

Faculty of Informatics

Faculty of Informatics - Papers

University of Wollongong

Year 2007

Human Tracking Technology in Mutual Legal Assistance and Police Inter-state Cooperation in International Crimes

K. Michael*

G. L. Rose†

*University of Wollongong, katina@uow.edu.au

†University of Wollongong, grose@uow.edu.au

This book chapter was originally published as Michael, K & Rose, G, Human Tracking Technology in Mutual Legal Assistance and Police Inter-state Cooperation in International Crimes, in Michael, K and Michael, MG, From Dataveillance to Überveillance and the Realpolitik of the Transparent Society, University of Wollongong, 2007, 241-256.

This paper is posted at Research Online.

<http://ro.uow.edu.au/infopapers/563>

Human tracking technology in mutual legal assistance and police inter-state cooperation in international crimes

Katina Michael

Senior Lecturer, School of Information Systems and Technology, University of Wollongong

Gregory Rose

Associate Professor, Centre for Transnational Crime Prevention, University of Wollongong

Abstract

The objective of this paper is to explore the role of human tracking technology, primarily the use of global positioning systems (GPS) in locating individuals for the purposes of mutual legal assistance (MLA), and providing location intelligence for use in inter-state police cooperation within the context of transnational crime. GPS allows for the 24/7 continuous real-time tracking of an individual, and is considered manifold more powerful than the traditional visual surveillance often exercised by the police. As the use of GPS for human tracking grows in the law enforcement sector, federal and state laws in many countries are to a great extent undefined or even contradictory, especially regarding the need to obtain warrants before the deployment of location surveillance equipment. This leaves courts ruling on transnational crimes in the precarious position of having to rely on age-old precedents which are completely void to the new capabilities of today's tracking technologies. On one side of the debate are civil libertarians who believe the individual's

right to be let alone is being eroded to the compromise of human rights, and on the other side are law enforcement agencies who wish to provide more precise evidence to judges and juries during hearings against suspects (particularly in issues pertaining to national security). This paper argues that there is a radical middle position, the *via media*: that a warrant process is legislatively defined and not only for MLAs but also to formalise existing informal inter-state police cooperation. Safeguards are required to overcome the potential misuse of human tracking technologies by police officials and others in positions of power. And this particularly in light of the emerging implantable high-tech identification and tracking devices now commercially available.

Keywords: inter-state police cooperation, law enforcement, intelligence, global positioning systems (GPS), human tracking, covert surveillance, privacy, human rights

1 Mutual legal assistance in locating the accused

Mutual Legal Assistance (MLA)¹ can be defined as a mechanism by which lawyers and the courts of one jurisdiction can request assistance from another. MLAs ensure that individuals cannot evade prosecution simply because the evidence to prosecute them is located in another country. The MLA document states the required assistance sought in the provision of evidence for criminal proceedings or proceedings about to commence.² Depending on the domestic law and that law of the requested State, the most common types of assistance that is usually obtained includes: witness interviews and material held by third parties (such as telecommunication documents, phone records, e-mail, facsimile billing and subscriber information).³ This paper deals with the latter and specifically the use of covert location-based surveillance. MLAs should be used when evidence cannot be gathered using informal police-to-police cooperation.

In the treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, the scope of assistance ranges from 'providing documents, records, and other articles of evidence; locating or identifying persons; and executing requests for searches and seizures and for

¹ Mutual legal assistance was developed during the 1960s but its origins can be found in the century-old practice known as "Letters Rogatory." Letters Rogatory is based on the principle of comity, when the '... courts of one state address a request to those of another state for judicial assistance in the form of taking the testimony of a witness or securing tangible evidence.' See M. Cherif Bassiouni, *Introduction to International Criminal Law*, International and Comparative Criminal Law Series (2003) 352. See also Ilias Bantekas and Susan Nash, *International Criminal Law* (2003) 231. MLAs abide by the *locus regit actum* rule.

² International Association of Prosecutors, *Basic Guide to Prosecutors in Obtaining Mutual Legal Assistance in Criminal Matters* (2004) 2.

³ *Ibid.* See also, the *Mutual Assistance in Criminal Matters Act 1987* (Cth). This Act should be read together with the following relevant Australian legislation: *Foreign Evidence Act 1994* (Cth), *Proceeds of Crime Act 2002* (Cth), *Telecommunications (Interception) Act 1979* (Cth), and the *Surveillance Devices Act 2004* (Cth). Only by studying the various Acts can one appreciate the complexity of MLATs and the various considerations that need to be grasped in making a request to a given state, or satisfying a request by another state.

restitution'.⁴ 'These forms of legal assistance can be conducted by the judicial, prosecutorial or law enforcement personnel of the requested state.'⁵ Mutual Legal Assistance Treaties (MLATs) can be bilateral or multilateral.⁶ 'As of the 1960s, the practice of many states (within Europe, Latin America, the United States, and Canada) shifted to bilateral MLATs... Still the number of bilateral MLATs is far less than bilateral extradition treaties, as is the number of states having national legislation on the subject...'⁷ States have become increasingly willing to negotiate MLATs,⁸ particularly since 11 September 2001 (9/11), as a means to increased access of evidence located abroad.⁹

What is unique about MLATs is that they are only really meant to benefit governments, and only governments can make exclusive use of evidence to satisfy a given request. However, governments are under no obligation to provide evidence and they can reject a request based on any number of grounds.¹⁰ MLATs in most instances contain provisions for human rights but through reservations and safeguards which are 'built-in'

⁴ Department of Foreign Affairs and Trade, *Treaty between the Government of Australia and the Government of the United States of America on Mutual Assistance in Criminal Matters, and Exchange of Notes* (2000).

⁵ Bassiouni, above 1, 354.

