Surveillance & Society

Article

Child Location Tracking in the US and the UK: Same Technology, Different Social Implications

Anne-Marie Oostveen

Oxford Internet Institute, University of Oxford, UK.
anne-marie.oostveen@oii.ox.ac.uk

Asimina Vasalou

London Knowledge Lab, UK.
minav@luminainteractive.com

Peter van den Besselaar

Organization Sciences, VU University Amsterdam,
The Netherlands.
p.a.a.vanden.besselaar@vu.nl

Ian Brown

Oxford Internet Institute, University of Oxford, UK.
ian.brown@oii.ox.ac.uk

Abstract

Real-time location tracking of individuals has become relatively easy with the widespread availability of commercial wearable devices that use geographical positioning information to provide location-based services. One application of this technology is to allow parents to monitor the location of their children. This paper investigates child location tracking technology in the US and the UK and compares its privacy implications. Although overall the price levels and the technical capabilities are the same, we find that the features of the technology are different depending on the social context. This can be attributed to national regulations and law that shape how a technology can be used. These laws and regulations, influenced by cultural frameworks, values, and morality, differ considerably between the countries. Clarifying the expected impacts of technology on the lives of users and other stakeholders in terms of these contextual factors will help to inform public debate about technical possibilities and societal needs.

1. Introduction

Parents express a range of concerns about their children when they are left unsupervised. Abduction, murder or road accidents are reported as the greatest concerns (Living Streets 2010), although there has been a decline of 34 per cent in traffic accident rates since 1994 (Department of Transport 2007) and the likelihood of 'stranger danger' is exaggerated in the minds of parents (Newiss and Fairbrother 2004). In 2009, 56 per cent of *murder* victims aged under 16 were killed by their parents, while 4 per cent of the victims were known to have been killed by strangers (Smith et al. 2010). In terms of stereotypical 'stranger' *kidnappings*, where a non-family member takes a child, the numbers are also lower than is commonly thought. Nonetheless, despite its rarity, this type of kidnapping is often widely reported in the media, fueling parental concerns over the safety of children. According to Gill (2007): 'It can be stated with near certainty that there are no more predatory child killers at large today than there were in 1990 or 1975. These statistics categorically refute the dominant media message that dangerous, predatory strangers represent a significant or growing threat to children'.

Oostveen, A., A. Vasalou, P. van den Besselaar and I. Brown. 2014. Child Location Tracking in the US and the UK: Same Technology, Different Social Implications. *Surveillance & Society* 12(4): 581-593.
http://www.surveillance-and-society.org | ISSN: 1477-7487

Besides the fear of such external threats, parents also worry about the harm that children can bring upon themselves when they are out on their own. For example, young children might wander off to a busy road or a fast flowing river, while teenagers might get involved with deviant friends, drink alcohol or use drugs, and engage in dangerous driving. Cradock (2004) points out that childhood, by its very nature, is a condition that requires protection from all manner of potential dangers and the responsibility of this protection falls with the parents.

One of the strategies to protect children and teenagers from harm is constant supervision and surveillance, or restricting their freedom by keeping them indoors. A worry noted over this heightened child protection, however, is that children are not allowed to develop their own coping mechanisms, or to do things their own way (Marx and Steeves 2010). Pain et al. (2005) argue (with reference to Hillman, Adams and Whitelegg 1990; Valentine and McKendrick 1997) that: ‘while accidents and physical and emotional abuse are in fact most common within the home, these fears mean that young people are increasingly restricted and supervised outdoors, at some cost to their autonomy, social interaction and health’. The authors also explain that people worry about an increasing range of risks that in reality are unlikely to happen, leading to a culture of anxiety.

Not surprisingly this universal anxiety or ‘paranoid parenting’ as sociologist Furedi (2001) calls it, creates an opportunity for businesses to sell products that assist parents in their efforts to monitor their children as closely as possible. Since 2001, real-time location surveillance has become relatively easy and affordable with the introduction of commercial wearable applications that use geographical positioning information to provide location-based services (Rooney 2010). Despite their commercial presence, however, our recent study shows that uptake has been stagnant (Vasalou, Oostveen and Joinson 2012). Among a representative sample of 920 parents this study investigated the *actual use* of tracking devices within the family and found that in fact only 1.7 per cent of parents use such technologies. Similarly, Thumala et al. (2013) observe that GPS trackers for children have not taken off as a mass consumer product. Despite this, as location tracking software is being increasingly developed to operate on mobile phones, in the future, technology push might tempt undecided parents, or those currently inhibited by current high costs or perceived complexity, to re-evaluate their decisions. Taking a reflexive approach to understand how the design of child tracking technologies can lead to harmful social outcomes is therefore timely.

The objective of this paper is to show how national legislation can lead to a similar generic technology being deployed differently across countries, in turn encouraging different social consequences. To achieve this, we take a bottom-up approach: we record the features of one-directional GPS (global positioning system) location tracking devices for monitoring children sold in the US and the UK and identify their common as well as distinct functionalities. We then explore the negative influence of child location tracking functionality on the trust relationship between parents and children, and reveal that instead of providing increased safety to children, this technology poses serious security implications. A key contribution of our paper is to show that the functionality of child tracking applications is dependent on the social and political contexts in which the devices are developed: compared to the UK, US legislation gives providers freedom to develop more privacy-intrusive features, thereby not only infringing on the privacy of children, but also impacting on the privacy of third parties.

