses expériences dans d'autres domaines scientifiques. Comme un chercheur le faisait remarquer devant le Congrès :

> … le projet du génome humain constitue un bon modèle nous permettant de voir comment une technologie émergente peut créer la controverse lorsqu'elle s'applique à

> la sphère publique. Le séquençage du génome humain comporte les mêmes préoccupations potentielles que d'autres domaines de recherche en génétique. La disponibilité accrue de l'information génétique soulève la question d'atteinte à la vie privée, de la mauvaise utilisation par les policiers et les compagnies d'assurances et de la discrimination par les employeurs. Les fondateurs du projet du génome humain n'ont pas essayé de faire taire ces préoccupations légitimes en limitant le discours, sur la place publique, aux avantages de ces nouvelles connaissances. Ils ont plutôt accueilli et encouragé activement le débat dès le départ en mettant de côté 5 % du budget annuel pour un programme visant à définir et à régler les questions éthiques, juridiques et sociales du projet.[80]

Les applications médicales potentielles des nanotechnologies soulèvent de nombreuses questions intéressantes concernant la participation du public. Si, par exemple, comme c'est le cas pour d'autres technologies émergentes, les applications en nanotechnologie sont principalement accessibles à ceux qui possèdent suffisamment d'argent pour se les offrir dès leurs premiers balbutiements, risquerait-il d'y avoir des inégalités entre les personnes qui ont amélioré leur qualité de vie grâce aux nanotechnologies et celles qui ne l'ont pas fait?[81] Si les nanotechnologies améliorent les capacités d'une personne, pourrait-il éventuellement y avoir une distinction entre les capacités personnelles et l'identité individuelle?[82] Les organisations qui favorisent les intérêts des transhumanistes, qui croient que la technologie peut être utilisée pour améliorer les êtres humains, font des pressions pour qu'il y ait moins de réglementation et davantage d'investissements dans les nanotechnologies.[83]

Certains ont décrit l'émergence d'une nouvelle tendance, soit celle des « partisans de la dignité » qui, du point de vue des utilitaristes et des droits de la personne, constitue un troisième groupe émergent dans les débats sur la bioéthique.[84] La vision des partisans de la dignité en matière de respect des droits de la personne est contenue dans le *Projet de déclaration universelle sur la bioéthique et les droits de l'homme,* publiée par le Comité international de bioéthique de l'UNESCO (Organisation des Nations Unies pour l'éducation, la science et la culture) et favorise le développement de la recherche scientifique dans un cadre qui respecte la dignité humaine.[85] La *Déclaration internationale sur les données génétiques humaines*[86], qui se préoccupe principalement de la collecte, du stockage et de l'utilisation des données génétiques humaines à des fins de recherche, mentionne expressément que la dignité humaine doit être protégée.[87] La déclaration reconnaît que l'identité d'une personne ne peut être réduite à ses caractéristiques génétiques et qu'elle est plutôt un mélange complexe de facteurs environnementaux, sociaux et culturels, incluant un élément de liberté.[88]

Bien que les droits de la personne puissent être respectés par le biais d'une exigence visant à obtenir un consentement éclairé, les partisans de la dignité humaine fondamentale disent qu'il se pourrait que dans certains cas, même avec un consentement éclairé, une biotechnologie donnée puisse la compromettre. Par exemple, il pourrait s'agir d'une application de biotechnologie qui modifie fondamentalement un trait humain intrinsèque.[89] Ce qui est intéressant à propos de la doctrine de la dignité est que le fait de donner son consentement ne règle pas la question – il existe une valeur de la dignité humaine plus élevée qu'il faudrait protéger.[90]

Un autre défi, distinct des implications des nanotechnologies sur la protection de la vie privée, est l'effet des matières minuscules, ou nanoparticules, sur la santé humaine. Des scientifiques croient que les nanoparticules pourraient avoir des effets néfastes sur la santé humaine pour deux raisons. Les premières études en laboratoire montrent que les nanoparticules, ou particules de matière nanométriques, peuvent pénétrer dans le corps plus facilement que les particules de plus grandes tailles. De plus, les nanotechnologies permettent aux structures moléculaires de se reproduire et potentiellement de s'auto‑assembler de manière à former des structures plus complexes. Cette capacité de se répliquer et de proliférer est préoccupante dans les cas où la matière serait néfaste pour la santé humaine ou pour l'environnement.[91] Les premières études laissent croire que les nanoparticules réussiraient non seulement à pénétrer facilement dans le corps, mais qu'elles pourraient également traverser les tissus corporels en passant d'un endroit du corps à un autre, ce qui causerait de l'inflammation et endommagerait les cellules.[92] Cependant, on ne connaît pas très bien la toxicité des

nanoparticules lorsqu'elles sont inhalées ou incorporées d'une quelconque manière.[93] En l'absence d'un cadre réglementaire, les sociétés américaines qui mettent au point des applications de nanotechnologie peuvent offrir de l'information générique concernant les propriétés de leurs produits à l'*Environmental Protection Agency.* Cela permet à ces sociétés de promouvoir leur collaboration avec l'*Environmental Protection Agency*, tout en atténuant les préoccupations du public concernant leurs produits.[94]

Conclusion

Les progrès réalisés en nanotechnologie peuvent faciliter la surveillance et accroître la capacité de traiter de l'information obtenue grâce à la surveillance.[95] Ces progrès technologiques peuvent avoir des effets sur la notion classique de vie privée : s'il devient plus facile et moins coûteux de recueillir et d'utiliser de l'information sur les personnes, cela pourrait devenir plus courant et, éventuellement, mieux accepté de façon générale.[96] L'évolution de l'informatique diffuse, avec divers réseaux d'information raccordés à de nombreux capteurs (possiblement invisibles), laisse supposer que les notions classiques de vie privée et d'espaces privés et publics pourraient devoir être redéfinies.[97]

En quoi cela aide-t-il le gouvernement américain à atteindre son objectif qui consiste à prévoir et à éviter les menaces à la sécurité nationale? Le gouvernement américain, par le biais de son ministère de la Sécurité intérieure, participe dans un sens à un vaste exercice de prévisibilité. Contrairement à la théorie des prévisions qui tente de prédire passivement les événements à venir, la prévisibilité est basée sur la notion que l'avenir soit constitué de plusieurs résultats possibles et qu'il est possible d'intervenir et d'agir sur ces résultats.[98]

L'information recueillie sera constituée de données brutes, c'est-à-dire d'information ne pouvant être considérée comme du « renseignement » de sécurité à moins de devenir un indicateur d'une menace potentielle, ou jusqu'à ce qu'elle le devienne. Étant donné les problèmes de compatibilité présents dans l'infrastructure technique actuelle, il est peu probable que ce type d'analyse de pointe soit réalisé dans un avenir rapproché.

Toutefois, certains des principes sous-jacents à l'élaboration d'une immense base de données renfermant de l'information biologique et d'autres renseignements personnels semblent être basés sur des notions classiques de théorie scientifique. Le modèle présenté dans le Plan national suppose que de l'information biologique, géographique ou autre sera recueillie et que l'analyse de ces données constituera une forme d'avertissement précoce qui permettra au gouvernement d'intervenir et d'éviter ce qu'il perçoit comme étant des événements dangereux.