⁶ The 1959 Council of Europe Convention on MLA in Criminal Matters which was ratified in 1962 was one of the first multilateral treaties and is recognized as an important step in international judicial co-operation. See Bantekas, above 1, 234.

⁷ Bassiouni, above 1, 353.

⁸ Bantekas, above 1, 231.

⁹ See, eg, Attorney-General's Department, *Annual Report 2004-2005* (2005) <[http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(CFD7369FCAE9B8F32F341DBE097801FF\)~80Recent+Statistics.pdf/\\$file/80Recent+Statistics.pdf](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~80Recent+Statistics.pdf/$file/80Recent+Statistics.pdf)> at 1 June 2007. The number of requests made by Australia carried forward from 2003–04 were 170, new requests made in 2004–05 were 151, requests finalized were 126, and requests continuing were 195. The majority of requests came from the United Kingdom, Netherlands, and the United States of America, and the majority type of assistance granted was for telecommunications and email records etc, and bank and business records. A similar number of requests were made to Australia, indicating that MLATs are highly reciprocal in nature.

¹⁰ Bassiouni, above 1, 354.

to protect the accused. It is important to note, that MLAs can only be executed by remaining in accordance with the law of the requested state, without violating third party rights. In the context of search for and seizure of evidence using location surveillance, this becomes very important.¹¹

2 Inter-state police cooperation for information gathering and sharing

Given the number of requests published in annual reports by government agencies, and the highly publicized media accounts of increasing transnational crime,¹² it is obvious that the collection and exchange of relevant information pertaining to a transnational criminal investigation happens through informal police cooperation at a federal level.¹³ One can conclude from this that mutual assistance and police-to-police assistance are complementary. However, while law enforcement and intelligence cooperation is increasing, it is not regarded in the same way from a legal perspective. For instance, there are no treaties applicable to law enforcement or police cooperation as there are for mutual assistance, nor are there codes of conduct for how information should be gathered and shared between government agencies.¹⁴ When

¹¹ Bantekas, above 1, 233-234. See also, *Model Treaty on Mutual Assistance in Criminal Matters*, adopted by General Assembly resolution 45/117, subsequently amended by General Assembly resolution 53/112 (entered into force 14 December 1990). In the context of human rights, see, Ian Brownlie and Guy S. Goodwin-Gill (es), *Basic Documents on Human Rights* (2002).

¹² See, United Nations Office on Drugs and Crime, *The Seventh United Nations Survey on Crime Trends and the Operations of Criminal Justice Systems (1998 - 2000)*, (2006) <http://www.unodc.org/unodc/crime_cicp_survey_seventh.html> at 4 June 2007. Compare with data found in Attorney-General's Department, above 9. The statistics for MLAs and national/international crime trends indicates that a great number of investigations do not go through the MLA process but via the more informal police-to-police cooperation route.

¹³ Bantekas, above 1, 236, 261. 'Despite the increased willingness of States to engage in formal methods of mutual legal assistance, there are many other less formal methods of evidence gathering, which permit law enforcement agencies to exchange information and material relevant to transnational investigations.'

¹⁴ Bassiouni, above 1, 368. Bassiouni is strong in his stance commenting: '[r]egrettably, this important form of international cooperation [ie police cooperation in transnational crime] has not yet been included in mutual legal assistance treaties.'

one considers the need for location surveillance¹⁵ and other forms of covert surveillance, particularly in the gathering of evidence, 'there are no legal or judicial safeguards to insure effective and regulated modalities of information-gathering and information-sharing between intelligence, law enforcement, and prosecutorial agencies.'¹⁶ In fact, regulation is the major problem here. How are potential abuses combated¹⁷ and how is effectiveness maintained? How can the accuracy of information be guaranteed? And what of privacy when international practices vary greatly? These are the challenges that new technologies and emerging law enforcement workflows pose on the due process of law.

As any other organization in a given jurisdiction, law enforcement agencies are bound by national criminal law at the domestic level. Yet, many have questioned whether this is enough given that intelligence and law enforcement agencies have been quite secretive about their practices. For the greater part the way that these particular organizations have shared intelligence has been outside legal or judicial supervision.¹⁸ Thus, the problem is two-fold: (i) a legal framework in most jurisdictions does not exist to aid in regulation, and (ii) there is a reluctance of members of the intelligence sector to provide transparency in their activities within a

¹⁵ Katina Michael et al, 'Location-Based Intelligence – Modeling Behavior in Humans using GPS' (2006) *International Symposium on Technology and Society (ISTAS '06)* 1.

¹⁶ Bassiouni, above 1, 369. See also, Commission New South Wales. Law Reform, *Surveillance: An Interim Report* (2001).

¹⁷ John S. Ganz, 'Comment: It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices' (2005) 95 *Journal of Criminal Law & Criminology* 1360. 'Finally, again from a policy perspective, some might argue that the failure to require warrants could lead to arbitrary and capricious use of GPS by police. As dissenting Nevada Supreme Court Justice Robert Rose noted in Osburn, "The automobile's use is a necessity in most parts of Nevada, and place a monitor on an individual's vehicle effectively tracks that person's every movement just as if the person had it on his or her person... I fear that in some instances, the monitor will be used to continually monitor individuals only because law enforcement considers them "dirty." In the future, innocent citizens, and perhaps elected officials or even a police officer's girlfriend or boyfriend, will have their whereabouts continually monitored simply because someone in law enforcement decided to take such action. This gives too much authority to law enforcement and permits the police to use the vehicle monitor without any showing necessity and without a limit on the duration of the personal intrusion.'"