2. Background and Motivation

In the past, surveillance was characterized by a top-down process as it was primarily performed by the authorities (Koskela 2009). Contemporary surveillance, however, has expanded beyond policing and espionage to surpass this original narrow meaning (Lyon 1994). In our current ‘surveillance state’ personal information is collected, stored and processed not only by governments but also by employers, and commercial companies. Furthermore, in recent years there has been a fundamental change in which surveillance has also become a primary feature of consumer products that come in the form of accessible, user-friendly, and cheap surveillance devices (Loader et al. 2014). High street retailers and spy technology shops sell a wide range of technical surveillance devices over the counter, which, according to Zedner (2009), has meant that surveillance is now an embedded, commonplace facet of everyday life in ways that were unimaginable 50 years ago. Surveillance technologies have thus been democratized and can be easily bought by ordinary consumers (Goold et al. 2010). Individuals now consume a number of security devices such as alarms, access control systems, WiFi video baby monitors, indoor video security systems, outdoor home surveillance cameras, and tracking equipment all of which are meant to protect themselves, their family, their homes, and their possessions.

The increased and diversified use of surveillance technologies by private individuals has consequences for social relations, morals, and actions, making it difficult to determine what the appropriate use of such technologies might be. In most countries law enforcement and other public sector organizations that wish to conduct any form of surveillance must have this authorized. Yet, there is no clear legislation in force relating to the authorization and overseeing of the surveillance activities of individuals who wish to conduct technical surveillance for their own ends. Thus, as Koskela (2009) rightly argues, ethical questions should be revisited in the context of new technologies and moralities, to weigh the unintended consequences of using security devices against their potential benefits, and to be able to determine 'whom' they actually benefit.

During the development of new technologies, public debates emerge about the possible societal consequences of these technologies. These debates may have important consequences for the acceptance or rejection of such innovations. Unfortunately, questions about the consequences of new technologies are often posed in a very black and white manner. For instance: Will GPS location tracking of individuals have negative privacy implications? People expect a straightforward 'yes-or-no' answer. However, there is no simple answer when judging a solution to a 'wicked problem' such as this one.[1]

Many different perspectives and theories are used to examine the effects of new technologies. Technological determinists argue that technological development is unstoppable and that no-one can be blamed for the way it progresses. As MacKenzie and Wajcman (1999) point out, this view focuses our minds on how to adapt to technological change and not on how to shape it. It neglects public discussion, choice and politics. Privacy implications that might occur because of the implementation of new technologies need to be analytically and empirically researched, as this may help a balanced societal debate, and a socially responsible use.

In line with this, social constructivists show that there are two levels on which the relationship between technology and society can be discussed: the *development* of technology and the *effects* of technology. The *development* of technology is a social process and does not take place in isolation from society. According to this view it is impossible to separate values, biases, and politics from technology. The social position and perspective of its creators are written into a technology. These parameters affect how questions and problems are defined and shape how technologies are designed to provide solutions. The *effects* of technology are socially conditioned. The effects depend on how people use the technology (or are allowed to use the technology). Technology is shaped by different influences as part of its development and then reshaped in use (Bijker and Law 1994).

It is difficult to predict the effects of a certain technology for several reasons. Firstly, there is often a disparity between the intentions of those designing and implementing technologies and their actual use. Secondly, the same technology can have many different effects, depending on the opinions, interests, and values of the users. Finally, national laws and regulations often determine how a technology can be used.

[1] A 'wicked problem' describes a problem that is difficult or impossible to solve because of incomplete, contradictory, and changing requirements that are often difficult to recognize.

Therefore, in studying new innovations, one needs to be deeply concerned with the context in which each new technology appears (Kling 2000). This is important in the case of location tracking devices because they are used in very varied situations for different surveillance purposes. There will be a difference in issues and concerns depending on whether such technology is used for monitoring goods, vehicles, pets or people. And even when we focus on location tracking just for people there are many different applications. Location monitoring devices are known to be used for tracking different user groups, such as elderly people with dementia (Landau et al. 2010; Miskelly 2005; Shoval et al. 2008), sex offenders (Nellis 2009; Janicki 2006; Renzema and Mayo-Wilson 2005), and lone workers where the employers have a legal 'duty of care' to monitor and protect staff working alone (Thumala et al. 2013; Barreras and Mathur 2007). In these cases the ethical issues will differ greatly compared to when one monitors children and teenagers going about their daily business.

Perusco, Michael and Michael (2006) point out that research into the development of location-based technologies has been far more advanced than the research on their potential societal implications. The present paper addresses this gap by focusing on *national laws* as one source of influence on development and effects, to investigate how child location tracking has been shaped and implemented in the US and the UK after its introduction a decade ago.

3. Methodology

A qualitative content analysis of both US and UK commercial location tracker websites was conducted in order to assess the features of the devices and whether there are significant differences between them. The sample consisted of 40 websites marketing tracking devices for children: 21 sites from the US and 19 websites from the UK. The criterion for inclusion in this study required that the website offer any kind of GPS location-based system to track, monitor and control children's and teenagers' activity.

