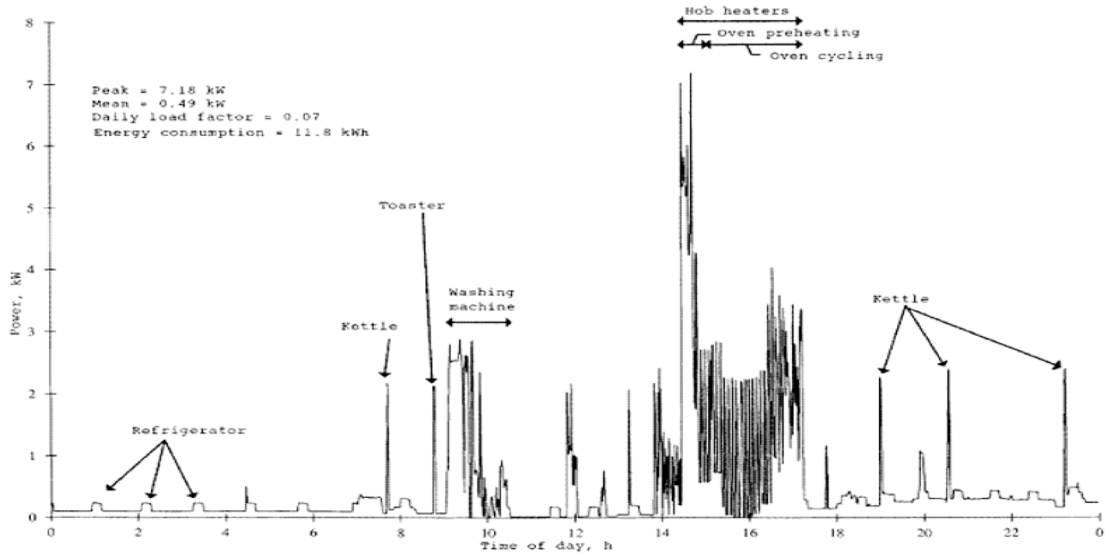
Draft Communications Data Bill – Call for Evidence

1. **Smart Meter Communications & Privacy - An Overlooked Aspect in the Draft Communications Data Bill?**

2. The Draft Communications Data Bill fails to adequately address privacy issues related to smart meter communications data. The UK Government presently wishes to introduce smart metering into all UK homes by 2019 and wishes to access all smart metering information. This highly intrusive plan would allow it access to highly detailed information on *all* individuals' lifestyles and whatever they are doing in their homes in real time (as well as through historical load data collected with such systems). Such a proposition appears extremely intrusive and completely unwarranted.

3. Unlike conventional meters that measure total energy use through day and night tariffs (which are normally read four times every year), smart meters allow energy use to be read with far finer granularity. The UK industry's draft technical specifications for smart meters state a requirement for real time information *every 5 seconds* for electricity and every 30 minutes for gas (SMDG 2011). The intended access to, and retention of, such data by the UK Government appears to be in direct contradiction to EU Privacy Law and Human Rights legislation (Anderson & Fuloria 2010).

4. Every electrical appliance has its own energy fingerprint readable by smart meters. Those accessing such information from smart meter data, either legally or illegally, have indications of the appliances individuals have and how often they use them.



5. Image source: Newborough & Augood (1999).

6. *"We … have the technology to record … (energy consumption) every minute, second, microsecond, more or less live... From that we can infer how many people are in the house, what they do, whether they're upstairs, downstairs, do you have a dog, when do you habitually get up, when did you get up this morning, when do you have a shower: masses of private data*. *… We think the regulator needs to send a strong signal to say that the data belongs to consumers and consumers alone. We believe that's a blocker to people adopting the technology*," Martin Pollock of Siemens Energy, quoted by Wynn (2010).

