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

ATELIER
DRAGON : INFORMATIQUE UBIQUISTE
Le Suivi Géodépendant

WORKSHOP
UBIQUITOUS COMPUTING DRAGON
Location-Based Tracking

26 septembre/September 26
13h30-16h

Série Terra Incognita, cahier de travail # 4/Terra Incognita, workbook series # 4

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

Table des matières / Table of contents

Biographies

Président : M. Alexander Dix, Ph. D.

M. Alexander Dix, titulaire d'une maîtrise en droit (Londres), a été élu commissaire à la protection des données et à l'accès à l'information par le Parlement de l'État de Berlin en juin 2005. Auparavant, il a exercé les fonctions de commissaire de l'État de Brandebourg pendant sept ans. Il compte 22 années d'expérience dans le domaine de la protection des données et a rédigé de nombreuses publications. À titre de spécialiste des télécommunications et des médias, il préside le Groupe de travail international sur la protection des données dans le domaine des télécommunications (« Groupe de Berlin »). Il est également membre du Groupe « Article 29 » des autorités européennes de protection des données, où il représente les autorités de protection des données des 16 États allemands (*Länder*).
Né à Bad Hombourg dans le Hesse, M. Dix a obtenu un diplôme en droit de l'Université de Hambourg, en 1975, une maîtrise en droit de la London School of Economics and Political Science (école d'économie et de science politique de Londres) de l'Université de Londres, en 1976, et un doctorat en droit de l'Université de Hambourg, en 1977.

Conférenciers

M^{me} Éloïse Gratton

Éloïse Gratton est associée dans le cabinet d'avocats McMillan Binch Mendelsohn, où elle travaille dans les domaines du droit commercial et des technologies de l'information. Avant de se joindre à ce cabinet, elle a été directrice des affaires juridiques et générales d'une entreprise de marketing sans fil. Elle est chef du conseil juridique de la Society of Internet Professionals, qui est établie à Toronto.
À titre de membre du Mobile Marketing Association Privacy & Consumer Acceptance Committee, elle participe activement à la rédaction de lignes directrices sur la protection de la vie privée pour l'industrie du marketing mobile. Elle est vice-présidente du Canadian IT Law Association Ad hoc Privacy Committee et conseillère principale (pour le Québec) de la Canadian Privacy Institute. M^{me} Gratton présente fréquemment des exposés dans le cadre de

Biographies

Chair : Dr. Alexander Dix

Dr. Alexander Dix, LL.M. (Lond.), was elected Commissioner for Data Protection and Freedom of Information by the Berlin State Parliament in June 2005. He was Commissioner of the State of Brandenburg for seven years and has 22 years experience in data protection and has published extensively. A specialist in telecommunications and media, he chairs the International Working Group on Data Protection in Telecommunications ("Berlin Group"). He is also a member of the Art. 29 Working Party of European Data Protection Supervisory Authorities, where he represents the Data Protection Authorities of the 16 German States (Länder).
A native of Bad Homburg, Hessen, he graduated from Hamburg University with a degree in law in 1975. He received a Master of Laws degree from London University after studies at the London School of Economics and Political Science in 1976, and a Doctorate in law from Hamburg University in 1977.

Speakers

Ms. Eloïse Gratton

Gratton is a partner at McMillan Binch Mendelsohn where she practices law in the areas of commercial law and information technology. Prior to joining the firm, she acted as Director of Corporate & Legal Affairs for a wireless marketing company. She serves as head of the Legal Council of the Toronto-based Society of Internet Professionals. As a member of the Mobile Marketing Association Privacy & Consumer Acceptance Committee, she actively participated in drafting privacy guidelines for the mobile marketing industry. She acts as Vice-chair of the Canadian IT Law Association Ad hoc Privacy Committee and is Senior Consultant (for Quebec) of the Canadian Privacy Institute. Ms. Gratton speaks frequently at national and international technology conferences and is a published author on emerging technologies and legal matters. She is the author of the CCH book entitled *Internet and*

conférences nationales et internationales portant sur la technologie et elle a publié divers articles sur les nouvelles technologies et les questions juridiques. Elle est l'auteure d'un livre publié par CCH intitulé *Internet and Wireless Privacy: A Legal Guide To Global Business Practices*.

M. David Lyon, Ph. D.

David Lyon est chercheur principal du Projet de globalisation des données personnelles et directeur du Projet de surveillance à l'Université Queen's.
À titre de professeur, il travaille sur diverses questions liées à la surveillance depuis les années 1980, époque où il soutient que la surveillance est l'un des principaux enjeux des sociétés de l'information dans son ouvrage intitulé *The Information Society: Issues and Illusions* (Polity 1988). Depuis lors, il a pris part à de nombreux débats sur les aspects politiques de l'information et la politique de l'information au Canada et dans le monde entier à la suite de ses recherches et publications, dont *The Electronic Eye* (1994), *Surveillance Society* (2001) et *Surveillance after September 11* (Polity 2003).
Il est le rédacteur en chef fondateur de la revue électronique *Surveillance and Society* et ses recherches portent particulièrement sur les cartes d'identité nationales, la sûreté et la surveillance de l'aviation de même que la promotion de l'étude internationale et interdisciplinaire de la surveillance, à l'échelle internationale. Il prépare actuellement *Identifying Citizens: Software, Social Sorting and the State*, ouvrage qui sera publié par Polity Press en 2008.

M. Michael G. Michael, Ph. D.

Michael G. Michael, Ph. D., M.A.(Hons), M.Th., B.Th., B.A., est théologien et historien. Sa conception de la technologie de l'information et de l'informatique est originale. Actuellement, il est chargé de cours honoraire à l'École des systèmes d'information et de technologie de l'Université de Wollongong, en Australie. Il coordonnait auparavant les questions liées à la sécurité de l'information et des communications et, depuis 2005, il est chargé de cours invité et formateur dans les domaines des services de localisation, de la TI et des droits des citoyens, des principes des affaires électroniques, et de la TI et de l'innovation. Il a présenté de nombreux exposés

Wireless Privacy: A Legal Guide To Global Business Practices.

Dr. David Lyon

David Lyon is the Principal Investigator of the Globalization of Personal Data Project and the Director of the Surveillance Project at Queen's University.
Professor Lyon has been working on surveillance issues since the 1980s, when he discussed surveillance as one of the key issues of information-based societies in *The Information Society: Issues and Illusions* (Polity 1988). Since then he has been involved in many debates over information politics and policy in Canada and around the world as a result of his research and publications including *The Electronic Eye* (1994), *Surveillance Society* (2001) and *Surveillance after September 11* (Polity 2003).
He is a founding editor of the e-journal *Surveillance and Society* and has particular research interests in national ID cards, aviation security and surveillance and in promoting the cross-disciplinary and international study of surveillance. He is currently preparing *Identifying Citizens: Software, Social Sorting and the State* for Polity Press (2008).

Dr. Michael G. Michael

Dr. Michael G. Michael, Ph.D., MA(Hons), MTh, BTh, BA is a theologian and historian who brings a unique perspective on Information Technology and Computer Science. Presently he is an honorary fellow in the School of Information Systems and Technology, at the University of Wollongong, Australia. He is the former coordinator of Information & Communication Security Issues and since 2005 has guest-lectured and tutored in Location-Based Services, IT & Citizen Rights, Principles of eBusiness, and IT & Innovation. He has presented papers at numerous IEEE conferences including the *International Conference on Mobile Business*, the *International*

lors des conférences de l'IEEE, entre autres l'*International Conference on Mobile Business*, l'*International Conference on Mobile Computing and Ubiquitous Networking* et *RFID Eurasia*. Il écrit actuellement en collaboration un livre intitulé *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*. Tout comme Katina Michael, il a introduit les concepts de « surveillance omniprésente » et d'« électrophore » dans les ouvrages consacrés à la protection de la vie privée et à la bioéthique.

M. John B. Morris jr

John B. Morris jr, est avocat général au Center for Democracy & Technology (Centre pour la démocratie et la technologie) et directeur du « projet sur les normes, la technologie et les politiques en matière d'Internet » de cet organisme. Avant de se joindre à CDT en 2001, M. Morris était associé dans le cabinet d'avocats Jenner & Block, où il a plaidé des causes sans précédent sur Internet et le droit relatif au premier amendement. Dans le cadre de son travail sur les normes à CDT, M. Morris a participé activement aux activités du Groupe de travail sur l'ingénierie d'Internet, y compris celles du groupe « GeoPriv » qui s'intéresse à des questions de localisation et de protection des renseignements personnels dans des contextes de communication sans fil et de protocoles de voix sur IP.
M. Morris a reçu son baccalauréat avec grande distinction de l'Université Yale et son J.D. de la faculté de droit de Yale, où il était rédacteur en chef du *Yale Law Journal*. Après ses études de droit, il a travaillé comme avocat au Southern Center for Human Rights, à Atlanta (Georgia), avant d'entrer au cabinet d'avocats Jenner & Block en 1990.

Conference on Mobile Computing and Ubiquitous Networking, and *RFID Eurasia*. He is currently co-authoring a book titled, *Innovative Automatic Identification and Location-Based Services: From Bar Codes to Chip Implants*. Alongside Dr Katina Michael he has introduced the concepts of 'überveillance' and 'electrophorus' into the privacy and bioethics literature.

Mr. John B. Morris, Jr.

John B. Morris, Jr. is General Counsel at the Center for Democracy & Technology, and the Director of CDT's "Internet Standards, Technology and Policy Project." Prior to joining CDT in 2001, Mr. Morris was a partner in the law firm of Jenner & Block, where he litigated groundbreaking cases in Internet and First Amendment law. As part of CDT's "Standards Project," Morris has actively participated in the work of the Internet Engineering Task Force, including the "GeoPriv" group working on location privacy in wireless and voice over IP contexts.
Mr. Morris received his B.A. *magna cum laude* with distinction from Yale University and his J.D. from Yale Law School, where he was the Managing Editor of the Yale Law Journal. Following law school, he worked as a staff attorney at the Southern Center for Human Rights in Atlanta, Georgia before joining Jenner & Block in 1990.

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

Longitude et latitude : *technologies géomatiques et préoccupations en matière de protection de la vie privée*

Longitude and Latitude: *location technologies and privacy concerns*

Par/by:

Murray Long
Murray Long and Associates

Mars 2007/March 2007

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

Lorsque Marco Polo est parti en quête de découvertes, une grande partie du monde était littéralement *terra incognita* — ni connue, ni cartographiée. Aujourd'hui, toute la surface de la Terre est cartographiée et de nouvelles technologies géomatiques permettent de repérer quelqu'un dans un rayon de 10 à 20 mètres n'importe où sur Terre.

Ce mémoire tient lieu de document-ressource pour l'**atelier sur la géolocalisation**. Il décrit les technologies de localisation et leurs diverses applications, permettant ainsi d'explorer les questions inhérentes à la protection de la vie privée, particulièrement celles qui touchent la localisation ou la surveillance des particuliers. Les participants sont invités à faire part de leurs préoccupations et de leurs idées au sujet de la localisation ainsi que des moyens pour assurer que le droit de contrôle des renseignements personnels en matière de localisation soient bien établis à une époque où les technologies de localisation prennent de l'expansion sur le marché.

Qu'est‑ce que la surveillance?

A Report on the Surveillance Society définit ainsi la surveillance : toute attention utile, routinière, systématique et ciblée prêtée aux détails personnels, au nom du contrôle, de l'admissibilité, de la gestion, de l'influence ou de la protection[1]. Lorsqu'elle est accomplie par l'entremise de moyens automatisés, elle est quelquefois appelée surveillance des données[2]. Les technologies géomatiques qui réussissent à repérer une personne ou un objet constituent des éléments critiques de la surveillance des données.

Que sont les technologies géomatiques?

Un document publié en 2005 par des chercheurs canadiens qui travaillent sur le projet de surveillance de l'Université Queen's définit les technologies géomatiques comme étant des technologies qui remplissent trois critères spécifiques : elles peuvent repérer les emplacements, les signaler sur une base continue et le faire en temps réel[3].

Autrement dit, elles peuvent repérer tout corps doté de dispositifs de localisation en tout temps, sans interruption, pourvu que les appareils continuent d'émettre des signaux de localisation qu'ils soient accessibles.

Ces chercheurs ont examiné deux technologies prédominantes dans les applications actuelles de localisation : celles qui repèrent un téléphone

When Marco Polo set out on his voyages of discovery, most of the world was literally *Terra Incognita*-- unknown and unmapped. Today, every part of the Earth's surface has been mapped and new location-based technologies can pinpoint someone's location within 10 to 20 metres, almost anywhere on Earth.

This paper serves as a resource document for the **Geo-tracking Workshop.** It describes location technologies and their various applications so as to explore the inherent privacy issues, particularly those involving tracking or surveillance of individuals. Workshop attendees are invited share their own concerns and insights about location tracking and how best to ensure that rights to control personal location information are solidly entrenched as tracking technologies expand in the marketplace.

What is surveillance?

Surveillance, as defined in *A Report on the Surveillance Society*, is any "purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection."[1] When accomplished through automated means, it is sometimes referred to as "dataveillance".[2] Location technologies that can pinpoint the whereabouts of a person or object are critical elements of dataveillance.

What are location technologies?

A 2005 paper published by Canadian researchers who are working on the Queen's University Surveillance Project defines location technologies as technologies that meet three specific criteria. They can pinpoint locations, they can report these continuously, and they can do it in real time.[3]

In other words, they can locate objects equipped with location-tracking devices at any time and without interruption provided the devices are turned on, emit tracking signals and the signals are accessible.

The Queen's researchers considered two technologies predominant in current location tracking applications: those that locate a cellular telephone or similar wireless device through technology that can be deployed in a cellular phone network; and those that can locate a GPS (Global Positioning System) receiver.

cellulaire ou tout autre appareil sans fil similaire au moyen d'une technologie utilisée dans le cadre d'un réseau de téléphonie cellulaire et celles qui peuvent repérer un récepteur GPS (Global Positioning System).