Prior to collecting the data, the unit of analysis was defined as the homepage plus all pages linked directly to this homepage (the second level of the site), all pages linked to those second level pages (the third level of the site), and pages linked to third level pages if these were present. Any hyperlinks that took the researchers outside the original website were not included in the study. The content of the 40 websites was harvested in a period of 10 days in June 2012, resulting in a total of 326 pages of text (127,909 words).

The websites in our study were analyzed for: (i) relevant characteristics of the suppliers, such as their nationality and their specific tracking business (child, personal, etc); (ii) different features of the devices as advertised and explained by the providers; and (iii) the framing of the devices in terms of privacy, independence, consent, trust, and so on, as this relates to the social implications studied in this paper. Throughout the paper, quotes taken from the commercial websites appear in *italics*.

The privacy issues related to location tracking are based on a survey of relevant literature. Finally, documents and legal experts were consulted to outline the effects of regulation that restricts the allowed functions and use of child location tracking devices.

4. Results and Discussion

The personal location-tracking market is increasingly targeting those responsible for the care of children and teenagers. We found 40 providers in the US and the UK, of which eight were solely dedicated to *child tracking devices*, while ten offered solutions for other *personal tracking* as well (e.g. people with dementia, adulterous partners, lone workers), whereas 22 sites promoted child trackers as one product of their *wider tracking* business (e.g. personal trackers, asset trackers, vehicle trackers). These categories are evenly distributed over the two countries (see Table 1).

The websites we reviewed communicate a shared problem definition: the requirement for safety framed against a high likelihood of risks materializing. To give one representative quote, '*Safety is the first and foremost reason as to why Child GPS tracking systems are becoming a necessity. With increasing crime rates, a simple walk to school or the park can have disastrous consequences'*. As we will show in our review of technological features, safety is implemented through control. As one website states, *'With this personal tracker it will be possible for you to better control your children by knowing where they are all the time'*.

There are many different personal tracking devices on the market, which range from (pay-as-you-go) services that track the SIM card in a child's mobile phone, to electronic wristbands, bracelets or watches, and specially tagged items of clothing that use GPS technology.

The recent miniaturization of GPS technology has made it possible to develop small and light wearable tracking devices, which are far more accurate than GSM (global system for mobile communications)-based systems. A GPS receiver collects data from at least four satellites to determine its position and the technology can accurately locate someone within a few metres. '*GPS tracking systems provide the perfect combination of child monitoring and technology. What makes a GPS tracking system designed for child monitoring applications great is that the GPS tracker will allow a parent to observe everywhere their child is without having the parent ever having to set their eyes upon the child'*. As Nellis puts it: 'Mobile communication and geolocation technologies enable connectivity across space in ways that produce a sense of human proximity without the element of physical presence that would once have been required' (2009: 107). Not only can personal GPS trackers give real-time information on where a child is 24 hours a day (online or via a mobile phone or PDA), but it is often also possible to see the movement history of a tracking device for up to twelve months. This history capability forms a breadcrumb trail on a map. If a child happens to go out of reach of a signal, you can see where the signal was dropped, when, and in which direction they were headed.

Most tracking devices can give an alert when the wearer goes outside a pre-set boundary or 'safe-zone'. This geo-fencing allows a parent to be notified if the child enters or leaves a pre-set security perimeter. While most devices have only the option of circular shaped geo-fences, some tracking solutions offer polygonal shaped exclusionary zones. This permits parents to create safe-zones with a much greater degree of specificity. Furthermore, if the child carrying the device needs to contact the parent or an emergency service, they can do so by pressing a panic button to call a pre-set number and receive emergency support. Other features mentioned on the websites are real-time monitoring of speed (to know whether a teenager is exceeding the speeding limit when driving), monitoring of temperature (in case a child is left alone in a hot car), and a drowning alert reacting to water: '*The slightest drop of water on the transmitter worn by the child will send a drowning alert to the receiver'*. Some trackers can monitor children's movement or conversations, without making them aware that this is going on. Finally, tracking devices may be connected to sex-offender databases, enabling parents to see when a child comes in the vicinity of a 'dangerous person's' residence. The latter two functionalities will be discussed in more detail in sections 4.2 and 4.3. Table 1 gives an overview of the different features as *mentioned* on the websites.

	UK			US			
	Child tracking (N=4)	Personal tracking (N=4)	Wider tracking (N=11)	Child tracking (N=4)	Personal tracking (N=6)	Wider tracking (N=11)	TOTAL (N=40)
Real-time tracking	4	4	11	4	6	11	40
Movement history	3	1	10	2	3	8	27
Panic button	2	3	8	3	2	4	22
Geofencing	1	3	9	4	5	10	32
Drowning alert	-	1	-	-	-	1	2
Speed alert	-	1	5	1	3	11	21
Temperature alert	-	-	-	1	1	-	2
Voice monitoring	-	-	-	1	1	2	4
Covert tracking	-	-	-	-	1	4	5
Predator alert	-	-	-	1	1	-	2

Table 1: *Surveillance features by provider type and country*

Having given an overview of the features these devices offer and the problem they aim to address, we now turn to three social issues at stake, namely privacy, trust, and security concerns.

