# Privacy, security and data protection in smart cities: a critical EU law perspective

*Lilian Edwards*[1]

## I. Introduction

"Smart cities" are a buzzword of the moment. Although legal interest is growing, most academic responses at least in the EU, are still from the technological, urban studies, environmental and sociological rather than legal, sectors[2] and have primarily laid emphasis on the social, urban, policing and environmental benefits of smart cities, rather than their challenges, in often a rather uncritical fashion[3] . However a growing backlash from the privacy and surveillance sectors warns of the potential threat to personal privacy posed by smart cities[4]. A key issue is the lack of opportunity in an ambient or smart city environment for the giving of meaningful consent to processing of personal data; other crucial issues include the degree to which smart cities collect private data from inevitable public interactions, the "privatisation" of ownership of both infrastructure and data, the repurposing of "big data" drawn from IoT in smart cities and the storage of that data in the Cloud.

This paper, drawing on author engagement with smart city development in Glasgow as well as the results of an international conference in the area curated by the author, argues that smart cities combine the three greatest current threats to personal privacy, with which regulation has so far failed to deal effectively; the Internet of Things(IoT) or "ubiquitous computing"; "Big Data" ; and the Cloud. While these three phenomena have been examined extensively in much privacy literature (particularly the last two), both in the US and EU, the combination is under-explored. Furthermore, US legal literature and solutions (if any) are not simply transferable to the EU because of the US's lack of an omnibus data protection (DP) law. I will discuss how and if EU DP law controls possible threats to personal privacy from smart cities and suggest further research on two possible solutions: one, a mandatory holistic privacy impact assessment (PIA) exercise for smart cities: two, code solutions for flagging the need for, and consequences of, giving consent to collection of data in ambient environments.

The paper falls into five main sections.

[1] Professor of E-Governance, University of Strathclyde, Glasgow. My thanks to Anastasia Gubanova, LLM candidate at the University of Strathclyde, for helpful and timely research assistance; and to CREATe and the Horizon Digital Economy Hub at Nottingham for helping sponsor the international conference, *Designing Smart Cities? Opportunities and Regulatory Challenges*, Strathclyde, April 2015 from which many insights were drawn for this paper. This research was thus supported by the RCUK funded Centre for Copyright and New Business Models in the Creative Economy (CREATe), AHRC Grant Number AH/K000179/1.A full web resource of the conference can be found at http://www.create.ac.uk/blog/2014/11/06/designing-smart-cities/ and papers from the conference were published as a special edition of the journal of Society for Computers and Law (SCL Journal, vol 26, issue 2, June 2015/July 2015 (http://www.scl.org/site.aspx?i=is43131 ) some of which are referred to below. My thanks also to Lachlan Urquhart (doctoral candidate, Horizon) who provided enormously useful research assistance for the conference, and editorship for the special edition; to all the speakers at the conference, whose expertise has helped me accelerate up my learning curve about smart cities; and particularly to Francesco Sindico (also of Strathclyde) who took charge of the environmental and energy side of the conference. Finally thanks are owed to the participants in the Amsterdam Privacy Law Scholars Conference 2015 where this paper was workshoped, especially Bert-Jan Koops and Eleni Kosta, and to Daithi MacSithigh for helpful reading and comments. The usual disclaimer applies. Links were all checked as valid as of 7 October 2015.

[2] See discusion in Annalisa Cocchia *Smart and Digital City: A Systematic Literature Review* ( Springer, 2014); also overview in the leading text Townsend, A *Smart cities : big data, civic hackers, and the quest for a new utopia* (W.W.Norton and Co, 2014).

[3] Rob Kitchin's *Programmable City* project, infra n 60 and Adam Greenfield,infra n 56, are outstanding counter-examples however

[4] See eg David Murakami Wood's surveillance studies Ubicity project at Queens Ontario infra n 104.

First, I sketch the rise of smart cities globally, both in the West and East and the less developed South, and discuss the key technological, economic and political drivers which have made them an unstoppable part of the future urban living conditions of  much of the global population. Rather than giving one formalistic definition of smart cities which will inevitably be a moving target and may not aid legal analysis, I try to sketch their key characteristics, focusing on two which are clearly problematic from a privacy frame: first, their dependence on technological infrastructures, big data, the IoT and the Cloud; and second , their financing and hence "ownership" in almost all cases by public-private partnerships (PPP).

Second, I lay out the well known vulnerability of smart cities, along with other venues for embedded IoT systems, to security threats and how this is approached by the law in the EU. This section covers well trodden ground and is therefore relatively short. It should be noted that considerations of "privacy" (wrongly so named and limited) in smart cities often stop here.

Thirdly, I turn to broader issues of  conceptual privacy law frameworks, and lay out what may be perceived as a basic underlying theoretical problem, ie,  that smart cities are, in essence, public places while traditionally privacy laws such as art 8 of the European Convention on Human Rights (ECHR) and US privacy torts have applied to private "bubbles" or zones focused on the body, the home and private communications. Drawing on ECHR case law as well as attitudinal research, I argue reasonable expectations of privacy even in public spaces, as in smart cities, are now both recognised by European law and needed by urban dwellers.

Fourthly, in the most crucial section of the paper, I address in some detail the three key threats to privacy and DP  already identified – the IoT, Big Data and the Cloud - and outline how each problem manifests itself to endanger the privacy of  smart city residents and users. In each sub-section I then try briefly to analyse how, and how well, EU DP law currently deals with regulating, preventing or solving these threats.

This section concludes pessimistically. Despite the many recent rhetorical assertions, politically required by the lobbying wars of the draft General DP Regulation (GDPR) and the Silicon Valley ideological thrust towards "permissionless innovation[5]",  that DP law remains fit for purpose in principle, and merely needs tweaked in its detail to address technological challenge, in fact, a number of key challenges so far appear relatively insuperable by legal regulation alone. Notable amongst these is  the issue of how to obtain meaningful prior consent in Internet of Things systems, especially where data is collected in public, as eg in smart road or smart transport systems. A second key issue identified is how ordinary users can have any feeling of control over the processing of their data when "big data" drives a coach and horses through the notion of purpose limitation and data minimisation, and the algorithms used to create inferences from it are opaque and capricious to them. Finally I note that in a post *Schrems* and Snowden world, the dependence of smart cities on Cloud infrastructure which may be located anywhere in the world also makes them highly dubious from an EU DP point of view.

Thus, in the fifth section, I turn to some solutions drawn not from law, but from "code" in the Lessigian sense, and discussion of Privacy by Design (PbD).  Three particular avenues for further promising investigation  are identified: (i) exploring the development of a holistic privacy impact assessment (PIA) for smart city data flows; (ii) finding new means for obtaining some kind of  standing or "sticky" consent to data processing decoupled in time from when the data is actually pervasively collected via the IoT; (iii) implementing a legal right to algorithmic transparency and finding ways of making this knowledge useful to ordinary users.

In conclusion however, the paper reverts to pessimism with the view that to preserve  privacy in smart cities we may need to move away from the liberal notion of "notice and choice" or, in

[5] Infra, n xx.

European terms, “consent” and informed specific control over processing, entirely, and look instead to an “environmental” model of toxic processes which should be banned or restricted notwithstanding user permission or substitute grounds for processing. This view, which is only tentiavely introduced here, will be justified further in future work.

## II. The Rise of Smart Cities

Increasingly, we live in cities. In the last two decades, urban centres have become the destination of choice for citizens and businesses seeking prosperity, stability and social and educational facilities, leading to the progressive abandonment of rural areas and the rising concentration of population within metropolitan areas. Over half the world’s population already lives in cities: by 2050, 66% of the world’s population are expected to live in urban areas, with nearly 90% of that increase in Asia and Africa.[6] This urbanisation process has become so prominent that in some states (eg, South Korea) the capital city generates as much as half of the country’s GDP[7] : cities are thus sometimes becoming regarded as more important than the countries in which they are located[8]. National governments often now establish ministries for cities (eg, in Brazil, India, UK)[9] while local city mayors, spearheading city redevelopment and expansion, have acquired significant standing and global reputations in cities like London, New York, Barcelona and Rio[10].

But cities bring with them serious challenges. Globally, high urban density seems inevitably to lead to problems including traffic congestion, energy supply and consumption issues, escalation of greenhouse gases emissions[11], unplanned development, lack of basic services, dramatic increase in waste disposal needs, and increases in crime and antisocial behaviour[12]. The political and social need to combat these problems (in particular, the rise of environmental concerns, as climate change worries become ever present), combined with the obvious potential for a lucrative market for technology and telecommunications companies developing digital and networked solutions (e.g. IBM[13], Cisco[14], Vodafone[15]), has given rise to the buzzword concept of *smart cities*[16]. This idea has been subsequently eagerly leapt on by national and municipal

[6] See UN Department of Economic and Social Affairs, *“World Urbanisation Prospects”*. United Nations, New York, 2014 revision, p. 1, available at http://esa.un.org/unpd/wup/Highlights/WUP2014-Highlights.pdf .

[7] According to Frost and Sullivan, Seoul accounts for approximately 50% of the country’s GDP; in Hungary and Belgium, Budapest and Brussels each account for 45%. See Frost and Sullivan, *Sense and the City. The application of Internet of things technologies for a more sensible city* (2014), p, 2, at http://www.frost.com/c/481418/sublib/display-market-insight.do?id=291820991 .

[8] See Sarwant Singh, *“Smart Cities – A $1.5 Trillion Market Opportunity”*. Forbes / Business (June 20, 2014), at http://www.forbes.com/sites/sarwantsingh/2014/06/19/smart-cities-a-1-5-trillion-market-opportunity/ .

[9] See Emily Moir, Tim Moonen and Greg Clark, Essay *“The future of cities: what is the global agenda?”* The Business of Cities (2014), p. 5, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/429125/future-cities-global-agenda.pdf [last visited September 3, 2015]

[10] Francesco Sindico, paper given at *Designing Smart Cities* (supra n1).

[11] Cities produce 50% of global waste and account for 60-80% of global greenhouse emissions. See UNEP (United Nations Environment Programme), *The Global Initiative for Resource Efficient Cities*, at http://www.unep.org/resourceefficiency/Policy/ResourceEfficientCities/Activities/GI.REC/tabid/771769/Default.aspx .

[12] See Edward L. Glaeser and Bruce Sacerdote “Why Is There More Crime in Cities?” Journal of Political Economy, Vol. 107, no. 6, part 2 (December 1999) 225.

[13] See at http://www.cisco.com/web/strategy/smart_connected_communities.html .

[14] See at http://www-03.ibm.com/innovation/us/thesmartercity/ .

[15] See eg Vodafone’s offer to let you design your own smart city a a game at http://www.designyourqatar.qa/ .

[16] The first study concerning the concept of smart cities is believed to date back to 1994. See, e.g. R.P. Dameri and A. Cocchia, *“Smart City and Digital City: Twenty Years of Terminology Evolution”*. ITAIS – Italian Conference of Information Systems (2013), p. 4, available at http://www.cersi.it/itais2013/pdf/119.pdf . The current leading academic non-vendor text is perhaps Townsend, supra n X..

political leaders, major global tech corporations, and international institutions and organizations alike (e.g. European Commission[17], OECD[18], ISO[19]) . Kitchin describes smart cities as an attempt to solve the fundamental conundrum of cities – reducing costs and creating economic growth, while at the same time producing sustainability, participation, an acceptable standard of civic services and quality of life - but warns that there are many different conceptions of smart cities and that a neo-liberal, market led, technocratic perspective tends to dominate, as opposed to an alternative paradigm, which is to see smart cities as "citizen centric", fostering social innovation, justice and engagement in what he terms a "smart society" [20]. Such dominance by the pure economic gain perspective may be damaging for consideration of both social needs and appropriate legal regulation, something which is beginning to trickle through as a concern in European policy circles, despite the general "relentlessly positive[21]" discourse around smart cities[22].

There is currently no single accepted definition of a "smart city" [23] and much depends on who is supplying the characteristics: industry, politicians, civil society and citizens/users are four immediately and obviously disparate sets of stakeholders. It is easier perhaps not to define smart cities but to elaborate their key features. The interlocking key infrastructure that is most often mentioned as making cities "smart" includes:

- networks of *sensors* attached to *real world objects* such as roads, cars, fridges[24], electricity meters, domestic appliances and human medical implants which connect these objects to digital networks (*the "Internet of Things"(IoT)*[25] , "ubiquitous computing" or ubicomp, or as Greenfield calls it, "Everyware"[26]). These IoT networks generate data in particularly huge amounts known colloquially as "*big data*" (see below).
- networks of digital communications enabling *real time data streams* which can be combined with each other and other and then be mined and repurposed for useful results;
- *high capacity , often cloud based, infrastructure* which can support and provide storage for this interconnection of data, applications, things and people.

[17] See, e.g. European Commission, *"Europe 2020: A strategy for smart, sustainable and inclusive growth"*, COM/2010/2020 FIN adopted 03/03/2010 at http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52010DC2020.

[18] See, e.g. OECD, *Science, Technology and Industry Outlook 2014*, OECD Publishing, at http://www.oecd.org/sti/oecd-science-technology-and-industry-outlook-19991428.htm .

[19] See, e.g. ISO (International Organization for Standardization), *Smart Cities.* Preliminary report 2014, ISO/IEC JTC 1 Information technology (2015), at http://www.iso.org/iso/smart_cities_report-jtc1.pdf .

[20] Rob Kitchin "The Promises and Perils of Smart Cities", in SCL special edition, supra n 1, at http://www.scl.org/site.aspx?i=ed42789 .

[21] See David Murakami Wood "Smart City, Surveillance City", in SCL special edition, supra n 1, at http://www.scl.org/site.aspx?i=ed43113 .

[22] See notably the statement in the recent European Parliament report on *Big Data and Smart Devices and their Impact on privacy* (Study for the LIBE Committee, September 2015) at http://www.statewatch.org/news/2015/sep/ep-study-big-data.pdf that "the European Commission perspective [on the Digital Single Market] is very much commercially and economically driven, with little attention paid to the key social and legal challenges regarding privacy and data protection." Coming as it does as an intervention from one EU institution to another as the GDPR goes into trialogue negotiations, this is an extremely barbed statement.

[23]. See comparison of terminologies for smart cities in Cochia, supra n X, pp. 18-19; see also De Santis R., Fasano A., Mignoll N., Villa A., *"*Smart city: fact and fiction*"*. Munich Personal RePEc Archive, Paper No. 54536 (March 15, 2014), pp. 3-6, at https://mpra.ub.uni-muenchen.de/54536/1/MPRA_paper_54536.pdf .

[24] The iconic dream of the smart connected fridge has finally entered the mass market via Amazon Dash – see "Amazon makes a Dash to take lead in the internet of things", *FT*, October 5 2015 at http://www.ft.com/cms/s/0/721c3c98-6a91-11e5-aca9-d87542bf8673.html#axzz3ntnpveRW .

[25] Discussed and defined in full at pp xx below.

[26] Adam Greenfield *Everyware: the dawning age of uniquitous computing* (2006, New Riders).

The claims made for smart cities in their advertising and similar hype vehicles are important both in their perception and execution. Smart cities are said to "*interconnect people, data, things, and processes under a dynamic global infrastructure"* [27]. Smart cities then utilise this networked infrastructure in order "*to improve economic, resource and political efficiency while enabling social, cultural and.. urban development.*"[28] As Bob Pepper, VP of Global Technology Policy for Cisco (a leading smart city vendor) put it: "*What makes a city smart is that it recognises the centrality of technology and information to improve its processes*"[29].