Néanmoins, d'autres technologies ont été ou peuvent être utilisées pour localiser les mouvements d'une personne, mais de manière plus sporadique. Par exemple, au Royaume-Uni, pays qui possède déjà la plus haute concentration de systèmes de télévision en circuit fermé (TVCF) à des fins de surveillance, la technologie de reconnaissance automatique des numéros de plaque d'immatriculation (RANPI) est un outil de surveillance et de maintien de l'ordre qui gagne rapidement du terrain.

Les systèmes TVCF conventionnels peuvent également être employés pour une localisation plus précise des personnes par le biais de logiciels de reconnaissance faciale. De par sa nature, la reconnaissance faciale n'est pas omniprésente puisqu'elle requiert que le sujet soit constamment visible par une série de caméras.

Les puces d'identification par radiofréquence (IRF) constituent une autre technologie de localisation potentielle. Elles sont devenues de plus en plus petites et de moins en moins coûteuses, menant à de plus grandes attentes en ce qui a trait à leur emploi au niveau des produits à usage personnel. Ces puces sont maintenant fréquemment utilisées pour repérer les conteneurs d'expédition et les palettes dans les ports et les entrepôts et elles sont maintenant intégrées aux produits à usage personnel, comme les articles vestimentaires. Elles peuvent repérer les employés dans l'enceinte d'une entreprise et surveiller la circulation des véhicules sur les autoroutes à péage.

Dans leur livre intitulé *Spychips*, Katherine Albrecht et Liz McIntyre décrivent de façon alarmante un monde futur dans lequel des milliards d'objets seraient munis de puces d'IRF et comment l'emplacement de tout objet et de toute personne serait connu en tout temps et serait accessible à quiconque aurait accès à des bases de données, avec ou sans autorisation[4].

Une telle capacité de surveillance dépendrait d'un immense réseau de lecteurs de puces d'IRF interconnectés car les appareils d'IRF ont une portée de lecture limitée allant de quelques centimètres à quelques mètres[5]. Cependant, les étiquettes d'IRF intégrées aux documents d'identification tels que les permis de conduire, les

Nevertheless, other technologies have been or could be used to track individuals' movements, but more sporadically. For example, in the UK, which already has the highest concentration of closed circuit television (CCTV) systems for surveillance, Automated Number Plate Recognition (ANPR) technology is a rapidly advancing policing and surveillance tool.

Conventional CCTV systems can also be used for more precise tracking of individuals using facial recognition software. By its nature, facial recognition is not ubiquitous as it depends upon individuals being continuously in plain view of successive video cameras.

Radio-frequency identification (RFID) chips are another potential location tracking technology. They have become increasingly smaller and cheaper, leading to greater expectations of their use in individual products. RFID chips are now widely used to track shipping containers and pallets at ports and in warehouses, and are now embedded in individual products, including articles of clothing. They can track employees within company premises and monitor vehicle use on toll highways.

Katherine Albrecht and Liz McIntyre, in their book *Spychips*, paint a disquieting picture of a future world where billions of items contain RFID chips and "the whereabouts of everything and everyone will be known at all times and accessible to anyone with access to the databases, authorized or otherwise".[4]

Such a surveillance capability would depend upon a massive network of interconnected RFID readers, since passive RFID devices have a limited reading range of a few centimetres to a few metres.[5] However, RFID tags embedded in identity documents such as drivers' licenses, immigration visas and passports will permit the intermittent tracking of individuals as they move through RFID-reader equipped checkpoints. The ultimate example of personalization of these devices is implanting them in humans for identification, to store emergency medical information, and even to replace the need for cash or a credit card when visiting a club.

Another intermittent surveillance technology is Wi-Fi Positioning Systems (WPS) which enable Wi-Fi network operators to pinpoint the location of wireless signal-emitting devices such as laptop computers to within 20 to 40 metres. The base of wireless computing users is growing exponentially, providing an exceptional opportunity for new

visas d'entrée et les passeports permettront d'effectuer un suivi intermittent des particuliers alors qu'ils traversent les postes de contrôle d'IRF. L'ultime exemple de la personnalisation de ces appareils est leur implantation dans les êtres humains à des fins d'identification ou d'entreposage de renseignements médicaux d'urgence ou encore pour éliminer le besoin d'avoir sur soi de l'argent comptant ou une carte de crédit lors de visites dans un club.

Les systèmes de positionnement Wi-Fi (SPW) sont un autre exemple de technologie de surveillance intermittente puisqu'ils permettent aux opérateurs des réseaux Wi-Fi de repérer l'emplacement des appareils sans fil émettant des signaux, comme les ordinateurs portables, dans un rayon de 20 à 40 mètres. Le nombre d'utilisateurs d'ordinateurs portables augmente de façon exponentielle, ce qui offre un potentiel exceptionnel pour les nouveaux services commerciaux mobiles, mais aussi pour une surveillance accrue des données.

Ce document examinera brièvement les questions relatives à la protection de la vie privée en matière de localisation qui sont associées aux technologies mentionnées ci-dessus, sous les entêtes suivants :

- Les téléphones cellulaires et les renseignements sur la localisation aux fins de l'intervention en cas d'urgence et les applications commerciales
- La géolocalisation dans la gestion de flottes commerciales et l'emploi de véhicules personnels
- La reconnaissance automatique des numéros de plaque d'immatriculation (RANPI) et les systèmes de localisation TVCF avancés utilisés pour la surveillance publique
- Le potentiel de localisation des technologies d'IRF
- Les SPW et la localisation d'appareils sans fil à usage personnel

Les téléphones cellulaires et les renseignements sur la localisation aux fins de l'intervention en cas d'urgence et les applications commerciales

La technologie

Étant donné la croissance rapide de l'usage des

commercial location-based services, but also increased dataveillance.

This paper will briefly consider the geo-tracking privacy issues associated with all of the above technologies, under the following headings:

- Cell phones and location information for emergency response and commercial applications
- GPS location tracking in commercial fleet management and in personal vehicle use
- Automated Number Plate Recognition (ANPR) and advanced CCTV tracking systems used for public surveillance
- The tracking potential of RFID technologies
- WPS and the tracking of computers and other wireless personal devices.

Cell phones and location information for emergency response and commercial applications

The technology

With the rapid growth in cellular telephone use, emergency services providers (known as Public Safety Answering Points or PSAPs) began demanding that cellular phones offer the same functionality as wireline telephones so police, fire and ambulance services could better locate wireless emergency calls. The first requirements for what is known as wireless E911 originated in the United States and required the introduction of new tracking technologies in the cellular phone network.

The rollout of wireless E911 in the United States, Canada and other countries has occurred in stages. In phase 1, network operators were required to provide PSAPs with limited cell/sector directional information and the cellular phone number of the caller. However, this information had little value in locating a caller, and was used primarily to identify the service to which the call should be routed.

In the second phase (required under revised U.S. Federal Communications Commission (FCC) rules), wireless carriers were expected to employ network-based location technologies to locate the mobile phone user within 50 metres for 67 per cent of 911 calls, and 150 metres for 95 per cent of calls.[6]

Ultimately, network-based technologies were inca-

téléphones cellulaires, les fournisseurs de services d'urgence (connus sous le nom de *centres de prise d'appels pour la sécurité du public* ou CPASP) ont commencé à exiger que les téléphones cellulaires offrent les mêmes fonctions que les téléphones fixes, de sorte que les services policiers, les ambulanciers et les services de prévention des incendies puissent mieux localiser leurs appels d'urgence. Ils ont d'abord exigé le service E911 sans fil qui provient des États-Unis et qui nécessitait l'implantation de nouvelles technologies de localisation au sein du réseau de téléphonie cellulaire.

Le déploiement du service E911 sans fil aux États-Unis, au Canada et dans d'autres pays s'est déroulé par étapes. Au cours de la phase 1, les exploitants de réseaux ont dû offrir aux CPASP de l'information directionnelle limitée sur tout téléphone cellulaire ou le secteur où se trouve le téléphone et le numéro de téléphone cellulaire de l'appelant. Toutefois, ces renseignements étaient peu utiles à la localisation des appelants et servaient principalement à l'identification du service auquel l'appel devait être acheminé.

Au cours de la deuxième phase (exigée en vertu de la version modifiée des règlements de la Commission fédérale des communications des États-Unis), les fournisseurs de services sans fil devaient utiliser des technologies de localisation basée sur le réseau pour repérer les utilisateurs de téléphones cellulaires dans un rayon de 50 mètres pour 67 % des appels au 911 et dans un rayon de 150 mètres pour 95 % des appels[6].

Ultimement, les technologies basées sur le réseau n'ont pas permis les niveaux de précision exigés et les fournisseurs de services sans fil se sont plutôt tournés vers les téléphones équipés de GPS qui peuvent communiquer des renseignements permettant la localisation à quelques mètres près lorsque la ligne de visée avec les satellites GPS n'est pas obstruée. Les autres solutions emploient des téléphones équipés de GPS ainsi qu'un traitement du signal au sein du réseau afin de mieux identifier l'emplacement de l'appelant dans un rayon allant jusqu'à 10 mètres[7].

Au Canada, le suivi de la localisation faisant partie de la phase 2 est présentement en cours d'essai sur le terrain alors qu'aux États-Unis, l'échéancier plus strict établi par la Commission fédérale des communications a poussé les fournisseurs américains à mettre pleinement en œuvre le système dans certaines communautés (aux États-

pable of meeting this accuracy standard and wireless carriers turned instead to GPS-equipped phones which can provide location information to within a few metres if there is clear line of sight to GPS satellites. Other solutions use a hybrid of GPS-equipped phones and signal processing within the network to better identify the caller's location to within 10 metres.[7]

In Canada, phase 2 location tracking is now in field trials while, in the U.S., more aggressive FCC deadlines have pushed U.S. carriers into full implementation in some communities. (In the U.S., a request from a PSAP is required for implementation of Phase 2 wireless E911 within a particular jurisdiction.) E112 is also being rolled out throughout the European Union, with phase 1 ubiquitous in theory by 2003 and higher performance location services expected to penetrate the market by 2006.[8] In reality, many EU countries have not yet begun to implement cellular location tracking, which has resulted in infringement proceedings against 11 EU members.[9]

The privacy implications

E911 services: Historically, the use of wireless location services for E911 purposes has generated little documented privacy concern as the benefits seemingly outweighed any associated privacy loss. Users of GPS-enabled phones can turn off the positioning capabilities, while network operators can restrict the use of location technologies to situations where a caller has dialled 911.[10] Contractual and regulatory rules can also bind PSAPs on their use of location information.

However, mounting concerns about cyber-crime and terrorist activities have now shifted the balance of national security and privacy and expanded the interest in collection and use of location information.[11] U.S. policy makers and regulators, in particular, have been seized with the importance of wireless location services following 9/11.

One report on E911 implementation in the U.S. stated: "the increased emphasis being placed on homeland security, the critical role played by E911 systems and services in assuring homeland security, and the increased dependence on wireless networks, make the automatic provision of location information with wireless emergency calls as much a national priority as a local one".[12]

Law enforcement and security access: The legal basis for U.S. law enforcement agencies to

Unis, les CPASP doivent présenter une demande s'ils désirent déployer la phase 2 de l'E911 sans fil sur un territoire donné). L'E112, pour sa part, est en cours de déploiement au sein de l'Union européenne. La phase 1 devait théoriquement être implantée partout au plus tard en 2003 et les services de localisation de haute précision devaient pénétrer le marché au plus tard en 2006[8]. En réalité, de nombreux pays de l'Union européenne n'ont pas encore commencé à mettre en œuvre la localisation par cellulaire, ce qui a entraîné des procédures juridiques contre 11 membres de l'Union[9].

Les conséquences sur la protection de la vie privée

Les services E911 : Historiquement, l'utilisation des services de localisation sans fil aux fins de l'E911 a généré peu de questions liées à la vie privée qui aient été documentées puisque les avantages semblaient surpasser les pertes. Les utilisateurs des téléphones équipés de GPS peuvent désactiver la fonction de positionnement et les exploitants de réseaux peuvent restreindre l'utilisation des technologies de localisation dans des situations où les appelants composent le 911[10]. Les règles et les règlements contractuels peuvent également lier les CPASP quant à l'usage qu'ils font des renseignements recueillis.

Toutefois, l'inquiétude croissante causée par la cybercriminalité et les activités terroristes a mis à l'épreuve la sécurité nationale et le respect de la vie privée tout en accroissant l'intérêt porté à la cueillette et à l'utilisation des renseignements provenant de la localisation[11]. Des responsables américains des politiques et de la réglementation ont été saisis de l'importance des services de localisation sans fil après les événements du 11 septembre 2001.

Un rapport portant sur le déploiement des services E911 aux États-Unis a indiqué que la recrudescence de l'attention portée à la sécurité intérieure, le rôle central des services et des systèmes E911 pour la sécurité intérieure et la dépendance accrue face aux réseaux sans fil font de l'offre automatique des services de localisation lors d'appels sans fil en cas d'urgence autant une priorité nationale que locale[12].