7. **Parties wishing smart meter data?**	**Potential use (partial listing)**
Utilities	Efficiency analysis, monitoring of electricity usage & load for forecasting & bills
Electricity usage advisory companies	To promote energy conservation & awareness measures
Insurance companies	Determining health care premiums based on unusual behaviours, that might indicate illness

Marketers	Profiling for targeted advertisements
Law enforcers	Identifying suspicious or illegal activities
Civil litigators	Determining when home occupied, by how many parties & activities undertaken
Landlords	To verify lease compliance
Private investigators	Monitoring for specific events
The Press	Information on famous individuals' movements & lifestyle
Creditors	Determination of behaviour that might indicate creditworthiness
Criminals	To identify the best times for burglary or to identify high-priced appliances to steal

Original source: SGIP (2010).

8. It was recently shown at the 28th Chaos Computing Congress (28c3) hacker conference that hacking into a smart meter could in, addition to identifying activity patterns in homes (including whether they were occupied) and the types of equipment being used, even allow identification of the movies being played by occupants. They stated that the security encountered was poor and the data resolution the meters provided was too high (Wisniewski 2012) – *as is the case with UK smart meters*.

9. Smart grid privacy issues			
Privacy threat		Service required	Existing protection mechanisms
Network threats	Shallow packet inspection	Anonymity	Anonymity networks
	Deep packet inspection	Confidentiality	Encryption
Data usage threats	Unauthorised usage/access	Access control	Policies, legislation, secure storage
	Customer privacy	Customer control of customer data	

Original source: Sooriyabandara & Kalogridis (2011).

10. Undertaking robust measures to anonymise smart metering data and remove recognisable appliance load signatures would help to address privacy concerns (Efthymiou & Kalogridis 2010, Kalogridis et al. 2010, Meserve 2009) - as would the retention of existing analogue meters which are also far better at protecting individuals' privacy (comment by present author).

11. Smart Meters being hacked could result in local and widespread disruptions, sensitive facilities being 'taken out', loss of data privacy (including information on the types of equipment individuals own, building occupancy patterns and identity theft). The adoption of smart meters can make the countries that use them considerably more vulnerable to hacking and expensive cyber terrorism and electromagnetic pulse threats (Jamieson 2012, Mills & LaMonica 2010, Peev 2012, Stop Smart Meters! (UK) (2012), Woolsey 2011). Cyber security expert David Chalk (2012) states that there is a "*100% certainty of a total catastrophic failure of the entire energy grid within 3 years*" creating a scenario "*worse than nuclear war.*" Such comments indicate a need for caution. [Additionally, it is now becoming recognised that the use of smart meters may not necessarily save energy (Hargreaves 2010) and can cause symptoms of ill health (Jamieson 2011) - *the RF/microwaves they normally emit during operation are now regarded as being possibly carcinogenic to humans* (WHO/IARC 2011)].

12. As noted by the Rt. Hon. Dr. Liam Fox MP, when he was Defence Secretary, "*As the nature of our technology becomes more complex, so the threat becomes more widespread. ... However advanced we become, the chain of our security is only as strong as its weakest link*."

13. **The smart metering system that the UK Government wishes to impose on its citizens, and the present Draft Bill's (covert) aim of accessing and data harvesting its communications data at the expense of hard won civil liberties, is ill conceived and would leave the nation vulnerable on many levels – *comment by present author.***

14. **Smart Meter Communications & Human Rights - An Overlooked Aspect in the Draft Communications Data Bill?**

15. **European Convention of Human Rights**

16. *"it [is] imperative that proper consideration is given to individuals' fundamental rights to privacy*," EC (2011). Under EU Data Protection Law, consumers' rights to privacy "*may not be overridden*".

17. A court in the Netherlands has already determined that the mandatory collection of non-essential fine-grained smart meter data – *such as the UK seeks to collect* - is against Article 8(1) of the European Convention of Human Rights. That ruling has led to mandatory smart meter installation being halted in the Netherlands (Cuipers & Koops 2008, metering.com 2009).

18. A report by the University of Tilburg for Consumentenbond (the Netherlands' main consumer organisation) concluded that smart meters could give away sensitive information that might fall into the hands of third parties (including police and insurance companies) on consumers' energy usage habits, including when individuals' leave and return to their homes (which could also be particularly useful to burglars). It further stated that the insights these intelligent monitoring devices would provide into living patterns and relationships could affect individuals' freedom to do as they please within their own homes and therefore be in breach of the European Convention of Human Rights (Cuipers & Koops 2008).

