Response from Stop Smart Meters! (UK)

Q1: Do you have any comments on the proposed legal re-drafting (at Annex 4) to take account of the changes that were consulted upon in the Open Letter consultation on proposed amendments to the roll-out licence conditions? These should be read in tandem with question 2 in Part 2.

If the proposed obligation for Smart Metering were carried out, serious breaches of human rights would result.

As has been acknowledged in parliament, Smart Meters are not obligatory - they can be refused. The language used in this document to highlight obligatory intentions appears to promote something unlawful.

Part 2, Q2: Do you have any comments on the Government's intention of clarifying the licence conditions on installation of advanced meters under the exceptions to the smart metering roll-out obligation, and do you have any comments on the proposed legal re-drafting (at Annex 4)?

Any intentions to make smart metering obligatory are, in fact, illegal.

A similar attempt by the Dutch Government to make such metering compulsory failed as a result of mandatory smart metering being proven in law to breach basic human rights. It had been intended by Maria van der Hoeven, who was the Dutch Minister of Economic Affairs at the time, that refusing the installation of a smart meter would have been punishable by either a 17,000 euros fine or six months in prison. (metering.com 2009).

The proposed obligatory Dutch rollout was opposed by both privacy watchdogs and consumer organisations, including Consumentenbond (the main consumer organization in the Netherlands) which commissioned a special report into the matter, which 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 buildings (which could be particularly useful to burglars) (Cuipers & Koops 2008).

The special report, primarily looking into matters related to domestic consumers, also stated that the insights these monitoring devices would provide into occupational patterns and relationships could affect individuals' freedom to do as they please and therefore be in breach of the European Convention of Human Rights. Similar claims may be brought in this country, with regard to the UK Human Rights Act 1998.

Additionally, the fact also has to be taken into consideration in the legal re-drafting that the European Court of Justice in Luxembourg has recently delivered a judgment that means the European Charter of Fundamental Rights, which

contains a host of legally binding new rights over those previously applicable in this country "is now valid in British courts" (Bentham 2013).

As noted by senior judge Mr Justice Mostyn:

"The constitutional significance of this can hardly be overstated. The Human Rights Act incorporated into our domestic law large parts, but by no means all, of the European Convention on Human Rights. Some parts were deliberately missed out by Parliament. ... The Charter of Fundamental Rights of the European Union contains, I believe, all of those missing parts and a great deal more. Moreover, that the much wider Charter of Rights would remain part of our domestic law even if the Human Rights Act were repealed." (Bentham 2013).

"The Charter of Fundamental Rights is part of the EU's 2007 Lisbon Treaty, which sets out rights to environmental protection and medical treatment, as well as civil, social and other rights." (Bentham 2013).

What follows are commentary abstracts taken from Jamieson 2011/2012 on just some of the human rights issues that could arise in Britain as a result of obligatory smart metering:

...

UK - Human Rights Act 1998

"Human rights are required to be part of all UK policy making (DCA 2006). This Act is one of the most important statutes ever passed in the UK (Hoffman & Rowe 2010)."

Article 2 - Right to life

"Everyone's right to life shall be protected by law. No one shall be deprived of his life intentionally save in the execution of a sentence of a court following his conviction of a crime for which this penalty is provided by law."

Right to Life: All EU States agree that the human embryo/fetus belongs to the human race (Hoffman & Rowe 2010). As research indicates that some RF/microwave regimes (at levels lower than current limits) may raise risk of infertility, miscarriage, and cause damage to both animal and human offspring (Cherry 2000); claims might be brought that increasing involuntary exposures to such regimes may be against individuals' right to life.

As shown in the case of LM & R v Switzerland (LMRS 1996), Article 2 is relevant in situations where health may be put at risk, and is not restricted to risk of death or actual death.

"When authorities are aware (or should be aware) of real risk to life they are under obligation to take appropriate mitigative action to protect those at risk (Hoffman & Rowe 2010)." DECC's apparent intention to mandatorily increase individuals'

exposures to a Group 2b carcinogen (microwave radiation) through the introduction of wireless smart metering (and the creation of additional "dirty electricity" on internal mains supplies from the switched mode power supplies of smart meters) fails to meet this obligation and actually makes the situation considerably worse.

At least one provider recognizes its legally liability for death or personal injury caused by negligence (Npower 2013). Other firms, involved in communications technology, are also aware of the likelihood of possible claims in the future related to biological damage potentially caused by manmade radiation.

Article 3 - Prohibition of torture

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

Article 3 embodies a fundamental human right. "... the right to freedom from bodily harm is second only to the right to life, and is equally based on the right which all people have a level of basic respect and dignity as human beings," (Hoffman & Rowe 2010)."

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). These appear very similar to descriptions provided by some electrohypersensitive (EHS) individuals describing how their condition makes them feel.