Scanning through numerous smart city projects and initiatives currently undertaken, eight key activities can be identified that often define a smart city, ie,

- smart governance,
- smart infrastructure,
- smart building,
- smart connectivity,
- smart healthcare,
- smart energy,
- smart mobility and
- smart citizens.[30]

These aspects are often used in comparative studies as indicators describing how "smart" urban areas are, for the purpose of ranking cities, often in a funding context.[31] For instance, according to the 2015 Juniper Research report, Barcelona is currently at the the top of the list of "smart cities", due to its all-encompassing use of new technologies, including a smart traffic light system which sets the lights at green until fire engines have passed, emergency response devices installed in the individual's home and connected through a (land or mobile) telephone line to a Call Centre, which can be contacted at the simple press of a button, and other innovations[32]. New York City, London, Nice and Singapore[33] currently round out the top five.[34] This ranking, has become critically important in recent years in driving future city developments and investments by both government and industry[35]; "smartness" has become a competitive index among cities for attention, funding and inward investment.

Smart cities are, accordingly, a global social, economic and political, as well as technological phenomenon. In the developed north, cities tend to be "retrofitted", or retrospectively

[27] See Roberto De Bonis and Enrico Vinciarelli, *"*From Smart Metering to Smart City Infrastructure. Could the AMI Become the Backbone of the Smart City?*",* Smart 2014: The Third International Conference on Smart Systems, Devices and Technologies (2014).

[28] United Nations, Bureau International des Expositions, Shanghai 2010 World Exposition Executive Committee. *Shanghai Manual – A Guide for Sustainable Urban Development of the 21st Century*, Chapter 8 (2010), p. 2.

[29] Quoted in Ellen P Goodman ed *The Atomic Age of Data: Policies for the Internet of Things* (Report of the 28th Annual Aspen Institute Conference on Communications Policy), Washington DC, 2015.

[30] See, e.g. Frost and Sullivan (2014), supra note 5, at p. 3; see also Rudolf Giffinger, Hans Kramar, Nataša Pichler-Milanović, *Smart City Profiles. Deliverable 2.1. Part 1*. PLEEC (May 2014) p. 5, available at http://www.pleecproject.eu/downloads/Reports/Work%20Package%202/Smart%20City%20Profiles/pleec_d2_1_smart_city_profiles_introduction.pdf .

[31] See, e.g. Rudolf Giffinger, Gudrun Haindlmaier and Hans Kramar, *"The Role of ranking in growing city competition"*. Urban Research and Practice (November 25, 2010): vol. 3, issue 3, pp. 299-312

[32] See at http://smartcity.bcn.cat/en .

[33] See Melissa Low "Many Smart Cities, One Smart Nation – Singapore's Smart Nation Vision", SCL special edition supra n 1 at http://www.scl.org/site.aspx?i=ed42881 .

[34] See Sam Smith, *"*Barcelona named 'Global Smart City - 2015'*"*. Juniper Research (February 17, 2015), at http://www.juniperresearch.com/press/press-releases/barcelona-named-global-smart-city-2015 .

[35] See Rudolf Giffinger, Gudrun Haindlmaier, *"*Smart Cities Ranking: An Effective Instrument for the Positioning of Cities?*"*, ACE: Architecture, City and Environment (February 25, 2010): vol. 4, issue 12, p. 7 .

reconsidered as "smart", to meet environmental, social, political or business targets. In the UK, smart cities are being actively promoted by the state via investment in "smart city demonstrators" placed in various cities, and via agencies such as Innovate UK (formerly NESTA), BIS (the government ministry for trade and industry), a state sponsored "digital catapult" worth £50m, and a 2015 £40m IoT initiative - all justified by the hope that the UK will become a world leader in this field, able "*to take advantage of up to a $40 billion share of the [£400 billion global] market place [for smart cities] by 2020*"[36]. In 2013, Glasgow, Scotland won a £24 million grant as smart city demonstrator, and used the funds, building on some existing infrastructure, to develop a series of initiatives, including intelligent street lights that brighten when pedestrians and cyclists are near and dim if there is less activity; a network of sensors installed under roads generating data which allows adjustable traffic lights to reduce traffic jams; a state of the art "smart CCTV" control centre; and a "data repository" of open civic data which can be exploited by academic researchers.[37] As a result it was claimed that "international acclaim" came in the form of a Geospatial World Excellence Award "*for providing leadership in demonstrating how older, more established cities can be transformed into Smart Cities of the future*".[38] Smart cities are thus not just a matter of producing less polluted or more efficient cities, but generate considerable political capital and big business opportunities along with a large potential export market[39].

In the developing world, smart cities are equally politicised but often play a different role, of enabling modernisation and development, responding to problems arising from population pressure, climate change, migration and rural to urban transition. Non-Western smart cities are often created from scratch "top down" rather than retrofitted[40]. India for example has vowed to create 100 new smart cities , allocating £760m to the project[41]. Most such developments are inspired by the "global east" (eg Japan, Singapore, Korea) : Africa is as yet not really on the smart cities map, though there are developments in, eg, South Africa[42]. Developing countries smart cities attract a different set of criticisms, that they are vehicles for creating gated smart enclaves of privilege, in a sea of millions of technology-deprived poor, are often established by compulsory and controversial land acquisition policies[43].

Smart city funding is significant. Historically, particularly in Europe, financial support from the cash-stricken post-recession public sector, at either national or municipal level, has not generally been sufficient to finance the radical technological deployments involved. Instead financing

[36] See BIS press release, 18 December 2013, at https://www.gov.uk/government/news/uk-set-to-lead-the-way-for-smart-cities .

[37] See Hamish Camdonell, *"Glasgow: the making of a smart city"*. The Guardian (April 21, 2015), available at http://www.theguardian.com/public-leaders-network/2015/apr/21/glasgow-the-making-of-a-smart-city . See further at http://futurecity.glasgow.gov.uk/ .

[38] See James Perkins, *"Future City Glasgow project recognized with two awards"*. Digital by Default News (July 2, 2015), available at http://www.digitalbydefaultnews.co.uk/2015/07/02/future-city-glasgow-project-recognised-with-two-awards/ .

[39] Within the academic economy, smart cities are also seen as a tempting opportunity to attract funding and kudos: major centres of research have been established (to name a few) at Fordham University (US), University College London (UK), Strathclyde Future Cities Unit (Scotland) and the Universitat Politècnica de Catalunya (Spain).

[40] An exception is Stellenbosch in South Africa which aspires to be a "smart town" enabled by proximity to major universities: see n 39 infra.

[41] See http://www.theguardian.com/cities/2015/may/07/india-100-smart-cities-project-social-apartheid . "India is going to see a huge urbanisation, the latest McKinsey study says by the year 2030 we will have 350 million [more] Indians getting into the process of urbanisation, by 2050, 700 million".

[42] See http://www.theguardian.com/global-development-professionals-network/2013/nov/21/smart-cities-relevant-developing-world .

[43] See the furore round the Indian Land Acquisition Act 2013 as amended : eg see https://in.news.yahoo.com/the-questions-we-should-be-asking-frequently-about-the-land-acquisition-act-060820434.html .

tends to be by Public-Private Partnership (PPP) [44], which can be defined as "*agreements between a public agency (federal, state or local) and a private-sector entity that uses the specific skills and assets of each sector for the delivery of a service for the general public.*"[45] A vaunted successful example of PPP funding is the Intelligence Operations Center in Rio de Janeiro which was built by IBM in preparation for the 2014 World Cup and 2016 Olympic Games.[46] Rio was regarded as one of the most dangerous cities on earth and there was felt to be a need to somehow reassure the influx of global visitors expected for the Olympics and World Cup. Hundreds of cameras and countless other sensors and devices placed throughout the city live-stream data onto a giant video wall of the Center for 24/7 monitoring, allowing city operators to immediately respond to crime, accidents, power outages, torrential storms and other occurrences. The Centre's citywide system, integrating data from some 30 agencies, was described by Anne Altman, general manager for IBM's Global Public Sector, as an all–seeing eye that can "*accurately gather, analyse, and act on information about city systems and services*" and "*recognizes the behaviour of the city as a whole.*"[47]

Such an example raises pointedly the question of who (if anyone) owns the data that smart cities produce and process in such vast amounts. Policing, surveillance, crowd control, emergency response, are all historically state functions, and citizens might expect the very sensitive data involved to be held by the state. Yet the likelihood in a PPP built city is that that data finds itself (at least partially or non exclusively[48]) in private control. Balabanovic and Galwas, who work at the centre of the UK smart cities industry, nonchalantly mention that "*City governments assume they will control smart city services, but we predict the E2C ["Environment-to-Citizen"] market will inevitably be dominated by global consumer services*", and cite the dominance over public sector offerings of existing private sector consumer applications in sectors such as maps, taxis, transport planning and fitness tracking; and the tendency of these markets to winner-takes-all network effects[49].

The lack of universal open or proprietary standards for exchange of data is another key issue driving data into private silos. The EU is attempting to mitigate this with by funding attempts to build interoperable protocols for private tech suppliers operating in smart cities, particularly in fields like energy and, generally, IoT systems[50]. Open data is often mentioned as a key matter for citizen engagement in smart cities eg the Glasgow data repository noted above is open to researchers; Rio also made a data portal open to the public with key datasets[51]. But as a worst case, a smart city may become the private data fiefdom of a monopoly technology or telecoms

[44] See Smart Cities Council, *Smart cities Financing Guide* (August 24, 2015), at http://smartcitiescouncil.com/resources/smart-cities-financing-guide and Smart Cities Stakeholder Platform, *Financing models for smart cities*, version 2.0 (November 2013), at https://eu-smartcities.eu/sites/all/files/Guideline-%20Financing%20Models%20for%20smart%20cities-january.pdf .

[45] Smart Cities Council (2015), supra, at 48.

[46] See BIS Research Paper No. 135, *Global Innovators: International Case Studies on Smart Cities*. ARUP, London, UK (October 2013), pp. 13-17, at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/249397/bis-13-1216-global-innovators-international-smart-cities.pdf .

[47] *"Intelligence Cities Forum: Anne Altman"*, National Building Museum (June 6, 2011), at http://www.nbm.org/media/video/intelligent-cities/forum/intelligent-cities-forum-altman.html . See also discussion in section 3 of BIS Research paper No 135 *Global innovators: International Case Studies on Smart Cities*, supra n 44.

[48] Rio claimed they received about 35% of municipal "smart" spending from private companies (see BIS paper, supra n 44).

[49] See Marco Balabanovic and Paul Galwas "Whose Smart City is it Anyway?" in SCL special edition, supra n 1 at http://www.scl.org/site.aspx?i=ed42880 ..

[50] See eg http://ercim-news.ercim.eu/en98/special/moving-towards-interoperable-internet-of-things-deployments-in-smart-cities .

[51] BIS paper, supra n 44, at 3.3.2.

provider. Sadowski, an Arizona University researcher on the future of cities, suggests that a paradigm example of a "top-down" smart city, Songdo in South Korea, "*is as much Cisco Systems city as it is South Korea's, because they have most of the contracts for the hardware and software that power it"*[52]. In the EU these questions form a part of ongoing worries and uncertainties about who owns and how to control "big data"[53], and suppliers too are sensitised to the issue as problematic for both cities and citizens: for example, one industry speaker allowing that "*what we do with the information we collect and who owns it are the key questions facing smart cities*[54]."

Accordingly at this stage this paper echoes, but with perhaps more concern, the conclusion of Goodman[55], who emphasises that conceptions of smart cities all share two features: "*They emphasise public-private partnerships and place information and communications technologies (ICT) at the core of smart city operation"*. Expanding on the latter part, smart cities, we have seen, are crucially dependent on three sets of technological phenomenon: the IoT; big data; and the Cloud. As will be discussed further below, serious privacy regulatory problems are associated with all three features, and smart cities, as the unholy union of all three, represent an interesting "use case" for privacy scholars. Finally, I have established that political and economic drivers for smart cities will not easily be derailed by quibbles about privacy and fundamental rights, and that academic literature has a role here to intercede for the public interest between political objectives and industry gain[56].

It would be remiss not to say in this introductory section, as may already be apparent from some of the above, that smart cities are also quite easy to dismiss as a creation of the much-noted technology "hype cycle"[57] which also brought us the dot.com bubble, "Web 2.0" and many other technowaves of enthusiasm. On this well known scale, smart cities may well be at the top of the "peak of inflated expectations" just before the "trough of disillusionment". Goodman tactfully suggests that "*the literature on smart cities can be decidedly utopian*"[58]. However given the volume of national pride, money and infrastructure that is being pumped into the smart cities paradigm, alongside what is generally cursory legal analysis if any, this writer maintains the phenomenon is worth examining further.

A second awkward question which should be raised, is why discuss privacy and smart cities? Why not privacy and the IoT, or privacy and big data, or even privacy and the collapse of the private/public spaces demarcation? Each of these now has a steadily growing literature. There are a number of answers to this. First, smart cities represent the synthesis of all of these

[52] "Interview: Jonathan Sadowski on the Future of Cities", *Hieroglyph*, October 14 2014.

[53] See inter alia, EU EDPS *Opinion on privacy and competitiveness in the age of big data* 26 March 2014; ICO (UK*) Big data and data protection* July 2014; Article 29 EU Data Protection Working Party *Statement on Big data* , September 2014, 14/EN WP 221; *Big Data and Smart Devices and Their Impact on our Privacy*, supra n XX..

[54] Vinnett Taylor, head of M2M, quoted in Emma Wright and Dianne Devlin "Smart Cities – Power to the Citizens?", *Computers and Law*, 16 April 2015 , now available online at http://www.bonddickinson.com/insights/publications-and-briefings/smart-cities-power-citizens .

[55] Supra n 27, at pp 43ff.

[56] Not all academic literature of course sees smart cities and the IoT as problematic for privacy, at least not in the same ways as this article does. See eg McKay Cunningham "Next Generation Privacy: The Internet of Things, Data Exhaust, and Reforming Regulation by Risk of Harm" Groningen Journal of International Law, Vol. 2, Ed. 2, 2014 who sees the IoT and smart cities as use cases indicating the need for reform of data protection law as an over inclusive and ungraduated failure; Gilad Rosner "No, the IoT does not need strong privacy and security to flourish", O'Reilly report, September 2015, summary at Radar, September 25, 2015 at http://radar.oreilly.com/2015/09/no-the-iot-does-not-need-strong-privacy-and-security-to-flourish.html .

[57] See http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp .

[58] Supra n 27 at 45. Although it "also has a dystopian thread" in its narratives of 24/7 surveillance and security vulnerability. See further below and Murakami Wood supra n 19. A notable early opponent of the smart mythos from a sociological perspective is Adam Greenfield: see *Against Smart Cities* ( 2013, Amazon Kindle publisher).

problems. In this sense they are a unique and important use case, which deserves special, bespoke attention. Second, as I have tried to demonstrate above, smart cities are important. In the future , the majority of us will be living in cities, and perhaps many of us, in "smart" or at least, not dumb, cities[59]. Investment in smart cities is only going to increase – as I wrote this paper, Obama pledged to spend a further $160m on smart cities[60] – and whatever terminology is used, data driven connected urbanism is not going away[61].

Thirdly, in each of the privacy literatures mentioned above, US literature tends to determine how the world sees these issues. US literature – including academic papers, conferences and industry and quango-funded reports - is in a better position to dominate the literature mainly because it is generally larger and better funded than its European equivalent, but also because US industry has in general been been ahead of Europe in understanding how quasi-academic discourse can help support the claims of more obvious outright lobbying. Yet the yawning cavern between EU and US conceptions of privacy, and their different approaches to how to legally regulate such (or whether to at all), especially in hot button areas such as big data, ubiquitous computing and private/commercial versus public interests, has been the privacy story of the millennium so far. A literature is needed which examines smart cities and privacy in terms of the EU social context and the mandatory rules of EU law, however vague, conflicted and about to be reformed (for the last three years and counting) they are. Arguably, a pragmatic and multidisciplinary academic literature is also needed which can mediate between the precise and legally impeccable but sometimes over-perfect interpretations of the A29 Working Party (A29 WP), and the commercial realities of a Europe in recession, and seeking commercial social solutions which involve inevitable compromise with private sector, globally based vendors.

