Strasbourg, 20 September 2013 T-PD(2013)08

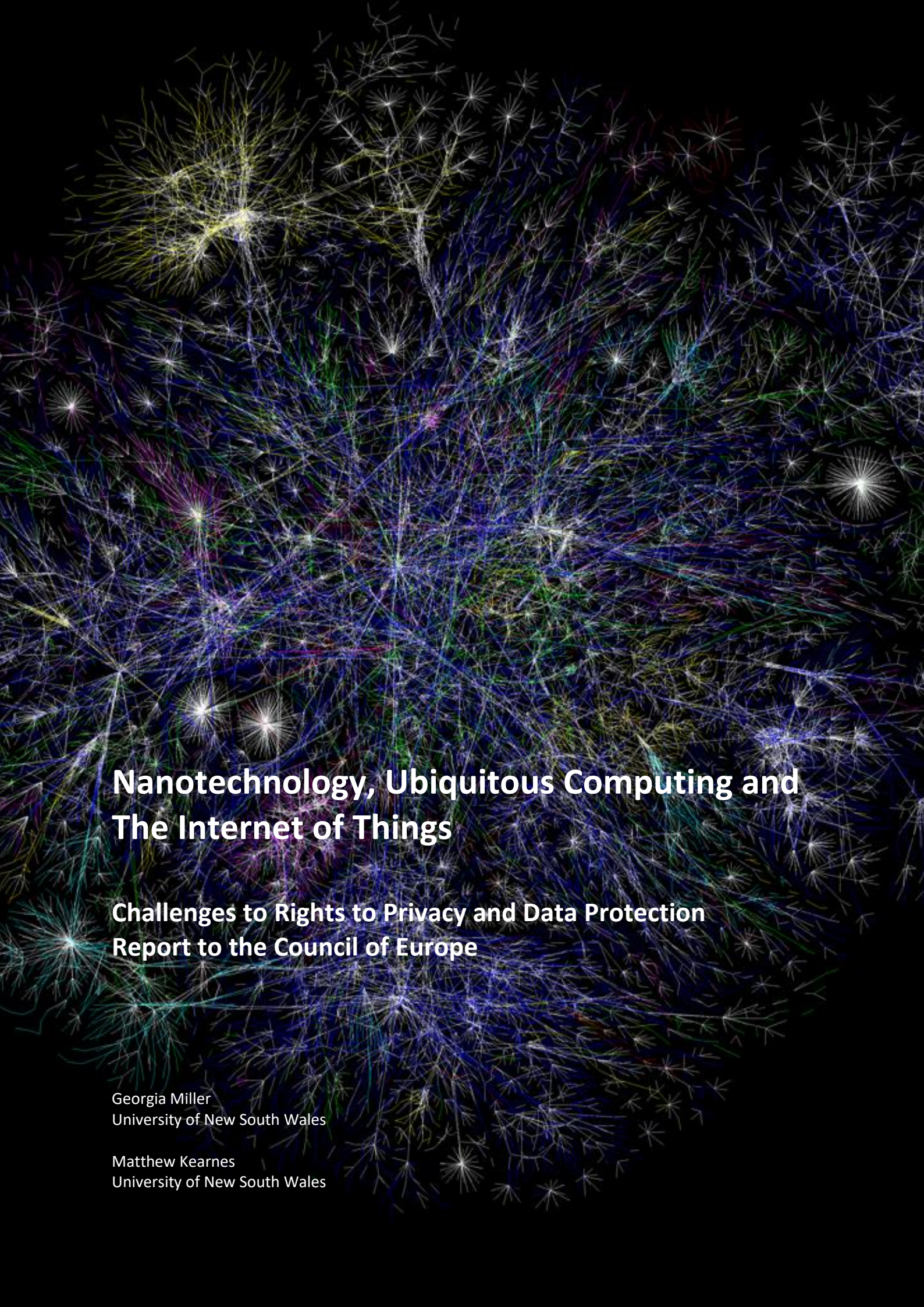
NANOTECHNOLOGY, UBIQUITOUS COMPUTING AND THE INTERNET OF THINGS:

Challenges to Rights to Privacy and Data Protection
Draft Report to the Council of Europe

The views expressed in this report are those of the authors and
do not necessarily reflect the official position of the Council of Europe

Georgia Miller
University of New South Wales

Matthew Kearnes
University of New South Wales
December 2012



Nanotechnology, Ubiquitous Computing and The Internet of Things

Challenges to Rights to Privacy and Data Protection
Report to the Council of Europe

Georgia Miller
University of New South Wales

Matthew Kearnes
University of New South Wales

Note on the Purpose of the Document

This report has been prepared pursuant to contract 560/12 for the Council of Europe by Georgia Miller and Matthew Kearnes.

The report is intended to provide an analysis of the privacy and data protection implications of nanotechnology, ubiquitous computing and domotics.

About the Authors

Georgia Miller is a PhD candidate in Environmental Humanities at the School of Humanities and Languages, University of New South Wales. Georgia's PhD thesis uses nanotechnology as a case study to explore how socio-technical imaginaries drive innovation policy and are mobilised within it, how framing and discourse is shaped by and affects political relations and interests, and how knowledge cultures affect regulatory and policy initiatives. She may be contacted at: g.miller@student.unsw.edu.au

Matthew Kearnes is a Senior Lecturer in Environmental Humanities at the School of Humanities and Languages, University of New South Wales. Matthew's research is situated between the fields of Science and Technology Studies (STS), environmental sociology and contemporary social theory. His current work is focused on the social and political dimensions of nanotechnology and synthetic biology, climate change and society, and the social and political dimensions of climate modification and geoengineering. He may be contacted at: m.kearnes@unsw.edu.au.

Cover Image

The cover image used in this report is a visual representation of the internet produced by The Opte Project (ww.opte.org/). It is used here under a Creative Commons Licence (CC BY-NC-SA 3.0)

Executive Summary

This report provides an analysis of the privacy and data protection implications of nanotechnology, ubiquitous computing and domotics.

We review three areas of current research – situated at the interface between nanotechnology and ubiquitous computing – including military nanotechnologies, research in nanomedicine and current developments in information technology and the internet of things.

We argue that these areas of research are likely to precipitate new modes of surveillance, data gathering and tracking devices, together with a range of sophisticated security, military and civilian applications.

We suggest that these developments are likely to pose significant challenges for existing rights to privacy and data protection.

In considering these implications we highlight a number of key concerns:

1. Enhanced military technologies and capabilities;
2. Function creep in new surveillance and monitoring technologies;
3. The intensification of social sorting;
4. Challenges to social relations;
5. New forms of location data and tracking techniques;
6. Concerns about information security and data protection; and
7. Wider concerns about accountability and transparency.

We suggest that there are a number of significant legal issues arising from these issues, that directly pertain to existing legislation on data protection, data protection and wider regulatory mechanisms. These include:

1. Challenges to existing data protection provisions;
2. Challenges to legal norms of informed consent;
3. Concerns about the containment of pervasive nanotechnologies and sensor technologies;
4. The use of self-regulation in nanotechnology governance; and
5. Concerns relating to the under-regulation of nanotechnologies.

In closing we suggest that given the range of issues we have analysed in this report we recommend that more detailed assessments will be required to fully understand the challenging social, ethical and legal implications of the convergence between nanotechnology and ubiquitous computing.

We also recommend that any future work conducted by the Council of Europe regarding these issues will require a thorough analysis to be carried, entailing close cooperation among the relevant CoE Committees.

Background

The aim of this report is to provide a review of current developments in nanotechnology, ubiquitous computing and what is increasingly being referred to as "domotics" – the integration of domestic architectures (*domus)* with information systems and devices (*imformatics*). The report will also provide an analysis of the potential impacts of these developments on the right to privacy and to data protection.

These areas of technological development represent the convergence of two domains of current research – nanoscience and distributed computing. Much of the existing literature suggests that advances in nanotechnology are likely to operate as a underlying suite of techniques that will enable the development of miniaturised and distributed information systems and the integration of informatics devices into a range of everyday consumer goods and household architectures. As we outline below the convergence of nanotechnology and research in ubiquitous and distributed systems is likely to result in the development of a range of new sensor technologies and advances in surveillance and monitoring techniques, deployed in civilian, military and security contexts. For these reasons advances in nanotechnology and ubiquitous computing are likely to intensify existing concerns associated with data collection and the right to privacy.

In order to provide some background to our review of these issues in this section of the report we outline definitions of the field and current trends in surveillance, data-mining and monitoring.

Defining Nanotechnology

Speaking at the California Institute of Technology, in 2000, President Clinton outlined the ambitions of what was, at that stage, the new field of nanotechnology:

> Just imagine, materials with 10 times the strength of steel and only a fraction of the weight; shrinking all the information at the Library of Congress into a device the size of a sugar cube; detecting cancerous tumours that are only a few cells in size. Some of these research goals will take 20 or more years to achieve. But that is why there is such a critical role for the federal government (Clinton 2000)

In this speech President Clinton drew inspiration from Richard Feynman's (1960) ground breaking essay "There is Plenty of Room at the Bottom" and from the futuristic vision of nano-scale machines popularised by Eric Drexler (1986). He suggests that an emerging capacity to miniaturise technology, and indeed to control and harness the material world at the nanoscale, will herald untold social and economic benefits.

President Clinton's speech is significant because it helps us to see two characteristic features of nanotechnology. Firstly nanotechnology is not a single area of technological development, but is rather a field of research defined by the capacity to manipulate matter at the nanoscale (10^{-9}m). Nanotechnology is commonly defined as an area of research and technological development that aims to exploit the novel properties of matter at the nanoscale, and more broadly the design and production of technological devices with nanoscale parts and components.

In their comprehensive study of nanotechnology the Royal Society and Royal Academy of Engineering (2004) define the field in the following terms:

> Nanoscience is the study of phenomena and manipulation of materials at atomic, molecular and macromolecular scales, where properties differ significantly from those at a larger scale.
>
> Nanotechnologies are the design, characterisation, production and application of structures, devices and systems by controlling shape and size at nanometre scale. (p. 5)

Nanotechnology can therefore be regarded as a platform of enabling techniques, rather than a discipline-specific or materials-specific undertaking (Whitman 2011).

A common distinction made in the literature is between early stage nanotechnologies and the potential for more advanced combinational developments based on convergences between disparate areas of scientific and technical endeavour, enabled by advances in nanoscale research. To date, much of the existing policy and regulatory literature has focused on early stage nanotechnologies – and particularly developments in nanomaterials and devices, focusing on the potential novel health and environmental risks of existing nanotechnology products. However, we will argue below that some of the most significant societal challenges posed by nanotechnology relate its potential to enable convergences between of allied areas of research in informatics and distributing systems research.

The development of nanoscale electronic and sensor devices has the potential to enable advances in ubiquitous computing and distributed and self-organising network systems. Applications in these areas are likely to emerge from the amalgamation of research on distributed networks and the capacity to produce nanoscale components and sensors. The development of 'smart' and 'self organising' networks, coupled with the use of nanoscale environmental and biomedical sensors, presents the possibility for the pervasive introduction of these devices into building design, medical devices and everyday consumer goods.