L'application de la loi et l'accès à la sécurité : La loi intitulée *Communications Assistance for Law Enforcement Act (CALEA)* a permis aux organismes américains d'exécution de la loi d'obtenir des renseignements sur la localisation des utilisateurs de téléphones cellulaires[13]. Cette

obtain mobile phone users' location information was established in the *Communications Assistance for Law Enforcement Act* (CALEA) .[13] The act directed the telecommunications industry to design, develop and deploy solutions to meet law enforcement requirements to conduct lawfully-authorized electronic surveillance. Location information protocols developed under CALEA permit law enforcement agencies—with a court order—to obtain whatever caller location information a wireless carrier is able to produce.[14]

Privacy advocates have raised concerns about potential lowering of standards for law enforcement agencies to obtain such information following passage of the *USA PATRIOT ACT* which expanded FBI surveillance powers. In 2005, two U.S. magistrates (in separate decisions) ruled that permitting the FBI and other police agencies to track the location of cell phone users under this *Act* under a routine tracking order, without showing some evidence of actual criminal activity, violated constitutional rights of protection against "unreasonable search and seizure."[15]

More recently, in 2006, a different judge determined that the FBI could monitor the location of Americans by constantly tracking their cell phone signals without providing evidence of criminal activity.[16]

In Canada, similar privacy concerns have been expressed about a proposed law to strengthen Canadian law enforcement intercept capabilities, including to obtain wireless location information under a production order where the police have "reasonable grounds to suspect" criminal activity. In response, Privacy Commissioner Jennifer Stoddart noted a former Supreme Court Justice's view that the day has now finally arrived when a device has been developed "that will be able to track our every movement for indefinite periods even without visual surveillance".[17] She urged that, at the very least, such unseen, ubiquitous and precise tracking capability should only be permitted on a higher threshold of "reasonable grounds to believe" rather than "reasonable grounds to suspect".[18]

One of the privacy concerns about law enforcement location tracking is that it introduces "wholesale surveillance." As U.S. privacy and security expert Bruce Schneier has written:

> "Years ago, surveillance involved trench-coated detectives following people down streets. It was laborious and expensive, and was only used when there was reasonable

loi exige du secteur des télécommunications qu'il conçoive, élabore et applique des solutions lui permettant de satisfaire aux exigences de la loi en matière de surveillance électronique. Les protocoles sur les renseignements liés à la localisation qui ont été développés sous le régime de la *CALEA* permettent aux organismes responsables de l'application de la loi d'obtenir, sous réserve d'une ordonnance d'un tribunal, tous les renseignements que les fournisseurs de services sans fil peuvent communiquer sur la localisation d'un appelant[14].

Les défenseurs du respect de la vie privée ont fait part de leurs préoccupations au sujet de l'affaiblissement potentiel des normes qui permettent à ces organismes d'acquérir de tels renseignements à la suite de l'adoption de la *USA PATRIOT Act.* Cette dernière a entraîné l'accroissement des pouvoirs de surveillance du FBI. En 2005, deux juges américains ont déclaré, dans deux décisions distinctes, que cette loi ne permettait ni au FBI ni aux autres organismes policiers de suivre la localisation d'un utilisateur de téléphone cellulaire à l'aide d'une simple demande de localisation sans preuve d'activité criminelle et qu'un tel geste constituait une infraction aux droits constitutionnels assurant la protection des citoyens contre toute enquête ou saisie déraisonnable[15].

Plus récemment, en 2006, un autre juge a déterminé que le FBI pouvait surveiller la localisation des Américains en effectuant le suivi continu des signaux de leurs téléphones cellulaires, et ce, sans devoir fournir de preuve d'activité criminelle[16].

Au Canada, des inquiétudes similaires ont été exprimées au sujet d'un projet de loi visant à permettre davantage l'interception légale de renseignements au Canada, notamment des renseignements portant sur la localisation sans fil obtenus à l'aide d'un ordre des forces policières lorsque celles-ci ont des motifs raisonnables de soupçonner une activité criminelle. Ce à quoi Jennifer Stoddart, commissaire à la protection de la vie privée, répliqua en citant un ancien juge de la Cour suprême qui affirme que le jour était enfin venu où un appareil pourra suivre à la trace chacun de nos mouvements pendant des périodes indéterminées, et ce, même sans surveillance visuelle[17]. Elle a argué qu'à tout le moins, une telle surveillance invisible, constante et précise devrait être permise sur une base plus restreinte, notamment en exigeant des motifs raisonnables de croire à l'existence d'activités

> suspicion of a crime. Modern surveillance is the police officer sitting at a computer with a satellite image of an entire neighborhood. It's the same, but it's completely different. It's wholesale surveillance."[19]

James Dempsey, Policy Director with the U.S.-based Center for Democracy & Technology, likened the implementation of E911 to turning cell phones into ankle bracelets, and called for stronger constitutional restrictions on law enforcement's ability to obtain court orders for location data.[20]

David Lyon, Stephen Marmura and Pasha Peroff of the Queen's University Surveillance Project have also pointed out the potential of E911 mobile phone location data to be used for greater police surveillance.

> "It seems equally likely that the continued development of [this] system in Canada will provide law enforcement in this country with ever more precise and revealing data on individuals suspected of committing illegal acts. At the same time, such developments will likely go unnoticed by many or most citizens."[21]

Consumer malaise: Lack of citizen concern about location tracking may become a more important issue as organizations, particularly communications carriers, offer commercial services based on mobile telephones. So far, services such as vehicle tracking for fleet operators are focussed on commercial users. However, as more precise location information becomes available, it will offer opportunities for location-based text messaging and advertising to consumers, as well as services aimed at finding individuals, such as child-locator or friend-locator services. Australian location services privacy expert Dr. Katina Michael, in fact, describes location-based technologies as a "cultural-changing force" where "pervasive computing will become a dominant force in the way we live, work, and interact with one another".[22]

As David Lyon and his colleagues point out, "the opportunities to develop new revenue options and pitch services directly to individual needs are endless, and could become increasingly attractive as LBS (location-based services) is integrated with a 'rise in complementary technologies such as digital mapping and wireless communications peripherals'."[23]

In *Internet and Wireless Privacy*, Éloïse Gratton

criminelles plutôt que de se fonder sur des soupçons[18].

Une des inquiétudes liées à la surveillance légale par localisation est de voir paraître une surveillance tout azimut. Bruce Schneier, expert américain en vie privée et en sécurité, a écrit :

> « Il y a des années, la surveillance était l'affaire de détectives en imper qui suivaient les gens dans les rues. C'était compliqué et coûteux et on ne le faisait que lorsqu'il était raisonnable de soupçonner un crime. La surveillance moderne, c'est plutôt un policier assis devant un ordinateur à regarder l'image satellitaire du quartier tout entier. C'est la même chose, mais, en même temps, c'est complètement différent. C'est la surveillance en bloc[19]. » [Traduction]

James Dempsey, directeur des politiques au sein du *Center for Democracy & Technology*, basé aux États-Unis, a comparé l'implantation de l'E911 à une transformation des téléphones cellulaires en bracelets émetteurs à la cheville et il a demandé l'imposition de restrictions constitutionnelles plus sévères régissant l'obtention, par les organismes d'exécution de la loi, d'ordonnances de la cour visant des données de localisation[20].

David Lyon, Stephen Marmura et Pasha Peroff, du projet de surveillance de l'Université Queen's, ont également fait remarquer qu'il est possible que les données de localisation provenant des téléphones cellulaires E911 soient utilisées dans le cadre d'une surveillance policière accrue.

> « Il semble tout aussi probable que le développement continu de ce système au Canada permettra une meilleure application de la loi au pays grâce à des données plus précises et plus révélatrices sur les personnes soupçonnées d'avoir commis des actes illégaux. Du même coup, de nombreux citoyens — sinon la majorité d'entre eux — ne remarqueront pas de tels développements[21]. » [Traduction]

Un malaise parmi les consommateurs : Le manque d'intérêt des citoyens pourrait devenir une question plus importante à mesure que les organismes, particulièrement les fournisseurs de produits de communications, offrent des services commerciaux par l'entremise du téléphone cellulaire. Jusqu'à maintenant, les services tels que le suivi des déplacements des véhicules au sein de flottes ont été axés sur les utilisateurs commerciaux. Toutefois, à mesure que des

cites research that consumer location services based on E911 technology could account for 40 per cent of a carrier's mobile data services revenue by 2007.[24] Ms. Gratton identified such services as emergency roadside assistance, mapping and security services for vehicles, proximity-based advertising, a friends finder service, M-commerce at point of sale, and even M-dating where your cell phone location helps a prospective partner locate you.

Useful v intrusive: A 2003 study suggested that individuals' concerns about the intrusiveness of mobile phone-based location services went down as the usefulness of the service went up. For example, of four proposed services, study participants considered most "privacy invasive" one that would allow a retailer to send a message suggesting it was time for lunch whenever a mobile phone user passed a restaurant. Considered less invasive were services that would automatically set the ring function to silent mode whenever the user attended a meeting, went to class, went to a movie or entered a restaurant. A service ranked highly useful but also highly intrusive would tell users the location of predefined friends, provided they also had mobile phones.[25]

Where to go from here?

The introduction of new mobile phone-based location services raises several important questions:

- What level of notice and consent should be required before carriers may use or disclose location information to third parties for commercial purposes?
- Under what conditions should law enforcement agencies have access to location information for surveillance purposes and what safeguards are required to prevent abuse of such access?
- What privacy solutions provide users greater control over their location information when using cellular phones or similar devices?

GPS location tracking in commercial fleet management and in personal vehicle use

The technology

The Global Positioning System (GPS) provides accurate location and timing data to users world-

renseignements de localisation plus précis deviendront disponibles, les consommateurs se verront offrir des services de messagerie et de publicité basés sur l'emplacement ainsi que des services visant à localiser des personnes, que ce soit un enfant ou un ami. Katina Michael, experte australienne en protection de la vie privée dans les services de localisation, décrit en fait les technologies basées sur la localisation comme étant une force capable de changer notre culture et par laquelle l'informatique entrera dans nos vies et deviendra une force dominante dans les modes de vie, de travail et d'interaction[22].

Comme l'indiquent David Lyon et ses collègues, « les occasions d'affaires qui se développent à partir des nouvelles sources de revenus et de la possibilité de vendre des services qui répondent directement aux besoins des consommateurs sont infinies et pourraient s'avérer de plus en plus attrayantes à mesure que les services basés sur l'emplacement seront intégrés à l'accroissement des technologies complémentaires comme la cartographie numérique et les périphériques de communication sans fil[23] ». [Traduction]

Dans le document intitulé *Internet and Wireless Privacy*, Éloïse Gratton cite des études qui révèlent que les services de localisation à l'intention des consommateurs basés sur la technologie E911 pourraient représenter 40 % de revenus provenant des services de données mobiles des fournisseurs d'ici 2007[24]. M^me^ Gratton a énuméré quelques-uns de ces services : l'assistance routière d'urgence, la cartographie, les services de sécurité automobile, la publicité selon l'emplacement, les services de localisation d'amis, le commerce mobile au point de vente et même les services de rencontre par téléphone cellulaire permettant à un partenaire potentiel de vous localiser.

Utile ou envahissant? Une étude réalisée en 2003 suggère que les craintes des consommateurs face aux services de localisation par l'entremise des téléphones cellulaires diminuent à mesure que croît l'utilité du service. Par exemple, des quatre services proposés, les participants à l'étude ont considéré qu'un service qui permettrait à un détaillant d'envoyer un message indiquant qu'il est l'heure de manger chaque fois que l'usager passe devant un restaurant était celui qui représentait la plus grande atteinte à la vie privée. À l'inverse, ils ont considéré les services qui placeraient les appareils en mode silencieux dès que les usagers seraient en réunion, en classe, au cinéma ou au

wide using 24 satellites and sophisticated signal triangulation technology. GPS is vital to commercial aviation and marine transportation, surveying and mapping, and a growing number of other commercial applications.

Originally developed as a military system, the Pentagon first made GPS available for commercial use under a selective availability policy which restricted signal accuracy to within 30 metres. On May 1, 2000, this signal degradation feature was turned off allowing civilian users to pinpoint locations with up to three metre accuracy. GPS is available free of charge, worldwide for peaceful civil, commercial and scientific applications.

To end reliance on the U.S system (which the Bush Administration has stated could be selectively disabled to prevent use by terrorist groups or hostile nations[26]), the European Union and European Space Agency are planning a competitive system known as GALILEO. However, disputes among European firms building the €3.2 billion project are likely to delay commercial operations until well after 2010.[27]

There are close to two million GPS/wireless devices in use in the U.S alone, monitoring fleet vehicles, trailers, construction equipment and mobile workers. The number is expected to grow to close to six million by 2009.[28] One analyst has predicted the number of commercial GPS users in the U.S. will reach nearly 70 million by 2011.[29]

The privacy implications

Two GPS applications have raised privacy concerns in recent years. The first is the growing use in fleet management systems to compute precise location of company vehicles, whether the vehicles are stationary or moving, and the speed and direction of travel. This data is often combined with vehicle diagnostics data and maintenance schedules to improve fleet efficiency. A linked use is other employee tracking, such as providing workers with GPS-equipped cell phones in order to monitor their location offsite.

The second application is the growing use of GPS technology in personal vehicles, including car rentals. A 2002 GPS world markets study estimated that in-vehicle navigation and telematics services would be the largest GPS market segment by 2006, accounting for 41 per cent of all GPS use.[30]

restaurant comme étant les moins envahissants. Une fonction permettant de trouver l'emplacement d'amis prédéterminés munis d'un téléphone cellulaire est considérée à la fois très utile et très envahissante[25].

Que nous réserve l'avenir?

La mise en marché de nouveaux services de localisation par téléphone cellulaire soulève plusieurs questions importantes :

- Quel préavis et quel degré de consentement devraient être nécessaire pour que les fournisseurs puissent utiliser ou divulguer des renseignements de localisation à de tierces parties pour des fins commerciales?
- Sous quelles conditions les organismes responsables de l'exécution de la loi devraient-ils avoir accès à ces renseignements pour des fins de surveillance et quelles mesures doit-on adopter afin d'éviter les abus?
- Quelles solutions permettent aux usagers d'exercer un plus grand contrôle sur les renseignements qui concernent leurs déplacements lorsqu'ils utilisent des téléphones cellulaires ou d'autres appareils similaires?

La géolocalisation dans la gestion de flottes commerciales et l'emploi de véhicules personnels

La technologie

Le système mondial de localisation (GPS) fournit des données spatio-temporelles précises aux utilisateurs du monde entier grâce à l'emploi de 24 satellites et à une technologie sophistiquée de triangulation des signaux. Le système est d'une importance capitale pour l'aviation commerciale et le transport marin, l'arpentage et la cartographie et un nombre croissant d'autres applications commerciales.