Finally, we need to discuss privacy and smart cities now, not at some indeterminate time later when we have worked through all the building-block categories of privacy problems involved. In the solutions section of this paper, it becomes apparent that perhaps the best way forward is privacy by design (PbD) : the idea of building privacy into the "code", ie, the architecture (within cities, in its real, materials sense, not merely using the term as Lessig does[62] as a metaphor for hardware and software). If we are building smart cities now, then we need to work out what PbD can do for society before, or at least, as, we design and build them.

## III Smart Cities: Security and Privacy

Smart cities are not a panacea for all ills, and they bring their own problems. Some, as already noted, revolve around practical issues such as funding, capacity, access to relevant technologies, interoperability of data, technical standardisation, etc. Others are political: buy-in by the national and local politicians, the energy companies, and the citizens themselves – a recent NESTA report, surveying numerous cities, points that many smart cities "*have failed to deliver on their*

[59] Or in smart towns or even villages: see Branka Dimitrijevic "From Transition Towns to Smart Cities: Opportunities and Challenges", in SCL special edition, supra n 1 at http://www.scl.org/site.aspx?i=ed43114 , citing Linlithgow, between Glasgow and Edinburgh as a town utilising "big data" for decision making and social innovation.

[60] See https://www.whitehouse.gov/the-press-office/2015/09/14/fact-sheet-administration-announces-new-smart-cities-initiative-help , September 14, 2015. See on EU funding of smart cities, both directly and via research programmes such as FP7, T H A Wisman "Purpose and function creep by design: Transforming the face of surveillance through the Internet of Things" European Journal of Technology, Vol 4, No 2, 2013at 2.1. See also *Telegraph*, "Who will pay for the Internet of Things?", 30 January 2015 at http://www.telegraph.co.uk/technology/internet/11377083/Who-will-pay-for-the-Internet-of-Things.html .

[61] See Kitchin, supra n 18.

[62] Lawrence Lessig *Code 2.0 (*Basic Books, 2006). See also Rob Kitchin, "From a Single Line of Code to an Entire City: Reframing Thinking on Code and the City*", Programmable City* WP No 4, Nov 2014, downloadable at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2520435 .

*promise, delivering high costs and low returns.. 'Smart cities' offer sensors, 'big data' and advanced computing as answers to these challenges, but they have often faced criticism for being too concerned with hardware rather than with people*[63]".

Two further issues are particularly germane to this paper situated as it is in law: *security*, by which I mean the susceptibility of data to either accidental or deliberate breaches as a result of technical or organisational failures; and *privacy*, in which I include the European *data protection* (DP) sense of the right of individuals to control the collection and processing, including further re-uses, of their personal data. Privacy is also strongly governed in Europe by art 8 of the European Convention on Human Rights which acts as a benchmark against which both EU DP rules and nation state laws can be judged.

*Security and vulnerabilities*

Cities and their infrastructure are already the most complex structures ever created by men, and interweaving them with equally complex smart cities solutions, reliant on wireless sensor networks and integrated communications systems, makes them extremely vulnerable to power failure, software errors and cyber-attacks.[64] Even a simple bug can have a huge impact on urban infrastructure.[65]

The insecurity and vulnerability of smart city systems is a commonly acknowledged phenomenon[66], which echoes, and largely derives from, the well known lack of security and trustworthiness of the IoT in general. The FTC in its influential 2015 report on the IoT, notes security risks as its greatest worry, both in terms of vulnerability of IoT devices themselves, leading to their compromise or failure, and their potential use to spread vulnerabilities through networks and to other systems (the "zombie" problem)[67]. For example, potentially, your smart, Internet-connected, fridge might be hijacked to send spam[68]. The FTC has already taken its first enforcement action against a vulnerable consumer IoT implementation: a company making baby monitors attached to the Internet, thus allowing parents to view live feeds of their infants from a distance, had its feeds "hacked" in nearly 700 cases[69]. Connected cars (or "autonomous vehicles") are another significant IoT use case where vulnerability to outsider hacking has already been demonstrated: eg, *Wired* reported in June 2015 how Jeep Cherokees could reliably be "hijacked" by external hackers while on the road[70]. Brown, in a 2015 report for the ITU, notes that "*electronic attacks can.. lead to threats to physical safety*" citing possible targets such

[63] See further NESTA *Rethinking Smart Cities From The Ground Up*, June 2015, http://www.nesta.org.uk/publications/rethinking-smart-cities-ground#sthash.398wQeB1.dpuf .

[64] See A Townsend, *"Smart Cities"*. Places Journal (October 2013) at https://placesjournal.org/article/smart-cities/ .

[65] See eg the San Francisco Bay Area Rapid Transport bug of November 2013, in Cesar Cerrudo, *"An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks"*, White Paper, IOActive, Inc. (2015), p. 10 at http://www.ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf .

[66] See inter alia Townsend, supra n 14; Goodman, n 27.

[67] See FTC Staff report *Internet of Things: Privacy and Security in a Connected World*, January 2015 at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (herafter FTC, 215).

[68] See Paul Thomas "Despite the news, your refridgerator is not yet sending spam", Symantec, Jan 23, 2013 at http://www.symantec.com/connect/blogs/despite-news-your-refrigerator-not-yet-sending-spam .

[69] Supra no 65, p 13, n 52 and https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet-connected-home-security-video-cameras-settles .

[70] See http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ . Another area of considerable worry is hacking of medical devices, both external (eg connected MRI machines – see BBC News "Medical devices vulnerable to hackers", 29 September 2015 at http://www.bbc.co.uk/news/technology-34390165 ) and implanted in human bodies (eg pacemakers, as famously shown in an episode of *Homeland*.) Even automated carwashers have their worries : see "Hacking at the carwash, yeh", 19 February 2015, at at http://www.darkreading.com/vulnerabilities---threats/hackin-at-the-car-wash-yeah/d/d-id/1319156 .

as medical pacemakers, insulin pumps and car brakes, and noting the possibilities for burglars to spot "smart metered" premises as currently unoccupied[71]. These worries only expand as the number of connected smart objects grows. Cisco eg predict that there will be 50 billion devices connected to the Internet by 2020. [72].

Why is the IoT so insecure? IoT devices, being, usually, small, very cheap, without independent power source and churned out in their millions, and historically for industrial not consumer use, are routinely designed with poor encryption strength and a lack of other security features[73]. The IoT heavily relies on wireless communications protocols or APIs that, due to the lack of mandatory technical and security standards, are usually "*only secured as an afterthought, or worse, not secured at all, transmitting data in the clear*."[74] The FTC report on IoT notes that companies making IoT devices may not have experience in dealing with security issues; that they have often been conceived as disposable; that patching of vulnerabilities may not have been envisaged or be possible to add; and that consumers in general have little or no idea about IoT security[75]. As a result default passwords are often installed in household appliances, never changed and routinely compromised: eg one website claimed that 73,000 webcams had been installed and were accessible over the Internet using a single, default, known password[76].

For smart cities, these problems carry over and will be multiplied by the complexities involved in multiple vendors and interoperating systems; and the effects may be far more devastating. Cerrudo asserts that most cities are implementing new technologies with little or no cyber security testing, meaning that, eg, traffic control sensors installed in Washington DC, New York, London, Lyon and other cities can be easily attacked with a simple exploit programmed on cheap hardware.[77] Brown adds that smart city vulnerabilities will be particularly hard to address given links to older public and private sector systems. Vulnerabilities in embedded architectures cannot be as simply patched digitally as conventional software, leading to a possible future of the "Internet of Junk"[78]. In short, smart cities are a security disaster waiting to happen.

*Solutions*

The application of DP law, including the PECD, to the security of the IoT is discussed in detail below (section V(i)) as part of its general privacy problem set. A particular solution to the security issue, which has already been partly implemented, is to mandate security breach

[71] See Ian Brown GSR discussion paper *Regulation and the Internet of Things* (ITU, 2015 ) (draft issued for discussion) at http://www.itu.int/en/ITU-D/Conferences/GSR/Documents/GSR2015/Discussion_papers_and_Presentations/GSR_DiscussionPaper_IoT.pdf .

[72] See Dave Evans, White Paper *"The Internet of Things. How the Next Evolution of the Internet is Changing Everything"*. Cisco white paper (2011), p. 3, at http://www.iotsworldcongress.com/documents/4643185/0/IoT_IBSG_0411FINAL+Cisco.pdf .

[73] According to the HP Fortify report, 70% of most commonly used IoT devices contain security vulnerabilities, including password security, encryption and general lack of granular user access permissions. See HP Fortify, Report *Internet of Things Research Study* (2014), p. 5, at *http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA5-4759ENW&cc=us&lc=en* .

[74] *Akamai, akamai's [state of the internet] report (2014), p. 1,* at https://www.antel.com.uy/wps/wcm/connect/2e38bd0047ad6c9682d3e7af6890d810/q3-2014-state-of-the-internet-report+(2).pdf?MOD=AJPERES .

[75] Supra n 65 at p 13.

[76] See Kevin Tofel "Got an IP webcam? Here are 73,000 reasons to change the password" GigaOm Research, 7 November 2014 at https://gigaom.com/2014/11/07/got-an-ip-webcam-here-are-73000-reasons-to-change-from-the-default-password/ .

[77] See Cesar Cerrudo, *"Hacking US (and UK, Australia, France, etc.) Traffic Control Systems"*. IOActive (April 30, 2014), available at http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html .

[78] The term seems to originate from security researcher Tod Beardsley. See http://panelpicker.sxsw.com/vote/54858. More politely, Townsend predicts that smart cities may be "buggy, brittle and bugged": see Townsend supra n 14 , ch 9.

disclosure. Currently this only applies to telecoms providers under art 4(2) of the Privacy and Electronic Communications Directive (PECD)[79] but will probably be extended to all data controllers by the GDPR [80] when and if it passes and is transposed. Data breaches of a certain level of severity will have to be reported to privacy regulators, although data controllers may have a defense if they have adopted adequate security measures.[81]

An obvious problem is the lack of global harmonisation on security legal standards, in a world of global procurement. The Budapest Cybercrime Convention provides a bare minimum of international harmonisation on security regulation but is principally aimed at enabling global law enforcement in criminal matters, not at promoting higher security standards for industry. It does not mandate civil liability (though art 13 allows for such to exist). It would be interesting, though outwith the scope of this article, to investigate if the various provisions being mooted to protect critical infrastructure from cyberwar attacks and cyber insecurity (see eg the 2008 Directive on European Critical Infrastructures 2008/114/EC and the proposed Directive 2013/0027) might extend to smart cities.

“Soft law” rather than hard law regulation of IoT security has been in the ascendance in the EU since 2013 or earlier.[82] Notably, a specialised but non mandatory PIA procedure for RFID chip installations (essentially an early subset of the IoT) was developed by Spiekerman and her team through consultation with relevant industries and policymakers[83]. This forms part of a general regulatory trend towards encouraging a proactive rather than retrospective approach to security risks with privacy by design (PbD)[84] principles. This approach was promoted in the Mauritius Declaration on the Internet of Things in October 2014 and by the FTC in their IoT report.[85] In Europe, a PbD requirement, alongside requirements for data protection impact assesments (DPIAs[86]) is expected to be included in the GDPR. All of these “code” solutions are discussed in more detail below in section VI.

A final key extralegal may be found in future in an adequate global cybersecurity insurance market[87]. This is something which has stalled to date, and is still emergent, but which may be kickstarted by a global move to mandatory security breach notification.

[79] 2002/58/EC.

[80] See European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereafter, General Data Protection Regulation or GDPR), COM(2012) 11 final, 2012/0011 (COD). January 25, 2012. The GDPR is expected to be passed by end 2015 and thereafter will probably have a two year transition period for member states to implement its demands.

[81] See Ricardo Tavares, “Rise of the machines”. (2014) 42 (3) *Intermedia* 28.

[82] A 2013 EU Commission consultation on IoT regulation found a diversity of views on whether IoT specific regulation was necessary (see http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation ). See further H.R. Schindler et al, *“Europe’s policy options for a dynamic and trustworthy development of the Internet of Things”* (SMART 2012/0053), prepared for the European Commission, DG Communications Networks, Content and Technology (CONNECT), Brussels (31 May 2013), at http://www.rand.org/pubs/research_reports/RR356.html

[83] See Sarah Spiekerman “The RFID PIA – Developed by Industry, Agreed by Regulators” in David Wright and Paul de Hert eds *Privacy Impact Assessment : Engaging Stakeholders in protecting Privacy* (Springer, 2011), discussed further infra p XX.

[84] See further below, p XX –XX.

[85] See 36th International Conference of Data Protection and Privacy Commissioners, 14 October 2014 at http://www.privacyconference2014.org/media/16596/Mauritius-Declaration.pdf ; FTC, supra n 65.

[86] See p xx below

[87] See World Economic Forum (2014), at p. 33. Price Waterhouse Cooper argue the change to mandatory security breach notification “may well be the catalyst to change the cyber liability insurance landscape in the UK”. (see *Information Security Breaches Survey*, HM Government (2015), p. 29, at http://www.pwc.co.uk/assets/pdf/2015-ISBS-Technical-Report-blue-digital.pdf .)

## IV Privacy

*The new PPP : Private-public-places.*

Conceptually, privacy in smart cities is an interesting conundrum. Historically, we have tended to protect a zone or “bubble” of privacy which begins with our bodies, embraces our homes and then extends to private communications we send out into the world. This is seen in the European Convention on Human Rights (ECHR) where art 8 famously demands respect for our “private and family life, home and correspondence”. By contrast, cities seem quintessentially a public space, where expectations of privacy (except by obscurity) have historically been low to zero. But as MacSithigh has cogently noted, in the information society many virtual spaces controlled by private interests have acquire a quasi-public character akin to town squares or public libraries, places where historically rights of speech, access to knowledge or assembly were traditionally exercised : notably online communities and search engines[88]. In “smart cities”, the reverse paradigm operates: what was historically public such as the town squares, the roads, the mass transit, the health and policing systems, is very likely now to be privately operated or at least full of privately operated sensors with the data collected held in private databases. These parts of cities have now become what might be called “private-public-places” (or transmuting MacSithigh, “pseudo-private” places.)

The growth of the information society and especially ubiquitous computing has already recognizably undermined this conception of privacy as relating to a spatially delimited “bubble”[89]. Koops has more recently robustly deconstructed this notion of natural essentialist “boundaries of private spaces”, arguing that “*place is no longer a useful proxy to delineate the boundaries of the private sphere*”. He points out that nowadays personal data that would have once have stayed safely at home, is now carried around or stored without much, if any, thought outside the home : on smartphones or other portable devices; on webmail servers; or in the cloud generally. Furthermore data that would have been opaquely safe at home is now often transparent to the world: for example, homes equipped with smart meters reveal finely grained detail of energy consumption and powered applications, and can have their occupancy and activities minutely observed from without[90]. Heat sensors, directional microphones and tiny surveillance drones can also breach the domestic wall. Finally, even in public spaces, where once people relied on “practical obscurity” for privacy protection (hence, arguably, not needing legal protection), the prevalence of surveillance via inter alia smart CCTV systems, ANPR (number plate) recognition, GPS and wi fi network tracking and cheap, reliable facial recognition software means that obscurity-in-public is pretty much at an end. Given this combination of “evaporating homes” and “ubiquitous trackability”, Koops argues we have moved towards an age of “’ubiquitous data’ in which private/place distinctions lose relevance. In smart cities, like the bar in *Cheers*, everyone knows your name.

How should we approach privacy regulation in such a domain? If your personal data is easily accessible in the “public” areas of a smart city, then should the same privacy protections apply as in a private dwelling? If you travel on a smart road or a smart connected public transport

[88] See Daithi MacSithigh “Virtual walls? The law of pseudo-public spaces” 2012 8(3) International Journal of Law in Context 394.

[89] See Colin Bennett “In Defense of Privacy” 2011 8(4) Surveillance and Society 485.