When we come to consider the implications of nanotechnology's application and development for privacy, security, and human rights, we must therefore consider a wide range of emerging fields: nanobiotechnology, nanopharmaceuticals and therapy, information technology and nanoelectronic systems, nanomanufacturing, nanocomputing and nanoassembly. As we will outline below this convergence between different research trajectories in nanotechnology and ubiquitous computing therefore represents a significant challenge for future democratic governance, the protection of privacy and data management (Hunter 2002)

The second characteristic feature of nanotechnology evident in President Clinton's speech is his invocation of the role of the State in supporting and coordinating the development of nanoscience research. In 2000 the US federal government launched a National Nanotechnology Initiative, a major research investment in the field with funding between 2001-2012 reaching $18 billion. During the 2000s comparable initiatives were launched in Germany, Japan, China, and the UK, while the European Commission launched a major funding initiative in nanotechnology in 2003 (European Commission 2004). Throughout this period public research funding constituted the major contributor to the growth of nanotechnology, compared to private R&D funding. In a recent review funding and publication patterns, Shapira and Wang (2010) suggest that this trend is likely to continue. Their list of the top ten global funders of nanoscience research is populated entirely by national and intra-national institutions: the National Science Foundation of China, the US National Science Foundation and the European Union, for example.

What this means is that nanotechnology is not simply a set of technical devices, but might be properly understood as a socio-political project (Jones 2011). This has important implications for considering the privacy and data protection aspects of nanotechnology. Rather than see

nanotechnology as a unified area of technological development, in this report we consider the divergent drivers and trends that are shaping research across nanotechnology and ubiquitous computing. In particular, we draw on recent research that has demonstrated a consistent trend toward the technological augmentation of surveillance, information collation and data mining together with the increasing automation of these systems (Humphreys 2011; Murakami Wood 2006; Raab et al. 2010). We argue below that advances in nanotechnology and ubiquitous computing, and the realisation of research goals in domotics, surveillance and the 'internet of things', are likely to intensify these trends. In parallel, the overlaps between civilian, military and security oriented research in nanotechnology represent a significant challenge for developing policy aimed at safeguarding rights to privacy and data protection.

We argue that these profound and important challenges are likely to extend current concepts of human rights and rights to privacy. Contemporary research has demonstrated a mutually reinforcing relationship between the norms of privacy and the coordination of surveillance and monitoring systems – and particularly the apparent paradox that constitutional rights to privacy require the intensification of surveillance and data monitoring systems (Murakami Wood 2006). In addition, current developments in domotics and pervasive computing, dependent on accurate locational data, appear to directly challenge existing privacy protection measures, as does the increasing occurrence of 'self-surveillance' and 'self-exposure' (Wright et al. 2010). That research in both nanotechnology and ubiquitous computing is likely to amplify these trends is, we argue, indicative of a wider conceptual challenge to existing concepts of privacy and data protection. Current research on privacy and human rights has suggested that "the anxieties associated with contemporary data collection are profound and important but that they are not easily articulated in human rights terms or addressed through the "right to privacy". This is in part because the legal articulation of the right to privacy is ill-suited to these anxieties and is likely to achieve little beyond, perhaps, providing reassurance that "something is being done"' (Humphreys 2011: 75). In this report we argue that advances in nanotechnology and ubiquitous computing are likely to precipitate an intensification of these anxieties and further challenge the adequacy of existing concepts of privacy and data protection.

In the following sections we summarise key developments in nanotechnology and ubiquitous computing and provide an analysis of key issues related to privacy and data protection. We review research developments across three fields: 'military nanotechnology', 'nanomedicine, therapy and enhancement' and 'information technology, domotics, and the internet of things'.

Military Nanotechnologies

Research and Potential Applications

One of the key drivers of research at the interface between nanotechnology and ubiquitous computing are a range of projected applications in defence and security applications. As such military-oriented research plays an important role in shaping research across these fields.

The world's leader in military nanotechnology research is the United States, although countries including China, Russia, Israel, Sweden, India and the United Kingdom are also investing in the field (Nasu and Faunce 2010). Since 2000 and the creation of the US National Nanotechnology Initiative, the US has allocated ⅓ to ¼ of its annual billion dollar plus research budget to the Department of Defense. Estimates are that the US currently spends 80-90% of global expenditure on military nanotechnology, which is about four to ten times as much as the rest of the world combined (Altmann 2008).

Universities are involved in much military nanotechnology research, including through high profile collaborations such as that between the United States Army and the Massachusetts Institute of Technology's 'Institute for Soldier Nanotechnologies' (ISN). Additionally, private companies including QinetiQ, BAE Systems, Industrial Nanotech Inc, and Raytheon, have also engaged in research, often in partnership with national governments, especially in the areas of nano-sensors and body armour (Nasu and Faunce 2010).

Nanotechnology applications, and those made possible by the convergence of nanotechnology with informational technologies have potential applications across the full spectrum of military and security domains. In particular, the development of cheap wireless-networked sensors, drones and animals for unobtrusive, large-scale surveillance is a key goal of military research with potential implications in civilian and commercial applications. In this section we outline key areas of research and development and analyse the privacy and legal issues associated with these developments.

Nanosensors

A key goal in contemporary nanoscience research is the development small, cheap sensors that incorporate nanoelectromechanical systems (NEMS) and are linked via wireless network systems – smart dust (Dickson 2007). Remote sensors are a particularly significant area of research in the development of military nanotechnologies. Sensors are considered important for intelligence gathering regarding local conditions, the movement of enemy troops or equipment, to monitor and assess real-time damage and to neutralise or undermine the effectiveness of an enemy's attack (Dickson 2007). Sensors and surveillance applications could also play a key role in improving the accuracy of weapons delivery and boosting the lethality of attacks, for example by providing information to adjust power levels or chemical agent concentrations to obtain a desired effect (NRC 2003). The development of 'smart dust', in the form of tiny 'motes', could theoretically be scattered over a battlefield or an entire region. Capturing data on temperature, pressure, vibration, acceleration, light, magnetics, or acoustics and communicate this information continuously. There are technical obstacles to the realisation of these devices, particularly in relation to reliable power supply, but also in relation to the reliability of transmission, false alarms and network coordination. A key vulnerability is to jamming via broad electromagnetic pulses. Nonetheless, the aim of the US is to develop smart dust that could "transform persistent surveillance for the warfighter" by 2025 (Dickson 2007).

In addition to informing offensive activities, nanotechnology-based sensors, coupled with increased computing power, could play a defensive role in applications for counter-terrorism and counter-

insurgency and for boosting biosecurity (Nasu and Faunce 2010). Nanotechnology sensors could support more effective detection of chemical, biological, radiological or explosive materials. For example the US Defense Threat Reduction Agency hopes that nanoscience will enable improved understanding of energy storage and transfer processes for use in indicators to locate radiological or nuclear materials (Shipbaugh 2012). Researchers are working with nanomaterials such as graphene to develop radiation sensing indicators that could be incorporated into everyday materials such as paint, corrosion-resistant coatings, ceramics or clothing, enabling widespread application (Robinson et al. 2012).

Distributed Surveillance Systems

The development of nanosensor technologies is also driven by the objective to develop new surveillance techniques and distributed monitoring capabilities. Researchers in Europe, the United States and Japan have sought to develop 'artificial' insects, implanted with sensors, electrodes and surveillance equipment. DARPA's Hybrid Insect Micro-Electro-Mechanical Systems project is reported to be inserting computer chips into moth pupae with the goal of hatching them into healthy "cyborg moths" (Weiss 2007). The aim is for such moths to have nerves that interface with an internal silicon chip so that operators could control their activities remotely. DARPA researchers are also reported to be raising cyborg beetles with power for various instruments to be generated by their muscles.

Work is also underway in brain-machine interfaces in animals to enable their use in surveillance activities or to deliver weaponry. Rats and monkeys have been the subject of brain electrode implants that enable rapid training to follow the instructions of the experimenter, even along arbitrary paths. Such animals could be used to carry video cameras or other sensors inconspicuously into enemy territories, or to deliver a remotely ignited explosive charge to its target (Altmann 2008).

New surveillance tools, coupled with high density data storage, vastly increased computing power and a new generation of wireless communication tools are also expected to enable increasingly automated computer-controlled battle management and logistics (Altmann 2008). Nanotechnology is expected to accelerate development of tanks, artillery and helicopters without crew.

Drones

The development of small drones for surveillance predates nanotechnology. The *Washington Post* reports that the US CIA developed a simple dragonfly snooper as long ago as the 1970s. Robotic fliers have been used by the military since World War II and Defense Department documents describe nearly 100 different models in use today. United States owned flying robots logged more than 160,000 flying hours in 2006 (Weiss 2007). Nonetheless, nanotechnology is expected to boost the sophistication and capabilities of such drones, while dramatically reducing their size and enabling longer flight times (Altmann 2008).

Implications of nanotechnology military R&D for privacy and security

The potential for vigorous investment in nanotechnology military research to negatively affect international political stability and security is relevant to the privacy dialogue. The renewed attention on privacy is partly a response to privacy infringements associated with boosted surveillance activities following the September 11 and other terrorist attacks.

Nanotechnology will increasingly enable the development of hostile systems and interactions that are characterised by small size, low cost and easy availability. This has implications for stability, complexity and verification (Altmann 2008). Nanotechnology could greatly increase complexity, by

boosting the number of state and non-state actors who have access to deadly weapons. This could in turn erode international stability by creating new pressures for states or groups to go to war, or to strengthen armed forces.

Nanotechnology may shift the balance between defensive and offensive capabilities (Whitman 2011). The development of counter-technologies, including those associated with detection and verification, may not keep pace with the development of offensive nano-military capabilities (NATO 2005). This, coupled with greater international political instability, could drive a new anxiety and appetite for further security crackdowns by government, while being used to justify further incursions on individuals' privacy.

The use of nanotechnology in military applications could amplify existing power asymmetries by further removing technologically superior sides from face to face combat. This could create new incentives for terrorist attacks outside traditional war theatres, a political environment in which the state's infringement of the privacy rights of its citizens becomes more likely.

The development of nanotechnologies through military research and development also has practical implications for privacy and civil liberties. Beyond the development of ubiquitous and persistent surveillance, military research is also a major driver in developing ICT implants for monitoring, treatment and identification, environmental and diagnostic sensors, security and identification technologies.

State of Deployment

Obtaining accurate information regarding the state of development of military research and the extent of real world application of nanotechnology in offensive and defensive applications is difficult. Even the current research goals of different states have been presented incorrectly, with potentially damaging political and security consequences (Altmann 2008).

Some nanotechnology-based sensors may be close to field deployment, if they have not been used already. Although optimistic predictions are that the US may not have effective smart dust until 2025, researchers at the University of California-Berkeley have already developed a surveillance 'mote' that is as small as a grain of rice (Dickson 2007). In 2003, Dr Akos Ledeczi of Vanderbilt University, with funding from DARPA, successfully used over 200 MICA2 motes in an urban environment to locate the position of a gunshot within two seconds with an average accuracy of one metre (Dickson 2007). The usefulness of a smart dust network depends on the reliability of the delivered information, even where there is interference from the operational environment. Current studies show up to a 20% loss in delivery of transmission information due to interference (Dickson 2007).