¹⁸ Bassiouni, above 1, 369.

judicial system.¹⁹ This issue has been exacerbated since 9/11 when the United States demanded that states share more information with them, and that their intelligence personnel gather more data so as to curb such terrorist²⁰ acts in the future.²¹ Recent events have shown the power of data accessibility, with numerous terrorist plots foiled by intelligence organizations, preventing mass casualties.²² But at the same time the rights of individuals to know that data is being collected about them, to be able to rectify erroneous data, to protect privacy is also important.²³ The whole debate over weapons of mass destruction (WMD) allegedly located in Iraq, which was later proven to be unreliable, indicated the systemic flaws in American intelligence which were blamed primarily on management.²⁴ Interestingly, the result of this flaw, quite legitimately, was for American intelligence agencies to increase information sharing even more.²⁵ One can be lead to the hypothesis that greater intelligence

¹⁹ Ibid.

²⁰ For comparative definitions of terrorism see, Claire De Than and Edwin Shorts, *International Criminal Law and Human Rights* (2003) 231-237.

²¹ Terrorism is considered to be just one reason why information gathering and sharing practices have increased, other notable transnational crimes include: drug and people trafficking, money laundering, and the smuggling of things. See eg, the role of intelligence in security informatics in Hsinchu Chen, *Intelligence and Security Informatics for International Security* (2006).

²² See, eg, Transportation Security Administration, *Information on Plot to Attack John F. Kennedy Airport* (2007) <http://www.tsa.gov/press/happenings/jfk_terror_plot.shtm> at 2 June 2007.

²³ Bassiouni, above 1, 370. There are however efforts between nations to broker agreements that do try to address data protection principles, at least in theory. See, eg, *Agreement Between the United States of America and the European Police Officer*, Europol file no. 3710-60r2 (Dec 6, 2001), *Supplement Agreement Between the United States of America and the European Police on the Exchange of Personal Data and Related Information*, Europol file no. 3710/60r3 (Dec. 20, 2002). "Europol is essentially a police coordination centre for collecting, analyzing and sharing information to help investigations being carried out in two or more EU countries". European Commission, *Freedom, Security and Justice for All* (2004) 19. See also, OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1981).

²⁴ GlobalSecurity.org, *Intelligence: Additional Views of Senator Olympia Snowe* (2004) <http://www.globalsecurity.org/intell/library/congress/2004_rpt/iraq-wmd-intell_olympia-snowe.htm> at 3 June 2007.

²⁵ Ibid. 'Surprisingly, the Committee's review reveals that even after the lack of information sharing was found to have played a key role in the intelligence failures of September 11, 2001,

effectiveness is proportional to the amount of information shared by states but this too has implications for privacy. Not only is the balance between personal privacy and national security almost impossible to achieve but intelligence born from “überveillance-type” regimes can introduce the potential for misinformation and misinterpretation. Going to one extreme or the other has negative implications- i.e. making all personal data public might increase transparency in the short-term but may have the equal effect of increasing identity fraud in the long-term, and not engaging in any information sharing practices would be detrimental to a nation’s security.

3 The nature of evidence and the new technologies

Evidence takes on two basic forms, that which is a written statement in place of oral transmission, and anything on which something can be recorded. High-tech gadgetry is becoming increasingly useful in storing recorded information digitally. Not only can miniature devices do so with incredible amounts of storage power but they can do so continually 24/7, using very little on-board battery power and with a relatively low degree of risk to humans. Digital documentary evidence that has been used in ad hoc tribunals for instance includes aerial photography, audio and video tapes, maps and sketches of plans, and a variety of digital record formats. ‘Such evidence is deemed admissible if it contains information of probative value.’²⁶ Digital evidence especially is prone to tampering however this is the emerging context in which courts now have to operate.

New technologies, which have allowed for covert surveillance to be performed without the permission of a given state, highlight the need for

intelligence agencies still fail to share information within and among its own cadre. ... For example, the CIA failed to share information on the reliability of two biological weapons sources with all Iraq biological weapons analysts. Information about the credibility of these sources, upon which many assumptions regarding Iraq’s biological weapons program were made, could have significantly altered analysts’ judgments. In addition, the CIA failed to share some intelligence reporting with other agency [unmanned aerial vehicle] UAV analysts on critical issues surrounding Iraq’s UAVs. ... The Committee’s review shows that the CIA continues to overly compartment sensitive HUMINT reporting and that this lack of information sharing prevented key analysts on certain issues from making fully informed judgments.’

²⁶ Bassiouni, above 1, 656.

regulation.²⁷ One need only point to the Echelon operation, which was first considered a wild conspiracy, but which was later shown to be a mass surveillance operation by the United States, United Kingdom, Canada, Australia and New Zealand on major European industries. 'It was in short a major scandal of governmental industrial espionage against friendly states.'²⁸ It is not being argued here that new technologies should not be exploited to their maximum potential to prevent or suppress criminality but they presently remain unregulated. So in admitting evidence that has been gathered in another country, national courts need to maintain that the evidence has been gathered within the confines of a given state's domestic law, and not by any other means.²⁹ If we cannot be confident in this, then not only are we making sweeping assumptions about the reach of laws but we are creating a law unto ourselves, to do as we please, as we see fit. When comparing the comprehensive and robust MLA process (although to some seemingly long-winded and bureaucratic), with just-in-time inter-state police cooperation, one can come to the resolution that there is a great divide that needs to be bridged. With reference to police cooperation, it must be said, that better processes with regulations at an inter-state and international level, can only increase the likelihood that cross-border criminals will be brought to justice and tried under the most suitable laws, resulting in a better outcome for all parties concerned.³⁰

In an attempt to bridge that gap the United Nations adopted the Convention Against Transnational Organized Crime in 2000 that addressed but did not regulate the question of inter-state law enforcement cooperation.³¹ Articles 26-28 raise the matter of bilateral and multilateral

²⁷ Bantekas, above 1, 240. 'Due to the nature of modern telecommunications systems, interception frequently does not require technical assistance from other States.'