[90] See Bert-Jan Koops “On Legal Boundaries, Technologies, and Collapsing Dimensions of Privacy” *Politica e Società* 3(2), p. 247-264, 2014. See also Ian Brown “Britain’s Smart Meter Programme: a case study in privacy by design” (2013) 28 Int Rev LCT 172 on the number of things an outsider can find out from a smart homes energy emissions – including “Do you typically arrive home after the bars shut?”, “Do you climb stairs when you are registered disabled?” and “If you have type 2 diabetes, why haven’t you used the treadmill in your living room in the fortnight and instead watched 480 hours of TV”? (slightly paraphrased by Edwards).

system, should these be part of the same "privacy bubble" as the home you occupy? What about a driverless "connected car", quite likely not owned by you, directed by a mixture of external sensor data, internal control and car to car communications and shared physically with others? These are ideas that Koops points out are already showing up as problems in fields such as criminal procedure and evidence – eg should my smartphone be protected from search in my home but not when I am arrested by the police? What about my laptop? What about the location data from my new BMW's GPS? [91] – but their full impact may be felt in smart cities, where we live, work, commute and play all in the full glare of pervasive data collection : an urban Panopticon, which Finch and Tene have inventively christened the "Metropticon[92]".

A key point in the "publicness" of smart cities is that data disclosures by residents in a "smart" city simply cannot be avoided. Finch and Tene point out that, unlike when choosing an online entertainment provider social network, a shopping site or a search engine (say), "*urban residents of smart cities have few alternatives to the government operated sensors and surveillance technologies .. deployed throughout the environs.. They will only have one smart grid, one subway system..*[93]*.*" This is particularly true when it comes to essential services such as health, emergency response and policing. Even despite the onslaught of market deregulation, most of us do not still have the opportunity (or desire) to shop around for our fire service or bin lorry. Interestingly, Finch and Tene see this as worrying because they fear the extra power it may give a paternalistic government eg to demand an obese citizen walks rather than takes the (smart, connected) bus to work, "thus saving lives and healthcare dollars". For a European, the likelier danger seems to be that such data will fall via PPPs into the hands of private providers and from there to the open market, with negative impacts if it reaches (say) insurers[94], employers or law enforcers. Finch and Tene argue the private marketplace has competition incentives to provide privacy which do not impact on governments. Yet this seems disingenuous: the history of private commercial Internet corporations has been one of a distinct lack of competition, where almost every company relies on standard privacy policies to take as much personal data as possible, relying on consumer ignorance and inertia[95], lack of transparency and the "lock in" effect of network effects in industries such as social networking, to restrict pushback by consumers[96].

Privacy law, as a sub branch of human rights law, has of course moved on somewhat from the days when privacy in public was a blatant contradiction in terms. In Europe, the seminal Strasbourg case of *von Hannover*[97] has required states to protect minimum reasonable expectations of privacy in public, even for public figures such as celebrity princesses. In the US,

[91] See *Riley v California* , US Supreme Court, July 25 2014, in which the US Supreme Court for first time decided that police needed warrants to search cellphones outside the home. Commentators noted the ruling almost certainly also applied to laptops etc : see Washington Post, June 25 2014 at http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0 .

[92] See Kelsey Finch and Omar Tene "Welcome to the Metropticon – Protecting Privacy in a Hyperconnected Town" 2013-2014 41 Fordham Urb. LJ 1581. The implications of a "Panopticon" may in fact be inappropriate to smart cities which are as much about peer to peer equiveillance and indeed sousveillance as traditional surveillance. The coinage is however arresting. See also Wisman's reference, n 138 supra.

[93] Supra n 90 at 1596.

[94] Life insurance companies have already started to offer better terms to customers who agree to wear FitBit-like personal health trackers and share the data. Fascinatingly, an app has already been created called "unfit Bits" which spoofs a stream of such data to fool the insurance company. "*Now you can play video games* and *harvest insurance perks, as your fitness monitor dutifully logs fake calories while strapped to your golden retriever or metronome*." See Olga Khazan "How to fake your workout" *The Atlantic*, 28 September 2015.

[95] See . Arnold, . Hillebrand, and M Waldburge, *"Personal Data and Privacy - Final Report - Study for Ofcom,"* WIK-Consult (May 2015), p 60 at http://stakeholders.ofcom.org.uk/binaries/internet/personal-data-and-privacy/Personal_Data_and_Privacy.pdf .

[96] See further in L Edwards "Privacy, Law, Code and Social Networking Sites" in I Brown ed *Research Handbook On Governance Of The Internet* (2013, Edward Elgar) .

[97] ECtHR, Application no 59320/00, 24 June 2004.

however, despite the shift towards privacy-favourable decisions in the criminal law concerning searches in public of smartphones, and the legitimacy of trackers placed on cars[98], in civil law it is still extremely difficult to establish a privacy cause of action relating to actions done, or data exposed in public[99]. Even in the UK, it is very difficult to convince a court that what goes on, or is said in public has any expectations of privacy attached in circumstances not involving obvious harassment by paparazzi. Surveillance and data mining of “open” social media intelligence (“SOCMINT”) for example, is regarded as lacking any element of privacy and thus not generally needing any police warrant or authorisation before it can be monitored, collected and data mined: even though such monitoring may contribute to profiling which in its turn may have substantial impact on individuals[100]. Similarly, the English Supreme Court recently held that a boy whose picture was captured on CCTV in the course of breaking the law as a rioter, had no rights to stop the police publicly spreading the image[101]. (In both these cases, of course, it could be argued that the public interest in preventing crime and terror would (and did, in the latter case) outweigh any individual expectations of privacy[102]. )

Data protection (DP) law, by contrast, does not make any crucial private/public distinction except in the exemption it gives to purely domestic or “household” processing of data[103]. Its category distinctions revolve around whether “personal data” – data relating to you which makes you “identified or identifiable”[104] - is processed, not where that processing happens. For this reason, and because of its EU rather than global focus, the rest of this paper focuses on DP law not on general privacy law.

It might be useful to ask at this point what expectations (if any) the public have of privacy protection in smart cities, or failing data on that[105], in their interaction with the IoT. Public trust and confidence in technologies are generally regarded as vital to their uptake, and doubt has already been recorded about public trust in IoT[106], partly because of the security threats already

[98] See n 89 supra; also *United States v. Jones*, 132 S. Ct. 945 (2012).

[99] See further Daniel Solove *The Future of Reputation* (2007, Yale UP), ch 7.

[100] See Demos Report on *Policing in an Information Age*, 2013 at http://www.demos.co.uk/publications/policinginaninformationage ; Lilian Edwards and Lachlan Urquart “Privacy in Public – A Reasonable Expectation? The Legality of Police Surveillance of Social Media”, forthcoming.

[101] See *In the matter of an application by JR38 for Judicial Review (Northern Ireland)* [2015] UKSC 42 .

[102] See observation in *Wood v Metropolitan Police Commissioner* [2008] EWHC 1105 (Admin) : [the English courts have] “*adopted a very robust approach to questions of interference with rights under Article 8(1) in relation to the taking of photographs in public places.. in assisting in the detection of crime*”.

[103] Which is indeed space-dependent but controversially so: cf the CJEU decision in *Lindqvist* Case C-101/01 , 6 November 2003 that just because a website was accessible to an indefinite number of people in cyberspace, its highly localised contents were not purely domestic or personal; similarly the more recent decision in *Rynes* Case C‑212/13 , 1 December 2014 that if a CCTV camera placed to protect a family home records images of the public street beyond, it must be more than a purely personal or domestic activity and thus caught by DP law. The CJEU rejected the idea in *Lindqvis*t that any non commercial processing was purely personal. A strong view exists that this exemption should be more a *de minimis* principle and less a spatial one.

[104] See DPD, art 2. I consider below the issue of when personal data is rendered non-identifying or anonymised.

[105] This writer is not aware of any empirical survey work on attitudes to privacy in smart cities (she intends to carry some out as Researcher in Residence at the Digital Catapult in 2016), and there is only the very beginnings of an academic literature on smart cities and privacy, with very little of it coming from legal, as opposed to information sciences, scholars. For the former, as well as Finch and Tene supra n 79, which falls within a published “smart law” symposium, see Julia Lane et al eds *Privacy, Big Data and the Public Good* (2014, CUP) and parts of Wisman, supra n 57. In criminology, interest is emerging in the privacy and surveillance aspects of smart cities – see notably Kitchin’s work already cited and continuing at The Programmable City, Maynooth University, Dublin (http://www.maynoothuniversity.ie/progcity/ ) and Murakami-Wood’s ongoing study of global smart cities and surveillance at Queens University, Ontario, Canada (http://ubicity.ca/about/#sthash.XDlXItKK.dpbs ).

[106] See eg the UK’s investment of £10m to build a “ Commitment to Privacy and Trust in the Internet of Things Research Hub (ComPaTRIoTs)” following the Blackett Review’s conclusion that developing the IoT must be informed by appropriate security, trust , ethics and privacy guarantees. See Blackett Review *The Internet of Things: making the most of the second digital revolution* (2014).

discussed and partly because of general feelings among ordinary users of loss of control over personal data to third parties, most often seen in contexts such as social networks, search engines and targeted advertising[107]. A recent European Commission survey on Internet of Things Governance[108] found that 67% of respondents agreed "*Internet of Things applications pose threats to the protection of an individual's identity*" and 81% were concerned about how data acquired from the IoT would be "*used, stored, and accessed by whom*".

A 2014 US based Pew Internet research project interestingly canvassed around 1700 experts for their predictions about the IoT. Some responses were extreme: "*There will be absolutely no privacy, not even in the jungle away from civilisation*". Others were resigned : "*We might as well inject ourselves into the Internet of Things. By 2015 we will long ago have given up our privacy. The Internet of things will demand – and we will willingly give – our souls…*"[109]. These surveys are probably untrustworthy in methodology but they do give a flavour of the crisis of confidence about privacy and trust in IoT environments, including smart cities.

## V Privacy threats : smart cities and dumb laws?

Much has been written about the potential demise of privacy as a result of the technological society we now inhabit. In this section, I will discuss three leading sources of technological threat to privacy, and argue that the smart city, as noted above, is the location for a "perfect storm" conjunction of these threats. I will attempt in each case to focus on what the key problems posed for European DP law are by each threat, especially in the context of smart cities. This discussion is necessarily abbreviated ; at least a book could be (and often has been) written on each problem below. In the next section, I canvas and critique some novel solutions to these problems drawn from both law and code.

### *(i) The Internet of Things*

The Internet of Things (IoT), also known as ubiquitous computing (ubicomp), ambient intelligence or pervasive computing has a long history in computer science but has only fairly recently come to the attention of lawyers. The Pew Research Center[110] defines the IoT as "*a global, immersive, invisible, ambient networked computing environment built through the continued proliferation of smart sensors, cameras, software, databases, and massive data centres in a world-spanning information fabric*". It is now over six years since the number of "things" connected to the Internet exceeded the number of people[111]. Predictions in 2013/14 for the number of things that will be connected to the Internet by 2020 vary significantly, with Gartner predicting 25 billion[112] and Cisco quoting 50 billion[113] but there is general agreement that the IoT will be a vastly significant feature of future societies. According to Gartner, smart cities are one of the key sectors for attracting investment in the IoT space[114].

[107] See general discussion in Lilian Edwards and Charlotte Waelde eds *Law and the Internet* (2009) chs14, 15 and 16; Eurobarometer attitudes to privacy survey, June 2015, summary at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf .

[108] *Conclusions of the Internet of Things public consultation*, February 2013. See resource page at http://ec.europa.eu/digital-agenda/en/news/conclusions-internet-things-public-consultation .

[109] See Pew Research Internet project , May 14, 2014, "The Internet of Things will thrive by 2025" at http://www.pewinternet.org/2014/05/14/internet-of-things/ .

[110] Supra n 107.

[111] FTC 2015, n 65 supra, at i.

[112] http://www.gartner.com/newsroom/id/2905717.

[113] http://share.cisco.com/internet-of-things.html.

[114] See Gartner: *Hype Cycle for the Internet of Things* (2015), available at https://www.gartner.com/doc/3098434/hype-cycle-internet-things- .

There is a growing literature on the potential threat the IoT poses to privacy and increasing public awareness of the IoT, especially in the smart city context[115], as a tool for pervasive surveillance. To give a flavour, the Guardian ran a series of articles on smart cities and privacy in 2015, which at one point opined:

> "*We may find ourselves interacting with thousands of little objects around us on a daily basis, each collecting seemingly innocuous bits of data 24/7, information these things will report to the cloud, where it will be processed, correlated, and reviewed. Your smart watch will reveal your lack of exercise to your health insurance company, your car will tell your insurer of your frequent speeding, and your dustbin will tell your local council that you are not following local recycling regulations. This is the "internet of stool pigeons", and though it may sound far-fetched, it's already happening.*[116]"

The key problem of the IoT, for privacy purposes, is that its devices were explicitly designed to be unobtrusive and seamless as a user experience ; as Weiser puts it, to weave themselves "*into the fabric of daily life until they are indistinguishable from it"*[117]. IoT systems, such as smart ambient lighting in a living room , or smart thermostats, such as NEST[118] are often designed to be contextually aware of the needs and desires of the user, collecting information about their daily practices and routines, whilst remaining "*invisible in use"*" and "*unremarkable*" to users.[119]

To contrast, when we share personal data in the *online* digital world – for example on Facebook, Google, Amazon or eBay - we are, even if dimly, aware of crossing a threshold into the domain of that platform, and usually have an opportunity, at least once, to give or withold our consent to data collection, before we start to use the service (even if in reality our main option is either to take or entirely reject the service). In the IoT, such notice and opportunity are predominantly absent by design. Even where unobtrusiveness is not a function specification, IoT devices simply do not usually have means to display privacy notices and/or to "*provide fine-tuned consent in line with the preferences expressed by individuals*," as devices are usually small, screenless or lack an input mechanism (a keyboard or a touch screen) [120]. The problem is bad in domestic homes, and gets worse in the public places of smart cities. While consumers may at least have theoretically had a chance to read the privacy policy of their Nest thermostat before signing the contract, they will have no such opportunity in any real sense when their data is collected by the smart road or smart tram they go to work on, or as they pass the smart dustbin[121] in the street.

It is easy to see that in such systems, the conventional safeguards of consent in European DP law, or "notice and choice" in the American Fair Information Processing Principles[122], will fail to operate as safeguards for consumer privacy. As Cas stated in an early paper, there is thus every

[115] See Weber 2010; de Hert, Gutwirth et al, 2008; Wisman, A29, Brown for ITU, FTC, Goodman 2015, Peppet 2015 all these supra or infra;

[116] "Hacked dog, a car that snoops on you and a fridge full of adverts: the perils of the internet of things ", *Guardian*, 11 March 2015 at http://www.theguardian.com/technology/2015/mar/11/internet-of-things-hacked-online-perils-future .

[117] M. Weiser (1991) "The Computer for the 21st Century" *Scientific American* p1 .

[118] See "What Google can really do with Nest, or really, Nest's data", *Ars technica*, 16 January 2014, at http://arstechnica.com/business/2014/01/what-google-can-really-do-with-nest-or-really-nests-data/ .

[119] Peter Tolmie et al "Unremarkable computing" *Proc. CHI '02.* ACM Press (2002), 399-406.

[120] Article 29 Working Party, *Opinion 8/2014 on the Recent developments on the Internet of Things*, WP 223 (2014), p. 7, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf (herafter "A29 WP IoT").

[121] See "City of London calls halt to smartphone tracking bins", BBC News, 12 August 2013.