Electronic 'noses' are sensing arrays that can be based on microscale as well as nanoscale components, and are designed to monitor for targeted chemical species or mixtures. These sensors have a wide range of current and potential applications, including for quality control in the food sector, environmental monitoring, in petrochemical prospecting, as well as in military settings. The US Lab on the International Space Station has already used an electronic nose to monitor for the sudden release, such as leaks or spills, of targeted chemical substances (Ryan 2012). The sensor is capable of detecting, identifying and quantifying targeted chemicals in the parts-per-million range in air.

It is possible that nanotechnology-enabled drones are either in use or close to field use. Small combat robots which do not use nanotechnology have already been deployed in combat. In 2006

the British Special Forces in Afghanistan used a remote controlled model aircraft, the 40cm wingspan 'Wasp Micro Air Vehicle', to attack snipers with an explosive charge (Leake 2006).

It has also been reported that unmanned aerial vehicles that use nanotechnology-based systems are now commercially available for surveillance purposes. Military equipment manufacturer BCB International promotes its SQ-4 MOUT (military operations in urban terrain) model as weighing less than 100 grams and fitting in the size of a palm (Minchin 2012). It claims the device will be useful in situations where there is a terrorist danger or where hostages have been taken. The SQ-4 MOUT can assess enemy location, identity and number, as well as damage. The flight range is designed to be between 300 and 500 meters and to have a flight duration of up to 20 minutes. The system offers a "perch and stare" facility which allows the device to alight on a building, switch off its engines and operate a camera for up to two hours.

However analysts have suggested that the technical development and deployment obstacles to the use of more sophisticated 'artificial' insects for surveillance and offensive applications, such as those being developed by DARPA, are so great that use in the field is unlikely to occur soon (Weiss 2007). Optimistic predictions were made in the early 2000s regarding the rapidity with which nanotechnology would deliver sophisticated applications. However the development of military applications, as with other areas of nanotechnology, has encountered unanticipated hurdles in the journey from lab discovery to usable application. Despite this, it is possible that work on nanomaterials for explosives, for amour and for armour piercing may be close to military application (Altmann 2008).

Nanomedicine, Therapy and Enhancement

Research and Potential Applications

Nanotechnology has diverse applications in the health care sector, including the development of new diagnostic and imaging applications, more potent pharmaceuticals and drug delivery mechanisms, and active implants and devices. The dominant research field in nanomedicine is drug delivery, which the European Union's Joint Research Centre found contributed 76% of total scientific publications, followed by *in vitro* diagnostics which contributed 11% (JRC 2008). In this section of the report we review a range of application areas with possible implications for privacy and data protection.

Drug Delivery Systems

Nano-based drug delivery systems aim to improve the bioavailability and pharmacokinetics of pharmaceuticals and to provide non-invasive routes of drug administration. Examples of drug delivery systems in development that use nanomaterials are liposomes, nanosuspensions, polymeric nanoparticles, dendrimers, fullerenes, carbon nanotubes, and inorganic nanoparticles (JRC 2008). Polymer-protein conjugates, polymer-drug conjugates, polymeric micelles and polymeric drugs are frequently classified as nano drug delivery systems.

One of the drug delivery devices undergoing clinical trials is a nanoparticle shell containing a chemotherapy agent (Resnik and Tinkle 2007). The shell is designed to release its active ingredients only when it encounters a cancer cell in the body, to which it binds. The chemotherapy agent then enters the cancer cell which is killed. This drug delivery system is designed to specifically target malignant cells, and researchers hope that it can minimise the impact of chemotherapy on healthy cells. However, it is also possible that nanoshells used to deliver drugs will accumulate in the body and cause damage. The US FDA classifies this as a "combination product" because it combines a drug (chemotherapy) and medical device (the nanoparticle shell).

Implants

Nanomaterials and nano components have increasingly been developed for medical implants. Major application fields are hard tissue implants, bone substitute materials, dental restoratives, soft tissue implants, and antibiotic materials for coating or disinfecting medical equipment. Nanomaterials have been developed for orthopaedic implants that have greater biocompatibility, promote new bone growth and which are hoped have longer life spans (Balasundaram and Webster 2006). Nano-based coatings have also been used on medical devices to boost their biocompatibility (Chapman 2005) or antibacterial properties.

Diagnostic Tools and ICT Interfaces

The next generation of medical applications will be made possible through greater and more specific physiological and health data provided by new medical surveillance and diagnostic tools. While this field is still far smaller than that of drug delivery, new information accessed through nano-diagnostics arguably poses the greatest challenges for privacy. Similarly the use of ICT implants for diagnostic purposes has to date attracted little attention. In the same way that NEMS based implants have been discussed above in relation to military applications for soldier surveillance and controlled drug delivery, nano ICT implants are now being developed to assist in both patient identification and data collection to improve treatment options. It is increasingly expected that 'radio-frequency identification' (RFID) implants will be able to transmit measurements of chemical or biological data and to monitor biological activity or physiological function (Aubert 2011).

Human ICT implants, especially those based on RFID technologies, are already employed across a number of different sectors for identification, data collection, diagnosis (European Group on Ethics in Science and New Technologies 2005) and even authorisation and security purposes (Rotter et al. 2012). RFID is a broad concept used to refer to technologies that enable data collection, through use of contactless electronic tags and wireless transmitters (OECD 2008). It is anticipated that the convergence of nanotechnologies with ICT in this field will underpin more sophisticated applications in coming years, especially in the lucrative healthcare sector. Carbon nanotube-based radio medical devices could hypothetically operate in the bloodstream (Jensen et al. 2007) or even within individual cells. Ultimately, this technology could potentially also support very small physiological sensors that could be implanted and then communicate with a single central unit in 'wireless body area networks' (Aubert 2011).

DARPA solicited in 2012 for research proposals to develop *in vivo* 'Nanoplatforms for Diagnostics' (DARPA 2012). The aim of the program "is to develop biocompatible nanosensors that provide continuous, noninvasive, and highly accurate measurement of a variety of conditions and substances within the living tissue of animals, plants, and insects using non-toxic materials with limited immunogenicity. These sensors will permit qualitative and quantitative assessment over large concentration ranges of both small (e.g., glucose, lactate, and urea) and large molecules (e.g., proteins, oligonucleotides, infectious agents, and chemical/biological threat agents) in the organism and environment through optical, electronic, thermal or magnetic mechanisms". The challenges required to develop more complex single chip, cellular scale, RFID-based ICT implants for biomedical devices are considered to be "solvable" using new nano-engineering and nano-fabrication capabilities (Burke and Rutherglen 2010). However chips that interface with nano-systems to enable not only active monitoring of human biological functions, but also remote activation or deactivation of biochemical activity at the cellular level, are considered a "vision" rather than a near-term possibility (Burke and Rutherglen 2010).

Nanobionics

Another emerging field is that of 'nanobionics', described by some as the convergence between biology and electronics. Nanotechnology does not yet play an important role in the manufacture of commercially available active implants. Nonetheless, there are many examples where nano-structured materials are being used for specific components of active implants, to improve the biocompatibility of implants, and to support more effective electrode-cellular interfaces (Wallace et al. 2012).

The Australian scientists who developed the 'bionic ear' (a cochlear implant to assist hearing-impaired people) are now working on a nanobionic project they hope could help regenerate damaged spinal cords (Cronin 2007). Their research uses a combination of nanobionics and polymers, producing a plastic material that can conduct electricity. The scientists hope that their ''smart polymer'' could be implanted into the damaged part of the spinal cord and electrically stimulated to promote growth of new nerves. The same team is also trying to develop a nanobionic implant that could be used to stop seizures in epilepsy sufferers (Wachsmuth 2012).

State of Deployment

Of the 200 companies internationally that the European Union's Joint Research Centre identified in 2008 as active in nanomedicine, 159 were start-ups and small-medium enterprises that focussed on the development of nanotechnology-based pharmaceuticals and medical devices (JRC 2008). JRC identified a further 41 major pharmaceutical and medical device corporations which had nanomedicine products on the market or which ran development projects in which nanotechnology played a role.

In the ten years up to 2008, 38 medical products that use nanotechnology were placed on the market (JRC 2008). The estimated total sales of nano-medical products were EUR 5.4 billion in 2004, of which sales of 23 nano drug delivery system (NDDS)-based products constituted EUR 4.2 billion (about 80%). This is a tiny share of the global pharmaceutical market which at the time generated annual sales of about EUR 390 billion.

Based on about 157 products that were at advanced development stage in 2008, the JRC estimated that the market of nanomedicine products would increase to about €15 billion in 2012, remaining dominated by NDDS (JRC 2008). A more recent and larger figure is cited by BCC Research LLC, which estimates that the global nanomedical market (including nanotechnology used in medical applications and devices) reached US$72.8 (€55.1) billion in 2011 and will reach US $130.9 (€99.1) billion by 2016 (BCC Research LLC 2012).

Nanotechnology-based therapies, *in vitro* diagnostics and imaging agents are still in an early stage of development, although it is expected that their importance will grow.

Nano drug delivery systems (NDDS) now on the market are first generation products that use nanomaterials to increase the solubility and therefore the bioavailability of drugs, or which concentrate drugs in particular tissues (JRC 2008). Just as the understanding of the unintended consequences of exposure to nanomaterials for human health and the environment remains rudimentary (Grieger et al. 2012), scientists are just beginning to understand the interaction of NDDS with the immune system, cells, and organs (JRC 2008).

So-called next generation nano-medicines will try to tailor the pharmacokinetic properties of drugs to the needs of individuals, thereby increasing their efficacy. This will require a more complex understanding of an individual's physiological function, for which it is hoped nano-diagnostics, including *in vivo* imaging and *in vitro* diagnostics, will assist.

Diagnostic devices and implants and surveillance applications, which may present some of the most pressing privacy challenges, are at a fairly early stage of development and deployment. There are four key types of implants: those designed to restore or repair human capabilities; those that aim to monitor biological conditions; those intended to identify an individual; and those that aim to enhance human capabilities (Hildebrandt and Anrig 2012).

The first generation of ICT human implants has been primarily focused on (Kosta and Bowman 2011). RFID technology was originally developed for identification, authentification and tracking of physical objects. A passive RFID tag—a small device attached to the object—emits identification data through radio waves in response to a query by an RFID reader which also supplies it power; an active RFID tag has its own power supply and emits data constantly (Hildebrandt and Anrig 2012), potentially enabling real time tracking of the label, and the device or individual with which it is associated.

Two hospitals in the US have already actively implanted *VeriChips* into patients who consent and pay to be a part of the system. As of June 2006 about 100 people had been implanted with this RFID for medical purposes (Foster 2006). Surprisingly, the system transfers most management responsibilities and ownership of medical records to VeriChip Corporation (Monahan and Wall 2007). Photographic company Kodak has patented digestible RFID tags (van den Hoven 2009). These can reportedly be attached to pharmaceutical products, enabling institutions such as prisons, psychiatric wards and hospitals to track medicine on the item level, even inside the human body. This could enable compliance management of prescribed medication (van den Hoven 2009).