4.1 Social Implications of Child Tracking Devices

Privacy

Compared with previous generations, children today face fewer risks overall. Childhood experts argue that children will never understand risk if society prevents them from experiencing it. These concerns are rooted in evidence that limited exposure to risks hinders the development of resilience, necessary for the future dealing with life's risks and dangers (Malone 2007; Abbas et al. 2011). According to these scholars, individuals and institutions should reject the philosophy of protection and instead adopt a philosophy of resilience (Gill 2007); allowing children freedom of movement is regarded as a prerequisite condition. This view is also expressed by privacy advocates who argue that everyone, including children, has the right to a private life, guaranteed by Article 12 of the Universal Declaration of Human Rights and underscored by Article 8 of the UN Convention on the Rights of the Child (Dowty 2008). Location tracking technology displays and records children's moment-to-moment movements: '*Never worry about your children disappearing the moment you look away, as you can always know exactly where your child is thanks to the child locator'*. This indicates that tracking technology is not neutral, but is designed to enhance parental control (Perusco and Michael 2007): parents can scrutinize and control where their children go by setting boundaries, and thus manage how risk is experienced (Mayer 2003). Hence, this new capability threatens to exacerbate an existing problem.

The UK government published a green paper called 'Every Child Matters' (2003) adhering to the notion that 'child protection is more important than privacy'. According to Dowty, this idea that protection and privacy are mutually exclusive shows a 'misunderstanding of the fundamental nature of privacy as a human right and its importance in child protection' (2008: 397). Dowty argues that the function of privacy is not just the concealment of wrongdoing, but is about autonomy and the control people have over personal boundaries and the means by which people define who they are in relation to others. As Perusco and Michael point out, 'autonomy is an important part of a person's identity' (2007: 9).

Despite evidence that overprotection by parents hinders the development of children we found that a number of providers attempted to obscure these consequences in suggesting that *more* monitoring will foster *more* independence. As one provider argued, *'Children wearing a KoolTrax Lite gain the confidence that help will be available if they need it, and with the reduced requirement to be constantly watched comes (paradoxically perhaps) more privacy, more freedom to play, learn, and live'.* Another described its location tracking system as a '*form of supervised independence'*.

Trust

Alongside their privacy implications, location-tracking devices threaten to undermine children's trustworthiness. Both Goold (2009) and Perusco (2007) note that the very existence of surveillance and monitoring implies some basic absence or withdrawal of trust. In other words, 'trust in technology is intrinsically related to the lack of trust in people' (Aas, Gundhus and Lornell 2009). Rooney (2010) asks whether the increased use of surveillance technologies on children is a response to the fact that we do not trust our children or that we do not trust others who are around them. She questions whether the use of these technologies as a form of control is an appropriate response to addressing a lack of trust or minimizing risk. Research has shown that trust leads to trustworthiness: 'This happens because, when others trust us, we become trustworthy beings. Further, it is through the act of trusting others that we learn to trust and we come to know the value of trust' (Rooney 2010: 347).

Children will develop into trustworthy adults only if their actions are hypothesized *a priori* to be trustworthy. Crucially, monitoring removes uncertainty and as such violates this precondition (Mayer 2003). Seemingly oblivious to this, websites emphasize the benefits of no uncertainty: *'For peace of mind you can keep a safe eye on them at all times giving you an additional level of security and reassurance that they are where they say they are'*. Others understate the role of trust, offering location tracking as a way of enforcing compliance: '*If you are the parent of a teen driver, a GPS car locator can be an invaluable source of peace-of-mind. Where are they? How fast are they going? With a GPS car locator you will never have to wonder again. Did you know that teen drivers are nearly 100x less likely to break the rules when they know that their actions are being tracked?'* Then there are websites that claim that GPS tracking will build and expand the trust between parents and children:

> *We say, 'Trust-But-Verify', a GPS vehicle monitoring system will act as a powerful deterrent for any negative behaviour. Furthermore, we believe that explaining to your teenager that a GPS vehicle system in their vehicle is implemented out of love and not mistrust. You want your teenager to live to their 21st Birthday...You also want the trust that exists between yourself and your teen to expand, having a GPS vehicle monitoring system believe it or not, will empower you and your teen to build a stronger foundation of trust.*

Even though using surveillance technologies for protection may be well-intentioned, it deprives children and teenagers of the possibility to extend their competence, confidence and skills and turns them into subjects of control (Marx and Steeves 2010; Rooney 2010).

Security

A final, pragmatic implication of location tracking is the inherent security risk they pose. Zedner argues that 'the temptation to seek technological solutions is rarely accompanied by sufficient anticipation of the fact that technologies may develop unpredictably or be subverted in ways that render them greater sources of insecurity than security' (Zedner 2009: 263). GPS systems can fail, they can contain vulnerabilities, and are not always error free, potentially creating a number of new dangers (Abbas et al. 2011; Perusco and Michael 2007). As Karim (2004: 495) points out, 'Personal locators have the ability to generate virtually limitless amounts of data about an individual'. Providers maintain that their devices are as secure as using shopping websites featuring a SSL structure that keeps all data encrypted so no one else can see it. They further argue that the only person able to see the tracking of the device is the registered user, giving the system a high level of security. One website reassuringly states that: '*the tracking system's platform incorporates encryption and a whole host of other advanced security features that are typically found at leading financial institutions*'. It is not clarified, however, what those advanced security features are or how they would stop insider threats. Neither is it clear who actually owns the location data: the individual subscriber, the service provider, or a third party that stores the information. And who is responsible for the authenticity, fidelity and accuracy of the information collected (Michael, McNamee and Michael 2006)? As a consequence, security experts observe that instead of offering protection, location tracking devices are capable of increasing the threats to children's safety and privacy as they are open to interception or errors. Dowty emphasizes: 'It is ironic that uncritical faith has been placed in technology that is marketed as fulfilling some kind of child protection function, when in reality it is capable of increasing the threats to children's safety and privacy' (2008: 398).