²⁸ Bassiouni, above 1, 371-373.

²⁹ Bassiouni, above 1, 374. See also, Bantekas, above 1, 255. Interestingly however, '... the Court is prepared to focus on the nature of the evidence rather than the fact that human rights standards have been breached.'

³⁰ David Lanham, *Cross-border Criminal Law* (1997) 44-45.

³¹ See also, Bantekas, above 1, 236. In Title VI of the Treaty on European Union (TEU) a similar hope was set out, to develop 'common action among Member States in the fields of police and

agreements inviting ‘... state parties in accordance with their national legal systems to develop national legislation permitting special investigative techniques’,³² which could then be extended beyond the borders and applicable to law enforcement and intelligence organizations. The articles specifically addressed forms of electronic surveillance and how they might be used in joint investigative operations. For example, although it took several years to agree on, Member States finally ratified a convention which would allow them in appropriate circumstances to intercept communications directly.³³ It should be highlighted that the convention was seen as going soft on data protection and in allowing for dubious practices such as that of cross-border observation, in actual fact, hot pursuit of suspects or fugitives by foreign police officers across borders.³⁴

There is ‘... no evidence [that] exists outside court proceedings.’³⁵ In common law countries facts must be proved beyond a reasonable doubt.³⁶ For a definite conclusion to be sought however, the evidence which has been gathered must also have been collected with the same level of confidence. ‘Implicit in the right to a fair trial is the rejection of evidence obtained in breach of fundamental human rights standards.’³⁷ New technologies and techniques however may not coerce an individual

judicial co-operation in criminal matters.’ The EU has been to some degree successful at achieving these goals, at least insofar as communicating standards, guidelines and protocols to Member States.

³² Bassiouni, above 1, 375. See also, Elia Zureik and Mark B. Salter (eds), *Global Surveillance and Policing: Borders, Security, Identity* (2005).

³³ Bantekas, above 1, 239, 259. ‘In addition to avoiding formal procedures, prosecuting authorities engage in informal mutual co-operation practices by simply allowing police officers in another jurisdiction access to evidence.’

³⁴ *Ibid* 279.

³⁵ Antonio Cassese, *International Criminal Law* (2003) 421.

³⁶ *Ibid* 425.

³⁷ Bantekas, above 1, 254-255, 284. Proceedings from the *Corpus Juris* Project in Europe stated ‘(1) [e]vidence must be excluded if it was obtained by community or national agents either in violation of the fundamental rights enshrined in the European Convention on Human Rights...’

to confessing to a crime, but may apply irregular methods of data collection that in some instances could be considered a type of intimidation.³⁸ A frequent happening in international criminal proceedings is when a prosecutor does not wish to disclose their source of information for reasons of confidentiality, safety, or other.³⁹ Quite often secret intelligence organizations are not prepared to tell the public how they obtained a particular record or document, and in many instances the evidence provided is still accepted.⁴⁰ Courts are faced with a difficult choice when it is obvious that unlawful means have been used to obtain evidence- excluding the evidence may mean doing away with the reliable information, while admitting it legitimized illicit and irregular modes of investigations.⁴¹

4 Human tracking technologies used for location intelligence

How are authorities able to locate individuals who are suspected of transnational crimes for the purpose of MLA requests and inter-state police cooperation? ‘Mobility is a basic and indispensable human activity that is essential for us to be able to lead independent lives on a daily basis’.⁴² Criminals suspected of a crime- like every other human being-

³⁸ Ibid 245, 246. See, eg, ‘[i]n *R v Terry*, the court also held that the Charter of Rights has no effect on law enforcement officials abroad, and as such does not render illegally obtained evidence inadmissible. ...However, the failure to reject evidence which was obtained not merely in breach of foreign law, but also in violation of international human rights standards ... is lamentable and demonstrates a lack of sensitivity and understanding of the rules operating in other legal systems.’

³⁹ Bassiouni, above 1, 656-657. ‘The problem, however, is when this evidence is provided by intelligence agencies who do not wish to have their sources disclosed. This issue of confidentiality of sources makes it difficult, if not impossible, to use valuable information.’

⁴⁰ Antonio Cassese, *International Criminal Law* (2003) 424.

⁴¹ Liam Byrne, ‘Admission of Evidence Obtained in Breach of Privacy Laws’ (2007) (78) *Precedent* 21. English, Canadian, American, Australian, Irish and Scottish courts all differ on their positions regarding what constitutes ‘lawful methods’ of data gathering for admittance of evidence in their courts.

⁴² K. Kayama, I.E. Yairi and S. Igi, ‘Semi-Autonomous Outdoor Mobility Support System for Elderly and Disabled People’ (2003) *International Conference on Intelligent Robots and*

require to move around in public space in order to satisfy basic living requirements. Someone who is moving can be tracked manually or digitally, even if they (or persons harboring criminals) are using cash to pay for their every transaction.⁴³ The information being gathered as a person moves from one place to the next can be considered a type of chronicle or breadcrumb. Today, given the high-tech devices available to law enforcement and intelligence organizations, an electronic chronicle⁴⁴ and electronic breadcrumb⁴⁵ can be gathered, stored, and manipulated for presentation at a later date. To allow oneself to be tracked can be a voluntary act, but in most cases it is imposed by a third party who has some control over the end-user.⁴⁶ Tracking can be obtrusive taking the form of overt surveillance⁴⁷ (ie the individual knows they are being followed), or as in most cases tracking is unobtrusive taking the form of covert surveillance (ie the individual is not aware that they are being

Systems 2606.