19. In the UK, Which?, the product-testing and consumer campaigning charity, is also calling for a halt to the smart meter rollout consumer over a number of issues and concerns including data security (Which? 2012).

20. **United Kingdom**

21. **UK - Human Rights Act 1998**

22. The Human Rights Act 1998 is based on the European Convention of Human Rights. It is one of the most important statutes ever passed in the UK (Hoffman & Rowe 2010).

23. **Article 3 - Prohibition of torture**

24. **"*No one shall be subjected to torture or to inhuman or degrading treatment or punishment*"** (HRA 1998).

25. The European Court defines 'degrading treatment' as "*… such as to arouse … feelings of fear, anguish and inferiority, capable of humiliating and debasing… and possibly breaking… physical or moral resistance*," (IUK 1980).

26. As noted by Hoffman & Rowe (2010), "*…all people have a level of basic respect and dignity as human beings.*" Prohibiting them enjoying proper privacy in their own homes through smart monitoring and surveillance of devices they use and personal timings they keep is potentially demeaning and degrading to both self-respect and dignity.

27. **Article 8 - Right to respect for private and family life**

28. **1. "*Everyone has the right to respect for his private and family life, his home and his correspondence.*"** (HRA 1998).

29. In the Draft Communications Data Bill (2012) the following is declared, "It is well established that … communications are covered by the notion of private life and correspondence in Article 8(1) [of the Human Rights Act 1998]. The case of Malone v UK (1984) 7 EHRR 14 (paragraphs 83 to 88) provides some

limited guidance on the application of Article 8 to State activities concerning communications data: "…. *a meter check printer registers information that a supplier … may in principle legitimately obtain [data], notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified*."" Emphasis added by present author.

30. The above quotation from the Draft Bill appears to *incorrectly* imply that the use of smart meter data obtained in such a fashion is therefore justified, desirable and legitimate. This appears misguided, particularly as such data can reveal so much about individuals' private lives to third parties without their express consent being given.

31. Privacy. The UK Government presently seeks to access to all UK metering information, every half hour with gas and *every 5 seconds* with electricity through smart meter readings from every UK household (SMDG 2011). This taken alongside the ability of technology to infer what members of the general public are doing in real time in parts of their own homes, and store data collected on what they have done in the past, represents a true threat to privacy and democracy.

32. The access to lifestyle information the Draft Bill seeks to allow is inconsistent with EU privacy law and, as mentioned previously, has already been successfully contested in the Netherlands (Cuipers & Koops 2008). It appears that claims that "*economic benefits outweigh the rights of those affected*" could be disputed related to:

33. The right for individuals to be able to enjoy their property in the manner to which they have become accustomed, as this may become compromised by having details of their private activities and peaceful use of possessions logged and accessible to third parties.

34. "*Respect for home and home life means more than just providing some form of dwelling or shelter: it extends to maintaining the situation to which a person has become accustomed, and the very permanence of which gives comfort*," (Hoffman & Rowe 2010).

35. **2. "*There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*," (HRA 1998).**

36. Article 8 may be violated through the potential weakening of "*national security, public safety or the economic well-being of the country*" by the introduction of smart meter technology and excessive data harvesting by the authorities and other parties if this Draft Bill if passed. *Refer to paragraphs 11 and 12 in this present document*.

37. **Article 14 - Prohibition of discrimination**

38. "*The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status,*" (HRA 1998).

39. It may be contested that data derived from smart meters, and other data recording and transmitting devices, may be used for discriminatory purposes by third parties. Possible examples include insurance companies that may determine health care premiums based on what they *perceive* to be unusual occupational lifestyle behaviours, and creditors making determinations on behaviours they *perceive* might indicate creditworthiness (SGIP, 2010).

40. **The First Protocol**

41. **Article 1: Protection of property**

42. "*Every natural or legal person is entitled to the peaceful enjoyment of his possessions. No one shall be deprived of his possessions except in the public interest and subject to the conditions provided for by law and by the general principles of international law*," (HRA 1998).