Our analysis of social consequences so far has been independent of the country where the tracking technology is being used. The next section presents a set of features (covert tracking, voice monitoring, and a predator alert) that only exist in the US (Table 1). We contrast the US to the UK to explain how national legislation has had a crucial impact on the design of these tracking devices. Our main thesis is that in the case of the less-regulated US market, the social implications we have covered thus far are magnified. Furthermore, we show that design features targeted at easing parents' anxiety also threaten the privacy and security of indirect stakeholders.

4.2 Covert or Overt Tracking

One of the big differences with regards to child tracking in the UK and the US is the data protection legislation that location-based services have to adhere to. From the content analysis of provider websites we learn that these statutes mean that location tracking of children can be done *covertly* in many US states. As one site boasts: '*No one has to know that this navigation system is covertly tracking their every move'.* By contrast, this surreptitious monitoring is not allowed in the UK. In the words of a UK provider: *'Despite what may have been said in the press or on blogs it is not possible to carry out mobile tracking secretly. Mobile tracking is regulated throughout the UK and all providers must ensure that an activation consent must come from each mobile before it can be tracked by a home user.'*

The European Union has a comprehensive set of privacy rules in its Data Protection Directive (1995), E-Privacy Directive (2009) and Data Retention Directive (2006), which explicitly requires telecommunications networks to obtain consent from individuals for location tracking (Cuijpers, Roosendaal and Koops 2007). In 2006, the mobile phone industry in the UK introduced a Code of Practice for the use of mobile phone technology to provide passive location services (Industry Code of Practice 2006). The code includes the key principles that tracking should be consent-based and not undermine customer privacy or be used for unauthorized surveillance. Consent also needs to be given by children. As the Code of Practice points out: 'Industry and the public alike do not want location services to be used to locate customers, particularly children, either without their knowledge or against their will'. The Code explains that if a child does not consent, his or her wishes must not be overridden and the service must not be activated. Furthermore, there are several safeguards that apply once registration has been completed. For instance, a child can request from the location service provider a list of all names and telephone numbers of persons authorized to track their mobile phone via the service. The child will also receive SMS alerts at random intervals as a reminder that their telephone is being tracked. This is echoed on several UK provider websites that go on to say: '*To comply with Home Office Rules we send regular text message reminders to each mobile phone to let the person carrying the mobile phone know that it can be tracked.'* Finally, children can withdraw their consent to the mobile phone tracking at any time.

An important limitation of this Code of Practice is that it only covers location-based services operated through the mobile phone *networks* and not services which obtain location information in other ways such as by using GPS technology through mobile phone handsets, wristbands or watches. The question therefore remains whether consent by children only applies to mobile phone networks or also to other tracking devices that rely on GPS? The European Data Protection Directive (1995) specifies that the data *subject* has to give his or her free and informed consent to process personal data which are capable by their nature of infringing fundamental freedoms or privacy. The 'Working Party on the Protection of Individuals with regard to the Processing of Personal Data' (2005) takes the view that when a service is offered to private individuals, consent must be obtained from the person to whom the data refer, i.e. the user of the equipment. This implies that in the case of parents using a location based service (phone or other GPS enabled device) in order to track and trace a child, consent needs to be given by both the subscriber (parent) as well as the user (child). Any commercial tracking in the UK will therefore have to be done overtly.

The US providers, on the other hand, turn the fact that their devices can be used covertly into a selling point, with one provider claiming that: '*Tracking your teenager using a GPS people tracker can effectively and covertly find out where your teenager is going, and where they have been.'* Because none of the American websites say anything about regulation with regards to consent, we approached American providers by email questioning them about this issue. The replies we received conveyed that vendors are unable to give legal advice and explained that in the US the law varies by state. Vendors therefore advise their customers to first check with a lawyer whether consent is needed before using their product to track someone. Legislation that would regulate the transmission and sharing of user location data—with exceptions for parents monitoring children—is under consideration by the US Senate (Franken and Blumenthal 2011). The Bill specifies that 'a covered entity may not knowingly collect, receive, record, obtain, or disclose to a non-governmental individual or entity the geo-location information from an electronic communications device without the express authorization of the individual that is using the electronic communications device'. However, there are several exceptions to this rule, one of which is the collection, recording and disclosure of geo-location information to a parent or legal guardian to locate a minor child.