Développé au départ comme système militaire, le GPS a d'abord été rendu disponible à des fins commerciales par le Pentagone en vertu d'une politique de disponibilité sélective qui limitait la précision des signaux à un rayon de 30 mètres. Le 1er mai 2000, cette limite a été abolie, permettant aux utilisateurs civils de repérer l'emplacement d'un objet avec une précision allant jusqu'à trois mètres près. Le GPS est disponible gratuitement à l'échelle mondiale pour des

Commercial vehicles/employee tracking: Employee tracking and use of GPS to track company vehicles has raised numerous privacy issues. In Canada, in an important finding under the federal *Personal Information Protection and Electronic Documents Act*, the Office of the Privacy Commissioner determined that

> i) employee consent was required to collect GPS location data that could be associated with an individual employee (although such consent could be implied through the employment relationship), and
>
> ii) the purposes for collecting such data must be reasonable.[31]

Reasonable purposes included asset protection and management, worker safety, and improved productivity by integrating GPS with the vehicle dispatch system.

However, the Office concluded that "performance management" of individual employees via inferences drawn from GPS data was overly privacy invasive and therefore in contravention of the law. The Commissioner stated that "[W]hile using GPS to track a vehicle is not overly privacy invasive, routinely evaluating worker performance based on assumptions drawn from GPS information impinges on individual privacy."[32]

In the U.S., where worker privacy rights are poorly protected by state or federal laws, only the State of Connecticut has legislation requiring employers that conduct electronic monitoring to post a notice in the workplace. In civil litigation, however, courts have set limits on employee surveillance outside the workplace, ruling that it must be reasonable, unobtrusive and for a job-related purpose.[33] Employers are, nevertheless, within their legal rights to use GPS monitoring within the workplace, subject to worker ability to limit use through labour actions. For example, the Teamsters Union won a battle with UPS that prevented the company from using GPS tracking for discipline purposes.[34]

In the European Union, where the EU Directive[35] requires employment information be protected under law, countries have developed guidelines on location monitoring. For example, the UK Information Commissioner has published guidelines specifying that employers must consider whether the benefits of monitoring justify the adverse impact. The guidelines add that, where private use of a vehicle is allowed, monitoring its movements when used privately, without the freely given consent of the user, will rarely be justified. The Com-

applications civiles, commerciales et scientifiques pacifiques.

Pour mettre fin à la dépendance quant au système américain (lequel, selon l'administration Bush, pourrait être désactivé sélectivement afin de prévenir son utilisation par les groupes terroristes ou les nations hostiles[26]), l'Union européenne et l'Agence spatiale européenne prévoient établir un système concurrentiel connu sous le nom de GALILEO. Cependant, des désaccords entre les firmes européennes chargées de la construction du projet de 3,2 milliards d'euros sont susceptibles de retarder les applications commerciales jusqu'à bien après 2010[27].

Il existe près de deux millions d'appareils GPS/ sans-fil aux États-Unis seulement, lesquels surveillent les flottes de véhicules, les remorques, le matériel de construction et les travailleurs mobiles. On prévoit que ce nombre passera à près de six millions en 2009[28]. Un analyste a prédit que le nombre d'utilisateurs d'appareils GPS commerciaux atteindra près de 70 millions d'ici 2011[29].

Les conséquences sur la protection de la vie privée

Dans les dernières années, deux applications GPS ont suscité des préoccupations quant à la protection de la vie privée. La première consiste en l'usage croissant de systèmes de gestion de flottes pour déterminer l'emplacement précis des véhicules d'entreprise, qu'ils soient stationnaires ou en mouvement, ainsi que leur vitesse et leur direction. Ces données sont souvent combinées à celles du diagnostic et de l'entretien des véhicules afin d'améliorer l'efficacité de la flotte. Fournir aux employés des téléphones cellulaires avec récepteur GPS permet également de surveiller leur emplacement hors site.

La deuxième application est l'usage croissant de la technologie GPS au niveau des véhicules personnels, y compris les véhicules loués. Une étude effectuée en 2002 portant sur les marchés mondiaux du GPS a estimé que la navigation automobile et les services télématiques formeraient le plus grand segment du marché GPS d'ici 2006, soit 41 % de toute utilisation du GPS[30].

La localisation des véhicules commerciaux et des employés : La localisation des employés et l'emploi de la technologie GPS pour repérer les véhicules d'entreprise ont suscité de nombreuses

missioner recommends a 'privacy button' or other arrangement that allows the monitoring to be disabled.[36]

Monitoring private vehicles: GPS devices have also found widespread use in private vehicles for mapping and manufacturer support services. General Motors' OnStar system, for example, is now used by more than four million subscribers and provides a platform for a range of new location-based services such as location-based advertising. As early as 2001, OnStar President Chet Huber explained how in-vehicle, location-prompted marketing might work:

> "At some point, you would set up your profile and all of the things you're shopping for – maybe not urgently shopping for but they're on your to-buy list – will get bounced against the database. You'll be driving along and it will say, 'Oh, by the way, within three miles of where you are now, that DVD player you said you wanted is on sale at Circuit City.'"[37]

While such location-based marketing would ostensibly be based on customers setting up profiles and consenting to sharing data with marketers, privacy advocates have raised questions about such services.

Beth Givens, founder of the Privacy Rights Clearinghouse, observed that, with the growing number of monitoring systems, "Now, the car is Big Brother".[38]

The event that shone the spotlight on auto monitoring was Acme Rent-a-Car's practice of using GPS to monitor its customers' driving speeds, then fining them directly if they exceeded 126 Km/ h (79 mph). Details of the monitoring were hidden in the fine print of the rental agreement. In one widely reported incident, Acme docked a customer $450 for speeding three times. A Connecticut court ordered Acme to stop this practice and pay back about $12,000 in fines it had collected since the monitoring began.

Where to go from here?

- To what extent is employee and customer surveillance reasonable or warranted?
- How should GPS system operators provide notice of monitoring and how should they obtain consent for such practices?
- Under what conditions should location data be

préoccupations quant à la protection de la vie privée. Au Canada, le Commissariat à la protection de la vie privée du Canada a déterminé que sous le régime de la *Loi sur la protection des renseignements personnels et les documents électroniques* :

> i) le consentement des employés est requis pour recueillir les données reliées à leur localisation (bien qu'un tel consentement pourrait être implicite par le biais de la relation d'emploi);
>
> ii) les fins pour lesquelles les données sont recueillies doivent être raisonnables[31].

Les fins raisonnables comprennent la protection et la gestion des biens, la sécurité des travailleurs et l'amélioration du rendement en intégrant le GPS au système de répartition des véhicules.

Toutefois, le commissariat a également déterminé que l'utilisation des conclusions tirées des données GPS dans le cadre de la gestion du rendement des employés portait trop atteinte à la vie privée et contrevenait à la Loi. La commissaire a déclaré que si l'utilisation du GPS dans le but de repérer un véhicule ne constitue pas une atteinte sérieuse à la vie privée, évaluer régulièrement le rendement des travailleurs à partir de conclusions tirées de données recueillies par le GPS a quant à elle une incidence sur la vie privée[32].

Aux États-Unis, là où les droits en matière de protection des renseignements personnels des travailleurs ne sont pas bien protégés par les lois fédérales ni par celles des divers États, seul le Connecticut a adopté une loi obligeant les employeurs qui choisissent d'effectuer une surveillance électronique d'afficher un avis à cet effet en milieu de travail. Cependant, lors de procès civils, les tribunaux ont limité la surveillance des employés à l'extérieur du milieu de travail de façon à ce qu'elle soit raisonnable, discrète et reliée à l'emploi[33]. Néanmoins, les employeurs ont le droit de faire appel à la surveillance GPS en milieu de travail, sous réserve de mesures syndicales permettant à l'employé de limiter son usage. Par exemple, la *Teamsters Union* a remporté une bataille devant UPS en empêchant l'entreprise d'utiliser la surveillance GPS à des fins disciplinaires[34].

Au sein de l'Union européenne, une directive[35] requiert que les renseignements liés à l'emploi soient protégés conformément à la loi; les pays ont élaboré des lignes directrices sur le repérage.

> made available to third parties, including law enforcement agencies?

ANPR and advanced CCTV tracking systems used for public surveillance

The technology

ANPR systems: Automated Number Plate Recognition (ANPR) technology, which the UK is now rolling out as a nation-wide policing and surveillance tool, is just one example of how video surveillance systems are being adapted with advanced digital surveillance features.

The UK ANPR system records license plate numbers using optical character recognition technology combined with digital cameras mounted in police vehicles, or in conjunction with existing CCTV systems. In a pilot project by 23 police departments underway since 1994, ANPR proved capable of checking up to 3,000 number plates per hour of vehicles traveling up to 160 Km/h. Newer infrared cameras produce an accuracy rate of 95 per cent. The Home Office is now implementing a national program and establishing a national vehicle intelligence data warehouse. Under such a system, every vehicle using public roadways could be recorded as it passed by strategically located ANPR cameras.[39]

Facial recognition systems: Another example of advanced video surveillance is the use of facial recognition technology. In 2001 Dr. Ann Cavoukian, Ontario's Information and Privacy Commissioner, investigated the use of such technology in Ontario's eight casinos which are regulated by a public body, the Ontario Alcohol and Gaming Commission.[40]

The casinos used a facial recognition technology developed by Biometrica Systems Inc. and a database of known and suspected casino cheats. Casinos also had access to a computer network that allows North American casinos to rapidly communicate with each other about suspected cheaters. Ontario casinos' use of this technology was overseen by specially trained police officers who only accessed the facial recognition software database when they had reasonable suspicion that an individual was engaging in criminal activity.

The privacy implications

The Commissioner concluded that this use of facial recognition technology coupled with video surveillance complied with the province's privacy legislation. However, she also determined that a pri-

Par exemple, le commissaire à l'information du Royaume-Uni a publié des lignes directrices spécifiant que les employeurs doivent déterminer si les bienfaits de la surveillance justifient les méfaits. On ajoute que dans les cas où l'utilisation privée d'un véhicule est permise, une surveillance de celui-ci sera rarement justifiée sans l'obtention du consentement de l'utilisateur. Le commissaire recommande l'installation d'un « bouton de respect de la vie privée » ou d'un autre dispositif qui permettrait de désactiver la surveillance[36].

Surveillance des véhicules privés : Les appareils GPS ont trouvé de multiples applications dans les véhicules privés dans le cadre de la cartographie et des services d'appui aux manufacturiers. Le système OnStar de General Motors, par exemple, est maintenant employé par plus de quatre millions d'abonnés et constitue une plate-forme pour une gamme de nouveaux services de localisation, comme la publicité selon l'emplacement. Dès 2001, Chet Huber, président d'OnStar, expliquait le fonctionnement de cette publicité :

> « L'usager saisirait son profil, et les articles qu'il désire acheter maintenant — ou même ceux qui ne sont pas urgents, mais qu'il devra acheter plus tard — seront ajoutés à la base de données. Lorsqu'il passera à proximité d'un endroit où les articles sont disponibles, le système l'en avertira en lui indiquant, par exemple, que le lecteur DVD qu'il cherche est en promotion à trois kilomètres à Circuit City[37]. » [Traduction]

Bien qu'une telle approche marketing viserait les clients prêts à établir des profils et à partager des données avec les spécialistes du marketing, les défenseurs de la vie privée ont soulevé des préoccupations à cet égard.

Beth Givens, fondatrice de Privacy Rights Clearinghouse, a observé qu'avec le nombre croissant de systèmes de surveillance, l'automobile est maintenant devenue *Big Brother*[38].

La pratique d'Acme Rent-a-Car, qui employait le GPS pour surveiller la vitesse de conduite de ses clients et leur imposer une amende s'ils dépassaient 126 km/h (79 mi/h), a mis en évidence la surveillance utilisée dans les véhicules automobiles. Les détails de la surveillance étaient subtilement dissimulés dans le contrat de location. Dans un incident hautement médiatisé, Acme a imposé 450 $ à un client pour avoir fait de la vitesse à trois reprises. Un tribunal

vacy impact assessment should have been conducted before the system was introduced and notices should be posted in casinos to advise patrons that police may be collecting their personal information by both video surveillance and face recognition technology.

Ms. Cavoukian also pointed out that this use of biometrically enhanced video surveillance is a far cry from the type of enhanced scanning used in other public environments. She cited the scanning by Tampa, Florida police of faces of an estimated 100,000 fans and workers at the 2001 SuperBowl. The images were digitally scanned and covertly compared to an extensive, customized database of known felons, terrorists and con artists.[41]

The American Civil Liberties Union (ACLU) was extremely troubled by this event and the announced use of facial recognition software for other public surveillance projects. The ACLU observed that it was "unprecedented expansion" in high-tech surveillance and the technology should not be used to create a "virtual line up" of Americans who are not suspected of having done anything wrong.[42]

This led New York lawyer Mark Milone to ask, in an article about biometric surveillance, "How many times a day do we want to be the subject of a lineup when we leave our homes?".[43]

Stating that such advanced surveillance facilitates the tracking of individuals, potentially on a national scale, Mr. Milone called for governments and industry to pay closer attention to the risks of such surveillance technology.

Integrating databases and surveillance systems: The technological capacity for biometrically-enhanced surveillance is increasing at a relentless pace. While systems now in place are geographically limited – for example, New York's Statue of Liberty now incorporates a facial recognition system linked to a U.S. database of terror suspects[44] – the time may come, as the ACLU warns, when the entire life of a city could be monitored, with vast databases of stored imagery that can be scanned with facial recognition technology to identify people, learn where they have been and perhaps even where they are at the present moment.[45]

The prospect of a Europe-wide database of passport, visa and residence permits has also prompted several European data commissioners to comment that such a system risks "becoming a

du Connecticut a ordonné à Acme de cesser cette pratique et de rembourser environ 12 000 $ en amendes qu'elle avait recueillies.