- ⁴³ Stephane Leman-Langlois, 'The Myopic Panopticon: The Social Consequences of Policing through the Lens' (2003) 13(1) *Policing and Society* 51, 54. 'The combination of face recognition, motion analysis and sound analysis could become very interesting in the near future.' Leman-Langlois writes of an 'omniscient surveillance.' See also, the notion of 'überveillance' in Katina Michael et al, above 15, 7.
- ⁴⁴ G. Pingali and R. Jain, 'Electronic Chronicles: Empowering Individuals, Groups, and Organisations' (2005) *IEEE International Conference on Multimedia and Expo* 1540.
- ⁴⁵ Wherify, *Wireless Location Services* (2005) <<http://www.wherifywireless.com/>> at 29 May 2007.
- ⁴⁶ R. Cucchiara, C. Grana, and G. Tardini, 'Track-based and Object-based Occlusion for People Tracking Refinement in Indoor Surveillance' (2004) *Proceedings of the ACM 2nd International Workshop on Video Surveillance & Sensor Networks* 81-87. Tracking is critical in the process 'of people motion capture, people behavior control and indoor video surveillance.' See also, Clive Norris, Jade Moran and Gary Armstrong, *Surveillance, Closed Circuit Television and Social Control* (1998).
- ⁴⁷ Stephen Green, 'A Plague on the Panopticon: Surveillance and Power in the Global Information Economy' (1999) 2(1) *Information, Communication & Society* 31. 'In the United Kingdom, Newcastle police claim that CCTV has led directly to 2,800 arrests from 1991-9, with 99 per cent of offenders pleading guilty when presented with video evidence ... In contrast to more radical libertarian accounts, the key point here is that not every sacrifice of individual autonomy and 'privacy' is the same as the loss of freedom...'

tracked).

Today, tracking is possible via a vast array of technologies- from GPS devices, to radio beepers, electronic mail, and even fixed and mobile telephony.⁴⁸ In fact, the use of a mobile phone in most more-developed countries means that a location fix within about 50 meters of the user's handset is possible, just by an individual having their phone on.⁴⁹ Increasingly, mobile phones are also being equipped with GPS chipsets which means that if a mobile device is outdoors, a service provider can perform a position fix within seconds if a request is made by the police.⁵⁰ And it is not only the location position fix that is revealing, even more telling is the continuous, real-time location information that can be gathered by a GPS, including accurate geodetic information, such as longitude and latitude, time and speed.⁵¹ Beyond statistical data, location intelligence 'reveals a great deal about one's preferences, friends,

⁴⁸ William A. Herbert, 'No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?' (2007) 2(2) *I/S: A Journal of Law and Policy* 410. "In contemporary American culture, some view the concept of freedom as being manifested in consumerism, with the ubiquitous cell phone as a primary symbol. It is doubtful that most cell phone users are aware that the same technology that grants them this sense of freedom, also results in wireless companies, receiving automatic and continuous updates regarding their location. Physical possession of a cell phone renders an individual vulnerable to location surveillance by government entities...'

⁴⁹ Katina Michael 'Location-based Services: a Vehicle for IT&T Convergence' in K. Cheng et al (eds), *Advances in e-Engineering and Digital Enterprise Technology* 467. It should be noted that GPS data is not foolproof. Speed miscalculations, location fix inaccuracies, signal dropouts, can all occur due to the physical structures that the GPS passes through, and even to changes in climatic conditions, and the presence of dense foliage.

⁵⁰ Lemay-Langlois, above 43, 46. 'First, there is *deterrence*: overt surveillance aimed primarily at discouraging potential offenders from actually committing crimes. Second, *intelligence gathering*: a police force may be interested in collecting images for their information content, to build files, understand relationships, create chronologies, etc. Third, *evidence*: evidence is information that meets basic legal requirements and is thus admissible in court to support the accusation of a suspect.'

⁵¹ Ganz, above 17, 1329. 'One model, which a Law Enforcement Technology Magazine reviewer called a "vehicle tracking system that would make James Bond envious," sells for \$2,396 per unit. Users pay \$59 per month of tracking data used. The product can be attached to a car in thirty seconds and operates anywhere in the United States, Canada and Mexico where cell towers exist.'

associations, and habits.⁵² Till now law enforcement agencies have used GPS to investigate murder cases, drug investigations, robbery, public corruption, probation violations and hostage situations.

5 GPS evidence in Court- case law examples in the United States

Although GPS technology has been used in law enforcement since the early 1990s,⁵³ it is only recently that a few cases have been heard regarding the validity of using GPS tracking technology on suspected criminals.⁵⁴ All of the cases presented here are based on case law in the United States. The Fourth Amendment in the United States Constitution is the main source of legislation pertaining to the protection of an individual's right to privacy. 'At present, the United States Supreme Court has not ruled on the applicability of the Fourth Amendment to most recent forms of human tracking technology.'⁵⁵ There have been some landmark cases however, that have pointed towards the requirements for warrants to conduct surveillance activities. Compare for instance the cases *Olmstead v. United States* with *Katz v. United States*. In 1928 the United States Supreme Court determined that the Fourth Amendment did not prohibit

⁵² April A. Otterberg, 'Note: GPS Tracking Technology: The Case for Revisiting *Knotts* and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment' (2005) 46 *Boston College Law Review* 663.

⁵³ Prior to GPS technology, less sophisticated technology was used, known as beepers. Beepers helped locate a vehicle once an event occurred, such as a car door opening or the ignition starting, or movement. Beeper technology could alert police officials to locate the originating position of the vehicle, and thereafter it would be tailgated using traditional visual surveillance means.