[122] See Gellman, Robert, *Fair Information Practices: A Basic History* Version 2.13 (February 11, 2015), p. 11, at http://bobgellman.com/rg-docs/rg-FIPShistory.pdf .

possibility that "*ubiquitous computing will erode all central pillars of current privacy protection".*[123]

EU law

EU law demands in art 7 of the Data Protection Directive (DPD) that data controllers have a lawful ground for processing of personal data[124], with consent being only one such ground among several[125]. Indubitably, many or most IoT systems in smart cities will process personal data, unless steps have been taken to effectively anonymise it (see below). Consent is defined in art 2 of the DPD as a "*freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*". This definition is, as we have seen, considerably troubled by the features of the IoT environment. In Europe, the Article 29 Working Party[126] has raised a significant number of issues about consent in addition to the sheer difficulty of giving it, including the fact that data may be shared automatically machine to machine, with no transparency to the user or opportunity to review; and that the *quality* of any user consent may be poor. Crucially, they state that "*the possibility to renounce certain services or features of an IoT device is more a theoretical concept than a real alternative.. such situations lead to the question of whether the users consent to the underlying data processing can then be considered as free, hence valid under EU law."*

But consent, it should be remembered, is not the only ground for lawful processing nor does it have any particular priority. If consent in EU DP terms is impossible, expensive or counter-productive to obtain, data controllers may well choose to avoid it entirely. Where IoT systems are used to prevent or detect crime (as with most smart CCTV systems) then data protection law may exemps processing from art 7's demands. Where local or national governmental agencies gather data for eg e-government systems, e-health, e-welfare, then a ground of "public interest" can also sidestep any need for consent. But for most commercial systems, what we might expect to come to see is a heavy reliance on the "legitimate interests" ground of art 7(f), which would be a worryingly easy way to avoid any semblance of user control. This is especially plausible given the likelihood of this ground emerging watered down still further in the final thrashout of negotiations in the GDPR[127]. The Art 29 WP clearly shares these concerns and goes out of its way in its 2014 Opinion to stress that, following *Google Spain*[128], it is unlikely processing of data via IoT revealing the "*individual state of health, home or intimacy, his/her location and .. his/her private life*" will "*be justified by merely the economic interest"* of an IoT stakeholder, given the need to balance this against the fundamental rights of the data subject[129].

Art 7 of the DPD may furthermore be read as overlaid by art 5(3) of the PECD, which requires, since its revision in 2009, that where "i*nformation*" is stored on the "*terminal equipment*[130] *of a*

[123] J Cas (2009) "Ubiquitous Computing, Privacy and Data Protection" in S Gutwirth et al (2009) *Computers, Privacy and Data Protection: An Element of Choice* (Springer) p167 .

[124] 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 (hereafter data Protection Directive or "DPD").

[125] Ibid, art 7(a).

[126] A29 WP IoT , supra n 119. See further on consent, E Kosta *Consent in European Data Protection Law (*Brill/Nijhoff, 2013).

[127] The EP *Big Data and Smart Devices* report notes "legitimate interests" as "the vaguest ground for processing" and a key worry as negotiations over the draft GDPR move into the trilogue (supra n 20 at 32).

[128] CJEU, 13 May 2014, case C-131/12, cited at A29 WP IoT, supra n 119, para 4.2.

[129] It should also be noticed that if *sensitive* personal data is processed – as will invariably be the case in a health related IoT system such as telemedicine for the aged, then processing can in most circumstamces only be legitimised by explicit consent and the "legitimate interests" ground will not do : DPD, art 8.

[130] This phrase is undefined in the PECD. The A29 WP IoT suggests helpfully it "be understood in the same manner as that of "equipment" in art 4(1)( c)" (para 4.1).

*user*", (or access if given to it when it is already stored there) the user must give consent to such storage, having been provided with "clear and comprehensive information" about the purposes for which that information will be processed. Consent is the *only* way such storage can be legitimised; there are no alternative grounds. Consent as noted above must be "informed" by prior comprehensive information, but need not be explicit. This provision was originally intended, in the early days of e-commerce, to control the placing of "legitimate" cookies on a user's computer without their knowledge and consent, as a privacy matter, as well as obviously harmful spyware or malware. It is now unclear how far this provision applies to data about users collected from sensors of various kinds in the "real world". Attempts were made during the passage of the 2009 amendments to the PECD to amend art 5(3) to give it a wider and clearer applicability to many other types of "devices" than cookies, notably "rootkits" of the type used in the Sony Mediamax scandal of 2003, but for political reasons, these resulted only in a change in the recitals[131]. Recital 56 of the PECD now reads: "*When such devices are connected to publicly available electronic communications networks or make use of electronic communications services as a basic infrastructure, the relevant provisions of Directive 2002/58/EC.. , including those on security, traffic and location data and on confidentiality, should apply*." Our main concern here is if art 5(3) applies to information collected about users by IoT sensors (such as RFID chips) – a question which is predicated on (i) whether such information is stored on the "*terminal equipment of the user*" and (ii) if, per recital 56, the networks the IoT sensors are connected to qualify as "public" enough to fall under the scope of the expanded post-2009 PECD.

When is IoT collected data stored in the "*terminal equipment.. of a user*"? The A29 Opinion[132] gives the example of a smart pedometer (say a Fitbit) owned and worn by a user A, and periodically synchronized via the Internet, which records and shares the number of steps taken by a user and their location. This would arguably be information which at the point of collection is "*stored in the terminal equipment of the user*" (even though it is then uploaded to the Fitbit cloud server for further processing) and so under art 5(3), the consent of A would be required. But if the same user has their location and kilometers travelled collected by a smart driverless or "connected" car, acting as a shared taxi service, is the "user" person A or is it the owner, or the operator (who may not be the same person) of the connected car? The A29 Opinion interprets this as meaning the consent of A remains required; this writer is less sure. Art 5(3) also refers to the equipment of a "subscriber" who hs the right to alternately give the relevant consent - which is a clear notion in the context of a mobile phone but much less so in a smart IoT public space environment. If we change the example further to steps counted by a smart path or escalator in a shopping mall, say, then it becomes increasingly hard to distort the English language to see the escalator as the "terminal equipment" of A as user, rather than of a "subscriber" who might be the mall manager or indeed, of no one at all.

A further problem is that the art 5(3) applies aince 2009 to where information is collected by devices connected to "*publicly available electronic communications networks*". If a smart city is "installed" by Cisco and many systems run on their private networks, do the rights in art 5(3) apply? Probably as this formulation was intended to extend coverage to private networks connected to the public Internet; but not with entire certainty. The European DP Supervisor criticised the failure to amend this scope restriction in 2009[133] but the alternate proposed

[131] See E Kosta "Peeking into the Cookie Jar ; the European approach towards the regulation of cookies" (2013) 21 IJLIT 380 and Citizens Rights Directive, recital 65 (Directive 2009/136/ECamending Directive 2002/22/EC.)

[132] Supra n 131.

[133]See the European Data Protection Supervisor's Second Opinion on the Review of the PECD, 9 January 2009 at http://www.edps.europa.eu/ . See also criticism from the European commission in in *Radio Frequency Identification (RFID) in Europe: steps towards a policy framework*" P6 COM(2007) 96 final 15 March 2007.

formulation, that the PECD should apply generally to "*publicly accessible private networks*" was unfortunately not added.

One further "get out of jail" card for IoT developers here is the exception from art 5(3) where storage is "*strictly necessary in order to provide a service explicitly requested by the subscriber or user*". It seems logically assertable that the location of a connected car must be collected for it to work and that service has been explicitly requested by the passengers and/or the operator (who is, one assumes, the "subscriber"?). What is less clear is (a) did they have any alternative, in which case art 5(3) is reduced to nugatory and (b) if the re-use of that location data for building a profile to provide targeted ads (say) benefits from the exemption.

One answer to many of the inclarities here would be speedy amendment of art 5(3) when the PECD comes up for review after the GDPR is finalised. Another would be for data controllers to avoid the issue entirely by making sure that such information if collected in public places was effectively de-identified so that it was not personal data at all. However this would sometimes be impossible if the service was to be delivered and more often would likely make it of little added commercial value. We discuss this below.

### *(ii) Big data*

Big data, like smart cities, is a buzz word which is much mentioned but has no one clear meaning[134]. It is frequently related to ideas of "volume, velocity and variety", with the emphasis on the first[135]. Big data has come to the fore for three reasons: the costs of both storage and processing of data have dramatically fallen; algorithms for analysing huge amounts of data have improved (hence, "data analytics" are a key part of the story) ; and, perhaps most importantly, the online data industries – and now the IoT industries - have created incredibly vast pools of data to mine.

Smart cities are consumers and producers of big data. Kitchin reports that post-millenium, the urban data landscape has been transformed, transitioning from "small" to "big" data, as the generation of datasets has become "*continuous, exhaustive… fine-grained, relational and flexible". "From a position of relative data scarcity, the situation is turning to one of data deluge*" [136]. In modern urbanity, data generated within traditional city infrastructure and utilities eg transportation, gas, electricity and water, have not only become digital flows, but are also now complemented by and combined with big data generated by commercial private companies (eg mobile phone operators, social media, website owners, often via commercial data brokers) and crowdsourced open data (eg citizen science initiatives). At present much of this data lives in silos; but increasingly it will be combined by public city managers and private service providers alike. , as is already the case in some smart city applications, eg the centralised control rooms for city monitoring found in Rio de Janeiro[137].

IoT applications are particularly prodigal in their creation of big data. The FTC in their IoT report noted that "*the sheer volume of data that even a small number of devices can generate is stunning.. [we heard that] fewer than 10,000 households ..*"*can generate 150 million discrete data points a day*""[138]. These massive volumes of granular data generated from IoT systems

[134] See inter alia discussions in reports cited at n 51. Big dat is so overused a term it has in fact been removed from the "hype cycle" by Gartner; see supra n 55.

[135] See eg ICO *Big data* report, supra n 51 at 6, drawing on Gartner Research work.

[136] Rob Kitchin "Data driven, networked urbanism", The Programmable City WP 14, 10 August 2015 at http://www.spatialcomplexity.info/files/2015/08/SSRN-id2641802.pdf .

[137] See discussion above n 44.

[138] FTC 2015 supra n 65 at 14.

allow inference of data on a previously unprecedented scale. Smartphones already allow inferences concerning a user's mood, stress levels, personality type, psychological disorders, smoking habits, demographic characteristics, sleep patterns, happiness and levels of exercise and movement[139]; the full IoT inputs of a smart city on its individual citizens will allow much, much more. As Wisman comments : "*Bentham's Panopticon is child's play compared to surveillance in a fully functioning IoT*[140]".

Smart cities thus both generate big data sets and function by processing them. In both cases, "big data" need not involve personal data, but almost invariably will do so. Even where data is generated with apparent anonymity – eg footfall in public squares - the relative ease of associating two large databases – say a fottfall database and a CCTV database - to identify persons, is by now well known[141]. The EDPS noted firmly in 2014 that "*it is now rare for data generated by user activity to be completely and irrevocably anonymised*"[142]. Datamining across more than one dataset to put together an identity of a known person from disparate sources, even where there have been attempts at deidentification, is sometimes called the "mosaic effect[143]". User pictures, real names or online nicknames can also often be used as unique or near unique identifiers across multiple databases. In privacy circles[144], the key worries around "big data" thus lie in:

(i) the potential for reidentification of allegedly anonymised or pseudonymised data

(ii) the repurposing of "big data" collected for purposes different from the original;

(iii) the lack of transparency as to how results are derived from big data, in particular where mere correlation (eg "young black men are more often involved in violent crimes" with causation ("young black men should be the first to be arrested on suspicion when violent crimes occur").

(iv) the trend towards exhaustive collection of "all the data" and away from the principle of minimisation of data collection generally promoted by DP law.

A particular worry revolves around the potential for subtle non-transparent discrimination based on data analysis[145] and the possible creation of a "data underclass", unable to access the same services and facilities as their peers because of their "big data" profile - a new kind of "red-lining"[146]. Acording to the A29 WP, "*analytics based on information caught in an IoT environment might enable the detection of an individual's even more detailed and complete life and behaviour patterns.*"[147] This might lead to the denial of insurance; exclusion from the sale of

[139] Ibid, drawing on Scott Peppet "Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security and Consent." Texas Law Review, forthcoming, 2014), pp. 66-67, at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2409074 .

[140] Wisman, supra n 58, section 3.

[141] See literature following Paul Ohm's seminal discussion, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2009) 57 UCLA Law Review 1701.

[142] EDPS, supra n 51 .

[143] See eg http://www.computerworld.com/article/2563635/security0/sidebar--the-mosaic-effect.html .

[144] See further discussion in Bert-Jaap Koops "The trouble with European data protection law" (2014) 4 (4) International Data Privacy Law 250.

[145] See on the due process implications of such (or lack thereof) " D Citron and F Pasquale "The Scored Society: Due Process for Automated Predictions" (2014) Washington Law Review, Vol. 89, 1. Such worries are already well known in the literature in relation to conventional *online* data profiling, as opposed to profiling involving IoT data: see notably the work of Oscar Gandy and Latanya Sweeney ; *Big Data and Smart Devices*, supra n 20 at 12, citing the revelation in April 2015 that female users were shown fewer targeted ads delivered by Google using data profiling techniques for higher paid jobs than male users (n 21 on p 12). On discrimination in smart cities particularly, see Finch and Tene, supra n 90 at 1602-1604.

[146] Marc Ambasna-Jones "The smart home and a data underclass" *Guardian* , 3 August 2015, at http://www.theguardian.com/media-network/2015/aug/03/smart-home-data-underclass-internet-of-things .

[147] A29 WP IoT, supra n 119 at 8.

certain luxury or high end products; sharing of compromising inferences with state agencies[148]; or even total exclusion from markets for service and essential utilities for those unwilling to share personal data. In a smart city the consequences of data exclusion would be physical as well as digital. Certain people (or their cars) might be physically restricted from entering some streets – a new type of "gated community" – or certain shops or entertainment complexes. The complex nature of public-private partnership in smart cities also seems important here – what happens to any right to assembly in public squares (or public speech generally) when all spaces are at least partly privatised?

Another practical worry is that IoT data is quite likely full of errors , and hence so would be the derived "big data" profiles. Townsend has already concisely predicted that smart cities and IoT systems  will be "buggy and brittle".[149] Kitchin emphasises that because datastreams in a smart city are all generated in different ways, using a plethora of instruments and standards, joining them together will result in misleading data of poor quality[150].

Big data and EU law

DP law interacts problematically with "big data" in at least three important ways: purpose limitation, algorithmic transparency and data minimisation.

First, and most importantly, DP is fundamentally based on the idea that data must be gathered for "specified, explicit and legitimate" purposes and not further processed in a way incompatible with those purposes[151].  This "*purpose limitation*" rule applies even where processing has been legitimised by a ground other than consent. Big data is quintessentially at odds with this principle. As Mayer-Schoenberger and Cukier put in in their best selling book, "*in a Big Data age , most innovative secondary uses haven't been imagined when the data is first collected*". Rather than regarding this as a problem, the authors continue excitedly: "*there is a treasure hunt underway*"[152]. It can be (and is) argued[153] that the big data assault on purpose limitation can be dealt with by a number of legal strategies, including asking consent for plausible re-uses at the start, obtaining a new consent to re-uses of data as they arise, or using a non-consent based ground such as "legitimate interests" to make repurposing lawful. However, in each case, it seems apparent that the solution is in fact illusory. A blanket consent to all possible reuses would itself be so vague as to fail the "specific and limited purposes" test; seeking a new consent would also most certainly involve prohibitive overheads for commercial and public service data controllers alike; and reversion to a "legitimate interests" test asks almost compellingly for abuse, given the difficulties of oversight and the delegation of the task of balancing commercial interests and user fundamental rights to the controller themselves.  Finally and most problematically, one much cited feature of data mining is that it may give you answers to questions not even previously thought of – providing answers to not just the "known unknowns" but the "unknown unknowns"[154]. In such scenarios, it is hard to see how any pretense at purpose limitation can prevail.

[148] See Brown, supra  n 69.

[149] Supra n 14.