In legitimizing covert tracking in the US, providers have begun to feature extreme covert operations more broadly as is illustrated by the possibility to eavesdrop on your children from afar:

> *Voice monitoring provides an additional tool for the safety of your child. If at any time you would like to know what's going on around your child, you can simply access this feature. Even during use the child never knows that you are listening in. This is very easy to do. You simply call the device's phone number. The device doesn't ring or beep. The device automatically picks up after 2 rings. Unless you begin to speak, the child will not know that a call has been placed and picked up. If you don't want to be heard, simply put your phone on mute.*

Looking at how the legal system regulates surveillance more broadly, it is known that governments, law enforcement and intelligence services have been using mobile phone tapping to perform surveillance in the UK and the US. For these purposes, courts will only authorize telephone monitoring when severe criminal activity cannot be detected in a less intrusive way. Illegal or unauthorized telephone tapping is considered to be a criminal offense. It is unclear how far this legislation impacts on the new development of voice monitoring as an additional surveillance tool in the domestic realm (such as in the parent-child context). The Electronic Frontier Foundation explains that: 'According to the Wiretap Act, it's a crime for anyone that is not a party to a communication—anyone that isn't one of the people talking, listening, writing, reading, or otherwise participating in the communication—to intercept the communication, unless at least one of the parties to the communication has previously consented to (agreed to) the interception.'[2] This seems rather straightforward, but the caveat is that the Federal Wiretap Act only requires one-party consent, which means that even if a child did not 'consent', it would be enough if the parents did in states that do not impose additional restrictions (Rahavy 2003). In some states minors are not allowed to give legal consent. While some courts have ruled that secret interception by a parent of a child's conversations is unlawful (Carr and Bellia 2003): 'the fact that the eavesdropping party is related by blood to one of the speaking parties […] does not immunize that person's activities from being described as eavesdropping' (People v. Durham 1992), other courts have been reluctant to extend the reach of the Wiretap Act to the parent-child context (Rahavy 2003). It is important to note that besides listening in on their own children, parents also breach the privacy of those who are interacting with their children such as friends, teachers and others.

4.3 Predator Alert

We have established that besides the direct users, i.e. the children, there are other stakeholders who can be negatively impacted through the introduction of specific features within tracking technologies. Analyzing the 40 provider websites we found another particularly striking example of this: the predator alert. This alert is a feature offered by several American providers, with one stating: *'Want to be notified when your child gets near the residence of a known sex offender? The Amber Alert GPS 3G ties into and collaborates with the national sex offender database. Simply put the device on your child and when your child comes within 500 feet of a registered sex offender's residence, you'll get an alert.'*

Sex offender registers exist in both the US and the UK as a means of post-release supervision with the purpose of creating a safer society. In both societies it is believed that there is no 'cure' for sex offenders, and that therefore the only way to control and contain their behavior is to monitor them when they are released back into the community. After release, certain categories of sex offender are ordered to notify the police in person of their name and address and any subsequent changes to their details. Their photographs, fingerprints, and national insurance numbers (UK) will be taken for future identification purposes. In many US states, information on the whereabouts of registered sex offenders is made available to the public (via local police stations, libraries or websites) by means of a pro-active community notification under versions of 'Megan's Law' (Nellis 2012). In the UK, the sex offender database is not open to the public and can only be accessed by the Police, the National Probation Service, and HM Prison Service personnel. However, a first limited disclosure of this kind of information was trialed in four UK counties in 2008 (BBC News 2008) and has been rolled-out further in 2011 (BBC News 2010). Thus, although the 'predator alert' feature is not yet possible in the UK, it might become an additional feature in the future.

The 'predator alert' illustrates the differences in legal frameworks, socio-political ideologies and penal cultures. Anglo-American societies favor a risk-averse approach to crime control that emphasizes public protection and victim prevention (Nellis 2012; McAlinden 2012). Many Western European countries on the other hand do not have sex offender registers. McAlinden (2012) discusses for example Scandinavian countries where the focus is on treatment: 'Such societies are characterized by a communitarian ethos and "penal welfarism" in which offenders are regarded as social beings that should be included in society and who need rehabilitation and re-socialization via correctional treatment rather than stigmatization and punishment'. Penal policies are 'shaped by a complex interplay of social, political and cultural factors' (ibid.). How societies deal with sex offending is related to historical and cultural contexts but is subject to change over time. It is possible that the UK will head in the direction of publicly available sex offender registers with proactive community notifications in the future.

[2] https://ssd.eff.org/book/export/html/14

The 'predator alert' feature has a profound impact on the privacy of sex offenders and members of their immediate family. Their lives can be negatively affected by public exposure. The constant scrutiny degrades and stigmatizes them and can even place them at risk of vigilantism (Nellis 2012). Furthermore, information about them stored in databases may be false or outdated and can erroneously impact on people with no criminal background who are nonetheless mistaken for offenders.

5. Conclusions

Although overall the price levels and the technical capabilities of location-tracking devices are the same in both the US and the UK, we do see that the technology impacts on the lives of the direct users and third parties in different ways. This can be attributed to the use context, especially law and regulations, which influences how a technology can be used. These laws and regulations, shaped by the existing cultural and political frameworks, differ considerably between the two countries. The tracking devices mirror the beliefs, values and morality of a society. As Green (2001) puts it:

> To argue that any technology is neutral is to ignore the social and cultural circumstances in which that technology was developed and the policy and regulatory regimes under which that technology is deployed. Neither technology nor culture is neutral—both reflect people and society, the power of different social groups and the outcomes of competing priorities.

Or as Wajcman (1991) points out: 'Technologies bear the imprint of the people and social context in which they are developed'.