43. *"The preceding provisions shall not, however, in any way impair the right of a State to enforce such laws as it deems necessary to control the use of property in accordance with the general interest …"*

44. The "*peaceful enjoyment of … possessions*", and the right for individuals to be able to enjoy their property in the manner they have become accustomed to *(such as being able to use their possessions as they have in the past [without worries about outsiders gaining unprecedented knowledge of their personal habits])*, may be compromised through inappropriate and unwarranted data harvesting and retention and use of such data by the authorities and others.

45. *Possible risks to property that would be increased through the use of smart metering include: data hijacking that could allow thieves to determine the types of electronic equipment individuals' possess (as a result of their unique electronic signatures) and also thieves gaining knowledge of when buildings are unoccupied. It is proposed by the present author that the introduction, or escalation, of such risks, through measures proposed in the Draft Bill, are contrary to the general interest.*

46. **"Human rights must be part of all policy making,"** UK Department for Constitutional Affairs (DCA 2006).

47. **References**

Anderson, R. & Fuloria, S. (2010), On the security economics of electricity metering, 9th Workshop on the Economics of Information Security, Harvard University, George Mason University in Arlington, VA, June 2010, 18 pp.

Chalk D. (2012), Cyber expert on SMART GRID: massive vulnerability, who's accountable?, http://www.youtube.com/watch?v=2c1sadZCO60&feature=related

Cuipers, C. & Koops, B.J. (2008), Het wetsvoorstel 'slimme meters': een privacytoets op basis van art. 8 EVRM, Universiteit van Tilburg.

DCA (2006), Guide to the Human Rights Act 1998: Third Edition, Department for Constitutional Affairs, http://www.justice.gov.uk/guidance/docs/act- studyguide.pdf

Draft Communications Data Bill (2012), Draft Communications Data Bill. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, June 2012, 123 pp. http://www.official-documents.gov.uk/document/cm83/8359/8359.pdf

EC (2011), Article 29, Data Protection Working Party Opinion 12/2011 on smart metering Adopted on 4 April 2011, 00671/11/EN WP 183, The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, http://ec.europa.eu/justice/policies/privacy/index_en.htm

Efthymiou C. & Kalogridis, G. (2010), Smart Grid Privacy via Anonymization of Smart Metering Data, First IEEE Int. Conference on Smart Grid Communications, Oct. 2010

Energy Savings Trust (2012), Smart Meters, http://www.energysavingtrust.org.uk/In-your-home/Your-energy-supply/Smart-meters

FIPR (2010), Consultation response on Smart Meters, The Foundation for Information Policy Research, http://www.fipr.org/100110smartmeters.pdf

IUK (1980), Ireland v United Kingdom (1980) 2 European Human Rights Reports: European Court Cases 25.

Fox, L. (2010), Keynote presentation at The First World Infrastructure Security Summit, Electric Infrastructure Security Summit, Westminster Hall, Parliament, UK, 2010.

Hargreaves, T. (2011), When practices strike back...: a longitudinal study of the impact of smart energy monitors on domestic energy-use practices. Presentation at the Royal Geographical Society (with IBG) annual International Conference, London. 2nd September 2011. Media release.

Hoffman, D. & Rowe, J. (2010), Human Rights in the UK (Third Edition), Pearson, London, 466 pp.

HRA (1998), Human Rights Act 1998, legislation.gov.uk, http://www.legislation.gov.uk/ukpga/1998/42/contents

IUK (1980), Ireland v United Kingdom (1980) 2 European Human Rights Reports: European Court Cases 25.