Des physiciens, des mathématiciens, des microbiologistes et d'autres scientifiques participent à l'élaboration d'un domaine d'étude connu sous le nom de « systèmes adaptatifs complexes », qui sont essentiellement subjectifs, non linéaires, non prévisionnels et mutables.[99] Le comportement d'un groupe d'êtres humains donné peut être caractérisé comme étant un système adaptatif complexe qui, tout en étant basé sur la biologie, n'est d'aucune façon limité par elle. Les systèmes humains tendent à démontrer un comportement normatif lorsqu'ils se situent entre le chaos et l'ordre, en présence de conflits qui ne sont toutefois pas débilitants.[100]

En créant les bases de données décrites dans le présent document, le gouvernement américain semble ne pas avoir réussi à tenir compte de la nature fluide du comportement humain et de son évolution. Les êtres humains, à titre d'individus ou de membres d'une communauté, constituent des systèmes adaptatifs complexes. Si les nanotechnologies font en sorte que l'informatique diffuse soit bientôt partie intégrante de nos vies quotidiennes, les personnes pourraient également les utiliser pour obtenir de l'information contextuelle sur leur environnement et pour modifier leur comportement en conséquence.[101] Il reste à voir si les investissements importants dans un système de surveillance d'une telle ampleur aideront réellement le gouvernement américain à prévoir et à éviter les menaces à la sécurité nationale.

Notes en bas de page

[1] Lisa Madelon Campbell, "Rising Governmental Use of Biometric Tech-nology: An Analysis of the United States Visitor and Immigrant Status Indicator Technology Program" (2005) 4 C.J.L.T. 99.

[2] Robert D. Pinson, "Is Nanotechnology Prohibited by the Biological and Chemical Weapons Conventions?" (2004) 22 Berkeley J. of Int'l Law 279 at 282.

[3] US., Nanoscale Science, Engineering and Technology Subcommittee, Committee on Technology, National Science and Technology Council, *The National Nanotechnology Initiative Strategic Plan* (2004) at iii

[4] Francisco Castro, "Legal and Regulatory Concerns Facing Nanotechnology" (Fall, 2004) 4 Chicago-Kent J. of Intellectual Property 140 at 140.

[5] Paris: Vuibert, 2005.

[6] Wayne C.]aeschke & Kimberly A Kluge, "Innovating from Pumps to Genes into the 'Nano-dimension': The Legal Consequences of the Insati-able Urge to Build a Better Mouse-trap" (2004) 22 Del. Law. 38 at 40.

[7] K. Eric Drexler, "Nanotechnology Summary" in *1990 Encyclopedia Britannica Science* and *the Future Yearbook,* 162 at 163 as cited in Glenn Harlan Reynolds, "Nanotechnology and Regulatory Policy: Three Futures" (Fall, 2003) 17 Harvard J. of Law & Technology 179 at 180.

[8] Office of the Press Secretary, News Release, "President Bush signs Nanotechnology Research and Development Act into Law" (3 december 2003), online: The White House <http:// www.whitehouse.gov/news/releases/2003/12/20031203-7.*html>.*

[9] Terry K. Tullis, "Application of the Government License Defense to Federally Funded Nanotechnology Research: The Case for a Limited Patent Compulsory Licensing Regime" (2005) 23 UCLA L. Rev. at 283.

[10] Castro, *supra* note 4 at 141.

[11] Pinson, *supra* note 2.

[12] Meridian Institute, "Nanotechnology and the Poor: Opportunities and Risks – Closing the Gaps Within and Between Sectors of Society" (January 2005) online: http://www.nanoandthepoor.org.

[13] Tullis, *supra* note 9.

[14] Dana E. Nicolau, "Challenges and Opportunities for Nanotechnology Policies: An Australian Perspective" (2004) 1:4 Nanotechnology L. & Bus. 446 at 459.

[15] *Ibid* at 460.

[16] US, Nanoscale Science, Engineering, and Technology Subcommittee Committee on Technology, National Science and Technology council *The National Nanotechnology Initiative - Research and Development Leading to* a *Revolution in Technology and Industry* (2006) at i.

[17] *Karen* Florini *et al.* "Nanotechnology: Getting it Right the First Time" (2006) 6:3 Sustainable Development L. & Policy 46 at 51.

[18] Office of Science and Technology Policy, Executive Office of the Presi-dent, News Release, "Nanoscale Scientific and Engineering Research and Development Extend Frontiers of Scientific Knowledge, Lead to Signifi-cant Technological Advances - Supplement to President's FY 2004 Budget Released Today" (17 October 2003).

[19] *Supra* note 16 at 35.

[20] Steve Jurvetson, "Transcending Moore's Law with Molecular Electronics and Nanotechnology", (2004) 1:1 Nanotechnology Law and Business 70 at 72.

[21] Thomas A Kalil, "Next Steps for the National Nanotechnology Initiative" (2004) 1:1 Nanotechnology L. & Bus. 55 at 59.

[22] Jurvetson, *supra* note 20 at 88.

[23] Lawrence Gasman, "Making Powerful Information Technology Available Everywhere: Nanotech and the Next Wave: Pervasive Computing" online: Foresight Nanotech Institute, <http:// www.foresightorg/challenges/it.php>.

[24] *Supra* note 8.

[25] "Where Nanotechnology & The Computer Industry Meet - Shrinking the PC" *Computer Power User* 2:3 (March, 2002) 56.

[26] Stephen Lovgren, "Computer made from DNA and Enzymes" *National Geographic News* (24 February 2003), online: National Geographic News <http://news.nationalgeographic.com/ news/2003/02/0224_030224_DNAcomputer.html>

[27] National Technology Initiative, "Applications/Products" online: National Technology Initiative <http://www.nano.gov/html/facts/appsprod.htm>.

[28] Jerry Kang & Dana Cuff, "Pervasive Computing: Embedding the Public Sphere" 62 Wash. & Lee L. Rev. 93 (2005) 93 at 99; also available at <http://ssm.com/abstract=626961>.

[29] *Ibid* at 112.

[30] *Ibid* at 99.

[31] *Supra* note 8.

[32] Pinson, *supra* note 2.

[33] Gasman, *supra* note 23.

[34] Kang & Cuff, *supra* note 28 at 101-102.

[35] Fiona N. Moore, "Implications of Nanotechnology Applications: Using Genetics as a Lesson" (2002) 10:3 Health L. Rev. 9.

[36] Nicolau, *supra* note 14 at 458.

[37] Mark A Lemley, "Patenting Nanotechnology" June 2005, Stanford Law School, John M. Olin Program in Law and Economies, Working Paper No. 304, at Social Science Research Network Electronic Paper Collection: <http://ssm.com/abstract=741326>, at page 8.

[38] 15 U.S.C.A §7501-7509.

[39] *Supra* note 8.

[40] *Supra* note 3 at iii.

[41] *Ibid.* In his covering letter to the Strategic Plan, John H. Marburger, Director of the Executive Office of the President, Office of Science and Technology writes that, since its inception in 2001, the NNI has sought to enhance national security, among other things.

[42] *Ibid* at 1.

[43] *Ibid* at 20.

[44] *Ibid* at 20.

[45] U.S., The Executive Office of the President, Office of Science and Technology Policy & The Department of Homeland Security, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection* (Washington, D.C., 2004) at 8.

[46] *Supra* note 3 à 21.

[47] National Nanotechnology Initiative, *Nanotechnology: from Imagination to Reality,* online: National Nanotechnology Initiative <http://www.nano.gov/html/res/fy04-pdf/fy04%20-%20small% 20parts/NNI_FY04_D_intro.pdf>

[48] *Supra* note 45.

[49] *Ibid.* at 2.