Que nous réserve l'avenir?

- Jusqu'à quel point la surveillance des employés et des clients est-elle raisonnable ou justifiée?
- Comment les opérateurs de GPS devraient-ils aviser les gens qu'ils pourraient faire l'objet de surveillance et comment devraient-ils obtenir leur consentement?
- Sous quelles conditions les données sur l'emplacement devraient-elles être mises à la disposition des tierces parties, comme les organismes d'exécution de la loi?

La reconnaissance automatique des numéros de plaque d'immatriculation (RANPI) et les systèmes de localisation TVCF avancés utilisés à des fins de surveillance publique

La technologie

Les systèmes de RANPI : La technologie de RANPI, que le Royaume-Uni est en train d'adopter en tant qu'outil de surveillance à l'échelle nationale, n'est qu'un exemple de système de surveillance vidéo adapté doté de caractéristiques de surveillance numérique avancée.

Le système RANPI du Royaume-Uni enregistre les numéros de plaque d'immatriculation à l'aide d'une technologie utilisant la reconnaissance des caractères optiques ainsi que les appareils photo numériques installés dans les voitures de police ou les systèmes TVCF existants. Dans le cadre d'un projet pilote en cours depuis 1994 visant 23 services de police, le système RANPI s'est avéré capable de vérifier, par heure, jusqu'à 3 000 numéros de plaque appartenant à des véhicules qui roulaient jusqu'à 160 km/h. Les nouvelles caméras à infrarouges sont précises à 95 %. Actuellement, le Home Office instaure un programme national et établit une base de données nationale provenant de la surveillance des véhicules. Sous un tel système, tout véhicule empruntant une voie publique pourrait être enregistré lorsqu'il passe aux endroits stratégiques où sont installées les caméras de RANPI[39].

Le système de reconnaissance faciale : La technologie associée à la reconnaissance faciale

mass surveillance infrastructure tracking the movements of all residents and citizens".[46]

The same can be said of any type of advanced surveillance system that relies on readily observable but uniquely identifiable information such as license plates and facial characteristics which can be linked to a specific location.

Where to go from here?

The privacy community needs to consider what positions it will take and what concerns it will raise as such systems inevitably expand in scope and use.

- Should system controllers be required to establish reasonable grounds for extensive surveillance systems?
- Is advising the subjects the only constraint on use of these systems?
- Are there situations when surveillance systems are too fundamental an invasion of privacy?

The tracking potential of Radio Frequency Identification (RFID) systems

The technology

RFID systems are an automated identification method that relies on storing and retrieving data from RFID tags using radio waves. The tags are miniaturized, low cost transmitters with varying reading ranges that can be embedded in products, vehicles, animals—and even humans. The tags can be "promiscuous", meaning they can be read by any RFID reader; or secure, requiring some type of password or authentication.

Implanting in humans has generated the most attention as a potential location tracking technology. In 2004 the *Chicago Sun-Times* reported that at least 160 federal prosecutors and investigators working for Mexico's Attorney General Office had received subcutaneous chip implants, with key members of the military, police and even staff in the President's office to follow.[47]

In Canada, RFID tags have replaced bar codes for tracking cattle destined for slaughterhouses, and for vehicle tracking on toll highways in two provinces. But, at least so far, government have not used them in any widespread public applications.

est un autre exemple de système de surveillance vidéo avancé. En 2001, D[re] Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario, a étudié l'utilisation d'une telle technologie dans huit casinos de l'Ontario qui sont réglementés par un organisme public, soit la Commission des jeux et de l'alcool de l'Ontario[40].

Les casinos ont employé cette technologie, conçue par Biometrica Systems Inc., ainsi qu'une base de données comprenant le nom des tricheurs connus ou soupçonnés. Les casinos avaient également accès à un réseau informatique permettant aux casinos d'Amérique du Nord de se transmettre des données rapidement. L'utilisation de cette technologie dans les casinos de l'Ontario a été supervisée par des policiers spécialisés qui n'ont accédé à la base de données du logiciel de reconnaissance faciale que lorsqu'ils avaient un soupçon raisonnable concernant une activité criminelle.

Les conséquences sur la protection de la vie privée

La commissaire a conclu que l'utilisation de la reconnaissance faciale et de la surveillance vidéo a respecté les lois relatives à la protection de la vie privée de la province. Cependant, elle a aussi déterminé qu'une évaluation des facteurs relatifs à la vie privée aurait dû avoir lieu avant l'introduction du système et que des avis auraient dû être affichés dans les casinos afin d'informer les clients que les policiers allaient possiblement recueillir leurs renseignements personnels au moyen de la surveillance vidéo et de la reconnaissance faciale.

En outre, M[me] Cavoukian a souligné que l'utilisation de ce type de surveillance vidéo améliorée sur le plan biométrique est loin du système à balayage amélioré qui est employé dans d'autres environnements publics. Elle a mentionné que des policiers de Tampa, en Floride, ont balayé environ 100 000 visages de partisans et de travailleurs dans le cadre du SuperBowl 2001. Les images ont été balayées numériquement puis secrètement comparées à une base de données exhaustive et personnalisée de criminels, de terroristes et d'arnaqueurs[41].

L'American Civil Liberties Union (ACLU) a été très troublée par cet événement et par l'annonce de l'utilisation du logiciel de reconnaissance faciale pour d'autres projets de surveillance publique. L'ACLU a observé qu'il s'agissait d'une expansion sans précédent en matière de surveillance haute technologie et que cette dernière ne devrait pas

The U.S. has considered their use for border security purposes, including a Department of Homeland Security request (since dropped) for information from commercial vendors for RFID tracking capabilities that could locate and identify a tag, with 100 per cent accuracy, inside a car, truck or bus from 25 feet away, while the vehicle was travelling as fast as 88 Km/h (55 mph).[48]

Considerable attention has been paid to the commercial uses of RFID tags, especially Wal-Mart's efforts to advance their use in supply chain management.

The privacy implications

Use of RFID systems in any purposeful applications designed to track individuals' movements has been slow to materialize, at least outside of an employment context. Nevertheless, privacy advocates remain concerned about the ability to link private and public RFID reader networks and databases for ubiquitous surveillance.

Researchers at the Queen's University Surveillance Project point out that RFID tags, with their relatively limited reading distance, cannot by themselves be used to track locations continuously or in real-time.[49] However, U.S. law professor Jonathan Weinberg suggests information sharing among operators of discrete reader networks could create a massive shared network which becomes a "Panopticon geolocator".[50]

Privacy activists also point out that the capacity of Electronic Product Code (EPC) tags is such that all objects around the globe could be uniquely identified, enabling the development of a global tracking and profiling infrastructure.[51] The key factor that permits such ubiquitous tracking is that most RFID chips are designed to be promiscuous.

Simson Garfinkel and Henry Holzman have explained that the vast majority of chips deployed so far are promiscuous because this approach is less expensive and the systems are easier to manage. The authors contrast these with secure tags, which only respond when a password or other authentication is provided, require passwords or encryption codes to be distributed in advance and properly controlled, creating an exceedingly difficult management problem.[52]

Professor Colin has also observed that location tracking can predict the trajectory of an individual, helping to ascertain not only where the individual is at a given moment, but also the individual's

servir à créer une séance d'identification virtuelle d'Américains dont on ne soupçonne pas qu'ils aient mal agi[42].

Dans un article sur la surveillance biométrique, Mark Milone, avocat de New York, a demandé : « Combien de fois par jour veut-on faire l'objet d'une séance d'identification en sortant de chez soi? » [43]

Déclarant qu'un tel système de surveillance avancé facilitait la localisation des personnes, potentiellement à l'échelle nationale, M. Milone a demandé aux gouvernements et à l'industrie de prêter plus d'attention aux risques qu'elle comporte.

L'intégration des bases de données et les systèmes de surveillance : La capacité technologique de la surveillance améliorée sur le plan biométrique augmente sans cesse. Alors que les systèmes maintenant en place sont limités géographiquement— par exemple, la statue de la Liberté de New York incorpore actuellement un système de reconnaissance faciale à une base de données américaine de terroristes suspects44— la vie entière d'une ville pourrait un jour être surveillée, comme le craint l'ACLU, à l'aide de vastes bases de données composées d'images stockées pouvant être balayées grâce à la reconnaissance faciale afin d'identifier les gens et de les repérer en tout temps[45].

La possibilité d'une base de données européenne sur les passeports, les visas et les permis de séjour a également incité plusieurs commissaires européens à dire qu'un tel système risque de devenir une infrastructure de surveillance collective qui surveille les mouvements de tous les résidents et citoyens[46].

C'est aussi le cas des types de systèmes de surveillance avancés qui dépendent de renseignements faciles à observer, mais uniques, comme les plaques d'immatriculation et les caractéristiques faciales pouvant être associées à un emplacement spécifique.

Que nous réserve l'avenir?

La communauté de la protection de la vie privée doit examiner ses positions éventuelles et les préoccupations dont elle fera part tandis que de tels systèmes prennent inévitablement de l'expansion en matière de portée et d'utilisation.

- Les opérateurs des systèmes devraient-ils avoir à établir des motifs raisonnables dans le cadre des systèmes de surveillance

likely destination. He states that a person may be very concerned that others would discover the end point of their journey. Equally important, he points out that current location technology is simply not sufficiently refined to connect identifiable individuals with precise geo-spatial coordinates, which can result in erroneous linkage of persons to locations.[53]

The privacy community, especially data commissioners and policy makers, have begun to address RFID location-tracking issues.

In 2003, a resolution, adopted at the 25th International Conference on Data Protection and Privacy Commissioners, advocated permitting individuals to delete data or destroy RFID tags in their possession. The resolution also stated that "[T]he remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns".[54]

In a 2005 working document, the Article 29 Data Protection Working Party noted the capability of RFIDs to "surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers".[55]

A subsequent policy framework for a 2006 European Commission workshop on RFID issues sought to identify the types of applications with privacy and data protection implications; address how proper usage of RFID technology can be ensured, including through self regulatory practices, additional legal provisions or other compliance mechanisms; and discuss privacy enhancing technologies for RFID deployment.[56]

Domestically, data commissioners have also moved on setting standards for use. For example, both Canadian Privacy Commissioner Jennifer Stoddart and Ontario Information and Privacy Commissioner Ann Cavoukian have developed industry guidelines and continue consulting industry and government on appropriate uses of RFID which may collect personal information.

European data commissioners in Germany (the Federal Commissioner), Italy and the United Kingdom have all issued detailed guidance on RFID use, with consumer consent required for continued activation of chips after a customer has pur-

exhaustifs?

- Aviser les gens est-elle la seule contrainte à l'utilisation de ces systèmes?
- Existe-t-il des situations où les systèmes de surveillance portent atteinte à la vie privée de façon trop fondamentale?

Le potentiel de localisation des systèmes d'identification par radiofréquence (IRF)

La technologie

Les systèmes d'IRF consistent en une méthode d'identification automatisée qui repose sur l'entreposage et la récupération des données provenant des étiquettes d'IRF qui utilisent des ondes radioélectriques. Les étiquettes sont des transmetteurs miniatures et économiques ayant diverses portées de lecture et qui peuvent être intégrées aux objets, aux véhicules, aux animaux et même aux humains. Certaines sont universelles et peuvent être lues par tout lecteur d'IRF alors que d'autres, plus sécuritaires, nécessitent un mot de passe ou une méthode d'authentification.

L'incorporation de ces étiquettes aux humains a généré le plus d'attention en tant que technologie de localisation potentielle. En 2004, le *Chicago Sun-Times* a signalé qu'au moins 160 promoteurs de la justice et enquêteurs fédéraux travaillant pour le ministère public du Mexique avaient fait l'objet d'une implantation sous-cutanée de puces et que des membres clés des services militaires et policiers ainsi que des employés du bureau du Président devaient également en recevoir[47].

Au Canada, les étiquettes d'IRF ont remplacé les codes à barres pour la localisation des bovins destinés aux abattoirs et des véhicules voyageant sur les autoroutes à péage, et ce, dans deux provinces. Jusqu'à présent au moins, le gouvernement ne s'en est servi pour aucune application publique d'envergure.

Les États-Unis ont envisagé leur utilisation à des fins de sécurité aux frontières, notamment à la suite d'une demande du département de la Sécurité intérieure (qu'il a depuis abandonnée) visant l'obtention de renseignements provenant d'entreprises commerciales dans le but de localiser et d'identifier des étiquettes d'IRF à une précision de 100 %, à l'intérieur d'une voiture, d'un camion ou d'un autobus situé à 25 pieds et se déplaçant à une vitesse allant jusqu'à 88 km/h (55 mi/h) [48].

chased an RFID-equipped product, and express prohibitions on unauthorized monitoring of people's movements.

Questions remain, however, about how effective such guidelines will be and whether widespread RFID deployment will indeed usher in an age of ubiquitous and invisible tracking, including use of such devices for police or security intelligence purposes.

Where to go from here?

- Are concerns about ubiquitous RFID tracking realistic or overblown as industry groups have repeatedly stated?
- Are voluntary guidelines or existing laws sufficient or do we need specific new laws to govern RFID use?
- Is specific technology—such as a mandatory "kill function" on RFID tags—required to protect public interests?
- Should individuals who refuse RFID tracking be legally entitled to equivalent non-RFID-based services and products?

Wi-Fi Positioning Systems: tracking wireless personal devices

The technology

"Wi-Fi" (short for wireless fidelity) is a term developed by the international Wi-Fi Alliance to describe wireless local area network products that are based on common technical standards and allow users of wireless devices to have broadband Internet communications in public areas or "hotspots".