⁵⁴ *Olmstead v. United States*, 277 US 438 (1928). *Katz v. United States*, 389 US 347 (1967). *United States v. Knotts*, 460 US 276 (1983). *United States v. Karo*, 468 US 705, 707 (1984). *Kyllo v. United States*, 533 US 27 (2001). *State v. Jackson*, 76 P.3d 217, 220 (Wash 2003). *State v. Peterson*, (Cal 2004). *People v. Lacey*, Indictment No 2463N/02, 2004 WL 1040676 (Nassau, NY County Ct. May 6, 2004), *People v. Gant*, 9 Misc 3d 611 (Westchester, NY County Ct. 2005). See also, Otterberg, above 52, 680. 'Only a few courts have specifically considered whether the monitoring of GPS tracking devices is distinguishable from the monitoring of the beepers in *Knotts* and *Karo*.'

⁵⁵ Herbert, above 48, 417.

the action of eavesdropping using telecommunications networks, while almost forty years later in 1967 the Court held that the FBI's use of a microphone on the roof of a payphone, without a warrant, constituted a violation of the Fourth Amendment.⁵⁶ Still, the Court ruled that using a tracking device to monitor vehicles or objects was not subject to the expectation of a privacy test. For example, a person traveling in a car on a public road from A to B had no reasonable expectation of privacy as he or she was out-n-about in full view of the public.⁵⁷ This decision was again reaffirmed in 1983 in the *United States v. Knotts* case when the Supreme Court again ruled 'that the police did not have to obtain a warrant under the Fourth Amendment before using a radio beeper to monitor the movement and location of a vehicle.'⁵⁸ The Court portrayed beepers as a mere replication of the traditional, manual, police visual surveillance conducted via physically tailing a vehicle.

In *Kyllo v. United States* in 2001 yet another twist to the interpretation of the Fourth Amendment was played out. The Supreme Court declared that protections within the boundaries of the home were only limited to devices that were not in "general public use".⁵⁹ When one considers the proliferation of mobile telephones many of which are now location-aware or GPS devices that are now found in up-market vehicle models, the United States human tracking possibilities look vast. What may this mean for average citizens wishing to take the law into their own hands and begin to track one another?

⁵⁶ Ibid 418-419, 420. '... by mandating for the first time that the police obtain a court-ordered warrant before engaging in electronic surveillance, the *Katz* decision established a significant judicial check on government agents randomly engaging in such surveillance.' In *Katz* it was also interesting to note a shift in emphasis from protecting a place where someone resides, to protecting the person from government intrusion.

⁵⁷ The definition of a 'public space' and that of a 'private space' has been open to debate in recent times. Is private only the space in which we reside- the four walls of our home when the blinds are down, and the inner lining of our roof? If so what happens when we walk outside our doorstep? Or even more precisely if a vehicle that has a GPS unit attached, enters a garage which is connected to the home?

⁵⁸ Herbert, above 48, 420-421.

⁵⁹ Ibid 424.

At the state and local levels, courts hold differing positions based on their jurisdiction. For the greater part, warrants must be obtained prior to the operation of an electronic device to track an individual. In Washington's highest court the power of GPS to be more than a tracking device was recognized:

[U]se of GPS tracking devices is a particularly intrusive method of surveillance, making it possible to acquire an enormous amount of personal information about a citizen under circumstances where the individual is unaware that every single vehicle trip taken and the duration of every single stop may be recorded by the government.⁶⁰

However, in the cases *People v. Lacey* and *People v. Gant* the opposite judgment was reached on the same question of warrant requirements for a GPS tracking device on a vehicle.⁶¹ This seemingly contradictory position of the State of Illinois is disturbing especially when one considers the federal constitution in context and the requirement for inter-state agreements in locating criminals or proceeds of crime. Two of the most high profile cases where data was gathered using a GPS and admitted as evidence was in the 1999 *State v. Jackson* and in 2003 *State v. Peterson*. In the *Jackson* case a judge executed a search warrant on Jackson's vehicles and residence for ten days, and then subsequently granted two more warrants which were extensions of time for the police to continue with covert surveillance.

Specifically, data showed that on November 6th, Jackson drove his truck to rural Springdale and parked without leaving for forty-five minutes. On November 10th, Jackson made a trip to Vicari and Springdale, two remote sites, where he remained for sixteen minutes and thirty minutes, respectively. The police discovered Valiree's body in a shallow grave at the Springdale site and promptly arrested Jackson.⁶²

⁶⁰ Ibid 431-432.

⁶¹ Ibid.

⁶² Tenison Craddock, 'Casenote: The Limitations on Police Regarding GPS Tracking Devices: A Necessary Hindrance?' (2005) 9 *Computer Law Review & Technology Journal* 506-507.

It was the Jackson case which really demonstrated the power of GPS tracking technology to justices all over America, in terms of the privacy implications. Counter-arguments grew however as questions were raised about trusting law enforcement personnel to act appropriately.⁶³ In addition, the question of the right to privacy by a suspected criminal also came to the fore.⁶⁴ It was not until the Peterson case that a judge reaffirmed that GPS location data was acceptable and fundamentally valid as a generic methodology to employ in gathering evidence for a trial.⁶⁵ What these example cases reveal is that the warrant process and admissibility of evidence varies dependent on the jurisdiction. This is magnified when one considers the absence of provisions in an international setting.⁶⁶

More recently the reliability of GPS data has come into question. While the technology can have almost pinpoint accuracy, it does suffer from technological limitations depending on environmental factors. There are a growing band of domestic GPS-related cases in the United States, which have either been lodged by individuals or unions,⁶⁷ challenging companies or employers regarding GPS accuracy and the individual's right to be let alone.⁶⁸ In most of the cases to do with accuracy, GPS

⁶³ Ganz, above 17, 1325. 'Global Positioning System (GPS)-based surveillance systems enable police to cheaply and easily gather intelligence and evidence they would otherwise have to obtain through more costly, cumbersome and risky means such as physical "tails" by pursuing officers. The efficiency gains GPS tracking provides are especially significant because they enable police to extend their operational capability with minimal incremental spending.'