In this case, the emergence of a risk-averse society and a surveillance society are two important social trends that can explain to some degree the development of—and interest in—location tracking technology worldwide. However, the effects of this technology do not have an autonomous logic and are partly determined by the national and local social context into which it is introduced. After all, technologies do not become stabilized artifacts after their initial 'global' design; different features can be modified or added. It is important that people realize that the introduction of new technologies is not just a process that happens to societies, but that it can become an active, deliberative process with public debate and a democratic choice influencing how a society chooses to use and shape technology. As shown, some features of location-tracking devices differ substantially between the US and the UK, with the US allowing more privacy intrusive monitoring of children which reflects a stronger aversion to private-sector regulation and state interference in parent-child relations. In the UK consent by children is the norm; US federal law on the other hand allows parents to track children secretly. This covert monitoring even extends to surreptitious eavesdropping.

Furthermore, US tracking devices offer the possibility of a predator alert that links the tracking technology to the national sex offenders register. This reflects the cultural belief that sex offenders are intractably risky or evil and that the public has 'a right to know', leading to an 'ethic of public protection and victim prevention', instead of an 'ethic of care' more common in many European countries (Nellis 2012). Since location tracking technologies are still relatively new, this is the time to ask normative questions about the possible societal implications. What will be the effects on privacy? And how will different cultures allow the technology to evolve over time? Ultimately, this will support the responsible development of wearable computing products that combine useful functionality with preservation of crucial values—such as privacy and trust.

Acknowledgement

This research work has been supported by the Network of Excellence in Internet Science (EINS) through EC's **7th Framework Programme** under Communications Networks, Content and Technologies, Grant Agreement n°288021.

References

Aas, K.F., H.O. Gundhus and H.M. Lomell, H.M. 2009. Introduction: Technologies of InSecurity. In: *Technologies of InSecurity. The Surveillance of Everyday Life*, eds K.F. Aas, H.O. Gundhus and H.M. Lomell, 1-17. London: Routledge.

Abbas, R., K. Michael, M. Michael and A. Aloudat. 2011. Emerging forms of covert surveillance using GPS-enabled devices. *Journal of Cases on Information Technology* 13(2): 19 – 33.

Barreras, A. and A. Mathur. 2007. Wireless Location Tracking. In: *Convenient or Invasive – The Information Age*, eds K. Larson and Z. Voronovich. Colorado: Ethica Publishing.

BBC News 2008. Sex offender alerts plan launched. 15 September 2008. http://news.bbc.co.uk/2/hi/uk_news/7612315.stm

BBC News 2010. Sex offender disclosure scheme to go nationwide. 3 March 2010. http://news.bbc.co.uk/2/hi/uk_news/8546126.stm

Bijker, W. and J. Law. 1994. General introduction. In: *Shaping Technology/building society: studies in sociotechnical change*, eds W. Bijker and J. Law. Cambridge: MIT Press.

Carr, J. and P. Bellia. 2003. *The Law of Electronic Surveillance*. Thomson Reuters.

Cradock, G. 2004. Risk Morality and Child Protection: Risk Calculation as Guides to Practice. *Science, Technology & Human Values* 29(3): 314-331.

Cuijpers, C., A. Roosendaal and B. Koops. 2007. Del 11.5: The legal framework for location-based services in Europe. *FIDIS Deliverables* 11(5).

Department for Transport 2007. *Child Road Safety Strategy 2007*.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

Directive 2009/136/EC of the European Parliament and of the Council of 25 November amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Dowty, T. 2008. Pixie-dust and Privacy: What's Happening to Children's Rights in England? *Children & Society* 22: 393-399.

Furedi, F. 2001. *Paranoid Parenting*. London: Allen Lane.

Franken, A. and R. Blumenthal. 2011. Location Privacy Protection Act of 2011. Bill S. 1223 To address voluntary location tracking of electronic communications devices, and for other purposes in the Senate of the United States.

Gill, T. 2007. *No Fear. Growing up in a risk averse society*. London: Calouste Gulbenkian Foundation.

Goold, B., I. Loader and A. Thumala. 2010. Consuming security? Tools for a sociology of security consumption. *Theoretical Criminology* 14(1): 3-30.

Goold, B. 2009. Technologies of surveillance and the erosion of institutional trust. In: *Technologies of InSecurity. The Surveillance of Everyday Life*, eds K.F. Aas, H.O. Gundhus and H.M. Lomell, 207-218. London: Routledge.

Green, L. 2001. *Communication, Technology and Society*. London: Sage Publications.

Hillman, M., J. Adams and J. Whitelegg. 1990. *One false move: a study of children's independent mobility*. London: Policy Studies Institute.

Industry Code of Practice 2006. Code of Practice for the use of passive location services in the UK. Version 1.1

Janicki, M.A. 2006. Better seen than herded: Residency restrictions and global positioning system tracking laws for sex offenders. *Boston University Public Interest Law Journal* 16: 285.

Karim, W. 2004. The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntary Availing Yourself to GPS Monitoring. *Journal of Law and Policy* 14: 485-515.

Kling, R. 2000. Learning about Information Technologies and Social Change: the contribution of Social Informatics. *The Information Society* 16: 216-232.

Koskela, H. 2009. Hijacking surveillance? The new moral landscape of amateur photographing. In: *Technologies of InSecurity. The Surveillance of Everyday Life*, eds K.F. Aas, H.O. Gundhus and H.M. Lomell, 147-167. London: Routledge.