[150] It is worth noting that DP contains a right for data subjects to correct errors in personal data about them. How should this right be exercised in an age of reused data and non transparent data profiling?

[151] DPD, art 6(b).

[152] Viktor Mayer-Schoenberger and Kenneth Cukier *Big Data: A Revolution That Will Transform How We Live, Work and Think* (John Murray, 2013) at 15.

[153] See Art 29 WP *Opinion 03/2013 on purpose limitation*; supplemented by WP 221, *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU,* September 2014.

[154] See Kirk Borne, TED talk, 10 June 2013, at https://www.youtube.com/watch?v=Zr02fMBfuRA .

Secondly, big data defies the fundamental DP idea of *transparency* of processing. Big data acts as a "black box"[155]; data goes in, outputs come out, but the algorithm that creates the result is usually invisible to the user and the results often inscrutable. Algorithms also learn and change, in a  semi autonomous fashion – making them remarkably hard to document. Finally algorithms are the ultimate trade secret – Google's fortune is arguably based entirely around its advances in search algorithm – and so companies will be remarkably unwilling to make them public. Opaque big data algorithms are dangerous because discrimination which might otherwise be illegal, eg on race or sexual orientation, can easily be hidden, deliberately or not,  behind the algorithmic veil (as discussed above). While subject access rights to find out what data is held about them by a data controller are reasonably well known ( at least to lawyers and campaigners), very little attention is paid to a right also granted by current DP law : to know the "*logic of the processing*" applied to your data[156]. This right to what might now be called algorithmic transparency has always been limited by a carve out to protect intellectual property and trade secrets[157] and may yet be further watered down in the GDPR[158] - but it remains at least a fig leaf to transparency. How it  can be applied and used as consumer protection in the big data world is hard to see: even if the controller actually knows what his algorithm is up to (which many now doubt in vast processing scenarios such as Google's search algorithm), how can the result be conveyed to the data subject in any comprehensible way?[159]

Thirdly, big data also stands in stark opposition to the principle that personal data collected  must be "adequate, relevant and not excessive" in relation to the purposes for which they are collected  and/or  further  processed[160]: a principle now reified in the draft GDPR as that of "*data minimisation"*.  Yet when data scientists are consulted, their passion for the newfound ability to collect "all the data", without the old fiddly statistical constraints of sample size, demographic representation, cleansing data of outliers et al, is palpable. Data minimisation is a peculiar restriction to a data scientist, as opposed to a privacy advocate, in an era where it is cheaper, easier and more useful to collect all the data than some of it, and where basic commercial and human drives point towards acquiring as much data as possible just in case it comes in useful for that "treasure hunt" in the future. As Buttarelli, the current EDPS recently declared: "*..there is a worrying drift towards thinking that with regards to personal information, whatever is possible is also desirable' if personal data are available, they should be collected and stored indefinitely and exploited for any expedient purpose"*[161].

These problems are not really soluble without either major alteration of big data business models or EU law. In fact most data mining, excessive collection  and subsequent repurposing of data is justified, not by proof of compliance with the DP law outlined above, but by the claim that what is processed is not personal data at all. As already noted above, the EDPS has called this out for what it usually is : the replacement of true anonymisation with pseudonymisation of dubious privacy-protective value, for the very good reason that far less commercial value, now or in the

[155] See Frank Pasquale *The Black Box Society* (Harvard UP, 2015).
[156] DPD, art 12(a).
[157] DPD, recital 41.
[158] See Lilian Edwards "Rise of the Algorithms", paper given at Gikii 2013, Bournemouth, slides at http://www.slideshare.net/lilianed/gikii-13-algorithms .
[159] Mayer-Schoenbeger and Cukier supra n 152 suggest a new profession of "algorithmist" who interpret these results to the ordinary user. It is hard to see how the user could check the algorithmist had it right, or check that they were acting independently of the data controller. See further below on algorithmic transparency, pX.
[160] DPD, art 6  ( c).
[161] Speech to the Academy of European Law, "Big data, big data protection: challenges and innovative solutions ", 11 May 2015 at https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2015/15-05-11_ERA_speech_EN.pdf .

future, can be extracted from truly anonymised data[162]. Pseudonymised data profiles, as used eg by social media and search engines to deliver targeted advertising, still allow individuals to be "singled out" and subjected to discriminatory treatment, simply not by name. A turf war is going on between what the Article 29 WP thinks is sufficient anonymisation, and what commercial businesses and some national regulators would like it to be[163], while meanwhile most users (and most lawyers) have no way of knowing what to make, if anything, of competing claims of successful anonymisation, pseudonymisation or encryption[164].

Yet despite having acutely identified the problems above and more, the Article 29 WP and the EDPS continue on the whole to maintain that data protection can survive big data without major reconstruction or demolition. "*The Working Party acknowledges that the challenges of big data might require innovative thinking on how some of these and other key data protection principles are applied in practice. However, at this stage, it has no reason to believe that the EU data protection principles, as they are currently enshrined in Directive 95/46/EC, are no longer valid and appropriate for the development of big data, subject to further improvements to make them more effective in practice*"[165]. This writer would counter argue that the faltering progress of the GDPR on key points such as the definition of consent, the extent of the "legitimate interests" ground for processing and the sudden invention of an ill thought out category of pseudonymous data[166] halfway through the legislative process, seem to tell otherwise.

The A29 WP , the EDPS and European privacy advocates in general may feel constrained to continually assert the effectiveness of the principles of DP as it stands because the alternative, forcibly presented by much of industry[167], some of science[168], and some US policy bodies[169] and scholarship[170], is to cede legal control over *collection* of data, in favour of deferring safeguards to the time of *use*. Such an approach has the comforting appearance of being steeped in pragmatism, social benefit and cost saving; enables state surveillance bodies to claim they are engaged in harmless "bulk collection" of metadata rather than illegal "surveillance"[171]; rubber-

[162] This is not just a problem for businesses. Medical researchers also complain that true anonymisation makes their research more difficult and less useful, especially to the patients who donated their data.

[163] See, Information Commissioner's Office,*Anonymisation: managing data protection risk code of practice.* (November 2012) available at https://ico.org.uk/media/1061/anonymisation-code.pdf ; cf Article 29 WP, *Opinion 05/2014 on Anonymisation Techniques* WP216 (April 10, 2014).

[164] Note the HP/Fortify IoT Research Study, supra n 70 at 4,: 80% of IoT devices tested raised privacy concerns , not least that as 70% transmitted unencrypted personal information, they were "one network misconfiguration away from exposing this data to the world".

[165] A29 WP 221.

[166] Revised article 4(2a) of the European Parliament draft.

[167] See Craig Mundie, *"*Privacy Pragmatism: Focus on Data Use, Not Data Collection*."* Foreign Affairs (2014) 29 at https://www.foreignaffairs.com/articles/2014-02-12/privacy-pragmatism. Mundie is a senior adviser to Microsoft; Letter from Daniel W. Caprio, Jr., Senior Strategic Advisor, Transatlantic Computing Continuum Policy Alliance, to Donald S. Clark and FTC (January 10, 2014), available at https://www.ftc.gov/sites/default/files/documents/public_comments/2014/01/00017-88305.pdf in which many large IoT players including AT&T, General Electric, Intel Corporation, and Oracle Corporation support the move.

[168] See for urban data and smart city researcher perspectives, several essays in Lane et al eds, supra n 103, especially chapter 7. "Date for the Public Good: Challenges and Barriers in the Context of Cities" : "*Privacy rules and regulations and bureaucratic silos often prevent city officials from obtaining and using data to address some of their most intractable problems*".

[169] See Executive Office of the President, *"Big Data: Seizing Opportunities, Preserving Values"* (2014), at p56, available at https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf. Note however the FTC's opposition to this approach: see FTC 2015, supra n 65, at vi–vii.

[170] See eg Fred H. Cate, Viktor Mayer-Schönberger, *Notice and Consent in a World of Big Data,* Microsoft Global Privacy Summit Summary Report and Outcomes (November 2012) at 5.

[171] See David Anderson *A Question of Trust – Report of the Investigatory Powers Review* , June 11 2015 (available at https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-report-of-the-investigatory-powers-review/ ).

stamps the “treasure hunt” and piling high of big data; and alleviates the intractable difficulties of getting a valid and informed consent out of passers by to data collection in the IoT. The problem is, as the FTC recognise, that delaying safeguards to use not collection simply does not protect privacy, either in actuality or in expectations. Once data is into the bag, it will be impossibly hard to police it at some later time when it has been processed, profiled, “anonymised”, data mined, reidentified, copied , mirrored and sent around the globe to various jurisdictions with varying laws, powers of enforcement and social norms re privacy. It will also be difficult if not impossible to find consensus on what uses are particularly pernicious. Particularly in relation to “sensitive data” as the FTC agree[172] – ie mainly, health data – people are understandably worried at the prospect of collection as well as of use.

In summary therefore DP law as currently constituted has no good answers for dealing with the privacy problems presented by Big Data. Answers may conceivably come from other legal instruments such as discrimination and employment law, or from assertion of due process rights under art 6 of the ECHR. Smart cities are likely to be venues for such disputes.

### *(iii) The Cloud*

Finally it has to be noted that, of course, most of the vast amount of data generated in smart cities will be stored in the Cloud. Cloud computing is typically based on the provision of resources to users from a network of servers and of providers and sub-providers, with data storage, software and infrastructure all made dynamically available “as a service”: usually with huge advantages in speed, cost and scaleability to the consumer or business using the Cloud. Data in the cloud typically has an unknown and varying place of storage and/or processing, often compounded by multiple back ups or distributed processing of data in multiple jurisdictions. It is sometimes possible to specify contractually that data will not be stored or processed outside the EU[173] but this is at present very unusual in the consumer market, for reasons of logistics on the part of the dominant US companies in the market, and the lack of a strong homegrown EU cloud industry sector. The widespread use of cloud computing for receiving and processing data from smart IoT devices and applications thus raises thorny legal issues revolving around jurisdiction and applicable law[174] compounded by the difference in privacy cultures already pointed out between the US (where most of the major cloud computing providers are based) and the EU.

### The Cloud and EU law

The DPD provides for the free flow of personal data to countries located outside the EEA only if the country or the recipient provides an “adequate” level of data protection, thus potentially limiting cross-border data transfers. Given the very small number of countries outside the EEA which have established they have “adequate” DP or similar regimes, the exemptions provided by Article 26 of DPD to enable transfer data out of the EEA have become crucial. They include a number of grounds including the consent of the data subject, the “safe harbor” scheme in the case of transfers to US companies, model contractual clauses and binding corporate rules (BCRs).

[172] FTC, supra n 65 at 39 and n 159. Note that the FTC do suggest that some “use based” restrictions or permissions should be accepted: eg an “expected use” (p 43) - one that is “consistent with the context of the interaction” should be allowed without consumer consent. It is hard to see how this gels with their admission that “it is unclear who would decide which additional uses are benficial or harmful” (p 44).

[173] Google has for example reputedly made this available to some UK universities implementing its Gmail services for free student and staff email.

[174] See discussion in A29 WP 196, *Opinion 05/2012 on Cloud Computing* , section 3 passim. For a general UK-focused overview of cloud computing law, see Christopher Millard ed *Cloud Computing Law* (OUP, 2013).

However, at the time of writing virtually all the legal routes to facilitate transfer of data to and from the Cloud (defined as potentially including storage outside the EU) are being challenged and imminently in crisis. The Art 29 Working Party, and the future draft GDPR have taken an increasingly hard line on data exports from Europe since the Snowden revelations, with the A29 WP arguing in particular that consent as an exemption should not be relied on where transfers are recurrent, massive or structural[175] The draft GDPR may also in future restrict use of consent where "*there is a significant imbalance between the position" of the data controller and the data subject"*[176] and it seems likely this will also cause problems in some cloud computing contracts. Finally and most significantly , summing up the frost in the CJEU since the Snowden affair, the CJEU has recently declared the entirety of "safe harbor" illegal, with a possible renegotiation now hard to see and future challenges likely also to Binding Corporate Rules (BCRs), model contractual clauses and other methods of legitimising data transfers to the US[177].

It is not at all easy to predict how the Cloud, or the law, will adapt themselves now "safe harbor" has been struck down. The decision may in fact be seen as more symbolic than anything else, given the relatively small number of US companies enrolled in safe harbor, and the large amount of data transfers out of the EU in fact facilitated by model contracts and other informal and more flexible arrangements (around 50% according to one estimate). One aspiring solution for European smart cities may be to help build and use a Europe-only cloud (also referred to as a "Schengen cloud") [178]. Deutsche Telekom AG, Germany's biggest telecoms provider, has apparently already started to implement such.[179]

(iv) *Interim conclusions*

It is striking how despite a long period of societal bemoaning of the "death of privacy" in the digital networked era, the principal privacy institutions of both the EU and US, aided by an increasingly aggressive CJEU, are nonetheless very determined to assert that the so-called corpse, or at least the DP version of it, is in fact alive and well. The reaction of the A29 WP quoted above is typical of Europe's watchdog body: DP is still fit for purpose and in principle does not need modified, though the detail may need some fine honing to deal with threats such as the increasing marginalisation of informed consent, big data, the IoT and the Cloud. The FTC's reaction is surprisingly similar: faced with the enumerated issues of IoT above, and even without the cultural foundation of an omnibus privacy law founded in human rights to depend on, they still assert "*protecting privacy and enabling innovation are not mutually exclusive and must consider principles of accountability and privacy by design*"[180].

But other voices from industry, security and policy grumble loudly beside them ; the UK as a business-friendly outlier in the privacy culture of Europe has been one of the principle voices

[175] See A29 WP Working Document 12/1998: *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, pp. 27-28. See also A29 WP, *Opinion 05/2012 on Cloud Computing* WP 196. para 3.5.2., p. 18.

[176] Article 7(4) of draft GDRP as per European Parliament. It remains uncertain if this provision will survive trilogue. See Paul Schwartz, "EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation", SafeGov (May 13 2013), at http://safegov.org/2013/5/13/eu-privacy-and-the-cloud-consent-and-jurisdiction-under-the-proposed-regulation .

[177] See *Schrems v Data Protection Commissioner of Ireland*, Judgment, Case C-362/14, 6 October 2015.

[178] See W. K. Hon, C. Millard, C. Reed, J. Singh, I. Walden, and J. Crowcroft, "Policy, Legal and Regulatory Implications of a Europe-Only Cloud." SSRN (November 21 2014), pp. 2-3, at http://www.picse.eu/sites/default/files/PolicyLegalandRegulatoryImplicationsof%20EuropeOnlyCloud.pdf .

[179] See Nicole Henderson, "With Plans to Double Business Cloud Revenue by 2018, Deutsche Telekom Extends Huawei Partnership" (June 15 2015), at http://www.thewhir.com/web-hosting-news/with-plans-to-double-business-cloud-revenue-by-2018-deutsche-telekom-extends-huawei-partnership .

[180] FTC, supra n 65 at 39.

pressing for a more "risk-based" application of DP law which has potentially found its way into various parts of the GDPR[181] ; and enforcement, rather than the principles themselves, remains the key failure point of DP law, even more so when taking account the effective landgrab by the EU over data processing by non EU companies working in EU markets ushered in by the *Google Spain*[182] case. Just as declaring "safe harbor" void will not in practice stop data flowing to Google, Facebook, Amazon et al, merely make it it a bit more difficult, so privacy in smart cities can also not be safeguarded by ever more exhortations to respect the law, particularly as that law becomes ever more baroquely complex and subtle to interpret[183]. In this writer's opinion, solutions in natural surveillance architectures such as smart cities must be built into the code of these cities – not just their software and hardware but their material design. This is the principle of "privacy by design", and in the final section, I examine this both in abstract, and with some concrete examples of solutions proposed by data scientists and human: computer interaction (HCI) specialists.