According to the Wi-Fi Alliance, by 2007 the number of Wi-Fi networks or public access "hotspots" is projected to number 530,000 in the United States, almost 800,000 in Europe, and more than a million in Asia.[57]

Linked to the growing number of public places where people can use laptop computers and other wireless devices, is the growth of Wi-Fi Positioning Systems (WPS) which can pinpoint the location of wireless devices to within 20 metres. One U.S. company, Skyhook Wireless, Inc., now has WPS coverage in major U.S. cities equating to 70 per cent of the U.S. population base, and is now

Une attention considérable a été prêtée aux fins commerciales des étiquettes d'IRF, particulièrement aux efforts de Wal-Mart pour faire avancer leur utilisation au sein de la gestion de la chaîne d'approvisionnement.

Les conséquences sur la protection de la vie privée

L'utilisation des systèmes d'IRF dans le cadre de toute application utile conçue pour localiser les mouvements des particuliers tarde à se concrétiser, du moins à l'extérieur du contexte de l'emploi. Toutefois, la communauté de la protection de la vie privée demeure préoccupée au sujet de la possibilité de relier les réseaux de lecteurs d'IRF privés et publics aux bases de données pour une surveillance omniprésente.

Les chercheurs qui travaillent sur le projet de surveillance de l'Université Queen's soulignent que les étiquettes d'IRF, avec leur portée de lecture relativement limitée, ne peuvent pas, elles seules, servir à repérer les emplacements sur une base continue en temps réel[49]. Cependant, Jonathan Weinberg, professeur de droit américain, suggère qu'un échange de renseignements entre opérateurs de réseaux de lecteurs discrets pourrait créer un réseau partagé massif qui deviendrait un « géolocalisateur panoptique »[50].

La communauté de la protection de la vie privée souligne également que la capacité des étiquettes à code de produit électronique (CPE) est telle que tous les objets de la planète pourraient se voir attribuer une identification distincte, permettant ainsi le développement d'une localisation globale et d'une infrastructure de profilage[51]. L'élément principal qui permettrait la localisation omniprésente réside en cela que la conception des puces d'IRF est de nature universelle.

Simson Garfinkel et Henry Holzman ont expliqué que la vaste majorité des puces déployées jusqu'à ce jour sont de type universel car cette approche est moins coûteuse et les systèmes sont plus faciles à gérer. Les auteurs comparent celles-ci aux étiquettes sécuritaires, lesquelles ne répondent que lorsqu'un mot de passe ou une autre méthode d'authentification est fourni et requièrent la distribution préalable et bien contrôlée de mots de passe ou de codes de chiffrage, créant ainsi un sérieux problème de gestion[52].

Par ailleurs, le professeur Colin a observé que la localisation permet de prédire la trajectoire d'une

expanding into Canada and Europe. Skyhook has also introduced Loki, a toolbar that provides location-based services to Wi-Fi users.

WPS can also be used inside buildings, where research suggests accuracy is possible to within one to three metres of a Wi-Fi equipped device.[58] Intel has set a goal of developing one-metre accuracy for both indoor and outdoor applications.[59]

WPS works by measuring the time it takes for signals to travel from every Wi-Fi access point that responds to a device's initial "who's-there" request. The more access points there are in a geographic area, the more accurate the measurement will be. It takes about two seconds for WPS to compute a user's location.

WPS has distinct advantages over other location technologies (including GPS) in dense urban locations as it does not require direct line of sight to a satellite. Some commercial services are being offered that combine both WPS and GPS, to provide ubiquitous location tracking in urban, suburban, rural and remote areas.

The privacy implications

The privacy concerns about the tracking capability have become more pronounced as municipal Wi-Fi systems are beginning to provide large-scale wireless access to the Internet in urban centres. The City of San Francisco's announced plans for a municipal Wi-Fi system prompted questions from such privacy groups as the Electronic Frontier Foundation (EFF), American Civil Liberties Union (ACLU) and Electronic Privacy Information Center (EPIC). They asked "Will users be tracked from session to session, creating an archive of their online activity? Will the Wi-Fi service provider try to commercialize the data? Will the data be protected from interception by others?".[60]

Discussions led to an agreement between the city and contracted service provider EarthLink Inc. that includes a comprehensive privacy policy to prevent sharing of any Wi-Fi-generated personal information without "voluntary affirmative consent of the user". The agreement also provides users with the right to opt-out of any collection of location information, except for criminal investigation, national security and civil legal proceedings.[61] These contract provisions, however, may do little to satisfy civil society groups.

At heart is the ability of corporate interests (in the case of civil suits), law enforcement and national

personne et donc de connaître non seulement l'endroit où elle se trouve, mais également sa destination probable. Selon lui, cette personne pourrait être très inquiète de savoir que d'autres découvriront sa destination. Il ajoute qu'il ne faut pas oublier que la technologie courante entourant la localisation n'est tout simplement pas assez sophistiquée pour permettre de lier des personnes identifiables à des coordonnées géospatiales précises et que des gens pourraient être faussement associés à des emplacements[53].

Les membres de la communauté de la protection de la vie privée, particulièrement les commissaires à la protection des données et les responsables des politiques, ont commencé à aborder les enjeux liés à la localisation par IRF.

En 2003, une résolution adoptée lors de la 25e Conférence internationale des commissaires à la protection des données et de la vie privée préconisait de permettre aux particuliers de supprimer les données ou de détruire les étiquettes d'IRF en leur possession. La résolution précisait aussi que la lecture et l'activation à distance des étiquettes d'IRF, sans que la personne qui se trouve en possession de l'objet étiqueté puisse influencer ce processus, soulèveraient d'autres questions pour la protection de la vie privée[54].

Dans un document de travail publié en 2005, le Groupe de protection des données établi en vertu de l'article 29 a souligné la capacité des étiquettes d'IRF de recueillir subrepticement diverses données toutes liées à la même personne; de suivre à la trace des personnes se déplaçant dans des lieux publics (aéroports, gares ferroviaires, magasins); d'étoffer des profils en surveillant le comportement des consommateurs dans les magasins, de lire les données détaillées des vêtements et des accessoires que portent les clients et des médicaments qu'ils transportent[55].

Un cadre stratégique subséquent élaboré en vue d'un atelier de la Commission européenne tenu en 2006 et portant sur les enjeux relatifs à l'IRF a cherché à identifier les types d'applications ayant une incidence sur la protection de la vie privée et des données, à aborder comment l'utilisation appropriée de la technologie d'IRF pourrait être assurée, y compris par l'entremise de pratiques autoréglementées, de dispositions légales additionnelles ou de mécanismes de conformité, et à discuter des technologies permettant d'accroître le respect de la vie privée dans le cadre du déploiement des dispositifs d'IRF[56].

security agencies to use location information to track and potentially uncover the identities of individuals seeking to preserve their privacy rights or even constitutionally protected rights of free speech. For example, civil society groups cite American courts as having recognized that Internet users "who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identities".[62]

With the heightened tension between privacy rights and security interests, the outstanding question in the case of municipal Wi-Fi systems is how far network operators will go to protect privacy interests in the face of legal demands to hand over location or other identifying information.

Other solutions to managing location privacy may result from the development of new privacy rules for location-emitting devices. The Internet Engineering Task Force (IETF) Geographic Location/ Privacy Working Group (Geopriv WG) has created a set of standards for sending location information over the Internet that incorporates privacy rules. The PIDF-LO (Presence Information Data Format - Location Object) privacy rules are designed to give users of location-emitting devices some control over how long location information can be retained by a third party and whether consent is provided for retransmitting this information.[63]

In a recent article, John Morris, Director of the Center for Democracy & Technology (CDT) Internet Standards, Technology and Policy Project, (who helped develop this standard) gives an example of how it might work. A wireless device user might send a message to a host server asking "Where is the closest Starbucks to where I am right now?" Depending on the user's privacy settings, the host could be required to respond to this query and then immediately discard the location information.[64]

Development of a more robust privacy framework is underway which will, in theory, give users considerable control over who can access location information and for what purposes. At the same time, users could define how granular the information can be – for example, an exact location or just that the user is in a particular city. Mr. Morris explains, "Geopriv offers the opportunity to convey fairly robust and potentially complex privacy rules along with location information". However, he adds the caveat--which applies to all location

Chez nous, les commissaires à la protection de la vie privée ont également établi des normes en matière d'utilisation. Par exemple, Jennifer Stoddart, commissaire à la protection de la vie privée du Canada et Ann Cavoukian, commissaire à l'information et à la protection de la vie privée de l'Ontario, ont toutes les deux élaboré des lignes directrices à l'intention de l'industrie et continuent à consulter l'industrie et le gouvernement sur l'utilisation appropriée des dispositifs d'IRF susceptibles de recueillir des renseignements personnels.

Les commissaires européens à la protection des données de l'Allemagne (le commissaire fédéral), de l'Italie et du Royaume-Uni ont émis des lignes directrices détaillées sur l'utilisation des puces d'IRF : le consentement des usagers est nécessaire pour que les puces demeurent actives après l'achat d'un produit doté d'une puce d'IRF et la surveillance non autorisée des mouvements est expressément interdite.

Toutefois, des questions demeurent à savoir si de telles lignes directrices sont efficaces et si la diffusion à grande échelle de l'IRF nous fera entrer dans une ère de surveillance généralisée et invisible, y compris l'utilisation de cette technologie à des fins de collecte de renseignements par les corps policiers ou les responsables de la sécurité.

Que nous réserve l'avenir?

- Les préoccupations à l'égard de la localisation par IRF omniprésente sont-elles réalistes ou exagérées, comme les groupes de l'industrie l'ont souvent déclaré?
- Les lignes directrices volontaires ou les lois existantes sont-elles suffisantes ou avons-nous besoin de nouvelles lois afin de régir l'utilisation de l'IRF?
- Est-ce qu'une technologie particulière, comme un dispositif d'arrêt sur les étiquettes d'IRF, est essentielle afin de protéger l'intérêt public?
- Les personnes qui refusent de faire l'objet de localisation par IRF devraient-elles avoir droit à des services et produits équivalents non associés à l'IRF?

Les SPW et la localisation d'appareils sans fil à usage personnel

La technologie

« Wi-Fi » (l'abréviation de *wireless fidelity*) est un

tracking technologies: "It can't, however, provide guarantees that those rules will be honoured or followed in any given situation".[65]

Absent such rules or regulatory control of location information, there are profound societal consequences to enhanced location tracking, as *A Report on the Surveillance Society* points out:

> "… the concern remains that consumer surveillance will continue to perpetuate and amplify social divides and sorting that is antithetical to democratic principles. Consumer surveillance then stands to increase as a 'cybernetic triage' separating consumers based on their presumed economic and political value rather than on their initiative and self-determination."

Not surprisingly, there are also profound differences in awareness and attitude towards location technologies and their privacy impacts based on age. Various researchers, for example the Pew Research Center, have found that teenagers and young adults embrace new technologies with more enthusiasm and have far less regard for privacy consequences.[66] This suggests the emergence of a generation that is techno-savvy but unfazed by the Orwellian possibilities of location technology.

Where to go from here?

- How do we foster greater understanding of the privacy impacts of technologies such as Wi-Fi positioning systems?
- If there are cultural, social and age divides that affect user attitudes towards technology, how can such divides be factored into the social acceptance of the technology, its purposes and consent to its use?
- What role should privacy commissioners and civil society and privacy groups play in addressing location information privacy impacts?

Bibliography

The following documents are useful further reading on geo-tracking.

A Report on the Surveillance Society, Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, a report for the UK Information Commissioner by the Surveillance Studies Network, September 2006.

terme qui a été créé par la Wi-Fi Alliance internationale pour décrire les produits du réseau sans fil local définis selon les normes techniques courantes et qui permet aux utilisateurs d'appareils sans fil d'avoir un accès à Internet à large bande dans les endroits publics ou les points d'accès sans fil.

La Wi-Fi Alliance prévoit que d'ici 2007, le nombre de réseaux Wi-Fi ou de points d'accès sans fil passera à 530 000 aux États-Unis, à près de 800 000 en Europe et à plus d'un million en Asie[57].

Associée à la hausse du nombre d'endroits publics où les gens peuvent utiliser des ordinateurs sans fil et d'autres appareils sans fil est la croissance du système de positionnement Wi-Fi (SPW) qui peut repérer l'emplacement d'appareils sans fil à une distance de 20 mètres près. Une entreprise américaine, Skyhook Wireless, Inc., possède maintenant une couverture Wi-Fi dans les villes principales des États-Unis, ce qui équivaut à 70 % de la population américaine, et est en train de s'étendre au Canada et en Europe. Skyhook, a également introduit Loki, une barre d'outils qui offre des services de localisation aux utilisateurs de la technologie Wi-Fi.

Par ailleurs, les SPW peuvent être utilisés à l'intérieur des bâtiments et les recherches suggèrent qu'il est possible d'y localiser un appareil Wi-Fi avec une précision d'un à trois mètres[58]. Intel s'est fixé comme objectif d'atteindre une précision d'un mètre pour les applications intérieures et extérieures[59].

Les SPW mesurent le temps que prennent les signaux pour voyager de chacun des points d'accès Wi-Fi qui répondent à la demande d'identification initiale. Plus il y a de points d'accès dans une région géographique, plus la mesure sera précise. Les SPW prennent environ deux secondes pour calculer l'emplacement d'un utilisateur.

Dans les régions urbaines denses, les SPW se démarquent par rapport aux autres technologies de localisation (y compris le GPS), car ils ne requièrent pas de ligne directe de visée à un satellite. Certains des services commerciaux offerts combinent les SPW et le GPS afin de fournir une localisation omniprésente dans les régions urbaines, suburbaines, rurales et éloignées.

Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, Jay Stanley and Barry Steinhardt, American Civil liberties Union, January 2003.

Location Technologies: Mobility, Surveillance and Privacy, David Lyon, Stephen Marmura and Pasha Peroff, The Surveillance Project, Department of Sociology, Queen's University, Kingston, March 2005.

On Your Tracks: GPS Tracking in the Workplace, Nanette Green Kaminski and William Tran, National Workrights Institute, Princeton, N.J., Feb. 2007.

RFID Applications, Security and Privacy, Simson Garfinkel and Henry Holtzman, editors, Addison-Wesley, New Jersey, 2005.