[50] *Ibid.* at 13.

[51] *Ibid.* at 15.

[52] *Ibid.* at 24.

[53] *Ibid.* at 26.

[54] *Ibid.* at 26.

[55] *Ibid.* at 27.

[56] *Ibid.* at 59.

[57] *Ibid* at 38. Biometric identifiers are physical and behavioral measure-ments or characteristics that include fingerprints, band geometry, facial features and deoxyribonucleic acid (DNA).

[58] *Ibid* at 41.

[59] *Ibid* at 67.

[60] Susan Martin & Philip Martin, "National Security Discussion: Interna-tional Migration and Terrorism: Prevention, Prosecution and Protection" (2004) 18 Geo. Immigr. L. J. 329, at 333.

[61] *Supra* note 45 à 71.

[62] Martin & Martin, *supra* note 60 at 337.

[63] Thomas M. McDonnell, "Targeting the Foreign Born by Race and Nationality: Counter-Productive in the War on Terrorism'?" (2004) 16 Pace Int'l L. Rev. 19, at 8.

[64] Margaret Chon & Donna E. Arzt, 'Judgn1ents Judges and Wrongs Remembered: Examining d1e Japanese American Civil Liberties Cases on their Sixtieth Anniversary: Walking While Muslim" (2005) 68 Law & Contemp. Probs. 215.

[65] Kang & CuIf, *supra* note 28 at 103.

[66] Robert J. Rhee, "Catastrophic Risk and Governance after Hurricane Katrina: A Postscript to Terrorism Risk in a Post-9/11 Economy" (2006) 38 Ariz. St L J 581 at 603.

[67] Ibid.

[68] Department of Homeland Security, online: <http://www.dhs.gov/indexshtm.>

[69] Ibid.

[70] Florini *et al. supra* note 17 at 51-52.

[71] Michael D. Mehta, "Regulating Biotechnology and Nanotechnology in Canada: A Post-Normal Science Approach for Inclusion of the Fourth Helix" (Paper presented at the International Workshop on Science, Technology and Society: Lessons and Challenges, National University of Singapore, 19 April 2002) [unpublished] at 7-8.

[72] *Ibid.* at 22.

[73] Beth Simone Noveck, "The Future of Citizen Participation in the Electronic State" (2004) 1:1 J. of Law and Policy for the Information Society 1 at 12.

[74] Gregory N. Mandel, "Technology Wars: the failure of democratic discourse" (2005) Il Mich. Telecomm. & Tech. L. Rev. 117.

[75] Bryn Williams-Jones, "A Spoonful of Trust Helps the Nanotech Go Down" (2004) 12:3 Health L. Rev. 10.

[76] *Ibid.* See also Emmanuelle Schuler, "A Prospective Look al Risk Communication in the Nanotechnology Field" (2004) 12:3 Health L. Rev. 28.

[77] William P. Cheshire, Jr" "Small Thirigs Considered: the Ethical Significance of Human Embryonic Stern Cell Research" (2005) 39 New Eng. L Rev. 573.

[78] Jaeschke & Kluge, *supra* note 6 at 80.

[79] National Nanotechnology Initiative, "Societal Dimensions" online: <http: / /www.nano.gov/html/society/home_society.html>.

[80] Testimony of Vicki Calvin, Director, Centre for Biological and Environmental Nanotechnology, before the House Committee on Science, 108th Congress (2003) in regard to *21st Century Nanotechnology Research and Development Act* of 2003. Also available online: House Committee on Science <http://www.house.gov/science/hearings/full03/apr09/ colvin.htm>.

[81] R. George Wright; "Personhood 20: Enhanced and Unenhanced Persons and the Equal Protection of the Laws" (2005) 23 Quinnipiac L Rev. 1047.

[82] *Ibid.*

[83] Edna F. Einsiedel & Greg McMullen, "Stakeholders and Technology: Challenges for Nanotechnology" 12:3 Health L. Rev. 5.

[84] Roger Brownsword, "Stern cells and Cloning: where the Regulatory Consensus Fails" (2005) 39 New Eng. L. Rev. 535 at 538.

[85] United Nations Educational, Scientific and Cultural Organization (UNESCO), International Declaration on Human Genetic Data (16 October 2003), online: UNESCO <http://portal.unesco.org>.

[86] United Nations Educational, Scientific and Cultural Organization (UNESCO), International Declaration on Human Genetic Data (16 October 2003), online: UNESCO <http://portal.unesco.org>.

[87] *Ibid.* at preamble.

[88] *Ibid.* at Article 3.

[89] Brownsword, *supra* note 84 at 553.

[90] *Ibid.*

[91] Albert C. Lin, "The Unifying Role of Harm in Environmental Law"(2006) 2006 Wis. L. Rev. 897.

[92] Jennifer Sass, Patrice Simms & Elliott Negin, "Nanotechnologies: The Promise and the Peril" (2006) 6:3 Sustainable Development Law & Policy 11, at l1.

[93] *Ibid.*

[94] *Ibid,* at 13.

[95] Chris MacDonald, "Nanotechnology, Privacy and Shifting Social Conventions" (2004) 12:3 Health L. Rev. 37.

[96] *Ibid.*

[97] Davis Baird & Tom Vogt, "Societal and Ethical Interactions with Nanotechnology ('SEIN') - An Introduction" (2004) 1:4 *Nanotechnology Law and Business* 391 at 394.

[98] Ian Kerr & Goldie Bassie, "Building a Broader Nano-network" (2004) 12:3 Health L. Rev. 57.

[99] Scott H. Hughes, "Understanding Conflict in a Postmodern World"(2004) 87 Marq. L. Rev. 681 at 683.

[100] *Ibid* at 684.

[101] Kang & Cuff. *supra* note 28.

Nanotechnology and the United States National Plan for Research and Development In Support of Critical Infrastructure Protection

Lisa Madelon Campbell †

In an effort to predict and avert threats to national security, governments in general, and that of the United States in particular, have devoted considerable resources to developing technological systems that gather information about individuals. In the past five years, the U.S. government has collected information about the movement of individuals across and within its national borders from various sources, including border security stations, law enforcement officials, and immigration authorities. Until recently, it seemed impossible for the U.S. government to draw useful analyses from all of the data it is collecting. The sheer volume and complexity of the information made it appear unworkable to perform an analysis in time to act pre-emptively. Now, developments in computing technology suggest that not only will it soon be possible to collect and process vast amounts of data, it will be possible to do so in real time, giving law enforcement officials unprecedented capacities to engage proactively.

This paper will examine the ways in which nanotechnology will likely revolutionize the computing industry, and the effect of these developments on the U.S. government's collection, processing, and dissemination of information about individuals for national security purposes. In an earlier article,[1] I examined the rising use of biometric, or physiological, data by governments in order to track individuals. One of the problems discussed in that paper was that while governments might collect vast amounts of information about individuals, they lacked the capacity to usefully process and analyze that information. Developments in nanotechnology are likely to change that.

This paper also considers the importance of engaging the public in the development of emergent nanotechnologies, due to privacy and health implications, and also because of the growing realization on the part of the scientific establishment that the success of any new technology depends in large part upon its acceptance by the community as a whole.

The Science of Nanotechnology

In order to understand how nanotechnology will forever alter methods of computing, it is necessary to first examine the science. In essence, scientists have discovered that at the level of the ultra-small, there exist computing capacities that far outstrip the storage and processing capacities of the most powerful computers in operation today. As is discussed below, in an interesting intersection between biology and technology, nanotechnology employs organic cells to create computing devices that will be able to store and process vastly greater amounts of information than existing computers.