Landau, R., G.K. Auslander, S. Werner, N. Shoval and J. Heinik. 2010. Families' and professional caregivers' views of using advanced technology to track people with dementia. *Qualitative Health Research* 20(3): 409-419.

Living Streets & Parentline Plus 2010. Is it safe to let our children walk to school? Report as part of national Walk to School Week.

Loader, I., B. Goold and A. Thumala. 2014. The moral economy of security. *Theoretical Criminology*. DOI: 1362480614531613.

Lyon, D. 1994. The electronic eye: The rise of surveillance society. Minneapolis: University of Minnesota Press.

MacKenzie, D. and J. Wajcman. 1999. *The Social Shaping of Technology*, 2nd edition. Buckingham: Open University Press.

Malone, C. 2007. The bubble-wrap generation: children growing up in walled gardens. *Environmental Education Research* 13(4): 513-527.

Mayer, R. N. 2003. Technology, Families, and Privacy: Can We Know Too Much About our Loved Ones? *Journal of Consumer Policy* 26: 419-439.

Marx, G.T. and V. Steeves. 2010. From the Beginning: Children as Subjects and Agents of Surveillance. *Surveillance & Society* 7(3/4): 192-230.

McAlinden, A. 2012. The governance of sexual offending across Europe: Penal policies, political economies and the institutionalization of risk. *Punishment & Society* 14(2): 166-192.

Michael, K., A. McNamee and M.G. Michael. 2006. The Emerging Ethics of Humancentric GPS Tracking and Monitoring. Proc. Int. Conf. on Mobile Business (ICMB'06): 1-10. IEEE.

Miskelly, F. 2005. Electronic tracking of patients with dementia and wandering using mobile phone technology. *Age and ageing* 34(5): 497-499.

Nellis, M. 2012. "Cold Intimacies": Community Notification, Satellite Tracking and the Ruined Privacy of Sex Offenders. In: *Managing Privacy through Accountability*, eds D. Guagnin, L. Hempel, C. Ilten, I. Kroener, D. Neyland and H. Postigo. London: Palgrave Macmillan.

Nellis, M. 2009. 24/7/365: mobility, locatability and the satellite tracking of offenders. In: *Technologies of InSecurity. The Surveillance of Everyday Life*, eds K.F. Aas, H.O. Gundhus and H.M. Lomell, 105-124. London: Routledge.

Newiss, G. and L. Fairbrother. 2004. Child abduction: understanding police recorded crime statistics. *Home Office Findings* 225.

Pain, R., S. Grundy and S. Gill. 2005. "So Long as I Take my Mobile": Mobile Phones, Urban Life and Geographies of Young People's Safety. *International Journal of Urban and Regional Research* 29(4): 814-830.

People v. Durham, 157 Misc. 2d 289, 596 N.Y.S 2d 289, 290 (County Ct, 1992).

Perusco, L. and K. Michael. 2007. Control, Trust, Privacy, and Security: Evaluating Location-Based Services. *IEEE Technology and Society Magazine* Spring 2007: 4-16.

Perusco, L., K. Michael and M.G. Michael. 2006. Location-Based Services and the Privacy-Security Dichotomy. Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking, London: 91-98.

Rahavy, S.K. 2003. The Federal Wiretap Act: The Permissible Scope of Eavesdropping in the Family Home. *Journal of High Technology Law* 11(1): 87-100.

Renzema, M and E. Mayo-Wilson. 2005. Can electronic monitoring reduce crime for moderate to high-risk offenders? *Journal of Experimental Criminology* 1(2): 215-237.

Rooney, T. 2010. Trusting Children: How do surveillance technologies alter a child's experience of trust, risk and responsibility? *Surveillance & Society* 7(3/4): 344-355.

Shoval, N., G.K. Auslander, T. Freytag, R. Landau, F. Oswald, U. Seidl and J. Heinik. 2008. The use of advanced tracking technologies for the analysis of mobility in Alzheimer's disease and related cognitive diseases. *BMC geriatrics* 8(1): 7.

Smith, K., J. Flatley, K. Coleman, S. Osborne, P. Kaiza and S. Roe. 2010. Homicides, Firearm Offences and Intimate Violence 2008/09. Supplementary Vol. 2 to Crime in England and Wales 2008/09. *Home Office Statistical Bulletin*, 21 January 2010.

Thumala, A., B. Goold and I. Loader. 2013. Tracking devices: On the reception of a novel security good. *Criminology and Criminal Justice*. DOI: 1748895813507067.

Valentine, G. and J. McKendrick. 1997. Children's outdoor play: exploring parental concerns about children's safety and the changing nature of childhood. *Geoforum* 28(2): 219-235.

Vasalou, M., A. Oostveen and A. Joinson. 2012. A case study of non-adoption: the values of location tracking in the family. *Computer Supported Cooperative Work (CSCW) 2012 Conference*, Seattle, USA.

Wajcman, J. 1991. *Feminism confronts technology*. Cambridge: Polity Press.

Working Party 29 2005. Note 31: 7.

Zedner, L. 2009. Epilogue: the inescapable insecurity of security technologies? In: *Technologies of InSecurity. The Surveillance of Everyday Life*, eds K.F. Aas, H.O. Gundhus and H.M. Lomell, 257-270. London: Routledge.