⁶⁴ Craddock, above 62, 510.

⁶⁵ Ibid 511.

⁶⁶ Byrne, above 41, 24. 'Different results can also arise depending on which privacy law is breached and what type of proceeding is in question.'

⁶⁷ Email from William Herbert to Katina Michael, 10 April 2007. '... The union ... is currently challenging employers who have imposed GPS technology unilaterally on union members.'

⁶⁸ See, eg, GPSTrackSys, *7th Circuit U.S. Court of Appeals Okays Surreptitious GPS Tracking by Police* (4 February 2007) <<http://gpstrackingsystems.biz/7th-circuit-us-court-of-appeals-okays-surreptitious-gps-tracking-by-police/25/>> at 1 October 2007. 'The fourth amendment protects against unreasonable search and seizure, but the judges ruled that the placement of a GPS tracking device without the suspect's knowledge, does not qualify as a search of his car. This is the first time the

speed miscalculations or position fixes are at the heart of the matter- employees have either been fined for speeding in a company vehicle (e.g. truck), or individual consumers have been charged an additional levy for allegedly crossing state boundaries (e.g. car hire).⁶⁹ In October of 2007, there were a few cases reported that stipulated that the U.S. government had terminated an employee's contract based on data collected covertly using the GPS chipset in the government-owned mobile handset carried by the employee.⁷⁰ Most of these latter cases have focused on the physical location of the employee- e.g. that employees were claiming financial remuneration for hours not physically worked at the office. But this too is open to misinterpretation- what if the employee worked through his/her lunch break, or took work home with them? We can see by this example how GPS data can reveal only partial truths and cannot be used as the sole piece of evidence. GPS data also has to be stored somewhere- and herein lies its greatest weakness- longitude and latitude position coordinates can be changed on the fly to fabricate evidence (for or against the defendant). Currently only 2 states in the U.S. require a company to let an employee know when they are monitoring them. These cases are only indicative of potential international issues that may arise when GPS is used to track suspects.

seventh circuit has weighed in on this issue, which other circuits have split on. The court equated GPS tracking to police physically following a car, or monitoring safety cameras to follow a car, neither of which amounts to illegal search and seizure.'

⁶⁹ See, eg, Anita Ramasastry, *Tracking Every Move You Make: Can Car Rental Companies Use Technology to Monitor Our Driving?* FindLaw (23 August 2005) <<http://writ.news.findlaw.com/ramasastry/20050823.html>> at 1 October 2007. 'First, let's look at the Connecticut case. It arose because American Car Rental had a policy of charging its clients \$150 for "excessive wear and tear" to the rental car, each time they drove over 79 miles per hour. American knew exactly when that occurred because its subsidiary, Acme Rental, used GPS installed in its cars to monitor renters' speed as they traveled. Whenever GPS reported that the customer drove at least 80mph for more than two minutes at a time, the company charged the customer's credit or debit card \$150.'

⁷⁰ See, eg, Allen Stern, *Man Fired Thanks to GPS Tracking* (31 August 2007) <<http://www.centernetworks.com/man-fired-thanks-to-gps-tracking>> Center Networks at 1 October 2007. 'The NY Post reports, "Schools Chancellor Joel Klein yesterday fired a veteran worker whose movements were tracked for five months through the GPS device in his cellphone, leading to charges that he was repeatedly cutting out early.'

6 Human rights v. national security

Privacy advocates and civil libertarians often point to the erosion of human rights through the development and application of novel technologies in the area of law enforcement. It is true, that the new innovations pose legal and political challenges but a balance must be struck between their usage for legitimate purposes such as in the case of fulfilling an MLA request or formalised inter-state police cooperation, and those that may be considered illegal and a breach of citizen privacy.⁷¹ The growing problem is not that these technologies are diffused commercially but the possibility that if they are used for law enforcement purposes, they will eventually find their way into government mandated schemes for the general populous.⁷² In quoting Jacques Ellul, privacy expert David Lyon, brings this notion to light:

“To be sure of apprehending criminals, it is necessary that *everyone* be supervised.” Substitute the word ‘terrorists’ for ‘criminals’ and we have an uncannily accurate description of the world since 9/11.⁷³

For now, sweeping legislative changes that have taken place post-9/11 have coincided with the widespread diffusion and use of human tracking technologies.⁷⁴ The United States has been criticized in particular for their departure from human rights standards; some even

⁷¹ Richard Abraham, ‘The Right to Privacy and the National Security Debate’ (2007) 78 *Precedent* 33. ‘...Australia lacks an adequate framework for balancing the right to privacy (and human rights in general) against competing rights and interests. ... This is not an argument against maintaining a strong security agency or enacting national security legislation. Instead, it is a call to improve the process by ensuring the effective protection of the very rights they are said to protect.’

⁷² Otterberg, above 52, 670. ‘...[B]ut what concerns privacy advocates is the tracking of suspects and those who have not yet been convicted of any crime. Privacy advocates draw parallels between such GPS tracking and the Orwellian state—one where the average citizen must live and move about while knowing the government may be watching and scrutinizing the individual’s every movement.’

⁷³ David Lyon, ‘Sorting for Suspects’ (2004) 70 *Arena Magazine* 26.