The ideas underlying nanotechnology were first described in ancient Greece by Democritus of Abdera (ca. 460-370 BCE), when he posited that all matter was composed of distinct, minuscule atoms, and the word "nano" stems from the Greek word for dwarf.[2] A nanometre is one-billionth of a metre, and nanotechnology involves the analysis and manipulation of matter at sizes approximately 1 to 100 nanometres.[3]

In the late 1950s, the Nobel prize-winning physicist Richard Feynman talked about rearranging atoms for information storage purposes.[4] Three decades later, the modern field of nanotechnology was born with the publication of K. Eric Drexler's "*Engines of Creation: The Coming Era of Nanotechnology*".[5] He initially described the devices that would allow atoms to be bound together into a multitude of stable patterns as 'assemblers. Drexler later formulated an intricate description of molecular manufacturing that would become possible through the use of these assemblers.[6] As he describes it:

> Nature shows that molecules can serve as machines because living things work by means of such machinery. Enzymes are molecular machines that make, break, and rearrange the bonds holding other molecules together. Muscles are driven by molecular machines that haul fibres past one another. DNA serves as a data-storage system, transmitting digital instructions to molecular machines, the ribo-

†Counsel, Department of Justice Canada. The views and opinions expressed in this paper, prepared for the *Canadian Journal of Law and Technology*, are solely those of the author and do not necessarily represent the views and opinions of the Department of Justice.

somes, that manufacture protein molecules. And these protein molecules, in turn, make up most of the molecular machinery just described.[7]

Nanotechnology operates on a minute scale: atomic and molecular levels, or 1/100 nanometre, can be compared to 1/100,000 of the diameter of a human hair.[8] Proteins and Deoxyribonucleic-acid ("DNA") are usually from 5 to 200 nm, whilst blood cells are 5,000 to 10,000 nm in size. Nanotechnology is not simply science on a minute scale; it is the manufacturing of materials and processes that have chemical and biological aspects that differ from manufacturing as we know it.[9]

Completely distinct from traditional forms of manufacturing, nanotechnology looks instead to biology as a model, organizing atoms and molecules to create sophisticated constructs that can perform extremely complex operations.[10] Nanotechnology is already in use in a number of diverse applications, including the titanium dioxide used as a transparent ingredient in sunscreen that cannot be seen when applied to the skin, and faster, smaller-sized computer memories.[11]

The Nanotechnology Industry

To date, more than 20 countries have developed nanotechnology programs, and the annual collective investment globally is estimated at $4 billion.[12] United States government officials have compared the probable socio-economic impacts of nanotechnology to the Industrial Revolution. In 2004, the global financial impact of nanotechnology was estimated at between $20–$50 billion in revenues.[13] The Japanese government is the biggest spender on nanotechnology among Asian countries, and their funding in the fiscal year 2003 outstripped the United States at $13 billion.[14] In its financing and regulation of emerging nanotechnologies, the European Union takes a somewhat different approach from the United States and Japan, placing greater emphasis on the potential returns to society.[15]

Over the last six years in the U.S., government spending for nanotechnology has nearly tripled, and the 2007 budget request for nanotechnology research and development is close to $1.3 billion.[16] The U.S. government is by far the heaviest investor in nanotechnology in the United States.[17] As the U.S. director of the Office of Science and Technology Policy has observed, "investments in nanoscale science and technology research and development are essential to achieving the President's top three priorities: winning the war on terrorism, securing the homeland, and strengthening the economy".[18] Put another way, the federal government seeks to exploit the potential of nanotechnology for broad economic and national security purposes.[19]

Molecular Computing Made Possible

Computing has evolved tremendously in the past three decades, and a concept called Moore's Law, or the doubling of transistor density every year and a half, developed as observers witnessed the increasing computing capabilities of devices currently in use. Put simply, "the computational power that $1,000 buys has doubled every two years".[20] Both size and cost have been reduced over time; a transistor that cost $1.00 in 1968 cost a mere ten-thousandth of a cent in 2002.[21]

However, the physical limits of the traditional semiconductor computer chip will soon be reached: it is impossible to fabricate smaller chips and maintain the same computing capacity. Because of this, molecular electronics, or computing on a cellular level, will become the next paradigm. Nanotechnology applications will increase the performance of electronic memory and embedded intelligence systems at a greatly reduced cost. As an example, a company based in Vancouver, Canada, is building a quantum computer with thumbnail-sized chips that will have more computing power than the aggregate of all computers built to date.[22]

Several computing firms are currently developing memory chips that are based on carbon nanotubes and that would vastly increase the storage capabilities of mobile devices.[23] To make carbon nanotubes, tiny sheets of graphite are rolled into extremely narrow cylinders that are mere nanometers in diameter. Their small size and efficient conductivity make them well-suited for use in electronic devices.[24] Abandoning the process of placing transistors onto silicon, these new technologies will rearrange molecules and atoms, carbon and other materials, enabling them to act as transistors, wires and processors that will be exponentially more powerful than computers we have today.[25]

In 2003, scientists in Israel announced that they had created a molecular computing machine that could be programmed and that was over 100,000 times faster than the fastest PC. Using a single DNA molecule as software, and enzymes as hardware, the chemical reactions that occur when these are mixed together allow them to perform computing operations.[26] While many applications are in development, some nanomaterials and technologies are currently in use. For example, the storage capacity in most computers can now be increased through the use of nano-thin layers of magnetic materials.[27]

This reduced size and increased computing capacity also has implications for the ways in which computers are used. The devices that are used to access the world-

wide web are becoming increasingly smaller and differentiated, such that they will soon be able to be incorporated, in a subtle and unobtrusive way, into the environment in which we live. Significantly, these computational devices can now sense information about the physical world in which they are situated, including visual images, sounds, and changes in temperature and electromagnetic resonance.[28] They have been described as "a digital nervous system grafted onto the material world":[29]

> What we can expect, then, are networks of miniaturized, wirelessly interconnected, sensing, processing, and actuating computing elements kneaded into the physical world. This animated control loop — of sensing data, processing it, then responding to it — can take place without direct human intervention or delay.[30]

The development of nanosensors, which would allow for accurate and instantaneous monitoring of events such as chemical warfare initiatives, is already underway.[31] Sensors will soon be built into a vast array of materials, such as gas sensors in motor vehicle engines and chemical detectors in water supplies.[32] Some predict that this will allow for the development of so-called "pervasive computing", where the primary communications device would be a more sophisticated version of today's hand-held computers. These more evolved devices would be telephones, and provide access to the worldwide web as well as to various networks and databases. The primary impediment to the development of this technology is the challenge of providing sufficient power sources for these devices — lithium batteries currently used in cellphones and notebook computers are not powerful enough for devices that would perform several more functions.[33]

While governments have an obvious interest in pervasive computing for reasons of efficiency and economies of scale, it is quite likely to spread on its own, in the same way that the worldwide web has, through individual citizens' desire for more information about the environments in which they operate.[34] As nanotechnology makes possible smaller and smaller computing devices that have even greater computing capabilities than their larger predecessors, it will be become both more economical and efficient to collect, store, process, and distribute vast amounts of information. This will inevitably impact on individual privacy and security.[35]

The U.S. National Nanotechnology Initiative

The federal government in the United States has long intervened financially in order to boost the development of added value technologies, and in particular, it did so after World War II.[36] The development of the modern computer came about largely as the result of government-funded military research projects during World War II.[37]

In 2003, the U.S. government passed into law the *21st Century Nanotechnology Research and Development Act* ("the Act"),[38] which has as its main purpose to develop commercial uses for nanotechnology. The Act allocates close to $5 billion in funding from 2004–2008 to the National Nanotechnology Initiative ("NNI"), an initiative that groups together the programs of nine federal agencies, including the National Science Foundation, the National Aeronautics and Space Administration, and the Department of Homeland Security. The federal administration describes the NNI as a top multi-agency research and development priority, and observes that federal spending on nanotechnology research increased by 83% in the previous two years,[39] and was expected to total $1 billion in the fiscal year 2005.[40]

One of the main goals of the NNI is to fund research and development that will enhance national security in the United States.[41] The vision of the NNI is described as "a future in which the ability to understand and control matter on a nanoscale leads to a revolution in technology and industry", [42] and towards this end the NNI commits to expediting the discovery, development, and deployment of nanotechnology in order to promote national security, among other things.