Information technology, Domotics and the Internet of Things

Research and Potential Applications

The use of RFID is expected to foster the convergence of information technology, surveillance and communications technologies, ultimately contributing to ubiquitous networked societies through which data relating to almost every aspect of an individual's life and work environments could be collected and linked (OECD 2008).

Precise collection of information on individuals' locations, travel routes and personal habits in the home is projected as enabling the development of 'smart' transport systems for "a safe and comfortable traffic environment" (Zhang et al. 2011), and domotics to underpin improved environmental sustainability in the household, stronger security and more tailored personal care for the elderly (Cook 2012). However the concept of 'persistent surveillance', and the capacity for unprecedented quantities of information about individuals' health and personal habits to be used for political and commercial purposes has attracted criticism from civil liberties advocates and scholars (CASPIAN et al. 2003, 2012; Monahan and Wall 2007).

In this section we outline some the key applications of these techniques.

RFID labelling systems

The use of RFID labelling systems for individual consumables has attracted concern from civil liberties groups concerned that surveillance will continue through supply chains and past the point of sale (eg CASPIAN et al. 2003). Should RFID tags not be deactivated in store – and there is no sign that they have been, at least in any systematic way – companies could exploit surveillance and track and trace capability to compile detailed information about the shopping habits, daily travelling routes and consumption patterns of individuals.

Clothing company Benetton planned to put RFID tags into every item of its clothing (van den Hoven 2009). The project was abandoned after it was met with strong objections from people concerned that their movements through the shop, whether or not they tried on the item first, which other shops they visited, their route home, their home address and even how long they retained the clothing for could become trackable by the company. Similarly controversial was UK supermarket chain Tesco's experiment with a camera which was activated when consumers took a packet of Gillette razors from the shelf (van den Hoven 2009).

Applications of interactive technologies which identify users, perhaps by RFID implants or alternatively through facial recognition or biometric technologies, while also recording and acting on information collected regarding personal habits and preferences, may be perceived to be more socially acceptable in different contexts. For example 'smart' cars could be developed which incorporate RFID readers that identify an authorised driver, open the door, adapt the seat height and position the mirrors (Rotter er al. 2012a).

Networked surveillance tools

Networked surveillance tools designed to collect, process and act on information about the habits, minute-by-minute location and recreational preferences of particular individuals underpin promises of environmentally efficient, labour-saving 'smart' houses (Science Daily 2012b). Proponents suggest that such homes will have security systems with facial recognition technology, appliances that are

interlinked and pre-programmed to reorder key goods when supplies are low, the capability to track the expiry dates of foods and medicines, and to alert the resident if dates are exceeded together with robots to perform mundane household tasks and to accept orders using speech recognition technology and heating and cooling in accordance with the household's routines (Future Homes 500 2011).

Houses that incorporate a high degree of surveillance and networked, automated appliances are increasingly being designed with ageing baby boomers in mind. Such homes are touted as offering 'interactive' or 'assistive' environments. Devices that monitor and interact with each other and a house resident are designed to extend the time that elderly people who lack strong social networks of support can stay in their homes, rather than enter a nursing home. 'Assistive environments' that 'anticipate' a resident's requirements for security, health, medical or even cognitive assistance are envisaged to enable the provision of remote care and medical advice (Cole 2012)

The Internet of Things

Perhaps the most transformative predicted development in information technology systems is the emergence of an "Internet of Things" (IOT). The International Telecommunication Union (ITU 2005) foresees that the IOT could usher in a new computing and communication era that will radically transform our industrial, community and personal spheres.

The IOT refers to the growing network of intelligent sensors, near field communication devices and RFID tags which increasingly connects electronically people, devices, objects and other 'things'. Proponents suggest that the IOT will enable "everything from tires to toothbrushes" to communicate electronically with each other, via direct or indirect connection to the internet (ITU 2005). In this way, everyday objects and devices could be connected to large databases and wireless networks.

The aim of the IOT is to enable objects, services and people to share continuously electronic information obtained from RFID tags and embedded sensors. In an optimistic scenario, this could enable minute by minute tracking, monitoring and management of devices, systems and physical interactions through remote sensing and control (Zhang et al. 2011). In its Strategic Research Agenda, the Cluster of European Projects on the Internet of Things (de Saint-Exupery 2009) envisaged that the IOT could enable remote management of a huge diversity of systems and sectors (Figure 1).

Aerospace and aviation	Oil and gas
Automotive	Safety, security and privacy
Telecommunications	Environmental Monitoring
Intelligent buildings	People and goods transportation
Medical technology	Food traceability
Healthcare	Agriculture and breeding
Independent living	Media, entertainment and ticketing
Pharmaceutical	Insurance
Retail, logistics, supply chain management	Recycling
Manufacturing, product lifecycle management	

Figure 1: Internet of things application domains, as envisaged by the Cluster of European Projects on the Internet of Things (de Saint-Exupery 2009)

Theoretically, by using RFID, the IOT could comprise millions of networked embedded devices in continuous contact with each other. RFID could link to GPS or GIS (Geography Information Systems) for accurate location data. The embedded sensors could obtain information about the physical attributes of environments, for example temperature, moisture, light, sound or the presence and absence of toxins, nutrients or drugs. This could then enable full automation and remote management of sectors that are now very labour intense, for example agriculture.

Chinese researchers have suggested that the IOT has the potential to enable highly precise and data-driven crop management, delivering higher productivity, less waste and more reliability for urban agriculture (Duan 2012). Such a management system would be based on unique identifiers associated with crops and farm goods. Sensors would continuously collect data related to growing conditions and communicate this via wireless networks to computers that would control management response. It would take the monitoring, assessment, decision making and response out of the hands of farmers and embed it in 'intelligent' systems which could be fully automated, ensure compliance with all pre-programmed regulations and record data relating to each step of the process for others further down the food supply chain to access.

RFID can be seen as the first intelligent networked sensor technologies that would enable the creation of an IOT (OECD 2008). Advances in miniaturisation and nanotechnology-based electronics are critical to developing the network ubiquity required for a comprehensive IOT (ITU 2005). The development of ever smaller integrated circuits at the nano-scale drives the production of very small tags, smart cards, smart labels and sensors, supporting the new monitoring and surveillance infrastructure that could underpin an IOT (van den Hoven 2009).

State of Deployment

Although their creation dates back to the Second World War, RFID technologies have experienced a rapid evolution and broad implementation throughout the economy in recent years (OECD 2008). One important driver for current market growth is improving traceability of goods in the supply chain with the aim of increasing supply chain efficiency, reducing theft and fraud, and saving costs.

Although RFID technologies continue to evolve and develop at a fast pace, they can be considered to have some level of 'maturity': they have already been deployed at small, medium and large scales in many countries, in several sectors and for various applications (Rotter et al. 2012a). RFID technology is now used in applications and fields "including passports, hospitals, transportation, ticketing, libraries, museums, counterfeiting, baggage tracking in airports and livestock tagging" (OECD 2008). RFIDs have also been used to track merchandise in large-chain stores such as Wal-Mart and Tesco. Many hospitals are implementing RFID systems to track inventory, patients, and personnel, with the goals of improving "workflow management" and reducing medical errors (Monahan and Wall 2007). In some cases, members of the public have volunteered to have RFID chips implanted to experience what have been promoted as 'ambient intelligence environments' (rather than 'persistent surveillance', Rotter et al. 2012).

Nonetheless, the technologies required to underpin a hypothetical IOT remain in development. Sensor and sensor network technologies that monitor environmental

parameters and communicate sensed data to other connected devices are less mature and generally deployed on a much smaller scale (Rotter et al. 2012a).

There is a growing use of some elements of a simplified IOT in sectors such as traffic management. ‘Smart transportation systems’ (STS) have built on surveillance-driven systems for traffic management and toll collection implemented in the early 2000s in Europe and Asia. Systems have moved from those based on camera and GPS to use of RFID signals attached to individual cars, with readers positioned throughout road networks. Traffic management systems increasingly seek to impose charges to road users at peak hours of demand, reduce congestion associated with accidents and encourage use of public transport. The STS system in Stockholm has reportedly reduced traffic congestion by 25% and urban air pollution by 10% (Zhang et al. 2011).

The promise of ‘smart’ housing is a long-standing one. Nonetheless, Washington State University researcher Diane Cook says it won't be long before our homes act as "intelligent agents" that use sensors and software to anticipate our needs and tend to tasks that improve our health, energy efficiency, even social media (Cook 2012).

The researchers who developed ‘InterHome’, in the UK, have said that the house can send alerts or text the home owners if it being burgled or the door has been left unlocked. The house is also designed to ‘learn’ from the routines, light and energy needs of its occupants to reduce energy use. In conjunction with wearable monitoring devices, the house can also send alerts if the resident has a fall or a stroke (University of Hertfordshire 2011). Test homes in Seattle have used monitoring of elderly residents to alert caregivers if they are not completing ordinary activities like rising, eating, bathing and taking medications (Science Daily 2012b).

Conclusions and Synthetic Analysis

Privacy and Public Interest Dimensions

Given the cross-cutting and interdisciplinary nature of research in nanotechnology and ubiquitous computing it is likely that these developments will precipitate significant privacy, data protection and legal concerns.

In this section of the report we synthesise these issues and provide an analysis of a range of privacy and public interest ramifications associated with these developments.

Enhanced Military Capabilities

The vision of many nanotechnology proponents is one where ultimately invisible warfare will be carried out with no presence on the battlefield of the nanotechnology-supported side (Reuters 2006). This would require highly accurate surveillance capabilities, in addition to a new generation of weaponry. This kind of asymmetric warfare has profound implications for equity and human rights; it could, at least initially, dramatically shift the power balance in favour of the nation able to wage war at a distance. It could also negatively affect international security by undermining the technologically superior side's commitment to compliance with international laws on armed conflict and human rights protection.

Forces equipped with smart dust surveillance capacity, long-range, highly accurate missiles guided by new generation surveillance systems, and drones or hybrid animal delivery systems for delivery of munitions to targets without exposure of their own personnel, could believe their physical distance from the site of conflict means they will not have to rely on reciprocal respect for humanitarian rules (Nasu and Faunce 2010). However nanotechnology-enabled asymmetric warfare could present serious new dangers for technologically advanced nations too, by creating new international instability. The dramatic power imbalance could increase the motivation for counter-attacks or acts of terrorism by states or individuals. This could in turn drive a renewed push for 'securitisation' and intrusive data collection on individual's and group's political sympathies and activities, which could be made possible by more widespread deployment of nano-surveillance tools.

The NATO Parliamentary Assembly committee that investigated the security implications of nanotechnology warned that "arms races are to be expected" (NATO 2005). If the US continues to spend such a great amount on developing nano-weaponry and military applications, and no preventative initiatives are undertaken, it is clear that other countries will increase their expenses too. If states see that a large-scale nanotechnology-enabled threat is not being addressed and managed effectively in arms control negotiations, there will be additional incentive to pursue their own rapid development of nano-arms.