## VI. Solutions?

### *(i) Privacy by Design and Privacy Impact Assessments*

*Privacy by design* (PbD) is an approach to protecting privacy by embedding it into the design specifications of technologies, business practices, and physical infrastructures[184]. PbD solutions (to pick a few that are particularly relevant to smart cities) include: restricting the amount of data applications collect to the minimum; encrypting data flows as default; anonymising personal data (see earlier comments on difficulties thereof); embedding privacy notices systems in user-friendly ways at appropriate times; restricting the retention periods of data ("data expiry"); providing menus of privacy settings which are in clear language and user friendly, and where defaults are particularly protective of children; using "flash cards" to make system designers think about privacy issues as they build their systems[185].

PbD, which builds holistically on the older notion of Privacy Enhancing Technologies (PETs) has already been applied to the big data issue to produce suggestions for "Big Privacy"[186] but there is little sign of it in the IoT debates to date (see issues examined above). The most radical solution via PbD to the problems around the IoT might be to argue that data collected by devices be held locally (and as far as possible processed locally) and thus maintained under the control of the user, rather than gifted to data controllers, in the Cloud or otherwise. This solution, sometimes known in the computer science world as "personal data containers" is receiving a great deal of attention from researchers[187]. While detailed critique is beyond the scope of this article, such solutions raise their own problems of security and comprehensibility to (and hence control by) average users in the current state of development. Hildebrandt and Koops go further

[181] Of course as the A29 WP themselves remind us, the DPD has always had some elements of risk assessment eg the different protection accorded ordinary and sensitive personal data. However their resistance to the idea in relation to big data and a move from restrcitions on collection to restrcitions on use is patent. See WP 218 *Statement on the role of a risk-based approach in data protection legal frameworks* , 30 May 2014.

[182] Supra n 127. Also see now Case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság,* Judgment, 1 October 2015.

[183] Or as Neil Brown put it on Twitter post *Schrems*: "*Law doesn't protect data — it just nudges behaviour. I use maths to encrypt my disk, not wrap it in a copy of directive 95/46/EC.*" (@neil_neilzone, 6 October 2015.)

[184] See https://www.privacybydesign.ca/ .

[185] See Ewa Luger, Lachlan Urquhart, Tom Rodden and M. Golembewski "Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process" *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (CHI 15), Seoul, 18-23 April 2014.

[186] See Anne Cavoukian and Drummond Reed *Big Privacy: Bridging Big data and the Personal data Ecosystem Through Privacy by Design, 2013,* at https://www.ipc.on.ca/images/Resources/pbd-big_privacy.pdf .

[187] See eg Malte Schwarzkopf et al "Personal Containers: Yurts for Digital Nomads", at http://www.cl.cam.ac.uk/~avsm2/perscon-d1.pdf .

and argue that where processing is controlled locally in devices, code constraints can be built in which reify the rules of law protecting users, a concept they name "ambient intelligence"[188]. However Koops and Leenes have also expressed doubts as to the practicality of architecture embedding DP rules, arguing that encoding privacy provisions in law is "*far from trivial*", most obviously because of the "*flexible*" (ie open textured) phrasing of most laws in the area and because of the lack of a "*privacy mindset*" in IT system designers[189].

As faith in legal privacy solutions has ebbed in the globalised information world, PbD solutions have arguably been given more and more visibility by policymakers and privacy regulators as well as academics. However in 2014, ENISA still reported that "*privacy and data protection features are, on the whole, ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realise privacy by design. While the research community is very active and growing, and constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice*."[190] For most companies, the motivations to code actively to protect privacy rather than to track data, remain few[191].

Recent empirical work by Irit, Hadar et al in which software engineers were interviewed in a number of employment settings, about their privacy coding practices, comes to similar conclusions[192]. They note that the engineering mindset often restricts the vocabulary used around privacy, and hence the action taken, to "security" in the sense of third party threats (section III above) rather than a wider view embracing ideas like consent and purpose limitation. 14 out of 27 engineers in the interview sample had no knowledge of privacy law, and only 4 could reference specific privacy laws. The organisational culture of commercial companies where some engineers worked, though giving lip service to privacy policies, actually largely ignored or discouraged consideration of PbD. Interestingly, the team also found considerable evidence that coders did not want to "take responsibility for privacy". Privacy was a social or moral issue and their domain was technology and engineering[193]. The paper concludes : "*Privacy by design? Well, not just yet… if PbD is ever to become a viable practice, a considerable change [needs] to be made."*

Despite these forbodings of futility, PbD will soon probably be mandated by law in the EU. A legal commitment to PbD (including "privacy by default") in the draft GDPR has been loosely agreed by all parties in the process, but has remained throughout maddeningly vague.[194] Recital 61 of the European Parliament pre-trilogue draft of the GDPR asserted that : "*the principle of data protection by design requires that data protection be embedded within the entire life cycle of the technology, from the very early stage, right through to its ultimate deployment, use and final disposal*." How ordinary

[188] See eg Mireille Hildebrandt and Bert-Jaap Koops "The Challenges of Ambient Law and Legal Protection in the Profiling Era" 2010 73(3) Modern Law Review 428.

[189] Bert-Jaap Koops and Ronald Leenes "Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the 'Privacy by Design' Provision in Data-Protection Law" (2014) 28 (2) International Review of Law, Computers & Technology 159

[190] G Danezis et al *Privacy and Data Protection by Design – from Policy to Engineering* (ENISA: Heraklion 2014) p iv.

[191] Koops and Leenes, supra n.188.

[192] "Are Designers Ready for Privacy by Design? Examining Perceptions of Privacy Among Information Systems Designers?", 2014 TPRC Conference Paper, abstract at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2413498. The authors kindly shared a draft with this writer.

[193] This writer has observed herself at multidisciplinary events that lawyers frequently look to technologists for privacy solutions while technologists do the exact opposite – a sort of regulatory "pass the parcel".

[194] Some guidance has been provided by the A29 WP for the IoT : supra n 119 at Section 7.1

engineers and coders, without substantive training or awareness of privacy in any detail, often working in small IoT or cloud businesses which are not customer-facing, and tasked to focus on speed and cheapness, will implement this holy grail in smart city applications, poses a very large problem for the future.

*Privacy Impact Assessments* (PIAs) are one approach to making PbD more viable and effective. They are also mandated by the draft GDPR (as "data protection impact assessments") though only in particular circumstances of novel or inherently risky processing[195]. The ICO's Code of practice on conducting privacy impact assessments defines a PIA as "*a process which assists organisations in identifying and minimising the privacy risks of new projects or policies*."[196] PIAs are now fairly widely used around the world by stakeholders in novel or sensitive areas such as medical or genetic technologies, to define and foresee privacy threats in order to develop solutions at the early stages of projects or programmes.[197] The outstanding example of thinking about applying PIAs systematically to an early IoT technology can be found in the work of Spiekerman and her team on the EU framework for a PIA for RFID chips[198] and the A29 WP has already recommended adapting the RFID framework to map threats in smart cities[199]. This framework has since been refined further to create the Data Protection Impact Assessment (DPIA) Template for Smart Grid and Smart Metering systems[200].

Spiekerman's assessment of the strength of the RFID PIA lies in its attempt to control a serious treat to privacy – data collection via the IoT – through a "relatively complete, holistic and proactive tackling of the problem". She also promotes its co-production with industry, its global acceptability and the flexibility of the solutions arrived at which could be adapted to particular industry sectors or technologies. Her doubts are however interesting. She admits that creating the RFID PIA was merely the "proof of concept" phase and that companies would have to be "really willing to comply with the rules that they have set for themselves". This is in fact exactly what Irit, Hadar et al found not to be the case and the anecdotally slow uptake on the RFID PIA seems to back this up. Another issue was uncertainty as to whose responsibility it was to kick off a PIA, and whether existing RFID implementations should be included in the PIA scheme (answer: no, unless there were "significant changes" in the application, such as expanding beyond original purposes) . The biggest question of all was sanctions. How would companies suffer if they did not undertake such a PIA, or gain if they did? This uncertainty will

[195] See discussion in Rolf Weber "Privacy management practices in the proposed EU regulation" International Data Privacy Law (2014) 4 (4): 290-297.

[196] ICO, *Conducting privacy impact assessments code of practice*, Version: 1.0 (February 2014), p. 5, at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

[197] See Center of Excellence for Information Sharing, *"How Do We Identify and Assess Risks to Privacy?"* available at http://informationsharing.org.uk/our-work/tools/scoping/how-does-the-partnership-assess-the-risks-and-benefits-of-the-information-sharing/how-do-we-identify-and-assess-risks-to-privacy/. See generally Wright and deHert eds at n 84 supra.

[198] Supra n 84. The final document produced is available at A29 WP, *Privacy and Data Protection Impact Assessment Framework for RFID Applications* (January 12, 2011), available at http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf . It is however non-mandatory and uptake has reportedly been low: see "The Societal Impact of the Internet of Things", report of workshop on the Internet of Thing organized by BCS, the Chartered Institute for IT, on 14 February 2013, pp. 11-12, at http://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf .

[199] See A29 (2014), supra note 119, at p. 21 .

[200] See Smart Grid Task Force 2012-14, Expert Group 2: Regulatory Recommendations for Privacy, Data Protection and Cyber-Security in the Smart Grid Environment, *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems* (March 18, 2014), p. 5, at https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf .

remain even if the GDPR passes in its current form given the vagueness of the criteria for when a DPIA is required.

Can a PIA usefully be carried out for a smart city as an entity? This is unlikely to happen *ab initio* in the Western world model of retrofitted smart cities, where ubiquitous computing acquires traction by slow aggregation (though Spiekerman would almost certainly say such additions form a "significant change") – but if we look to a future where smart cities (or new sections of them) are routinely built top down, as in India and Korea, then the challenge is both more likely. Greenfield and brownfield development schemes in the UK are already routinely preceded by impact assessments of various kinds eg relating to population, traffic flows etc, and these seem broadly successful despite the complexities. Traditional PIAs however assume an ability to map data inputs, flows, and outputs, identify the "owners" (controllers) of the data and bring these stakeholders together to make decisions, ideally with one person at the top of the decision-making hierarchy. In a smart city, as we have seen, there will be hugely multiple interacting data flows, multiple data owners/controllers and different jurisdictions of storage and processing, with all of these varying over time and creating feedback loops with each other. The city mayor or municipal government may well feel they have the power and duty to control the final design – but actual (though perhaps not legal) control may rest with private vendors or investors and their sub and sub-sub-providers in the Cloud. Future cities may even have "adaptive architectures" which begin to decide themselves what data to collect and how to process it[201]. Algorithms will be opaque and change as they learn in ways such that even data controllers may have little idea what exactly is happening in their data silos and conduits. In this "*Kafkaesque machinery that manipulates lives based on opaque justifications*"[202] we will need to think very hard about how to get PIAs useful. This will be as much a job for urban planners, engineers and architects (among others) as privacy experts.

Notwithstanding it would be good to see a research effort begin to think about how a PIA might start to map potential risks, and explore PbD solutions in a dedicated way for smart cities[203]. A role for co-ordination and standardisation here (important for global impact[204]) might fall to a number of bodies including the BSI and ISO[205] authorities. PIAs are also ripe for expansion to explicitly investigate a number of other fundamental human rights or eithical areas problematic in smart cities. For example, as briefly mentioned above, big data profiling has serious implications for discrimination practices, due process (eg, evidence used to construct crimes) and freedom of speech (eg when public social media are data mined). A holistic PIA – a precautionary but also enabling framework for "ethics by design"[206] – would be a magnificent obsession indeed.

[201] Holger Schnädelbach " Smart Cities: The Built Environment as the Interface to Personal Data" in SCL special edition, supra n 1.

[202] Taken from Omar Tene and Jules Polonetsky "Big data for All: Privacy and User Control in the Age of Analytics" 11 Nw J. Tech and Intell. Prop. 239 at 243.

[203] An interesting US contribution from Michael Froomkin suggests a model taken from environmental impact assessments to regulate mass surveillance in urban areas. See "Regulating Mass Surveillance as Privacy Pollution: Learning from Environmental Impact Statements", draft available at SSRN, last revised Nov 2014 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2400736 .

[204] It should be noted of course that there are still considerable dissenters from the value of "prior warning" approaches such as PIAs at all : see eg Adam Thierer, championing the value of "permissionless innovation" over the "precautionary principle": see Thierer "The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation" (21) Richmond Jnl of Law and Technology 1 at http://jolt.richmond.edu/v21i2/article6.pdf.

[205] See BSI work on standards in smart cities at http://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/ . For ISO contribution, see n 17 supra.

[206] See some foreshadowing of this in work to be commissioned at n 103 above.

### *(ii) Applying PbD more specifically to smart cities*

In this section I want to focus closely on one problem, that of obtaining informed consent in IoT environments. Consent is important because, while not the only legitimate ground for processing in EU DP law, it is the most global standard of legitimacy (given the US non-mandatory concept of notice and choice), and most likely to engender user trust. Where sensitive data is collected furthermore, eg health data, in the EU scheme explicit consent will generally be required. As noted above, getting meaningful consent in IoT environments is a hard problem. If PbD can aid us here, it has a fighting chance of helping elsewhere. Consent is also an area where a cross disciplinary literature related to the IoT has begun to accumulate from computer science, security, HCI, ethics, medicine and psychology as well as law.

Various approaches have already been canvassed by researchers, usually in a rather aspirational way. Traditionally, consent is given at the time that data is collected. The FTC and others have came up with a number of existing good practice approaches to obtaining such consent[207] in a world of multiple tiny devices with no user interfaces, designed to be as unobtrusive as possible. We can catalogue this sort of approach as not deconstructing traditional "notice and choice" but clarifying the choices, or boosting the notice, to meet the constraints of IoT.

*Improved traditional "notice and choice"*

These strategies include :

(i) directing customers to video tutorials to guide them through privacy settings pages (drawn from Facebook) or alternately providing "set up" wizards to get data collection choices right[208];

(ii) homes or other locations might have detailed control "dashboards" or "management portals" where consumers could review with some clarity what data they had chosen to share from time to time across different applications or via different devices;

(iii) putting QR codes on IoT devices, which could be scanned by customers using their smartphones, to give them easy access to privacy policies or other advice;

(iv) providing icons to convey privacy-related information, such as a flashing light that appears when an IoT device connects to the Internet; different icons might flash up to show different levels of risk, and/or different types of data collection.

(v) Customers might ask "just in time" for privacy and security settings to be sent to them via emails or texts

None of these seem to get us much further in the context of smart cities, especially in busy public settings such as smart transport networks. Will users really stop to retrieve, read and consider privacy policies on their phones, even shortened ones, even if acquired via QR codes, while trying to catch a smart tram or hail an autonomous car/taxi or buy a pizza from a passing drone? Most non-IoT research on consent and privacy policies says

[207] See FTC , 2015, supra n 65, at pp. v and 41-42.

[208] In the IoT, unlike on Facebook, these menus or tutorials would presumably have to be navigated via another connected device the user has access to which does have a screen eg smartphone. This is clumsy to say the least.

not, and the problems only get worse in the IoT[209]. Icons may be more easily grasped, and thus of more use: but also raise large issues of recognisability, confusion, global standardisation and interoperability: to date, no single framework for privacy icons has emerged nor has any of the very many aspiring schemes of privacy icons caught on as a global standard, or even been much used[210].

The key problem remains as already discussed, that even if methods can be found for giving some kind of notice/information, the consents obtained in the IoT are almost always going to be be illusory or at best low-quality in terms of the EU legal demand for freely given, specific and informed consent.[211] If use of smart devices becomes unavoidable in a smart city, then "notice and choice" simply becomes an inapplicable paradigm.