National defence and security are seen as areas of cross-cutting application; in pursuit of these goals the NNI is working towards the development of "systems with the speed and capacity to enable command, control, communications, surveillance, reconnaissance, and information dominance".[43] While some 14 departments and agencies participate to some extent in the development of nanotechnology for national defence and security purposes, as can be expected these drivers are of primary interest to the departments of Homeland Security and Defense.[44]

The Department of Homeland Security has also established a virtual National Cyber Security research and development Center. The Center is the umbrella organization through which the department's funding for cyber-security research and development activities is distributed.[45] The departments of Homeland Security and Defense are participating in the development of nanotechnology-based systems that will increase the speed of computers, and allow for stable and expanded memory out of their interest in surveillance and communications.[46] Of the 23 federal agencies that participate in the NNI, 11 have research and development budgets for nanotechnology.

Through funding either in whole or in part from the NNI, nano-electro-mechanical sensors have already been developed that can detect and identify even a single molecule of a chemical warfare agent. On the computing front, funding from the NNI has aided in the development of prototype data storage devices, based upon molecular electronics, that have data densities one hundred times that of the highest density commercial devices that are currently available.[47]

The U.S. National Plan

The *National Plan for Research and Development in Support of Critical Infrastructure Protection,*[48] ("the Plan") published by The Executive Office of the President, Office of Science and Technology Policy, and the Science and Technology Directorate of the Department of Homeland Security in 2004, underscores the interconnectedness between government, private industry, and individual citizens. As the Plan observes, "critical infrastructures are not just building and structures — they include people and physical and cyber systems that work together in processes that are highly interdependent."[49]

The Plan outlines one of the primary goals for critical infrastructure protection: to integrate monitoring and surveillance systems with data collection, analysis, and the production of reports. What the authors of the Plan hope this will provide is "real-time situational awareness capability" that would provide what they describe as a "national common operating picture". They predict that "the heart of the system would be a sensor network that is intelligent, self-monitoring, and self-healing to allow continuous operation for situation monitoring and information transfer."[50]

The authors of the Plan rightly foresee that this will be made possible if current predictions about the development of computers are realized. Rather than relying upon wires and electricity, computers in the future will be based upon biological processes that use molecules and chemical exchanges. Quantum computers will likely be able to transmit information through the spin of an electron, allowing them to perform vastly more complex functions than today's computers.[51]

The transformational developments in computing power come at an opportune time for lawmakers in the United States, because, as the authors of the Plan observe, "massive amounts of data will need to be processed and analyzed to selectively filter out background signals in order to detect anomalies or patterns". All of this data will need to be set in the context of information received from various sensors, and be further analyzed if it is to be of any use to the law enforcement and intelligence community.[52]

Predicting what people will do is a difficult business. However, the Plan states:

> The detection of intent involves examining combinations of observations, actions, relationships, and past history in order to accurately sense whether a person, group, or series of events might be the purveyor of or precursor to terrorist events.[53]

The intelligence and law enforcement community may be aided in this respect through the use of so-called "psychologically/physiologically-oriented sensors" that could reveal an individual's state of mind.[54] The Plan forecasts that:

> Intelligent systems will have multiple types of sensors, communication capabilities so they can "talk" to each other, and computing capabilities so they can perform analyses, compare sensed data and analyses, and learn based on analyses and experience. To be pervasively deployed, such smart sensors need to be low-cost, durable, accurate, self-calibrating, and environmentally adaptable. The sensors and systems of sensors will need to be "taught" to be threat-aware, self-configuring, and self-healing. They may be wired or wireless or a combination of the two — but they must be informationally secure.[55]

These advanced systems will include "smart networks" that communicate with each other and organize tasks so as to collaborate, adjusting themselves to respond to evolving situations.[56] The Plan recognizes the need to incorporate into computer modeling systems as many biometric measurements as possible, in order to reinforce the accuracy of identification and authentication systems.[57]

These research and development efforts are geared towards what is described in the Plan as "dynamic situational control", essentially, a somewhat ambitious plan to collect vast amounts of data from people, objects, and sensors, analyze this data and then infer actions or intent so as to control the outcome of a given situation:

> Dynamic control is the ability to integrate and act on the multiple streams of data collected from people, objects, detectors, and a variety of data systems, such as freight tracking data, airline passenger manifests, Interpol, FBI, local police records, financial information, etc.[58]

Towards the conclusion of the Plan there is some, albeit brief, mention of the necessity of protecting individual and privacy rights. The authors suggest that it will be important to understand the impacts of developing huge databases that contain information about citizens living in the United States and elsewhere.[59]

Implications of Governmental Use of Nanotechnology in Surveillance

Even if developments in nanotechnology make these new computing capabilities a reality, some challenges remain. The United States government is already implementing, as a research and development priority, multi-database monitoring systems that provide information to law enforcement personnel. The United States Visitor and Immigrant Status Indicator Technology Program, a universal entry-exit program promulgated by the Department of Homeland Security, will collect vast amounts of information about individuals as they arrive and depart from the country. Included among the vast array of information collected will be name and gender, biometric information, citizenship, place of residence and complete address while in the country.[60]

As the authors of the National Plan euphemistically observe, however, "the bulk of these systems will continue to contain legacy technology for which interfacing may be the best that can be done to improve security. These legacy elements are not always capable of integration or intelligent collaboration".[61] This is a reference to the fact that numerous and diverse databases have been

developed through law enforcement initiatives over the past two decades. Many of these employ incompatible technologies and collect data based upon differing sets of rules, with the result that they cannot simply be combined into a single, searchable database.

The government's desire to collect a wide array of information may reflect the knowledge that individual profiling, which is in essence what is being done, is ineffective if it is done using only raw characteristics such as race, for example. Race alone cannot predict human behaviour; and overreliance upon it can mislead law enforcement authorities and place innocent persons at risk of investigation.[62] Governmental policies involving the racial profiling of Arabs, Muslims, Sikhs and South Asians in the United States since 2001 have failed to uncover substantial terrorist criminal activity against the United States, which points to the failure of race alone as a predictor of violent behaviour.[63] As several commentators have observed, the notion of the "terrorist" that has developed in the political culture in the United States is an intricate formation that includes aspects of race, nationality, and religion. It may unfairly cast members of certain groups are being more likely to commit acts of violence.[64]

Similarly, while the spread of pervasive computing will make it much easier to situate and track the movements of individuals,[65] geographical location alone is not a reliable indicator of future behaviour. So what type of information is the government trying to collect? As many types as possible, it would appear. Persons wishing to cross national borders will be required to provide intimate biological information about themselves, and this information will be stored and used to positively identify them as they move within the U.S. This information will be compared with information from law enforcement officials, border stations, and immigration officials.