Function Creep

Function creep is an increasingly recognised feature of the development and intensification of contemporary surveillance systems. A recent report to the UK Information Commissioner noted that "Personal data, collected and used for one purpose and to fulfil one function, often migrate to other ones that extend and intensify surveillance and invasions of privacy beyond what was originally understood and considered socially, ethically and legally acceptable" (Murakami Wood 2006: 9).

In the case of the development of pervasive surveillance and monitoring systems for military purposes, there is no reason to assume that once the capability for persistent surveillance is developed and affordable, that its use will be limited to essential military-related activities. It may prove very attractive for states and state-sanctioned intelligence gathering organisations to collect data on foreign individuals or governments, or to develop for intelligence information on their own citizens or on particular sections of the population. This could result in political dissidents, or those at the margins of society, experiencing a compromise of their rights to privacy. If people knew or suspected that they were being monitored round the clock, and that the new computing power of nanotechnologies enabled routine integration and analysis of this information, this could have a distorting effect on individuals' actions (Cribbs 2007).

New surveillance technologies may be appealing to commercial actors as well as states or law enforcement bodies. As the network of researchers involved in their development grows, and as the cost of persistent surveillance technologies diminishes, it appears likely that at some point in the future some of these capabilities will be available commercially. Nano-based surveillance capabilities could be seen to offer a way to collect information on competitor firms, thereby securing a commercial advantage. Further, companies in controversial sectors facing some level of civic objection could seek to use nano-surveillance capacity as a tool to neutralise or threaten dissidents.

In the area of medical devices and the use of RFID implants, there may be a growing expectation that people in certain occupations will accept non-health related RFID implants 'voluntarily'. RFID chips have been designed to interlink with security clearance systems, for example in the Mexican Attorney General's office and Ohio security firm examples above (Rotter et al. 2012a). One hundred and sixty people at the Mexican Ministry of Justice have been implanted to help trace them in the event of kidnapping (van den Hoven 2009). It may be the case that security firms, police departments, the public service, the armed forces or other employers will increasingly expect employees to accept RFID implants.

Even where being implanted with an RFID chip is not mandatory, or technically mandatory, it may be increasingly the case that being implanted with an RFID chip enables employees to engage in higher security clearance, or higher paid, work.

Social Sorting

Social sorting is also an increasingly recognised effect of the intensification of surveillance systems (Lyon 2003). Defined as systems of categorisation and classification that afford "different opportunities to different groups and often amounts to subtle and sometimes unintended ways of ordering societies, making policy without democratic debate" (Murakami Wood 2006: 10). These effects are likely to be intensified by developments in nanotechnology and ubiquitous computing.

Nanotechnology's use in the medical field is expected to dramatically increase the kinds of health information that can be provided. Health data, including that produced via cellular level monitoring, may become a site of new discrimination and social classification. Employers or health insurers may require individuals to undergo certain forms of new testing or monitoring as a precondition of employment or coverage. With ever increasing amounts of health and predictive health data available to people, pressure may grow for individuals to seek new forms of diagnosis even where their health appears to be acceptable. This could raise ethical conundrums where hereditary diseases are identified that affect family members (who have elected not to seek diagnosis), or where a confirmed

diagnosis of disease is impossible, but a range of risks is identified (JRC 2008).

As the cost of broad-spectrum diagnoses is reduced, there may be a growing societal expectation that individuals will 'take responsibility' for their own health by seeking detailed health data. Indeed, some companies marketing health-monitoring equipment are already touting this as a desirable scenario (as well as one in which there would be large-scale uptake of their products). However it is likely that for many diseases or genetic traits, treatment options will lag identification capability. Further, even where treatment options are available, access to them may be restricted by cost.

Many 'restorative' ICT technologies such as cardiovascular pacemakers or cochlear implants are sometimes considered to be socially desirable and uncontroversial – even to be 'exemplary' applications (for example see Tadeusiewicz et al. 2012). However devices that seek to 'cure' disability may pose other ethical and cultural dilemmas. Not all differently abled people perceive themselves to be 'disabled', or want to be 'cured' of their condition, or to supplement or replace or supplement their abilities via technology.

Ethicists have voiced concern that it may increasingly be seen that differently abled people have a social responsibility to use new technologies to 'normalise' their abilities, rather than society having a responsibility to support the participation and inclusion in the community of people who have a range of abilities (Wolbring 2008; Carrera 2009). If technology can provide perfect 'cures' for disability, it may be seen that disability becomes 'elective', and that society has less obligation to provide social and institutional support for differently abled people (Sparrow 2005).

Offering differently abled people access to ICT implants can also raise profound challenges to the sense of self of the individual, and to the cultural identity of the communities of which these individuals form part. 188,000 people internationally had received cochlear implants as of April 2009 (Tadeusiewicz et al. 2012). However, through the 1980s and early 1990s, parts of the deaf community mobilised to protest the use of cochlear implants (Sparrow 2005). These people rejected the very idea of trying to find a "cure" for deafness. Rather, they argued that deaf people should not be thought of as disabled but as members of a minority cultural group.

Influences on Social Relations

In the IOT, 'things' are expected to become active participants in business, information and social processes where they are enabled to interact and communicate among themselves (ITU 2005). 'Things' would therefore exchange data and information obtained through sensing, react autonomously to physical events and in turn influence their environment by running processes and creating services even in the absence of direct human intervention (ITU 2005).

Even without a fully developed IOT, the extensive use of sensors and RFID technologies is likely to have a profound impact on everyday behaviour and social relations. Detailed data regarding individuals' behaviour and habits may increasingly be accessed by those who have authority or power over them, and preferred to any personal account of activity, work contribution or health: "aggravation of existing power asymmetries can be seen as a likely undesirable outcome whether between nurses and administrators, patients and hospital staff, customers and retail outlets, or citizens and the state" (Monahan and Wall 2007). In this way, such technologies may present new threats not only to individual control over

personal data, but also to informational equalities, and informational justice and discrimination (van den Hoven 2009).

There may be other profound social changes associated with the rise of home surveillance and domotic systems. Such technologies are promoted as enabling elderly people to remain living in their own homes longer, rather than making the transition to a nursing home as their physical or mental health deteriorates. However while domotics and 'assistive environments' may well result in people living longer alone in their own homes, such technologies may not necessarily lead to improved quality of life and conversely elderly people may face growing social isolation as a result of technologies marketed as offering them greater peace of mind.

L*ocation Data and Tracking*

RFID tags and sensors could produce and process a huge amount of information about the location and properties of objects, and also indirectly about the identity and behaviour of the people associated with these objects. Prolonged or even coincidental co-location of RFID tags with items that have a unique identifier, for example RFID used in a permanent medical implant or in credit cards, or which are registered as belonging to certain owners, can establish the identity of the 'owners' of other tagged items (van den Hoven 2009).

Commentators have also raised concerns that medical or other RFID implants could enable the tracking and tracing of individuals (Kosta and Bowman 2011). This has been countered with assurances that RFID implants for humans are not large enough to store batteries sufficient for active signal emission, and therefore persistent remote surveillance (Aubert 2011). However, even if implants can never themselves alone provide the capacity for remote surveillance, when co-occurring with items that do have location trackers, such as mobile phones or laptop computers, location information could be linked to identity data (see also CASPIAN et al. 2003, 2012). Even where RFID are not implanted in devices, but carried on goods or embedded in devices, potential exists for this 'identification by association' (European Commission 2005).

The European Data Protection Directive (European Commission 2007) appears to provide that active consent is essential for acceptance of surveillance or tracking activities, including those associated with RFID. The Directive even provides that active consent cannot be seen to be provided where a special (and unequal) relationship exists, for example between employee and employer. However this is not a principle that is universally recognised, and the issue of consent for RFID surveillance is becoming a site of legal contention.

RFID technology has been increasingly employed as a 'barcode replacement' in production lines and the logistics chain of enterprises. Uptake is expanding in diverse sectors including medical and health care, defence and agriculture (Rotter et al. 2012a). Radio-frequency identification technology is increasingly deployed for identifying and tracking humans. In the US in 2010, a preschool in Richmond, California embedded RFID chips in regulation clothing to track its charges (Clark 2012). A US company, Radiant RFID, recently secured a 5-year contract with the New Jersey Office of Homeland Security and Preparedness to use RFID to track evacuees, pets, emergency transport vehicles and equipment in the event of a natural disaster. The company claims that its RFID 'solution' will cover 18% of the US population (PR Web 2012).

As use of RFID tags for tracking people becomes more widespread, it appears plausible that RFID implants will also increase. The first recorded human implantation of an RFID device

was in 1998; the first device approved by an authority for human use, the *VeriChip*, was in 2004, by the United States Food and Drug Administration (Rotter et al. 2012a). No health data is stored on the *VeriChip*, but rather a number to enable rapid patient identification. This is promoted as enabling more timely delivery of medical care that is appropriate to the individual.

Several recent studies have found that societal acceptance of RFID implants is low, although acceptance is slightly higher for 'life saving' applications (Hildebrandt and Anrig 2012). However should more individuals choose to accept implants of RFID sensors, challenges to privacy and other civil liberties may be magnified. The permanent and physical link between an RFID tag and the individual implanted with it makes RFID implants more susceptible to privacy risks than any other kind of contactless token (Rotter et al. 2012a).

Information Security and Data Protection

A key vulnerability of RFID-based systems is the low levels of security and data protection. Radio signals can, in principle, be sent and read by anyone: there could well be cases of "sniffing, skimming and spoofing". In a commercial setting, the potential exists for one business to spy on another business through its supply chains (Rotter et al. 2012a). A cloning attack has already been used on some RFID tags used for transport road tolling and fuel purchase (van den Hoven 2009).

Just by walking near a person with a 'skimmer', RFID data on a card can be read and then written to another card, allowing for the relatively easy compromising of security. RFID 'hackers' have cheerfully demonstrated to journalists their ability to steal and clone RFID-based access cards, tamper with RFID-held data, change price tags stored on RFID and clone the unique identification number stored on a *VeriChip* RFID implant (Newitz 2006). When *VeriChip*'s director of communications was asked about the potential for cloning of chips to result in mistaken identity or even identity fraud, he suggested that while "an excellent security system" the implants shouldn't be used alone, and that paper-based ID checking should also take place (Newitz 2006).

The potential for an RFID chip or implant, or its unique identification number, to be cloned, could enable a new kind of identity theft. This could conceivably result from an effort to evade scrutiny or surveillance if RFID chips were routinely used to identify citizens, or to track prisoners. RFID implant identity theft or duplication could stem from a desire to duplicate security access associated with a particular chip. There are reports that identity theft via RFID on cards has already occurred in order to gain access to secure areas or systems (Monahan and Wall 2007).

RFID tags could be used as attack vectors for malicious software or malware or for denial of service attacks. A group from the Free University of Amsterdam has shown that RFIDs can be infected by viruses that can spread via middle ware into databases where they can propagate (van den Hoven 2009). This bodes poorly for the future security of databases based on information obtained from RFIDs, whether this is commercial, medical or security. It poses not only privacy risks, but also potentially security risks, for example in the instance of interactive medical implants linked to infected databases.