Spychips: how major corporations and government plan to track your every move with RFID, Katherine Albrecht and Liz McIntyre, Nelson Current, Tennessee, 2005.

.

End Notes

[1] Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, *A Report on the Surveillance Society*, a report for the UK Information Commissioner by the Surveillance Studies Network, September 2006, p. 4.

[2] Roger Clarke defined dataveillance as "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons." Roger Clarke, "Information Technology and Dataveillance," *Communications of the ACM*, Volume 31, 1988, pp. 498-512.

[3] David Lyon, Stephen Marmura and Pasha Peroff, *Location Technologies: Mobility, Surveillance and Privacy*, The Surveillance Project, Department of Sociology, Queen's University, Kingston, March 2005, p.6.

[4] Katherine Albrecht and Liz McIntyre, *Spychips: How major corporations and government plan to track your every move with RFID,* Nashville: Nelson Current, 2005, p. 59.

[5] The read range depends upon the type of RFID used. RFID units with their power source typically used in commercial asset tracking applications can be read from a distance of 100 metres or more. The reading range of passive units (the RFID relies on the energy from the reader to transmit a return signal) varies according to the

Les conséquences sur la protection de la vie privée

En ce qui concerne la capacité de localisation, les inquiétudes pour la vie privée ont pris de l'ampleur depuis que les systèmes SPW ont commencé à fournir un accès sans fil à grande échelle au réseau Internet dans les centres urbains. Lorsque la ville de San Francisco a annoncé ses plans pour la mise sur pied d'un système Wi-Fi municipal, cela a soulevé des questions de la part de la communauté de la protection de la vie privée, comme l'Electronic Frontier Foundation (EFF), l'American Civil Liberties Union (ACLU) et l'Electronic Privacy Information Center (EPIC). On a demandé si les utilisateurs allaient être suivis d'une séance à l'autre (archivant ainsi leur activité en ligne), si les fournisseurs de services Wi-Fi tenteraient de commercialiser les données et si celle-ci allaient être protégées de l'interception des autres[60].

Les discussions ont mené à une entente entre la ville et le fournisseur de services EarthLink Inc., laquelle comprend une politique de confidentialité exhaustive empêchant l'échange de renseignements personnels générés par les SPW sans le consentement volontaire de l'utilisateur. En vertu de l'entente, les utilisateurs ont le droit de refuser toute collecte de renseignements en matière de localisation sauf dans des situations liées à une enquête criminelle, à la sécurité nationale ou à une poursuite au civil[61]. Cependant, ces dispositions pourraient ne pas satisfaire les groupes de la société civile.

Au cœur du débat, on retrouve la possibilité que des intérêts corporatifs (en cas de poursuites civiles) et les organismes responsables de l'exécution de la loi ou de la sécurité nationale utilisent des renseignements provenant de la localisation et qu'ils découvrent par le fait même l'identité de personnes désirant préserver leur vie privée ou leur droit à la liberté de parole assuré par la Constitution. Par exemple, des groupes civils citent les tribunaux américains qui ont reconnu que les internautes qui n'ont commis aucun crime devraient pouvoir participer à des activités en ligne sans craindre que quiconque désire les harceler ou les humilier puisse les amener en cour pour des motifs frivoles uniquement dans le but d'utiliser les pouvoirs de la cour pour découvrir leur identité[62].

Dans l'atmosphère tendue qui règne entre les groupes de défense du droit à la vie privée et ceux qui favorisent la sécurité, il reste à savoir

antenna size and its frequency range from a few centimeters to a few metres.

[6] Dale N. Hatfield, "A Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Service," prepared for the Federal Communications Commission, 2002, p. 7.

[7] *Location Technologies: Mobility, Surveillance and Privacy*, p.16.

[8] Helios Technology Ltd., "Caller Location in Telecommunications Networks in view of enhancing 112 Emergency Services: Recommendations towards a European policy and implementation plan, June 2002, p. 3.

[9] "EU telecoms rules: Commission takes steps to ensure that emergency services can locate callers," European Union news release, Brussels, April 6, 2006.

[10] Aaron Futch and Christine Soares, "Enhanced 911 Technology and Privacy Concerns: How has the Balance Changed since September 11?," 2001 Duke Law & Technology Review 0038, October 2001, p. 3.

[11] Ibid, p. 8.

[12] Hatfield, "A Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Service," p. 16.

[13] 47 USC 1008.

[14] Patricia Moloney Figliola, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, Congressional Research Service Report to Congress, Dec. 2006, pp. 3 & 7.

[15] Declan McCullagh, "Feds cell phone tracking denied," C/Net News.com, October 28, 2005.

[16] Declan McCullagh, "Judge lets Feds track cell phones," C/Net News.com, January 6, 2006.

[17] Justice Gérard La Forest, in *R v. Wise* [1992] 1 S.C.R. 527 at p. 560.

[18] Jennifer Stoddart, Privacy Commissioner of Canada, *Response to the Government of Canada's "Lawful Access" Consultations*, May 5, 2005.

[19] Bruce Schneier, "Bigger Brother," *The Baltimore Sun, October 4, 2004*.

[20] Chris Oakes, "E911 turns cell phones into tracking devices," *Wired News*, January 6, 1998.

[21] *Location Technologies: Mobility, Surveillance and Privacy*, p. 44.

[22] Katina Michael, *Location-based services - a vehicle for IT&T convergence*, *Advances in E-Engineering and Digital Enterprises Technology*, Proceedings of the Fourth International

jusqu'où iront les exploitants de réseau Wi-Fi municipaux pour protéger la vie privée des usagers quand la loi exige qu'ils remettent des renseignements au sujet de l'emplacement et de l'identité de ces derniers.

D'autres solutions de gestion de la vie privée en matière de localisation pourraient découler de l'élaboration de nouvelles règles sur la protection des renseignements personnels en ce qui a trait aux appareils de localisation. L'Internet Engineering Task Force (IETF) et le Geographic Location/Privacy Working Group (Geopriv WG) ont établi un ensemble de normes pour l'envoi de renseignements en matière de localisation par Internet qui incorporent les règles sur la protection des renseignements personnels. Les règles du PIDF-LO (Presence Information Data Format - Location Object) sont conçues pour permettre aux utilisateurs d'appareils de localisation de décider s'ils consentent ou non à la collecte de renseignements en matière de localisation et pour leur donner un certain contrôle sur le temps pendant lequel une tierce partie peut retenir ces renseignements[63].

Dans un article récent, John Morris, directeur du Center for Democracy & Technology (CDT) Internet Standards, Technology and Policy Project et collaborateur dans l'établissement de cette norme, fournit un exemple de la méthode de fonctionnement. Un utilisateur d'un appareil sans fil pourrait envoyer un message à un serveur hôte et demander : « Où est le Starbucks le plus près d'ici? ». Selon les paramètres configurés par l'utilisateur, le serveur hôte pourrait devoir répondre à cette question et supprimer les renseignements immédiatement après[64].

Un cadre de protection de la vie privée plus rigoureux est en cours de développement, ce qui devrait théoriquement offrir aux utilisateurs beaucoup de contrôle sur les gens qui peuvent accéder aux renseignements en matière de localisation et les fins envisagées. En même temps, les utilisateurs pourront déterminer jusqu'à quel point les renseignements sont granulaires—par exemple, le fait de savoir que l'utilisateur est à un emplacement précis ou dans une ville particulière. Selon M. Morris, Geopriv offre la possibilité de transmettre des règles sur la protection des renseignements personnels assez rigoureuses et potentiellement complexes ainsi que des renseignements en matière de localisation. Toutefois, il pose une mise en garde (laquelle s'applique à toute technologie de localisation) : on ne peut pas garantir que ces

Conference on e-Engineering and Digital Enterprise Technology (e-ENGDET) (pp. 467-477), Professional Engineering Publishing Limited., UK, 2004.

[23] Ibid, p. 30. Lyon et al cite Claire Tristram, "Has GPS lost its way?," *Technology Review*, 1999.

[24] Eloïse Gratton, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, CCH Canadian Limited, Toronto, 2003.

[25] Louse Barkuus and Anind Dey, L*ocation-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns*, Intel Research, Berkeley, July 2003.

[26] Ted Bridis, "White House wants plans for GPS shutdown," Associated Press, December 15, 2004.

[27] Helena Spongenberg, Power Struggle jeopardizes EU Galileo satellite system, euobserver.com, March 15, 2007.

[28] Source: news release by C.J.Driscoll & Associates concerning its *2005-06 Mobile Resource Management Systems Market Study*, September 20, 2005.

[29] Matt Hamblen, "Mobile business 2.0: It's location, location, location," *Computerworld*, March 14, 2007. Me. Hamblen quotes data from Brent Iadarola, an analyst with Frost & Sullivan.

[30] Sameer Kumar and Joel Stokkeland, "Evolution of GPS technology and its subsequent use in commercial markets," *International Journal of Mobile Communications*, Vol. 1, Nos. 1/2, 2003, p. 190. The authors cite the Allied Business Intelligence study, "GPS World Markets 2002."

[31] *PIPEDA case summary #351, Use of personal information collected by Global Positioning System considered, Office of the Privacy Commissioner, November 9, 2006.*

[32] Ibid.

[33] Murray Singerman, "GPS Invasion of Worker Privacy," *Maryland Bar Association Journal*, May/ June 1004, p. 55. Mr. Singerman cites Pemberton v. Bethlehem Steel Corp., 66 Md. App.133 (1986) as establishing limits of worker surveillance outside of the workplace.

[34] Nanette Green Kaminski and William Tran, *On Your Tracks: GPS Tracking in the Workplace*, National Workrights Institute, Princeton, N.J., Feb. 2007, p. 13.

[35] Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995, on the protection of individuals with regard to the

règles seront honorées ou suivies dans une situation donnée[65].

Comme l'indique *A Report on the Surveillance Society*, en l'absence de telles règles ou de contrôle réglementaire des renseignements produits par la localisation, les technologies de localisation avancées peuvent entraîner de sérieuses conséquences sociales :

> « On continue à se demander si la surveillance des consommateurs continuera à se perpétuer et à amplifier les divisions sociales et le triage qui sont contraires aux principes démocratiques. La surveillance des consommateurs risque de devenir un triage cybernétique qui les sépare en raison de leur présumée valeur économique et politique plutôt que de leur sens d'initiative et d'autodétermination. » [Traduction]

Il n'est pas surprenant de constater les différences profondes qui existent entre la sensibilisation et l'attitude envers les technologies de localisation et les répercussions sur la protection de la vie privée fondées sur l'âge. Divers chercheurs, y compris le Pew Research Center, ont trouvé que les adolescents et les jeunes adultes accueillent les nouvelles technologies avec plus d'enthousiasme et sont beaucoup moins préoccupés par les répercussions sur la protection de la vie privée[66]. Cela suggère l'émergence d'une génération adepte des technologies, mais non intimidée par les possibilités orwelliennes liées aux technologies de localisation.

Que nous réserve l'avenir?

- Comment favoriser une meilleure compréhension des répercussions sur la protection de la vie privée dans le domaine des technologies, comme les SPW?
- S'il existe des divisions associées à la culture, à l'aspect social et à l'âge qui ont une incidence sur l'attitude des utilisateurs envers la technologie, comment ces dernières peuvent-elles être prises en compte dans l'acceptabilité sociale de la technologie et ses applications et l'obtention du consentement en vue de son utilisation?
- Quel rôle devraient jouer les commissaires à la protection de la vie privée, la société civile et la communauté de la protection de la vie privée lorsqu'ils abordent les répercussions, sur la protection de la vie privée, de la localisation?

processing of personal data and on the free movement of such data.

[36] UK Information Commissioner, *The Employment Practices Code*, June 2005, p. 70.

[37] Rachel Konrad, "Meet the future: Our cars, ourselves," CNET News, June 22, 2001.

[38] John Schwartz, "This Car Can Talk. What It Says May Cause Concern," *New York Times*, December 29, 2003.

[39] PA Consulting Group, *Driving crime down: Denying criminals the use of the road*, a report to the Home Office, October 2004, pp. 37-40.

[40] Information and Privacy Commissioner/Ontario, Investigation Report PC-010005-1: The Use of Biometric Face Recognition Technology in Ontario Casinos.

[41] Ibid, p. 4.

[42] American Civil liberties Union and House of Representatives Majority Leader Dick Armey joint statement: "Proliferation of Surveillance Devices Threatens Privacy," Washington, DC, July 11, 2001.

[43] Mark Milone, "Biometric Surveillance: searching for identity," *The Business Lawyer*, American Bar Association, Chicago, Nov. 1, 2001.

[44] AP news report, *Face-scanning system used at Statute of liberty*, New York, May 28, 2002.

[45] Jay Stanley and Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, American Civil Liberties Union, January 2003, p. 3.

[46] An Open Letter to the European Parliament on Biometric Registration of all EU Citizens and Residents, authored by Privacy International, Statewatch and European Digital Rights, Nov. 30, 2004.

[47] Will Weissert, "Mexican justice ministry staffers get chip implants," *Chicago Sun-Times*, July 15, 2005.

[48] Evan Shuman, "U.S. Homeland Security Delays RFID Plan," *eWeek*, Feb. 28, 2006.

[49] *Location Technologies: Mobility, Surveillance and Privacy*, p.14.

[50] Jonathan Wienberg, "RFID, Privacy and Regulation," in *RFID Applications, Security and Privacy*, edited by Simson Garfinkel and Beth Rosenberg, Addison-Wesley, New Jersey, 2005, p. 91.

[51] Beth Givens, "Activists: Communicating with Consumers, Speaking Truth to Policy Makers," in *RFID Applications, Security and Privacy,* p. 432.

Bibliographie

Les documents suivants constituent d'autres ressources utiles portant sur la géolocalisation.

A Report on the Surveillance Society, Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, un rapport du Surveillance Studies Network à l'intention du commissaire à l'information du Royaume-Uni, septembre 2006.

Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society, Jay Stanley et Barry Steinhardt, American Civil liberties Union, janvier 2003.

Location Technologies: Mobility, Surveillance and Privacy, David Lyon, Stephen Marmura et Pasha Peroff, The Surveillance Project, Département de sociologie, Université Queen's, Kingston, mars 2005.

On Your Tracks: GPS Tracking in the Workplace, Nanette Green Kaminski et William Tran, National Workrights Institute, Princeton, N.J., février 2007.

RFID Applications, Security and Privacy, Simson Garfinkel et Henry Holtzman, éds, Addison-Wesley, New Jersey, 2005.

Spychips: how major corporations and government plan to track your every move with RFID, Katherine Albrecht et Liz McIntyre, Nelson Current, Tennessee, 2005.

Notes de bas de page

[1] Kirstie Ball, David Lyon, David Murakami Wood, Clive Norris, Charles Raab, *A Report on the Surveillance Society*, un rapport du Surveillance Studies Network à l'intention du commissaire à l'information du Royaume-Uni, septembre 2006, p.4.

[2] Roger Clarke définit la surveillance des données comme suit : [Traduction] « l'utilisation systématique de systèmes de données personnelles pour faire enquête ou surveiller les gestes ou les communications de personnes ». Roger Clarke, "Information Technology and Dataveillance," *Communications of the ACM*, volume 31, 1988, pp. 498-512.

[3] David Lyon, Stephen Marmura et Pasha Peroff, *Location Technologies: Mobility, Surveillance and Privacy*, The Surveillance Project, Département de sociologie, Université Queen's, Kingston, mars 2005, p.6.

[52] Simson Garfinkel and Henry Holtzman, "Understanding RFID Technology," in *RFID Applications, Security and Privacy*, p. 18.

[53] Colin J. Bennett and Lori Crowe, *Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada*, University of Victoria, June 2005, p. 37.

[54] International Conference of Data Protection & Privacy Commissioners, Resolution on Radio-Frequency Identification, Final Version, Nov. 20, 2003.

[55] Article 29 Data Protection Working Party, *Working document on data protection issues related to RFID technology*, Jan. 19, 2005.

[56] European Commission, *Policy Framework Paper* for RFID workshop, May 11, 2006.

[57] The Wi-Fi Alliance, "Enabling the Future of Wi-Fi Public Access," p. 5. This paper cites growth projections from a 2003 research paper, "Wi-Fi Hotspot Opportunities," by Dr. Daniel Sweeney for Forward Concepts, an Arizona research firm. The Wi-Fi Alliance is a global, non-profit industry organization established to promote the adoption of a single worldwide-accepted standard for high-speed wireless local area networking.

[58] Y. Wang, X. Jia, H.K. Lee, "An indoors wireless positioning system based on wireless local area network infrastructure," paper presented at the 6th International Symposium on Satellite Navigation Technology Including Mobile Positioning & Location Services, Melbourne, July 2003, p. 13.

[59] Precision Location Research at Intel, Intel Corporation paper, 2005.

[60] Electronic Frontier Foundation news release, "How Far Would You Go For Muni WiFi?", Oct. 21, 2005.

[61] Wireless Broadband Internet Access Network Agreement between the City and County of San Francisco and EarthLink, Inc., Jan. 5, 2007, pp. 20-21.

[62] *Columbia Insurance Co. v. Seescandy.com*, 185 F.R.D. at 578.

[63] For more information on this standard, see: www.ietf.org/html.charters/geopriv-charter.html

[64] John Morris and Jon Peterson, "Who's watching You Now?", *IEEE Security & Privacy*, IEEE Computer Society, January/February 2007, p. 78.

[65] Ibid.

[66] Pew Research Center, *The Internet News Audience Goes Ordinary*, January 14, 1999, p. 24. In a 2006 University of Minnesota survey (Internet

[4] Katherine Albrecht et Liz McIntyre, *Spychips: How major corporations and government plan to track your every move with RFID,* Nashville: Nelson Current, 2005, p. 59.

[5] La capacité de lecture dépend du type de dispositif d'IRF utilisé. Dotées des sources d'énergie typiquement utilisées dans les applications commerciales de suivi des biens, les unités d'IRF peuvent être lues à une distance de 100 mètres ou plus. La capacité de lecture des unités passives (les puces d'IRF dépendent de l'énergie du lecteur pour transmettre un signal de retour) oscille, selon la taille de l'antenne et la gamme de fréquences, de quelques centimètres à quelques mètres.

[6] Dale N. Hatfield, "A Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Service," préparé par la Commission fédérale des communications, 2002, p. 7.

[7] *Location Technologies: Mobility, Surveillance and Privacy*, p.16.

[8] Helios Technology Ltd., "Caller Location in Telecommunications Networks in view of enhancing 112 Emergency Services: Recommendations towards a European policy and implementation plan", juin 2002, p. 3.

[9] « Réglementation de l'UE en matière de télécommunications : la Commission prend des mesures pour garantir que les services d'urgence puissent localiser les appelants », communiqué de presse de l'Union européenne, Bruxelles, 6 avril 2006.

[10] Aaron Futch et Christine Soares, 'Enhanced 911 Technology and Privacy Concerns: How has the Balance Changed since September 11?," 2001 Duke Law & Technology Review 0038, Octobre 2001, p. 3.

[11] Ibid, p. 8.

[12] Hatfield, "A Report on Technical and Operational Issues Impacting the Provision of Wireless Enhanced 911 Service," p. 16.

[13] 47 USC 1008. 7

[14] Patricia Moloney Figliola, *Digital Surveillance: The Communications Assistance for Law Enforcement Act*, rapport du Congressional Research Service au Congrès, décembre 2006, pp. 3 et 7.

[15] Declan McCullagh, "Feds cell phone tracking denied," C/Net News.com, 28 octobre 2005.

[16] Declan McCullagh, "Judge lets Feds track cell phones," C/Net News.com, 6 janvier 2006.

Use and Privacy Attitudes Survey), 31 percent of students said that, in general, they think their Internet activities are anonymous.

[17] Juge Gérard La Forest, dans *R c. Wise* [1992] 1 R.C.S. 527 à la p. 560.

[18] Jennifer Stoddart, commissaire à la protection de la vie privée du Canada, *Réponse à la consultation du gouvernement sur l'accès légal*, 5 mai 2005.

[19] Bruce Schneier, "Bigger Brother," *The Baltimore Sun*, 4 octobre 2004.

[20] Chris Oakes, "E911 turns cell phones into tracking devices," *Wired News*, 6 janvier 1998.

[21] *Location Technologies: Mobility, Surveillance and Privacy*, p. 44.

[22] Katina Michael, *Location-based services - a vehicle for IT&T convergence*, *Advances in E-Engineering and Digital Enterprises Technology*, Proceedings of the Fourth International Conference on e-Engineering and Digital Enterprise Technology (e-ENGDET), Professional Engineering Publishing Limited, Royaume-Uni, 2004, pp. 467-477.

[23] Ibid, p. 30. Lyon et al cite Claire Tristram, "Has GPS lost its way?," *Technology Review*, 1999.

[24] Eloïse Gratton, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices*, CCH Canadienne Limitée, Toronto, 2003.

[25] Louse Barkuus et Anind Dey, *Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns*, Intel Research, Berkeley, juillet 2003.

[26] Ted Bridis, "White House wants plans for GPS shutdown," Associated Press, 15 décembre 2004.

[27] Helena Spongenberg, Power Struggle jeopardizes EU Galileo satellite system, euobserver.com, 15 mars 2007.

[28] Source : communiqué de presse de C.J.Driscoll & Associates à propos d'une étude intitulée *2005-06 Mobile Resource Management Systems Market Study*, 20 septembre 2005.

[29] Matt Hamblen, "Mobile business 2.0: It's location, location, location," *Computerworld*, 14 mars 2007. M^e^ Hamblen cite des données de Brent Ladarola, un analyste de Frost & Sullivan.

[30] Sameer Kumar et Joel Stokkeland, "Evolution of GPS technology and its subsequent use in commercial markets," *International Journal of Mobile Communications*, vol. 1, n^os^ 1/2, 2003, p. 190. Les auteurs citent une étude intitulée Allied Business Intelligence, "GPS World Markets 2002."

[31] Résumé de conclusions d'enquête en vertu de la *LPRPDÉ* n^o^ 351, Examen de l'utilisation des renseignements personnels recueillis au moyen

d'un système mondial de localisation, Commissariat à la protection de la vie privée du Canada, 9 novembre 2006.

[32] Ibid.

[33] Murray Singerman, "GPS Invasion of Worker Privacy," *Maryland Bar Association Journal*, mai/ juin 2004, p. 55. M. Singerman cite Pemberton c. Bethlehem Steel Corp., 66 Md. App.133 (1986) qui fixe les limites de la surveillance des travailleurs à l'extérieur du lieu de travail.

[34] Nanette Green Kaminski et William Tran, *On Your Tracks: GPS Tracking in the Workplace*, National Workrights Institute, Princeton, N.J., Février 2007, p. 13.

[35] Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

[36] Commissaire à l'information du Royaume-Uni, *The Employment Practices Code*, juin 2005, p. 70.

[37] Rachel Konrad, "Meet the future: Our cars, ourselves," CNET News, 22 juin 2001.

[38] John Schwartz, "This Car Can Talk. What It Says May Cause Concern," *New York Times*, 29 décembre 2003.

[39] PA Consulting Group, *Driving crime down: Denying criminals the use of the road*, un rapport au Home Office, octobre 2004, pp. 37-40.

[40] Commissaire à l'information et à la protection de la vie privée de l'Ontario, rapport d'enquête, Enquête PC-010005-1 – La reconnaissance biométrique des visages dans les casinos de l'Ontario.

[41] Ibid, p. 4.

[42] Déclaration conjointe de l'American Civil liberties Union et du représentant du parti majoritaire à la Chambre des représentants Dick Armey : "Proliferation of Surveillance Devices Threatens Privacy," Washington, DC, 11 juillet 2001.

[43] Mark Milone, "Biometric Surveillance: searching for identity," *The Business Lawyer*, American Bar Association, Chicago, 1er novembre 2001.

[44] Reportage d'AP, *Face-scanning system used at Statue of Liberty, New York, 28 mai 2002.*

[45] Jay Stanley et Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, American Civil Liberties Union, janvier 2003, p. 3.

[46] Lettre ouverte au Parlement européen sur

l'inscription des données biométriques de tous les résidents et citoyens de l'UE, par Privacy International, Statewatch et European Digital Rights, 30 novembre 2004.

[47] Will Weissert, "Mexican justice ministry staffers get chip implants," *Chicago Sun-Times*, 15 juillet 2005.

[48] Evan Shuman, "U.S. Homeland Security Delays RFID Plan," *eWeek*, 28 février 2006.

[49] *Location Technologies: Mobility, Surveillance and Privacy*, p.14.

[50] Jonathan Wienberg, "RFID, Privacy and Regulation," in *RFID Applications, Security and Privacy*, Simson Garfinkel et Beth Rosenberg, éditeurs, Addison-Wesley, New Jersey, 2005, p. 91.

[51] Beth Givens, "Activists: Communicating with Consumers, Speaking Truth to Policy Makers," in *RFID Applications, Security and Privacy,* p. 432.

[52] Simson Garfinkel et Henry Holtzman, "Understanding RFID Technology," in *RFID Applications, Security and Privacy*, p. 18.

[53] Colin J. Bennett et Lori Crowe, *Location-Based Services and the Surveillance of Mobility: An Analysis of Privacy Risks in Canada*, Université de Victoria, juin 2005, p. 37.

[54] Conférence internationale des commissaires à la protection des données et de la vie privée, résolution sur l'identification par radiofréquence, version finale, 20 novembre 2003.

[55] Groupe de protection des données établi en vertu de l'article 29, *Document de travail sur les questions de protection des données liées à la technologie RFID (radio-identification)*, 19 janvier 2005.

[56] Commission européenne, *Policy Framework Paper,* atelier sur l'IRF, 11 mai 2006.

[57] The Wi-Fi Alliance, "Enabling the Future of Wi-Fi Public Access," p. 5. Ce document cite les prévisions de croissance d'un document de recherche de 2003, "Wi-Fi Hotspot Opportunities," par D[r] Daniel Sweeney pour Forward Concepts, un groupe de recherche de l'Arizona. The Wi-Fi Alliance est une organisation mondiale sans but lucratif qui a été mise sur pied pour promouvoir l'adoption d'une norme mondiale reconnue en matière de réseau local sans fil à haute vitesse.

[58] Y. Wang, X. Jia, H.K. Lee, "An indoors wireless positioning system based on wireless local area network infrastructure," document présenté à la 6[e] Conférence internationale sur la technologie de navigation par satellite y compris les services de localisation et de positionnement mobile,

Melbourne, juillet 2003, p. 13.

[59] Recherche sur la précision de la localisation chez Intel, document d'Intel Corporation, 2005.

[60] Communiqué de presse de la Electronic Frontier Foundation, "How Far Would You Go For Muni WiFi?", 21 octobre 2005.

[61] Wireless Broadband Internet Access Network Agreement between the City and County of San Francisco and EarthLink, Inc., 5 janvier 2007, pp. 20-21.

[62] *Columbia Insurance Co. c. Seescandy.com*, 185 F.R.D., p. 578.

[63] Pour tout renseignement sur cette norme, voir : www.ietf.org/html.charters/geopriv-charter.html

[64] John Morris et Jon Peterson, "Who's watching You Now?", *IEEE Security & Privacy*, IEEE Computer Society, janvier/février 2007, p. 78.

[65] Ibid.

[66] Pew Research Center, *The Internet News Audience Goes Ordinary*, 14 janvier 1999, p. 24. Dans une étude de 2006 de l'Université du Minnesota (Internet Use and Privacy Attitudes Survey), 31 % des étudiants ont dit qu'ils pensaient que leurs activités sur Internet étaient en général anonymes.