A significant reason for the U.S. government's investment in nanotechnology is to collect information and prevent actions that may threaten national security. As recent catastrophes have shown, however, government acting alone is often singularly incapable of reacting swiftly and appropriately. As some have noted, decision-making in the 21st century, and the power that goes with it, is de-centralized.[66] Private entities are vertically and horizontally implicated at almost every level of governance, and are involved in even the most demanding business of a nation, such as military engagement.[67] An example of this is a committee convened by the U.S. Directorate for Science and Technology of the Department of Homeland Security. The Directorate has as one of its missions the objective of enhancing the technical capabilities of the department's operations.[68] Another body within the department, the Homeland Security Science and Technology Advisory Committee, identifies research areas that are of potential importance to the security of the United States. In an interesting intersection between the needs of researchers for funding and the government's need for research into greater computing power, this Committee consists of 20 scientists who are not government employees, and who have established records of distinguished service in relevant fields such as engineering and emergency response.[69]

Public Engagement in Emerging Nanotechnologies

In addition to the privacy implications developments in nanotechnology may have, there are tangible health and environmental implications. As well, the scientific community's view of public engagement has evolved in recent years. There is a growing realization that it is crucial to consult with, and involve the public in, the development of emerging technologies in order for those technologies to be accepted and in order to properly manage risks. Critics suggest that amidst the large sums that are being spent on nanotechnology research and development, insufficient monies are being allocated to risk management and research into the health and environmental effects of emerging nanotechnologies.[70]

Scholars have recommended a so-called "post-normal" approach for inclusion of members of the public in the development of emerging technologies. They suggest that engaging the public and creating feedback mechanisms will both expand the knowledge base and identify important values and possible areas of conflict.[71] Involving the public in this way transforms individual citizens into a form of "extended peer community" that can help to assess emerging technologies.[72]

The Danes employ a method called the "Danish Consensus Conference" through their Board of Technology, an administrative agency of the government, to create policy statements regarding highly technical issues. The United States Congress employed a similar methodology when it created citizen juries on nanotechnology policy.[73] But to be effective, this has to be more than focus-group testing in a marketing sense. It has to be a feedback loop that takes into account concerns raised and modifies the approach accordingly, in order to build credibility and truly minimize risks.

The challenges of involving the public include the highly technical and complex nature of the terminology — as we have seen with patent issues, terms and concepts in nanotechnology are unlike anything that most members of the public would ever have encountered. Yet, as some authors have pointed out, it is essential that scientists communicate with other members of the public, and become involved in the policy issues that arise with emerging technologies. When they fail to do so, science can become destabilized and overly politicized.[74]

Several commentators on developments in nanotechnology point to the European experience with genetically modified foods, where scientists failed to take into account the general public's mistrust of this technology and the devastating financial impact that that would have on the industry.[75] Private industry, researchers, and government alike have come to realize the importance of informing the public about emerging technologies in a transparent manner that is accountable to public concerns.[76]

Developments in nanotechnology are similar to those in stem cell research in that they involve novel, highly technical scientific developments with potentially enormous societal and political implications. In both cases, the legislative process has not progressed at the same rate as scientific breakthroughs.[77] One of the understandable difficulties with involving legislators and the public is the highly technical nature of nanotechnology applications. The same problem has confounded those rushing to patent new nanotechnology applications. It is difficult for those not intimately involved with emerging nanotechnologies to even imagine some of the new concepts, let alone comprehend them, in order to make informed decisions about their uses. Consider, for example, a patent issued to Cornell University in 2004, for "Entropic Trapping and Sieving of Molecules", a process which retrieves responses to electrical stimuli in order to facilitate the downwards passing of larger molecules while smaller ones remain behind. As has been observed, the behaviour of molecules at the level of nanotechnology runs counter to the way in which we generally understand matter to react.[78]

In the fall of 2005, the United States National Science Foundation provided $20 million to a Nanoscale Informal Science Education Network that will develop public education exhibits and programs in science museums. Another $14 million was awarded to universities to allow them to conduct research on the social implications of developments in nanotechnology. As well, the so-called "Societal Dimensions Program Component Area" of the NNI expects to fund $43 million in 2006 for education and research on the societal implications of nanotechnology, including privacy concerns that may arise from the use of sensors created through nanotechnology.[79]

This may be an indication that the government is borrowing from its experiences in other fields of scientific development. As one researcher observed while testifying before Congress:

> ... the Human Genome project provides a good model for how an emerging technology can defuse potential controversy by addressing it in the public sphere. Mapping of the human genome carries with it many of the same potential concerns as do other fields of genetic research. The increased availability of genetic information raises the potential for loss of privacy, misuse by the police and insurance companies, and discrimination by employers. The founders of the Human Genome Project did not try to bury these legitimate concerns by limiting public discourse to the benefits of this new knowledge. Instead, they wisely welcomed and actively encouraged the debate from the outset by setting aside 5% of the annual budget for a program to define and address the ethical, legal and other societal implications of the project.[80]

Potential medical applications of nanotechnology raise numerous interesting questions about which the public will undoubtedly wish to engage. If, for example, as with other emergent technologies, nanotechnology applications are mainly accessible to those with sufficient wealth to afford them in their initial stages, might there be inequalities between persons who have been "enhanced" by nanotechnology versus those who have not?[81] If nanotechnology enhances a person's capabilities, *quaere* whether there will be any distinction between personal capabilities and individual identity.[82] Organizations that promote the interests of transhumanists, individuals who believe that technology may be used to enhance human beings, press for less regulation and greater investments in nanotechnology.[83]

Some commentators have described a new "dignitarian view", which, along with utilitarian and human rights perspectives, forms an emerging triangle in debates about bioethics.[84] The dignitarian view informs the *Preliminary Draft Declaration on Universal Norms on Bioethics*, published by the International Bioethics Committee of the United Nations Educational, Scientific and Cultural Organization ("UNESCO") and promotes the development of scientific research within a framework that respects human dignity.[85] The International Declaration on Human Genetic Data,[86] which is principally concerned with the collection, storage and use of human genetic data for research purposes, specifically provides that human dignity must be protected.[87] The Declaration recognizes that an individual's identity cannot be reduced to genetic characteristics, and that it is a complex mixture of environmental, social and cultural factors, including an aspect of freedom.[88]

Whereas human rights concerns may be largely addressed through a requirement to obtain informed consent, dignitarians would argue that there may be situations where, even with informed consent, a given biotechnology attacks fundamental human dignity. An example of this would be an application of biotechnology that fundamentally altered what is understood to be an inherently human trait.[89] What is interesting about the dignitarian point of view is that the giving of consent does not end the matter — there is a higher value of human dignity that it would seek to protect.[90]