Radio frequency signals can be easily jammed to stop or at least complicate system functioning (Rotter et al. 2012a). Malicious attack by hackers using viruses or other disabling activities could pose a very serious risk to the viability of sophisticated management systems

based on RFID, for example in global logistics chain management, transport systems or healthcare. A 2006 study documented the susceptibility of individual RFID tags to computer 'worms' or viruses, which can be spread through radio waves (Knight 2006). The potential for mass communication of such a virus is great: infected RFID tags could infect any other RFID tags with which they came into contact, whether on devices or products, or even in medical RFID implants. Monahan and Wall (2007) warn that the vulnerability of RFID-based systems to hacking or information warfare is "severe"; "systemic vulnerability and risk of sabotage are clear threats to the systems and to any institutions that rely upon them".

In the event that the IOT develops, for example underpinning the basis of urban agriculture in China, as some researchers have proposed (Duan 2012), a virus attack or system malfunction could mean the failure of systems on which people are reliant for basic needs. Although the IOT is often promoted as a resilient one (eg ITU 2005), in some instances it would appear to amplify the vulnerability of systems to technological failure or digital attack. Even some enthusiastic proponents of developing the IOT have warned that in the event of a virus attack, factories could close, social disorder could emerge, perhaps with fatal effects (Liu 2011).

Health-related implants pose the potential for medical-related security breaches, especially where active implants enable remote or wireless access to control drug release or therapies. For example neural interfaces that stimulate the brain have been developed for patients with movement or affective disorders such as Parkinson's disease, chronic pain, tremors associated with multiple sclerosis and dystonia (Tadeusiewicz et al. 2012). Should such a device be 'hacked' or used maliciously, it could have serious implications for the patient (Hildebrandt and Anrig 2012). A malicious attack on an implanted medical device could directly threaten the life of the patient, for example by changing the implant's parameters or triggering the device to cause defibrillation (Rotter and Glasson 2012). Yet most of these devices are currently manufactured without even basic control access measures.

RFID implants that monitor the health status and physiological function of individuals will contain sensitive medical information, and will be designed for this information to be subsequently transmitted to an external device. This presents the potential for a compromise of an individual's privacy, through unauthorized retrieval of this information *in situ* from the chip, or through unauthorised or illegitimate access to or communication of the information once stored externally. Many RFID chips contain unique numeric identifiers that can be linked back to a database containing, in some cases, personal data such as a person's name and health data, and in some instances also financial or security-related information (European Group on Ethics in Science and New Technologies 2005). Given that some of the world's largest petrochemical, investment banking, beverage and energy companies (which presumably have strong IT security systems) have had their internal IT systems hacked, and highly sensitive files stolen (Elgin et al. 2012), this raises questions about the long-term security of patient information.

Accountability and Transparency

A substantive challenge to individuals' privacy, commercial confidentiality and states' sovereignty is associated with the surveillance capabilities of nanotechnology. Smart dust and other sensors could potentially be deployed and retained for many years, not necessarily only during conflict. In fact there may be a strategic advantage to ensuring deployment and effective operation of persistent surveillance systems outside of and in advance of any potential conflict, to provide reconnaissance data and to provide early notice

of any developments or preparation for irregular attacks (Dickson 2007). Similar concerns relate to surveillance carried out by hybrid animals or other very small drones.

Further, there are policy challenges, and arguably ethical challenges, inherent in the strong links between research into military and medical applications of nanotechnology. As noted earlier, development of the next generation of sophisticated nano sensor-based implants, touted as critical to the future of treatments and medical interventions, is being driven by the US military (DARPA 2012). Reflecting on the interface between military research and advances in nanomedicine Monahan and Wall (2007: 155) suggest that physiological surveillance systems will be shaped by and reflect commercial, military and political goals: "there are discernable politics, therefore, in the kinds of systems perceived as valuable, and thus being funded, and in the overlaying of networks for pervasive monitoring onto existing and new infrastructures". Further, they suggest that the act of collecting health data by such systems will itself play a role by "abstract[ing] bodies and physiological systems from social contexts, facilitating hyper-individualized control and commodification of life functions" (p. 155).

Legal Issues

Given these issues there are likely to be a range of legal and regulatory ramifications arising from the convergence between nanotechnology and ubiquitous computing, specifically in the area of privacy and data protection. We note the Opinion of the European Data Protection Supervisor (EDPS 2010: 2): "The EU has a strong data protection/privacy legal framework, the principles of which remain completely valid in the digital age. However, one cannot be complacent. In many instances, ICT raise new concerns that are not accounted for within the existing framework. Some action is therefore necessary to ensure that individual rights, as enshrined in EU law, continue to provide effective protection in this new environment."

In this section of the report we synthesise these concerns and provide a**n** analysis of legal issues and implications.

Data Protection

Researchers have argued that nanotechnology is likely to boost the accessibility and use of body monitoring technologies and implants (Kosta and Bowman 2011). The increasing use of health monitoring equipment is likely to dramatically increase the amount of health and physiological data collected about body functions (heart rate, hormone levels, temperature etc). This new wave of health and physiological monitoring applications will in turn drive new socio-technical feedback mechanisms that in the view of some researchers will mark "the point at which the monitoring of bodies turns into surveillance" (Monahan and Wall 2007).

The European Union has arguably the strictest data protection and privacy legislation in the world, although some observers have pointed to problematic inconsistencies attached to the lack of protections for data obtained or processed for security or law enforcement purposes (Wright et al. 2010). The main legal instrument that applies to the processing of personal data in the European Union is the Data Protection Directive, monitored by an advisory body, the Article 29 Data Protection Working Party (European Commission 2008). Nonetheless, it is interesting to consider how such legislation will interact with a growing body of health data collected in conditions of active consent, for 'health' purposes, often in commercial settings.

Although there are no nano-specific provisions, Europe's privacy laws are designed to be applicable to all technologies. Identity and medical information is required to be processed in accordance with the privacy and data protection regimes such as the Data Protection Directive (European Commission 1995). The deployment in Europe of medical and therapeutic nanotechnologies, nano-ICT human implants and RFID technologies linked to personal data will "most likely" therefore trigger the European data protection legal framework (Kosta and Bowman 2012).

Privacy and security issues associated with data collecting applications and implants have received particular attention. The Organisation for Economic Co-operation and Development has advised that "RFID systems that collect data related to identified or identifiable individuals raise specific privacy issues that should be considered as a priority challenge to the adoption of the technology" (OECD 2008: 5). Nonetheless, data protection challenges associated with RFID are clearly not specific or exclusive to implants, but also surround the growing use of RFID in consumer products, as recognised by the European Data Protection Supervisor (EDPS 2010).

European privacy and data protection provides for strong protection of an individual's rights to privacy, to the processing of their "personal data" and "sensitive data", and for strict obligations for the person or agency responsible for data processing (the 'data controller'). However, we recognise that technical vulnerabilities of RFID chips may call into question the possibility for data controllers to meet legal responsibilities. For example the Data Protection Directive provides that the data subject has the right to be informed whether their personal data are being processed (Kosta and Bowman 2012). The data subject has the right to know the purposes of the processing, the categories of data concerned and the recipients to whom the data are disclosed. Yet presently, RFID chips provide information to any reader that prompts them, with no record that this information has been sought or extracted. This means that irrespective of whether the information held on a RFID chip is of a highly personal or low risk nature, and whether or not it occurs on a work-based authorisation card or in a medical implant, it is vulnerable to unauthorised access and even cloning.

In work of the Article 29 Data Protection Working Party on both RFID (European Commission 2005) and electronic health records (European Commission 2007), strong emphasis has been given to the importance of incorporating privacy by design features, or privacy enhancing technologies in ICT products and electronic systems. Nonetheless, available evidence shows that neither manufacturers of ICT products (such as RFID but also social networking and browser applications), nor data controllers in either the private or public sector have managed to consistently implement or market privacy by design features in their products (EDPS 2010). We note the EDPS' observation that the reasons for this may include lack of economic incentives or institutional support, or insufficient demand. It is also possible that this results from a lack of clarity in legal obligations.

The Data Protection Directive and the ePrivacy Directive require that adequate privacy safeguards are incorporated into RFID and other applications (EDPS 2010). However – and importantly – we note the EDPS Opinion that whereas these two Directives "are helpful towards the *promotion* of privacy by design, in practice they have not been sufficient in *ensuring* that privacy is embedded in ICT" (EDPS 2010: 7). In particular, we highlight the EDPS observation that data protection controllers do not have enough powers to ensure the embedding of privacy by design features or privacy enhancing technologies in products. We therefore emphasise that legal obligations must be adapted to reflect current technological scenarios and to enforce compliance, including through making mandatory incorporation of privacy by design features and settings, deactivation of RFID features at the point of sale as a default, and other measures recommended by the EDPS (2010).

Privacy advocates internationally have suggested that in the future employers, insurance providers or other authorities could require detailed health information, made possible by new-generation nano-diagnostics. At present it appears that there are legal barriers to demands for such access in Europe. Belgian legislation actually rules out the possibility that an employee could provide consent to his or her employer for the processing of sensitive data (which includes health data), given their special relationship (Kosta and Bowman 2011). Further, we recognise that several European documents have already restricted or prohibited the access to health data by employers and insurance providers (for example Recommendation No. R (92) 3 on Genetic Testing and Screening for Health Care Purposes; Recommendation (2002) 9 in the insurance sector; WP29 Working Document on electronic health records, 2007; WP29 Working Document on Genetic Data, 2004). Moreover, we note that the problematic nature of consent provided by employees to employers –mentioned

explicitly in the Belgian law cited above – is a general issue that has been reflected in the data protection debate at both national and international level legislation, as the Council of Europe also experienced during its discussion on Recommendation (89)2. Nonetheless, we stress that in this fast moving area of medical and monitoring development, maintaining privacy protection will require ongoing vigilance to ensure that legal protections remain adequate.

Consent

Companies who choose to RFID label their products may continue to collect data on the handling, and the handlers, of their products, long after the products have left the store. This could be coupled with other forms of data mining to develop a detailed picture of their customers or potential customers. Further, hackers or others able to gain access to stored information about patterns of behaviour, travel preferences or consumption habits of individuals may get access to personal data without the person's informed consent. Electronic health records have already been dogged by scandals revealing many cases of hacking (EDPS 2010).

The issue of consent – in particular, one's inability to provide or withdraw it - may become critical. People may have no real choice to refrain from participating in the digital realm since their belongings will automatically register them and communicate data relating to them (van den Hoven 2009). Whether they like it or not, constellations of RFID tags will mean that individuals increasingly show up in databases as clouds of tagged objects and personal data. Although there are few current examples of IOT-like systems, a recurring concern is that pervasive surveillance, coupled with RFID capability, presents an 'inevitable' future (OECD 2008); that is, where pervasive surveillance and tracking is not optional.

This poses a central challenge to the basis of Europe's privacy and data protection laws, which are founded on the principle of consent. Further, should an internet of things develop, it will encompass widespread use of embedded sensors that possess senses such as smell and sight and which have high levels of computing and communication power. In such a scenario, concepts of 'data request' and 'data consent', on which European privacy laws are anchored, risk becoming outdated (ITU 2005). We note the EDPS (2010) has highlighted the Internet of Things as an area requiring closer attention, including in the implementation of actions proposed by the Commission in its 2009 Communication on the Internet of Things.