⁷⁴ Alan Davidson, ‘Electronic surveillance regulations’ (2004) 24(9) *Proctor* 31. ‘The [Patriot] Act authorizes nationwide execution of court orders for pen registers, trap and trace devices, and access to stored email or communication records.’

going as far as concluding that they have shown disregard for the fundamental principles of international law.⁷⁵ Australia also has received similar backlash by international political commentators:

The new legislation has serious implications for bodily, territorial, communications and information privacy, specifically the *Australian Security Intelligence Organization Legislation Amendment (Terrorism) Act 2003* (Cth); *Anti-Terrorism Act (No. 2) 2005* (Cth); and the *Telecommunications (Interception) Amendment Act 2006* (Cth).⁷⁶

Perhaps what is most disturbing about the new legislation is its lack of clarity in explicitly stating what devices can and cannot be used. For instance, in the Australian Commonwealth Anti-Terrorism Act, a tracking device is defined as: ‘...any electronic device capable of being used to determine or monitor the location of a person or an object or the status of an object.’⁷⁷ An electronic device could range from a GPS wristwatch to an electronic ultra high frequency (UHF) bracelet to an invasive radio-frequency identification (RFID) implant. In the United States, the phrase “electronic instrument” is used instead.⁷⁸ While legislation is drafted with the knowledge that technology changes occur at a fast pace, there is an increasing requirement for clarity, especially as embedded ‘beneath the skin’ technologies rise to the fore. Chip implants clearly violate the individual’s private space, ie, they penetrate the body. For civil libertarians the question is who decides whether someone is a suspect to

⁷⁵ Bantekas, above 1, 18-19.

⁷⁶ Abraham, above 67, 32.

⁷⁷ Anti-Terrorism Act (No. 2) 2005 (Cth) s100.1(1)

⁷⁸ Robert Chalmers, ‘Orwell or All Well? The Rise of Surveillance Culture’ (2005) 30(6) *AILJ* 260. ‘At the COAG meeting, the Commonwealth and States agreed on enhanced tracking (perhaps even pre-crime electronic bracelets for people subject to control orders) and other extended law enforcement powers, subject to extended sunset provisions.’ See also, Europa, ‘Ethical aspects of ICT implants in the human body: opinion presented to the Commission by the European Group on Ethics’ (2005) <<http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/05/97&format=HTML&aged=0&language=EN&guiLanguage=de>> at 29 April 2007.

a crime? And if someone is innocent until proven guilty then how can a government justify the use of tracking devices upon one of its citizens? The argument is that technologies like GPS tracking technology are manifold more powerful than police visual surveillance and that high-tech devices allow police to monitor people ‘...for a much longer period of time, with much less chance of detection.’⁷⁹

7 Recommendations

There are many recommendations that can be made towards the use of human tracking technologies in inter-state police-to-police cooperation. However, first there must be an acknowledgment that there is a via media in ‘protecting citizens’ reasonable expectations of privacy and permitting law enforcement officials to do their job.’⁸⁰ The via media is the radical middle, the radical centre, centrism, and the third way philosophy.⁸¹ When one considers the extreme polar arguments they are inherently flawed. Compare for instance the staunch position of some civil libertarians who see all forms of surveillance in all circumstance as a degradation of human rights versus some secret police organizations who wish to by-pass all legal procedures. There is surely a middle position with a workable solution. Parts of the solution may include the constitution of uniform procedures to be set up and adopted for inter-state police cooperation, just as there currently are treaties for MLA requests, police self-regulation to be more explicit about the acceptable use of human

⁷⁹ Otterberg, above 52, 697-698. ‘The resultant lengthy, detailed record of one’s location then provides a comprehensive picture of one’s life. Location information reveals everything from daily habits like stopping at the same coffee shop on the way to work, to associations with other people, to visits to locales that reveal much more about a person’s particular characteristics, affiliations or beliefs—such as a gay bar, a certain church, synagogue, or mosque; a strip club; or various political and civic organizations.’

⁸⁰ Simon Bronitt and Henry Mares, ‘Privacy in the Investigative Process: Striking a Balance?’ (2002) 14(3) *LegalDate* 2. See also, Bantekas, above 1, 75. ‘In the preamble [of the Council of Europe Convention on Cybercrime] reference is made to the need to maintain a balance between the interests of law enforcement and respect for fundamental rights.’ See also, Colin J. Bennett and Rebecca Grant (eds), *Visions of Privacy: Police Choices for the Digital Age* (1999).

⁸¹ See also, Lanham, above 30, 55.

tracking technologies with embedded prohibitive clauses, and the mandate for warrants and court orders to be obtained prior to the implementation and monitoring of an individual.⁸² A more difficult goal to achieve is the alignment of state and federal laws of countries pertaining to human tracking technologies and their limitations in terms of admissible evidence in a trial.⁸³ This will come with time as more and more international cases are heard on the matter of location intelligence being used in a court of law to help in the conviction of a criminal.⁸⁴ These recommendations are not merely meant to solve band-aid 'jurisdictional problems' when police track individuals across state lines but are recommendations towards a common protocol.⁸⁵ Perhaps some of the more pressing questions that courts will face in the shorter term are: when is it appropriate to use particular types of electronic devices for surveillance, for how long, and to monitor what type of activity.⁸⁶ These questions become even more complicated when we consider them across borders.⁸⁷

⁸² Ganz, above 17, 1325-1326. 'While the use of GPS tracking devices grows among law enforcement, federal law remains largely undefined regarding the need to obtain warrants before their deployment. State law presents a similarly mixed picture...'

⁸³ Ibid. 'The federal-state split is a function of differing constitutional conceptions of personal privacy.'

⁸⁴ Bassiouni, above 1, 682. 'The need to harmonize the criminal international criminal justice system and national criminal justice systems' is a matter that is relevant to human tracking technology as well.

⁸⁵ Otterberg, above 52, 679.

⁸⁶ Chalmers, above 78, 260.

⁸⁷ Malcolm Anderson and Joanna Apap, *Police and Justice Co-operation and the New European Borders* (2002).