Another challenge, quite apart from the privacy implications of nanotechnology, is the effect that miniscule matter, or nanoparticles, may have upon human health. Some scientists suggest that nanoparticles may have adverse effects upon human health for two reasons. Early laboratory studies suggest that nanoparticles, or bits of matter on the nanoscale, may enter the body more easily than larger bits of matter. As well, nanotechnology

allows molecular structures to reproduce, and potentially, to self-assemble into more complex structures. This capacity to replicate and proliferate is of concern if it involves matter that is harmful to human health or the environment.[91] Early studies suggest that nanoparticles not only enter the body easily, they may pass through bodily tissues from one area of the body to another, causing inflammation and damaging cells.[92] Not much is known, however, about the toxicity of nanoparticles when inhaled or otherwise taken into the body.[93] In the absence of a regulatory framework, the U.S., companies developing nanotechnology applications may offer generic information about the properties of their products to the Environmental Protection Agency. This would in turn allow those companies to advertise their collaboration with the Environmental Protection Agency as a way of mitigating public concerns about their products.[94]

Conclusion

Developments in nanotechnology may both facilitate surveillance and increase the power to process information obtained through surveillance.[95] These developments in technology may have an effect on traditional notions of privacy: if it becomes easier and less expensive to gather and use information about people, it may become more common, and eventually, more generally accepted.[96] The evolution of pervasive computing, with various information networks connected to many — and possibly invisible — sensors, suggests that traditional notions of privacy and private and public spaces may need to be re-defined.[97]

So what does all of this do for the U.S. government's goal, described above, of foreseeing and averting threats to national security? The U.S. government, through its Department of Homeland Security is, in a sense, engaging in a vast foresighting exercise. Distinct from forecasting, which passively tries to predict future events, foresighting is based on the notion that there are many possible outcomes in the future, and that it may be possible to intervene and affect these results.[98]

The information that will be collected is raw data, mere information that cannot be characterized as security "intelligence" unless, and until, it becomes an indicator of a potential threat. Given the problems with compatibility of the existing technical infrastructure, it is unlikely that this type of sophisticated analysis will occur at any point in the near future.

More fundamentally, however some of the principles underlying the development of a massive database of biological and other personal information appear to be based upon traditional notions of scientific theory. The model outlined in the National Plan presupposes that biological, geographical, and other information will be collected, and that analysis of this data will provide a form of early warning system that will enable the government to intervene and prevent what it conceives of as harmful events.

Physicists, mathematicians, microbiologists and other scientists are developing a field of study known as "complex adaptive systems", which are inherently subjective, nonlinear, nonpredictive, and mutable.[99] The behaviour of a given group of human beings can be characterized as a complex adaptive system which, while grounded in biology, is by no means locked in by it. Human systems tend to exhibit emergent behaviour when they exist in a realm between chaos and order, where there is some conflict but not debilitating conflict.[100]

In building the databases described in this paper, the U.S. government appears to have failed to take account of the fluid nature of human behaviour and evolution. Human beings, both as individuals and in the communities that they form, are complex adaptive systems. If nanotechnology will soon make pervasive computing a part of our daily lives, then individuals may use it as well to gain contextual information about their environments and to modify their behaviour accordingly.[101] It remains to be seen whether the huge financial investment in a massive surveillance system will actually assist the U.S. government in predicting and averting threats to national security.

Notes:

[1] Lisa Madelon Campbell, "Rising Governmental Use of Biometric Technology: An Analysis of the United States Visitor and Immigrant Status Indicator Technology Program" (2005) 4 C.J.L.T. 99.

[2] Robert D. Pinson, "Is Nanotechnology Prohibited by the Biological and Chemical Weapons Conventions?" (2004) 22 Berkeley J. of Int'l Law 279 at 282.

[3] U.S., Nanoscale Science, Engineering and Technology Subcommittee, Committee on Technology, National Science and Technology Council, *The National Nanotechnology Initiative Strategic Plan* (2004) at iii.

[4] Francisco Castro, "Legal and Regulatory Concerns Facing Nanotechnology" (Fall, 2004) 4 Chicago-Kent J. of Intellectual Property 140 at 140.

[5] 1st ed, (New York: Anchor Books, 1986).

[6] Wayne C. Jaeschke & Kimberly A. Kluge, "Innovating from Pumps to Genes into the 'Nano-dimension': The Legal Consequences of the Insatiable Urge to Build a Better Mousetrap" (2004) 22 Del. Law. 38 at 40.

[7] K. Eric Drexler, "Nanotechnology Summary" in *1990 Encyclopedia Britannica Science and the Future Yearbook*, 162 at 163 as cited in Glenn Harlan Reynolds, "Nanotechnology and Regulatory Policy: Three Futures" (Fall, 2003) 17 Harvard J. of Law & Technology 179 at 180.

[8] Office of the Press Secretary, News Release, "President Bush signs Nanotechnology Research and Development Act into Law" (3 December 2003), online: The White House <http://www.whitehouse.gov/news/releases/2003/12/20031203-7.html>.

[9] Terry K. Tullis, "Application of the Government License Defense to Federally Funded Nanotechnology Research: The Case for a Limited Patent Compulsory Licensing Regime" (2005) 23 UCLA L. Rev. at 283.

[10] Castro, *supra* note 4 at 141.

[11] Pinson, *supra* note 2.

[12] Meridian Institute, "Nanotechnology and the Poor: Opportunities and Risks — Closing the Gaps Within and Between Sectors of Society" (January 2005) online: <http://www.nanoandthepoor.org>.

[13] Tullis, *supra* note 9.

[14] Dana E. Nicolau, "Challenges and Opportunities for Nanotechnology Policies: An Australian Perspective" (2004) 1:4 Nanotechnology L. & Bus. 446 at 459.

[15] *Ibid.* at 460.

[16] U.S., Nanoscale Science, Engineering, and Technology Subcommittee Committee on Technology, National Science and Technology council, *The National Nanotechnology Initiative — Research and Development Leading to a Revolution in Technology and Industry* (2006) at i.

[17] Karen Florini *et al* "Nanotechnology: Getting it Right the First Time" (2006) 6:3 Sustainable Development L. & Policy 46 at 51.

[18] Office of Science and Technology Policy, Executive Office of the President, News Release, "Nanoscale Scientific and Engineering Research and Development Extend Frontiers of Scientific Knowledge, Lead to Significant Technological Advances — Supplement to President's FY 2004 Budget Released Today" (17 October 2003).

[19] *Supra* note 16 at 35.

[20] Steve Jurvetson, "Transcending Moore's Law with Molecular Electronics and Nanotechnology", (2004) 1:1 Nanotechnology Law and Business 70 at 72.

[21] Thomas A. Kalil, "Next Steps for the National Nanotechnology Initiative" (2004) 1:1 Nanotechnology L. & Bus. 55 at 59.

[22] Jurvetson, *supra* note 20 at 88.

[23] Lawrence Gasman, "Making Powerful Information Technology Available Everywhere: Nanotech and the Next Wave: Pervasive Computing" online: Foresight Nanotech Institute, <http://www.foresight.org/challenges/it.php>.

[24] *Supra* note 8.

[25] "Where Nanotechnology & The Computer Industry Meet — Shrinking the PC" *Computer Power User* 2:3 (March, 2002) 56.

[26] Stephen Lovgren, "Computer made from DNA and Enzymes" *National Geographic News* (24 February 2003), online: National Geographic News <http://news.nationalgeographic.com/news/2003/02/0224_030224_DNAcomputer.html>

[27] National Technology Initiative, "Applications/Products" online: National Technology Initiative <http://www.nano.gov/html/facts/appsprod.htm>.

[28] Jerry Kang & Dana Cuff, "Pervasive Computing: Embedding the Public Sphere" 62 Wash. & Lee L. Rev. 93 (2005) 93 at 99; also available at <http://ssrn.com/abstract=626961>.

[29] *Ibid.* at 112.