Further, the sufficiency of consent as a pre-condition for new nano-based surveillance capabilities is complicated by contemporary trends towards self-surveillance and self-exposure (Wright et al. 2010). Increasing numbers of people purchase electronic applications for their phone or wearable patches to monitor their jogging, workouts or sleep and are happy to share this information with others or to store it online. Increasingly, mobile phone applications are designed to monitor users' preferences for restaurants, entertainment and transport options, and to alert the user to the presence of any friends should they enter the vicinity (Scipioni 2011). Whereas there are increasing calls for greater in built measures to protect the location and behavioural privacy of the users of such applications, information may be willingly shared by individuals without a full understanding of where this data may be aggregated or how it may be used. Indeed the EDPS (2010: 14) observes that "Whereas legally speaking Internet users are considered data controllers and are bound by the EU data protection and privacy legal framework, in reality, they are often unaware of this role. Generally speaking they have a poor understanding that they are processing personal data and that there are privacy and data protection risks involved in publishing such information". New technologies may even be altering people's perceptions

of privacy: researchers in Tel Aviv found that 'smart' phone users were 70% more likely than regular mobile phone users to believe that their phones offered them a high level of privacy (Science Daily 2012a).

The growth of domotics and the emergence of an interlinked internet of things also challenge the principle of consent and complicate the development of policy measures to protect privacy. Researchers actively working on the internet of things have expressed the hope that one day it will enable the automated interlinking of employees' bedside alarm clocks, kitchen coffee pots, their employer's workplace rostering, their town's traffic surveillance systems and their own cars (Science Daily 2012c). Should such a system be established at a city-wide level, it is difficult to see how the principle of consent could be protected; there may be great social pressure to participate, even should an individual wish not to. Further, despite assurances that privacy measures will be built into the internet of things, the effectiveness of such a system relies on a great degree of privacy (location, behaviour, preferences) being relinquished.

The European Group on Ethics takes a strong stand on the extent to which the consent of an individual could qualify as a sufficient legal ground for implantation with an ICT or RFID device (Hildebrandt and Anrig 2012). The EGE seems to conclude that Article 8 of the Convention of Human Rights overrules the consent of the individual in the specific case of human implants, due to the invasive nature of this technology and its potential violation of human dignity.

The EGE finds that the even in the case of consent, the proportionality principle of Article 6 of Data Protection Directive would rule out implants if used to monitor or authorise access to public premises (Hildebrandt and Anrig 2012). Nonetheless, it is interesting to reflect on how such strong views and existing legal protections may intersect with the growing drive towards greater securitisation in Europe. We recognise that each individual's right to privacy is recognised in Article 8 of the European Convention on Human Rights and the relevant case-law. To meet the requirements of this law, public safety needs must always be reconciled with the obligation to respect the principle of proportionality in relation to any measure restricting the fundamental right to privacy. This implies the obligation to demonstrate that any measure taken corresponds to an "imperative social need"; measures which are simply "useful" may not legally restrict fundamental rights and freedoms, including of privacy. However it is possible that what is now considered to be a 'violation of human dignity' will at some future point be deemed to be necessary to protect public safety from a terrorist or other threat. The US Federal government has recently experimented with RFID cards in immigration documents for foreign visitors, while the CEO of the company Digital Applications has stated on National Television that their RFID chip could be used to tag immigrants and monitor their movements (van den Hoven 2009).

Containment

The 'boundary defying' possibilities of nanoscience and nanotechnology pose especial problems for containment as they cut across established regulatory systems. There is already a problem with emerging technologies blurring traditional distinctions between military and civilian applications. For example as developments in genomics proceed, there is a convergence between chemical and biological weapons; such weapons must increasingly be viewed as a "continuous biochemical threat spectrum" (Wheelis and Dando 2005).

Nanotechnology, its applications in neurobiology, pharmaceuticals and sophisticated drug delivery systems, further complicates this. For example nanoparticles developed to

transport therapeutic drugs across the blood-brain barrier could also be used to carry incapacitating or lethal agents (Nordmann 2004). Technologies developed to tailor therapy to an individual's needs could be used to produce chemical or biological warfare agents that would affect only people with certain genetic traits, or a particular individual. Whitman (2011: 110) argues that "once nanotechnology becomes ubiquitous, its capacity to adapt quickly from civilian to military use will be close to an inherent quality of the technology".

Despite concerns over multiple use it is unclear how containment policy could or should operate where a particular technology has socially useful as well as offensive or destructive applications. This has a direct bearing on whether containing some areas of military development is even hypothetically possible. For example the same single carbon nanotube-based radio miniaturisation research that could help enable radio frequency identification (RFID)-based physiological monitoring of patient's health could also support development of smart dust for military use (Aubert 2011). Widespread use of nano RFID-based track and trace and surveillance technologies in medicine or commerce could make limiting the use of the same technologies in a military context impossible – it is unrealistic to expect that the military will not take full advantage of a technology available in commerce (Altmann 2010).

Self Regulation

One of the key ways in which nanotechnology has been regulated is through the use of self-regulatory mechanisms and the use of soft-law (Kearnes and Rip 2009). In the area of privacy and data protection related to the growing use of RFIDs, "Privacy by Design", privacy impact assessments, and adoption of voluntary measures by companies to mitigate risks to privacy were key features of the Privacy Impact Assessment (PIA) framework for RFID applications. This framework was proposed by the industry and endorsed by the Article 29 Working Party in February 2011 (European Commission 2011).

Nonetheless, compliance with any self-regulatory framework for nano-based ICT and RFID devices may not be complete. Voluntary measures for reporting of commercial use of manufactured nanomaterials and related toxicological data have been highly unsuccessful. Initiatives in the United Kingdom, USA and Australia have had very low response and participation rates (Breggin et al. 2009); (NICNAS 2010); (US EPA 2009). For this reason, although self regulatory frameworks are a useful tool, they must remain complemented by the framework of data protection principles which is composed by mandatory requirements.

Compliance even with mandatory requirements may also be incomplete, or interpretation of legal requirements may be unclear. In compliance with the European Directive, privacy and security features have to be ensured in RFID (as in other sectors), as highlighted in the WP29 Working document on RFID (European Commission 2005). This means that it is a mandatory requirement that all RFID implants have built-in privacy and security features. Yet examination of commercial products suggests that this is not universally implemented (EDPS 2010). RFID chips currently answer any reader's request, usually with a message containing their unique identifier, which can be linked to personal data (Rotter et al. 2012a). It therefore appears that this legal responsibility may not be well understood, or may be disputed by some manufacturers. As noted earlier, this may require legal update to ensure that data protection measures reflect the reality of technological use.

Further, technical and economic constraints may be a barrier to effective implementation of privacy protection measures. The OECD (2008) has observed that cost, technical factors and limited availability of privacy by design features may act as barriers to industry's self-regulation. In their current form RFID chips hold too little data for effective encryption or

other data protection measures and can easily be read, rewritten, or destroyed by anyone with the technical means (Monahan and Wall 2007).

Even were new measures to ensure enforcement of mandatory privacy by design features implemented, "innovative and unpredicted cracking techniques are likely to emerge" (OECD 2008: 5). Further, enforcement of only technical measures to support privacy —although useful in their own right— may not adequately address the totality of issues associated with the use of RFID for medical, monitoring or surveillance purposes. Measures to prevent chips responding to interrogation by any reader, or other password-protection-based privacy mechanisms for chips, are likely to rely on humans safeguarding PINs and are unlikely to be entirely reliable.

Finally, there is also a divergence of opinion regarding the extent to which new nano-based surveillance technologies require that existing data protection legislation be updated or supplemented. Researchers have queried the adequacy of existing regulation to safeguard privacy and protect data when this relates to security or surveillance measures, criminal law, and data collected by private parties (Wright et al. 2010). There is also ongoing debate about whether or not the internet of things will require separate data protection legislation, for example as occurred at the recent *4th Annual Internet of Things Europe* conference.

Under-regulation

Nano-weapons are an under-regulated form of military technology in international law. There is an absence of international law that governs the acquisition, development and use of nano-weaponry. This "creates a hiatus where such weapons can be used experimentally and without adequate scrutiny" (Nasu and Faunce 2010, 58).

Nano-weaponry could technically be regulated by existing international agreements such as the Biological and Toxin Weapons Convention or the Chemical Weapons Convention, or those which restrict the use of poisonous gases, blinding laser weapons, anti-personnel mines or cluster munitions, or even under international humanitarian law (although its basic principles remain problematically indeterminate; Nasu and Faunce 2010). However it is likely that unless nanotechnology is used to replicate banned weapons, it could exploit allowances in arms control agreements (Pinson 2004).

There is the potential for other agreements to be adapted to accommodate nanotechnology, for example The Convention on the Use of Certain Conventional Weapons or the Geneva Convention (Whitman 2011). However securing specific nanotechnology-specific measures will be very difficult politically, given both the enthusiasm surrounding nanotechnology's potential in military circles, as well as its cross-cutting and platform characteristics.

Surveillance capability is central to military aspirations for nanotechnology. Yet, the development of non-weapons-based, but still potentially destabilising applications, including in the surveillance sector, falls outside existing arms control treaties (Whitman 2011).

Closing Statement

Given the range of issues we have analysed in this report we recommend that more detailed assessments will be required to fully understand the challenging social, ethical and legal implications of the convergence between nanotechnology and ubiquitous computing.

We also recommend that any future work conducted by the Council of Europe regarding these issues will require a thorough analysis to be carried, entailing close cooperation among the relevant CoE Committees.

References

Altmann, Jurgen (2008), 'Military uses of nanotechnology - Too much complexity for international security?' *Complexity,* 14 (1), 62-70.

--- (2010), 'Military applications: special conditions for regulation', in Graeme A. Hodge, Diana M Bowman, and Andrew D Maynard (eds.), *International handbook on regulating nanotechnologies* (Cheltenham: Edward Elgar Publishing Inc), 372-88.

Aubert, Herve (2011), 'RFID Technology for human implant devices', *Comptes rendus a l'Academie des Sciences,* 1 March 2011,, 1-18.

Balasundaram, Ganesan and Webster, Thomas (2006), 'A perspective on nanophase materials for orthopedic implant applications', *Journal of Materials Chemistry,* 16 (38), 3737-45.

BCC Research LLC (2012), 'Nanotechnology in medical applications: The global market (HLC069B)', (Wellesley, Massachussetts: BCC Research LLC).

Breggin, Linda, et al. (2009), 'Securing the promise of nanotechnologies: Towards transatlantic regulatory cooperation', (London).

Burke, Peter and Rutherglen, Christopher (2010), 'Towards a single-chip, implantable RFID system: is a single-cell radio possible?' *Biomedical Microdevices,* 12 (4), 589-96.

Chapman, Paul (2005), 'Nanotechnology in the pharmaceutical industry', *Expert opinion on therapeutic patents,* 15 (3), 249-51.