Jamieson, I.A. (2012), Smart Meters – Smarter Practices: Addendum - EMP & Cyber Security, http://www.radiationresearch.org/images/Documents/addendum_emp__cyber_security_120320.
Jamieson, I.A. (2011), Smart Meters – Smarter Practices, http://www.radiationresearch.org/index.php?option=com_content&view=article&id=173
Kalogridis, G. et al. (2010), Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures, First IEEE Int. Conference on Smart Grid Communications, Oct. 2010.
Landis+Gyr (2008), PolyPhase BS Standard Credit Meter 5219 Technical Data, Document number: IB057, 4pp. http://www.landisgyr.com/uk/en/pub/products_and_solutions.cfm?eventProducts=products.ProductDetails&ID=91&catID=23
Meserve, J. (2009), 'Smart Grid' may be vulnerable to hackers. CNN.com, http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/#cnnSTCText)
metering.com (2009), Smart meters not to be compulsory in Netherlands, http://www.metering.com/node/15062
Mills, E. & LaMonica, M. (2010), Money trumps security in smart-meter rollouts, experts say. InSecurity Complex, cnet NEWS, http://news.cnet.com/8301- 27080_3-20007672-245.html?tag=mncol;txt
Newborough, M. & Augood, P. (1999), Demand-side management opportunities for the UK domestic sector, IEE Proceedings of Generation Transmission and Distribution 146(3), pp. 283–293.
OTLB (2010), Interview with EFF: How Smart Meters Violate our Right to Privacy, http://stopsmartmeters.org/2010/09/22/interview-with-eff-how-smart-meters-violate-our-right-to-privacy/
Peev, G. (2012), Government plans to install smart meters in our homes 'will leave us open to cyber attack', Daily Mail, 8th June 2012, http://www.dailymail.co.uk/news/article-2156648/Government-plans-install-smart-meters-homes-leave-open-cyber-attack.html#ixzz24MOrvedx
Quinn, E.L. (2009), Privacy and the New Energy Infrastructure, Social Science Research Network, 09, pp. 1995-2008.
SGIP (2010) NISTIR 7628, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, The Smart Grid Interoperability Panel - Cyber Security Working Group, National Institute of Standards and Technology, Vol. 2, pp. 30–32, http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf, pp. 30-32.
SMDG (2011), Industry's Draft Technical Specifications. Document drafted by industry, stakeholders under the Smart Metering Design Group (SMDG) set up under the Great Britain (GB) Smart Metering implementation programme (SMIP). 297 pp., http://www.decc.gov.uk/assets/decc/11/tackling-climate-change/smart-meters/2393-smart-metering-industrys-draft-tech.pdf
Sooriyabandara, M. & Kalogridis, G. (2011), Smart Grid Privacy by Design, ETSI 6th Security Workshop, Sophia Antipolis, France, 19th Jan 2011, PowerPoint presentation, http://docbox.etsi.org/Workshop/2011/201101_SECURITYWORKSHOP/S5_SECURITYinSMARTGRIDS/SOORIYABANDARA_TOSHIBA_SmartGridsPrivacy byDesign.pdf
Stop Smart Meters! (UK) (2012), FBI: Smart Meter hacks likely to spread — Utilities are unprepared, http://stopsmartmeters.org.uk/fbi-smart-meter-hacks-likely-to-spread-utilities-are-unprepared/
Which? (2012), Which? calling for a halt to the smart meter roll-out? http://www.which.co.uk/energy/creating-an-energy-saving-home/guides/smart-meters-and-energy-monitors-explained/smart-meter-roll-out/
WHO/IARC (2011), IARC classifies radiofrequency electromagnetic fields as possibly carcinogenic to humans, Press Release No. 208, World Health Organization, 31st May 2011.
Wisniewski, C. (2012), Smart meter hacking can disclose which TV shows and movies you watch, nakedsecurity, http://nakedsecurity.sophos.com/2012/01/08/28c3-smart-meter-hacking-can-disclose-which-tv-shows-and-movies-you-watch/
Woolsey, J. (2011), CIA Director calls Smart grid "Stupid" due to Security problems, http://www.youtube.com/watch?v=MAid1bS8t9U
Wynn, G. (2010), Privacy concerns challenge smart grid rollout, http://www.reuters.com/article/2010/06/25/us-energy-smart-idUSTRE65O1RQ20100625

48. **Disclaimer**

49. This document is intended to help guide policy decisions, advance knowledge and stimulate further research. Whilst all reasonable precautions have been taken to ensure the validity of the information given, no warranty is given towards its accuracy. It is not intended as a final statement on this topic or potential biological effects. No liability is accepted by the author for damages arising from its use and/or interpretation by others.