[30] *Ibid.* at 99.

[31] *Supra* note 8.

[32] Pinson, *supra* note 2.

[33] Gasman, *supra* note 23.

[34] Kang & Cuff, *supra* note 28 at 101-102.

[35] Fiona N. Moore, "Implications of Nanotechnology Applications: Using Genetics as a Lesson" (2002) 103 Health L. Rev. 9.

[36] Nicolau, *supra* note 14 at 458.

[37] Mark A. Lemley, "Patenting Nanotechnology" June 2005, Stanford Law School, John M. Olin Program in Law and Economics, Working Paper No. 304, at Social Science Research Network Electronic Paper Collection: <http://ssrn.com/abstract=741326>, at page 8.

[38] 15 U.S.C.A. §7501–7509.

[39] *Supra* note 8.

[40] *Supra* note 3 at iii.

[41] *Ibid.* In his covering letter to the Strategic Plan, John H. Marburger, Director of the Executive Office of the President, Office of Science and Technology writes that, since its inception in 2001, the NNI has sought to enhance national security, among other things.

[42] *Ibid.* at 1.

[43] *Ibid.* at 20.

[44] *Ibid.* at 20.

[45] U.S., The Executive Office of the President, Office of Science and Technology Policy & The Department of Homeland Security, Science and Technology Directorate, *The National Plan for Research and Development in Support of Critical Infrastructure Protection* (Washington, D.C., 2004) at 8.

[46] *Supra* note 3 at 21.

[47] National Nanotechnology Initiative, *Nanotechnology: from Imagination to Reality*, online: National Nanotechnology Initiative <http://www.nano.gov/html/res/fy04-pdf/fy04%20-%20small%20parts/NNI_FY04_D_intro.pdf>

[48] *Supra* note 45.

[49] *Ibid.* at 2.

[50] *Ibid.* at 13.

[51] *Ibid.* at 15.

[52] *Ibid.* at 24.

[53] *Ibid.* at 26.

[54] *Ibid.* at 26.

[55] *Ibid.* at 27.

[56] *Ibid.* at 59.

[57] *Ibid.* at 38. Biometric identifiers are physical and behavioral measurements or characteristics that include fingerprints, hand geometry, facial features and deoxyribonucleic acid (DNA).

[58] *Ibid.* at 41.

[59] *Ibid.* at 67.

[60] Susan Martin & Philip Martin, "National Security Discussion: International Migration and Terrorism: Prevention, Prosecution and Protection" (2004) 18 Geo. Immigr. L. J. 329, at 333.

[61] *Supra* note 45 at 71.

[62] Martin & Martin, *supra* note 60 at 337.

[63] Thomas M. McDonnell, "Targeting the Foreign Born by Race and Nationality: Counter-Productive in the 'War on Terrorism'?" (2004) 16 Pace Int'l L. Rev. 19, at 8.

[64] Margaret Chon & Donna E. Arzt, "Judgments Judges and Wrongs Remembered: Examining the Japanese American Civil Liberties Cases on their Sixtieth Anniversary: Walking While Muslim" (2005) 68 Law & Contemp. Probs. 215.

[65] Kang & Cuff, *supra* note 28 at 103.

[66] Robert J. Rhee, "Catastrophic Risk and Governance after Hurricane Katrina: A Postscript to Terrorism Risk in a Post-9/11 Economy" (2006) 38 Ariz. St. L.J. 581 at 603.

[67] *Ibid.*

[68] Department of Homeland Security, online: <http://www.dhs.gov/index.shtm>

[69] Ibid.

[70] Florini *et al. supra* note 17 at 51-52.

[71] Michael D. Mehta, "Regulating Biotechnology and Nanotechnology in Canada: A Post-Normal Science Approach for Inclusion of the Fourth Helix" (Paper presented at the International Workshop on Science, Technology and Society: Lessons and Challenges, National University of Singapore, 19 April 2002) [unpublished] at 7-8.

[72] *Ibid.* at 22.

[73] Beth Simone Noveck, "The Future of Citizen Participation in the Electronic State" (2004) 1:1 J. of Law and Policy for the Information Society 1 at 12.

[74] Gregory N. Mandel, "Technology Wars: the failure of democratic discourse" (2005) 11 Mich. Telecomm. & Tech. L. Rev. 117.

[75] Bryn Williams-Jones, "A Spoonful of Trust Helps the Nanotech Go Down" (2004) 12:3 Health L. Rev. 10.

[76] *Ibid.* See also Emmanuelle Schuler, "A Prospective Look at Risk Communication in the Nanotechnology Field" (2004) 12:3 Health L. Rev. 28.

[77] William P. Cheshire, Jr., "Small Things Considered: the Ethical Significance of Human Embryonic Stem Cell Research" (2005) 39 New Eng L. Rev. 573.

[78] Jaeschke & Kluge, *supra* note 6 at 80.

[79] National Nanotechnology Initiative, "Societal Dimensions" online: <http://www.nano.gov/html/society/home_society.html>.

[80] Testimony of Vicki Colvin, Director, Centre for Biological and Environmental Nanotechnology, before the House Committee on Science, 108th Congress (2003) in regard to *21st Century Nanotechnology Research and Development Act* of 2003. Also available online: House Committee on Science <http://www.house.gov/science/hearings/full03/apr09/colvin.htm>.

[81] R. George Wright, "Personhood 2.0: Enhanced and Unenhanced Persons and the Equal Protection of the Laws" (2005) 23 Quinnipiac L. Rev. 1047.

[82] *Ibid.*

[83] Edna F. Einsiedel & Greg McMullen, "Stakeholders and Technology: Challenges for Nanotechnology" 12:3 Health L. Rev. 5.

[84] Roger Brownsword, "Stem cells and Cloning: where the Regulatory Consensus Fails" (2005) 39 New Eng. L. Rev. 535 at 538.

[86] United Nations Educational, Scientific and Cultural Organization (UNESCO), International Declaration on Human Genetic Data (16 October 2003), online: UNESCO <http://portal.unesco.org>.

[86] United Nations Educational, Scientific and Cultural Organization (UNESCO), International Declaration on Human Genetic Data (16 October 2003), online: UNESCO <http://portal.unesco.org>.

[87] *Ibid.* at preamble.

[88] *Ibid.* at Article 3.

[89] Brownsword, *supra* note 84 at 553.

[90] *Ibid.*

[91] Albert C. Lin, "The Unifying Role of Harm in Environmental Law" (2006) 2006 Wis. L. Rev. 897.

[92] Jennifer Sass, Patrice Simms & Elliott Negin, "Nanotechnologies: The Promise and the Peril" (2006) 6:3 Sustainable Development Law & Policy 11, at 11.

[93] *Ibid.*

[94] *Ibid*, at 13.

[95] Chris MacDonald, "Nanotechnology, Privacy and Shifting Social Conventions" (2004) 12:3 Health L. Rev. 37.

[96] *Ibid.*

[97] Davis Baird& Tom Vogt, "Societal and Ethical Interactions with Nanotechnology ('SEIN') — An Introduction" (2004) 1:4 *Nanotechnology Law and Business* 391 at 394.

[98] Ian Kerr & Goldie Bassie, "Building a Broader Nano-network" (2004) 12:3 Health L. Rev. 57.

[99] Scott H. Hughes, "Understanding Conflict in a Postmodern World" (2004) 87 Marq. L. Rev. 681 at 683.

[100] *Ibid.* at 684.

[101] Kang & Cuff, *supra* note 28.