*"Pre-consent"?*

An alternate approach which might look more promising, is to reconsider how consent might be given in the IoT world, conceiving it as an ongoing process, rather than a one-time choice at the point of data collection[212]. We have some precedent for this in the offline world in the form of advance "opt-out" preference systems, such as the UK Telephone Preferences Service[213], where a user can say they do not wish to receive junk mail or be cold-called at any time in the future. Online, attempts to transfer this model to the placement of cookies by websites in the form of "do not track" (DNT) systems have so far been resounding failures, with attempts to negotiate between browser manufacturers, websites, and policymakers from EU and US ending in abject collapse[214]. The DNT fiasco showed up a number of problems: first, does "do not track me" mean "do not collect my data" or merely "do not use my data to send me targeted adverts, but collect it anyway?"; second, in a self regulatory system, how can websites be compelled to obey the DNT tag; third, how can the user know if there is compliance or not, given the information assymetry? The second problem in particular persists even if one

[209] See eg A M McDonald, L F Cranor "The Cost of Reading Privacy Policies" (2008) 4 Journal of Law and Policy for the Information Society 540. The Ofcom commissioned report *Personal data and Privacy* , supra n 101, Annex at p 64, considered that existing problems with non-reading of privacy policies would only be exacerbated by the IoT, especially given more and more devices would become connected, demanding more and more complicated privacy policiesto be read. Furthermore, reading a privacy policy might take longer than the actual length of interaction with the IoT device, reducing further incentive to read. Information assymetruies would also be increased in the IoT : "*consumers will be very likely to lose any ability to assess possibilities for data uses in the IoT*", again rendering privacy policies fairly useless.

[210] See survey in Lilian Edwards and Wiebke Abel *The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services,* CREATe Working Paper 2014/15*, at* *http://www.create.ac.uk/blog/2014/10/31/create-working-paper-201415-the-use-of-privacy-icons-and-standard-contract-terms-for-generating-consumer-trust-and-confidence-in-digital-services/* Successful examples of the use of icons to provide consumer information do exist "off-line" eg energy use by applications, laundry instructions and nutritional labelling; and in the digital world, such as the use of Creative Commons icons to indicate the permissions given by the creator of a copyright work. The best known online privacy icons set (PIS) is probably that sponsored by Mozilla and found at https://disconnect.me/icons . It is possible the GDPR may mandate privacy icons as graphic representations of privacy policies which may hasten standardisation.

[211] See text at n 124 above, and below.

[212] Or use (see below). See further Ewa Luger and Tom Rodden "An informed view on consent for UbiComp" *Proceedings UbiComp '13 , Proceedings of the 2013 ACM international joint conference on Pervasive and ubiquitous computing,* pp 529-538 ACM, New York.

[213] http://www.tpsonline.org.uk/tps/index.html . While a self regulatory initiative, this system is backed by EU and UK law, giving it enforcement teeth via the ICO. DNT systems, as created by W3C and browser writers, do not benefit from this.

[214] See (cynically) "W3C's failed Do Not Track crusade tumbles to ad-blockers' Vietnam", *The Register* ,29 Jul 2015 at http://www.theregister.co.uk/2015/07/29/dnt_dead_in_the_water/ .

regime (eg the EU) legislates to require DNT as mandatory, but another (eg the US) does not. A number of commentators have proposed in effect extending the DNT model to the IoT, notably Weber with his call for a right to a "silence of the chips[215]" – but none have so far made a workable suggestion in a global environment.

From HCI literature (and as far as this writer knows, not yet absorbed into the legal lexicon) comes another suggestion decoupling the time of giving consent from the time of collection of data, which is that of "*sticky privacy preferences*". The idea here is that the privacy choices you made earlier are remembered by smart systems, and applied the next time a choice needs to be made. The FTC suggest that a single device in a smart home – a home appliance that acts as a hub – could learn a consumer's preferences based on prior behaviour and apply them to new appliances and new uses. This has some promise: psychologically, behaviour is often consistent, and such systems could use big data profiling over time for good not evil. But even the early primitive examples we have of smart machine learning in homes, eg, the NEST thermostat, which learns how users like their home heated at different hours, show problems with the outcomes: users complain, eg, that the house is heated how they like , yes, but it costs them more than in the old days when explicit choices had to be made about when to turn the heating up. It might be better to skip this stage and move on to fully fledged programmable software agents which we can use to make "*semi-autonomous*" choices for us about our privacy in ambient environments[216]. This idea is gaining some currency in computing science research circles[217] but as yet has not proved itself in the wild. To a lawyer as opposed to a data scientist, it seems unlikely that the difficult personal, ethical, social and financial choices involved in collection and use of personal data, not to mention the problem of changing contexts, can be reliably modelled by pre-coded agents, even ones that learn as time progresses[218] – but the approach is in theory at least a little hopeful.

*Moving away from notice and consent entirely*

Many European commentators are moving towards the notion that notice and choice, or consent as a ground for legitimising processing, is simply broken. Users, as has been proven over and over again, have neither the resources, opportunity, inclination, or motivation to give meaningful consents[219] in the current online environment and this is only exacerbated by the IoT[220]; yet their individual chimeric choices are allowed to rubberstamp patterns of data collection which are increasingly damaging for society. Simulataneously, on the other side of the Atlantic, some writers are also arguing that responsibility for ensuring ethical and responsible data collection should be on the data collectors, not the hapless users. In this case, though, the acknowledgement often comes

[215] See further Rolf Weber and Romana Weber, *Internet of Things: Legal Perspectives (*Springer, 2010) at 39. See also A29 WP IoT n 119 at 22, suggesting that IoT devices must offer a "do not collect" option to subscribers. This would not prevent the data of third parties being collected however.

[216] See eg Gomer, shraefel and Gerding "Consenting agents: semi-autonomous interactions for ubiquitous consent", *Proceeding UbiComp '14 Adjunct Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing*: Adjunct Publication, pp 653-658, ACM New York at http://dl.acm.org/citation.cfm?id=2638728.2641682 .

[217] And, very recently, in law and IT circles : see eg Polonetsky who proposes obtaining consent in advance through profile management portals that would allow consumers to determine what information they agree to share. See Jules Polonetsky, Comments of the Future of Privacy Forum on Connected Smart Technologies in advance of the FTC "Internet of Things" Workshop, (July 10, 2013).

[218] And one wonders, how easy would such agents be to hack? Would our privacy agents need DRM, or anti virus protection?j

[219] See the interesting interdisciplinary project on Meaningful Consent in the Digital Economy at http://www.meaningfulconsent.org/ .

[220] See n 207 supra.

with a catch: the transfer of legal or ethical safeguards to the time of *use* of the data not its collection, with safeguards (if any) varying according to use[221]. As already noted above[222], this could be the kind of loophole, well meant or otherwise, which might actually spell the final death of data protection.

Ethical constraints on data collectors, regardless of whether or not users give meaningless consents, are being promoted as a new approach. It is not uncommon for professionals such as doctors, lawyers, even architects, engineers or electricans to be held to a higher level of conduct than the basic law demands, by professional codes, BSI standards or organisational seals. Such "soft law" guarantees are often seen as effective in competitive consumer-facing markets where good behaviour can attract business. However the data collection markets to date are famously not competitive in this sense, as a result of information asymetries plus network effects. Can ethical standards be presented as a selling point to users or industry? The EDPS seems to think so: his latest opinion at time of writing[223] recommends a "new digital ethics" for "accountable controllers" in which empowered prosumers will be able to disclose data without fearing the loss of their "dignity". Such ideas have appeal within academic research communities, and may offer help in sensitive public sector services such as health, as well as in relation to new and potentially dangerous innovation[224]. But although there is some evidence from US cloud computing after Snowden, and panic reactions to security breaches, that industry will move to higher standards of care than the law requires where there has been a crippling loss of trust[225], the lack of causality between the slow drip drip of "ordinary" data disclosure and eventual harms to users means there is generally no such Eureka moment where consumers lose all faith.

So, finally biting an unwelcome bullet, the way forward may simply be to admit that consent is only a first step to lawful processing and that regardless of such permission, certain uses of that data, on the environmental model, are toxic and thus prohibited. In other words, to make new law, not rely on unenforceable "ethics". Obvious examples of possibly prohibited practices include targeting advertising to children, targeting alcohol, diets and drugs to addicts and anorexics, and making use of data gathered in inherently private places such as bathrooms. But beyond this there is, of course, almost no consensus (and even these might be argued as a fair part of the free market by some US industry). Given the whittling away in the draft GDPR to date of even existing rights to object to automated decision making and profiling, we should not hold our breath waiting for, say, a globally respected regulated and enforceable code of conduct for certain data collecting sectors[226].

One distinct area where we might look for legal intervention, in particular in reference to the IoT, big data and smart cities, is the area of algorithmic transparency. Although I expressed uncertainty above that such transparency is actually available in the world of big data and learning algorithms, techniques for reverse engineering what is going on the "black box" will no doubt improve[227], and it is certainly one of the best potential tools

[221] See eg Obama's *Big Data* report, supra n 169 at 56 and Cate, Cullen and Mayer-Schoenberger, supra n 170.
[222] P xx.
[223] EDPS Opinion 4/2015 *Towards a New Digital Ethics* (September, 2015) .
[224] See eg HC Science and Technology Committee *Responsible Use of Data*, 4th Report of 2014-15, 19 November 2014.
[225] See *Ethical Code of Practice for Big Data Analysis* (Hewlett Packard, 2015 – shared privately with author); Digital Catapult *Trust in Personal data: a UK Review* (2015) at http://www.digitalcatapultcentre.org.uk/wp-content/uploads/2015/07/Trust-in-Personal-Data-A-UK-Review.pdf ; Tho cf Rosner, supra n 54.
[226] See second half of Edwards and Abel, supra n 208.
[227] Block chains may also offer opportunities for external audit and verification of algorithms.

for shining a light on what data profilers are actually up to. The little known right in the DPD of data subjects to obtain "*knowledge of the logic involved in any automatic processing of data concerning him*"[228] should be unambiguously retained and indeed explicitly extended to deal with all big data processing, and with some reasonable cutting down of the current hiding place provided by IP rights and trade secrets[229].

*Science fiction*

How would we design the perfect future world which lets us, both individually and as a society, make the most of every positive feature of living in smart cities while maintaining our right to a private life? One tempting solution is found in Hannu Rajaniemi's *The Quantum Thief*[230]. In Rajaniemi's far future city, people can choose to be invisible to all forms of data collection and tracking by assuming a technological shield known as a "gevulot[231]". Certain public spaces in the cities exist where gevulots cannot be used so that accidental communion and public speech can still occur, but otherwise all interaction and data disclosure with other citizens is negotiated by the gevulot.

> "*When two citizens randomly meet on the street their gevulot automatically exchanges privacy preferences and negotiates specific concessions. If someone does not want to be seen by you, then your gevulot will automatically blur/mute them out by interfacing with your visual cortex. If they wish to talk to you, then you will have to negotiate a gevulot contract which specifies whether this is going to be a public or private conversation, whether or not its contents can be shared with others, how much of it will be remembered by both parties, whether emotional reactions should be shared or if facial expressions and voice inflections should be algorithmically normalized.*[232]"

Is this "total privacy society" the world we want to live in? Leaving that aside as a hanging question, some elements of this utopia/dystopia are already visibly in sight. There are moves towards DRM for personal data – which might allow you to control who does what with your data - and to track its provenance wherever it goes[233], even possibly where combined into profiles or pseudonymised. Joseph Lorenzo Hall of the Centre for Democracy and Technology has suggested a "General Privacy Menu" which could allow consumers to control the amount and nature of data collected by IoT sensors and devices in sensitive locations, such as home and workplace, through development of a standard element to the networkable components of IoT objects.[234] There is in general a great deal to anticipate in the emergence of a new discipline of "HDI"[235], human-*data*

[228] DPD, art 12(a).

[229] See recital 41 and note even the current text says "*these considerations must not, however, result in the data subject being refused all information*".

[230] Gollancz, 2011.

[231] Apparently Hebrew for "borders".

[232] An excellent paraphrase, better than this author could muster, from Luke Maciak "Total Privacy Societies: *The Quantum Thief* by Hannu Rajaniemi" , August 10 2011 at http://www.terminally-incoherent.com/blog/2011/08/10/total-privacy-societies-the-quantum-thief-by-hannu-rajaniemi/ .

[233] See eg Siani Pearson and Marco. C. Mont "Sticky Policies: An Approach for Managing Privacy across Multiple Parties" IEEE, 2011 vol.44, Issue No.09 - Sep , pp60-68.

[234] See Joseph Lorenzo Hall, Center for Democracy & Technology (CDT), Comments for November 2013 Workshop on the "Internet of Things" (June 1, 2013), p. 4 at https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00028-86211.pdf .

[235] See Mortier R et al "Human-Data Interaction: the Human Face of the Data Driven Society", University of Cambridge, 2014 at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2508051 .

interaction, which proposes "*placing the human at the centre of the flows of data and providing mechanisms for citizens to interact with those systems and data explicitly*". It it a long way off but the "*computational turn*"[236] which has so quickly impacted our privacy may turn again to give us tools with which it can be managed, both for our own purposes and for societal good.

## VII Conclusion

The future of smart cities is important. They may offer solutions to some of our worst problems – conserving energy and creating a sustainable environment, maintaining public safety, engendering community, rescuing millennials from depression and loneliness, reducing road deaths. In cities with areas of mixed and multiple deprivation like the writer's own home town, Glasgow, their appeal is obvious and not to be rejected, even if a degree of cynicism on how much benefit will accrue to vendors and municipal leaders rather than the residents is reasonable. But even within this context, privacy and security are important : if not simply as a fundamental right, then instrumentally, as a prerequisite to keeping the trust and engagement of smart city dwellers. By now, as a society, we have a number of salutary stories of what happens when technology is perceived as dangerous and out of control, rationally or irrationally: eg the backlash against GM crops and their products; the fear of "killer robots"; and the recent Scottish Government ban on fracking, self admittedly based not on evidence but on public disquiet[237], all come to mind.

In the privacy sphere, probably the most obvious recent defeat of innovation by privacy fears has been the rise and fall of the wearable Google Glass, with its users labelled Glassholes, banned from shops and public spaces and occasionally even attacked. If we lose faith in the physical architecture of our cities, homes and vehicles then the backlash may be much worse – as perhaps seen in the current outrage at the revelations of VW's falsifications of its diesel cars' emissions tests. We might see resistance to surveillance in smart cities, as we have seen resistance to CCTV by the young in the form of hoodies. If a significant number of users in smart cities refuse, say, to engage with services provided via smart devices or environments , we may produce a new underclass of the digitally dispossessed or marginalised, unable perhaps to vote, claim welfare, or access medical services. These are all worrying futures we should try to avoid.

This paper has tried to establish that while the political and economic drivers of smart cities tend towards technology supremacism, smart cities, at least in Europe, will still suffer as a project if they fail to get privacy right; and that at the moment this failure is very likely, suffering as they do from the combination of three of the most difficult issues for modern privacy law to regulate: the IoT, big data and Cloud based infrastructure. Even in the EU with its history of strong rights-based laws, DP solutions applicable to smart cities are so far generic and tenuous, and look to be getting further away not nearer, even after three years of negotiations on the GDPR. "Code" solutions may be more useful and should certainly be investigated to supplement the law. Four particular suggestions for further research and legislative and policy involvement are herein promoted:

[236] See further Mireille Hildebrandt and de Vries eds *Privacy and the Computational Turn* (Routledge , 2013).

[237] See "SNP announces indefinite fracking ban in Scotland ", *Telegraph*, 28 January 2015, at http://www.telegraph.co.uk/news/earth/energy/fracking/11375332/SNP-announces-indefinite-fracking-ban-in-Scotland.html .

(i) Investigation into the potential for a smart city PIA or DPIA;

(ii) Investigation into the technical and social potential of methods of giving "pre-consent" or "sticky consent" to deal with the constraints of the IoT;

(iii) Legislating for algorithmic transparency and researching ways of making algorithmic data comprehensible to consumers;

(iv) Moving at least partially away from consent or "notice and choice" as a main mechanism for validating data collection and processing; connectedly, prohibiting certain data processing activities (which?) even where there is consent.