Clark, Liat (2012), 'Anonymous targets school for suspending student who refused a tracking chip', <http://www.wired.co.uk/news/archive/2012-11/27/anonymous-texas-rfid-takedown>, accessed November 29.

Cole, David (2012), 'Researchers see 'smart homes' as safety net for elderly', <http://school.eecs.wsu.edu/node/830>, accessed 20 December.

Cook, Diane (2012), 'How smart is your home', *Science,* 335 (6076), 1579-81.

Cribbs, Julian (2007), 'The dwarf lords: Tiny devices, tiny minds and the new enslavement', *Online Opinion*. <http://www.onlineopinion.com.au/view.asp?article=6323>, accessed 21 December 2012.

Cronin, Danielle (2007), '"Nano bionics" gives hope to paraplegics', *The Canberra Times,* 24 May 2007.

DARPA (2012), 'In vivo Nanosensors for Diagnostics (IVN: Dx). Solicitation Number: DARPA-BAA-12-33', <https://www.fbo.gov/index?s=opportunity&mode=form&id=68a4659ef859ffdff9222df42b5230bb&tab=core&_cview=0>, accessed 8 December.

de Saint-Exupery, Antoine (2009), 'Internet of things: Strategic research roadmap', (Surrey: Internet of Things Initiative).

Dickson, Scott A (2007), 'Enabling battlespace persistent surveillance: The form, function, and future of smart dust', *Blue Horizons Paper* (Maxwell, USA).

Drexler, K E (1986), *Engines of Creation: The Coming Era of Nanotechnology* (New York: Anchor Books).

Duan, Yan-e (2012), 'Research on IOT technology and IOT's application in urban agriculture', *Advanced Materials Research,* 457-458, 785-91.

EDPS (2010), 'Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy', (Brussels: European Data Protection Supervisor).

Elgin, Ben, Lawrence, Dune, and Riley, Michael (2012), 'Coke gets hacked and doesn't tell anyone', *Bloomberg* <http://mobile.bloomberg.com/news/2012-11-04/coke-hacked-and-doesn-t-tell.html>, accessed November.

European Commission (1995), '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 [the "Data Protection Directive"]'.
--- (2004), 'Towards a European Strategy for Nanotechnology', (Luxembourg: Commission of the European Communities).
--- (2005), 'Article 29 Data Protection Working Party: Working document on data protection issues related to RFID technology. 10107/05/EN WP 105', (Brussels).
--- (2007), 'Article 29 Data Protection Working Party: Working Document on the processing of personal data relating to health in electronic health records (EHR). 00323/07/EN WP 131', (Brussels).
--- (2011), 'Privacy and data protection impact assessment framework for RFID applications. 12 January 2011'.
European Group on Ethics in Science and New Technologies (2005), 'Ethical aspects of ICT implants in the human body', in Stefano Rodotà and Rafael Capurro (eds.), (Brussels: European Commission,).
Feynman, R (1960), 'There's plenty of room at the bottom: an invitation to enter a new field of physics', *Engineering and Science,* 23 (5), 22-36.
Foster, AL (2006), 'The bionic CIO: Harvard Medical School's technology chief tests a controversial implant on himself', *The Chronicle of Higher Education,* 52 (41), A30-32.
Future Homes 500 (2012), 'Future Home', <http://www.futurehomes500.com/>, accessed 20 December 2012.
Grieger, Khara D, et al. (2012), 'Environmental risk analysis for nanomaterials: Review and evaluation of frameworks', *Nanotoxicology,* 6 (2), 196-212.
Hildebrandt, Mireille and Anrig, Bernhard (2012), 'Ethical implications of ICT implants', in Mark N Gasson, Eleni Kosta, and Diana M Bowman (eds.), *Human ICT Implants: Technical, Legal and Ethical Considerations, Information Technology and Law Series 23* (The Hague, The Netherlands: Asser Press).
Humphreys, S (2011), *Navigating the Dataverse: Privacy, Technology, Human Rights* (Geneva: International Council on Human Rights Policy).
Hunter, R (2002), *World Without Secrets: Business, Crime, and Privacy in the Age of Ubiquitous Computing* (Chichester: Wiley).
ITU (2005), 'The Internet of Things', (Geneva).
Jensen, K, et al. (2007), 'Nanotube radio', *Nano Letters,* 7 (11), 3508-11.
Jones, R. A. L (2011), 'What has nanotechnology taught us about contemporary technoscience?' in T Zülsdorf, et al. (eds.), *Quantum Engagements: Social Reflections of Nanoscience and Emerging Technologies* (Amsterdam: IOS Press), 13-26.
JRC (2008), 'Nanomedicine: Drivers for development and possible impacts', in Volker Wagner, et al. (eds.), (Seville: European Commission Joint Research Centre, Institute for Prospective Technological Studies,).
Kearnes, M B and Rip, A (2009), 'The emerging governance landscape of nanotechnology', in S Gammel, A Lösch, and A Nordmann (eds.), *Jenseits von Regulierung: Zum politischen Umgang mit der Nanotechnologie* (Berlin: Akademische Verlagsgesellschaft).
Knight, Will (2006), 'RFID worm created in the lab', *New Scientist*, (15 March 2006,).
Kosta, Eleni and Bowman, Diana M (2011), 'Treating or tracking? Regulatory challenges of nano-enabled ICT implants', *Law and Policy,* 33 (2), 256-75.
Leake, Christopher (2006), 'Six-inch Talibanator; It's the SAS's newest weapon... a remote controlled 'toy' plane that wipes out enemy snipers on impact', *The Mail on Sunday, 16 July*.
Liu, Pu (2011), 'A brief research of the internet of things', *Applied mechanics and materials,* 55-57, 1679-82.

Lyon, D (ed.), (2003), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London: London).

Minchin, Philippe (2012), 'Nano surveillance takes off', *Intersec: The Journal of International Security,* Nov/ Dec 2012.

Monahan, Torin and Wall, Tyler (2007), 'Somatic surveillance: Corporeal control through information networks', *Surveillance and Society,* 4 (3), 154-73.

Murakami Wood, D (ed.), (2006), *A Report on the Surveillance Society* (Report to the UK Information Commissioner by the Surveillance Studies Network. Wilmslow, UK: Information Commissioner's Office).

Nasu, Hitoshi and Faunce, Thomas A (2010), 'Nanotechnology and the international law of weaponry: Towards international regulation of nano-weapons', *Journal of Law, Information and Science,* 20, 21-53.

NATO (2005), '179 STCMT 05 E - The security implications of nanotechnology', (NATO Parliamentary Assembly,).

NICNAS (2010), 'Nanomaterials: Summary of 2008 call for information on the use of nanomaterials', (Sydney: Australian Government, Department of Health and Ageing).

NRC (2003), 'An assessment of non-lethal weapons science and technology', (Washington DC).

OECD (2008), 'Radio-frequency identification (RFID): A focus on information security and privacy', *OECD Digital Economy Papers* (138; Paris: OECD).

Pinson, Robert D (2004), 'Is nanotechnology prohibited by the biological and chemical weapons conventions?' *Berkeley Journal of International Law,* 22 (2), 279-309.

PR Web (2012), 'State of New Jersey awards Radiant RFID 5-year emergency management solution contract', *San Francisco Chronicle,* 18 October 2012.

Raab, C, et al. (2010), *An Update Report on Developments Since the 2006 Report on the Surveillance Society* (Report to the UK Information Commissioner by the Surveillance Studies Network. Wilmslow, UK: Information Commissioner's Office).

Resnik, D. B. and Tinkle, S. S. (2007), 'Ethical issues in clinical trials involving nanomedicine', *Contemporary Clinical Trials,* 28 (4), 433-41.

Reuters (2006), 'Israel developing anti-militant 'bionic hornet'', 17 November 2006.

Robinson, Joshua A, et al. (2012), 'Investigation of graphene-based nanoscale radiation sensitive materials', in Thomas George, M. Saif Islam, and Achyut Dutta (eds.), *Micro- and Nanotechnology Sensors, Systems, and Applications IV* (SPIE Proceedings).

Rotter, Pawel, et al. (2012), 'Potential application areas for RFID implants', in Mark N Gasson, Eleni Kosta, and Diana M Bowman (eds.), *Human ICT Implants: Technical, Legal and Ethical Considerations, Information Technology and Law Series 23,* (The Hague, The Netherlands: Asser Press), 29-39.

Royal Society and Royal Academy of Engineering (2004), *Nanoscience and Nanotechnologies: Opportunities and Uncertainties* (London: Royal Society and Royal Academy of Engineering).

Ryan, M A (2012), 'The process of developing an instrument: the JPL electronic nose', in Thomas George, M. Saif Islam, and Achyut Dutta (eds.), *Micro- and Nanotechnology Sensors, Systems, and Applications IV* (Baltimore, Maryland: SPIE Proceedings).

Science Daily (2012a), 'Smart phones are changing real world privacy settings. 10 May 2012', *Science Daily*.

--- (2012), 'First the smart phone, now the smart home: Technology anticipates, meets our needs for health, efficiency. March 29', <http://www.sciencedaily.com/releases/2012/03/120329170435.htm>, accessed 20 December.

--- (2012c), 'The internet of things: Smart houses, smart traffic, smart health. 26 June', *Science Daily*.

Scipioni, Marcello Paolo (2011), 'Towards privacy-aware location-based recommender systems.' *IFIP Summer School 2011* (Trento, Italy).

Shipbaugh, Calvin (2012), 'Basic research interests in nanoscale radiation sensing', in Thomas George, M. Saif Islam, and Achyut Dutta (eds.), *Micro- and Nanotechnology Sensors, Systems, and Applications IV* (Baltimore, Maryland: SPIE Proceedings).

University of Hertfordshire (2012), 'Energy-efficient intelligent house that can monitor health', <http://www.herts.ac.uk/news-and-events/latest-news/Intelligent-House.cfm>, accessed 20 December.

US EPA (2009), 'Nanoscale Materials Stewardship Program Interim Report', (Washington DC,: US Environmental Protection Agency, Office of Pollution Prevention and Toxics).

Wachsmuth, Lisa (2012), 'Bionic implant offers epilepsy hope', *Illawarra Mercury,* 30 November 2012.

Wallace, G, et al. (2012), 'Nanobionics: The impact of nanotechnology on implantable medical bionic devices', *Nanoscale,* 4, 4327-47.

Weiss, Rick (2007), 'Dragonfly or insect spy? Scientists at work on robobugs', *Washington Post,* 9 October 2007.

Wheelis, Mark and Dando, Malcolm (2005), 'Neurobiology: A case study of the imminent militarization of biology', *International Review of the Red Cross,* 87 (859), 560.

Whitman, Jim (2011), 'The arms control challenges of nanotechnology', *Contemporary Security Policy,* 32 (1), 99-115.

Wright, David, et al. (2010), 'Sorting out smart surveillance', *Computer Law and Security,* 26 (4).

Zhang, Min, Yu, Tao, and Zhai, Guofang (2011), 'Smart transport system based on "the internet of things"', *Applied mechanics and materials,* 48-49, 1073-76.