The needs of "at risk" EHS individuals and others, whose health may be detrimentally effected by manmade electromagnetic radiation (i.e. everyone), should be taken into account with regard to metering provisions for both domestic and non-domestic situations.

Article 5 - Right to liberty and security

"Everyone has the right to liberty and security of person. No one shall be deprived of his liberty save in the following cases and in accordance with a procedure prescribed by law. ..." (HRA 1998).

'Security of person' is legally defined as "The legal and uninterrupted enjoyment by a man of his life, his body, his health and his reputation."

Claims may be brought that 'Security of person' may be seriously compromised by the microwave regimes created by smart meters causing/exacerbating conditions of ill health [As previously mentioned, at least one provider recognizes its legally liability for death or personal injury caused by negligence (Npower 2013). As it is already known that many claims of adverse health effects have arisen abroad as a result of smart meter installations, it appears highly possible that claims of negligence may arise in Britain over the use of such

technology in both business and domestic situations and that such claims may prove exceedingly costly to those found liable.

Additionally, the provision of sensitive fine grained data on the activities of individuals and companies to third parties may also risk damaging reputations and thereby breach this right. It is admitted by at least one energy provider [with regard to its domestic customers] that the data they will collect from smart meters will also be supplied to members of their group "based in countries outside of the European Economic area (EEA)... [which] may not have the same data protection standards as we do in the UK" (Npower 2013). The risk of sensitive commercial information from fine-grained data provided by smart meters finding its way into the hands of undesirable third parties appears quite high and may prove undesirable to many businesses.

Under Article 5, the rights of vulnerable individuals may be violated if emissions from Smart Meters and other forms of electronic technology prevent them from being able to go where they wish ... unhindered by man-made electromagnetic field regimes detrimental to their well-being.

Article 5 suggests that the needs of those adversely affected by manmade radiation should be more taken into account when metering structure is being developed.

It also suggests that there is a need to ensure that metering should not adversely affect liberty and/or security. Unfortunately, wireless smart meters greatly exacerbate such problems. Commercially sensitive data may be revealed by the fine-grained data that smart meters can provide to third parties, including those in criminal fraternities involved in burglary and/or industrial espionage. Such issues include: *"data hijacking from Smart Meters that may allow thieves to determine the types of electronic equipment they possess (as a result of their unique electronic signatures) and when [buildings are unoccupied]".*

Article 3: "*Everyone has the right to life, liberty and security of person.*"

Life - As mentioned by Jamieson (2011): *"As research indicates that some RF/microwave regimes (at levels substantially lower than [UK] current limits) may raise risk of infertility, miscarriage, and cause damage to ... offspring (Cherry 2000); claims might be brought that increasing involuntary exposures to such regimes (whether at work or at home) may be against individuals' right to life."*

Cyber-security issues of smart meters

"'Just as securing and managing the physical defence of the country is a unique challenge, so is protecting the UK's critical infrastructure from threats of cyber terrorism. ... Traditional security technologies are in no way up to the challenge." Mark Darvill, Director of security firm AEP Networks (AEPN 2010)."

Similar concerns are being voiced abroad. Experts at the IEEE Smart Grid Comm 2010 conference warned that consumers and utilities' infrastructures are

becoming more vulnerable to cyberattack due to increased security vulnerabilities and the two-way communication of smart grids as compared to existing systems. They predict that the smart grid will present up to 440 million possible points to be hacked by 2015 (Schwartz 2010).

"It is recognised by the US Government Accountability Office (US GAO) and the US Department of Energy (US DOE) that the present transition to smart grids is leaving electric grids open to increased cybersecurity weaknesses that risk damaging their efficient operation (Mills & LaMonica 2010, US GAO 2011)."

Built in security: The US GAO states that "increasing the use of new system and network technologies can introduce new, unknown vulnerabilities. ... our experts stated that smart grid home area networks ... do not have adequate security built in, thus increasing their vulnerability to attack."

To counter such risks, over $30 million (£18.62 million) has been awarded to address these cyber-security and reliability issues. (Schwartz 2010). Even with such massive funding, some experts still express grave concerns (Mills & LaMonica 2010). 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)."

Manipulation of smart grid data: Electricity theft is a cause of great concern to utility companies, and already there are devices existing that allow Smart Meters to be altered remotely to register less energy consumption than actually used (Mills & LaMonica 2010). Assistant Professor Le Xie of Texas A&M University notes that it is likely that some attackers could be virtual traders seeking to benefit financially through intercepting and manipulating smart grid data to place safe bets on energy demands (Schwartz 2010).

Blackout attacks: Network security experts state that once a hacker gains access to the smart grid he/she may gain control "of thousands, even millions, of [smart] meters and shut them off simultaneously." Individual hackers may also be able to substantially raise or lower power demand, disturbing the local power grid's load balance and creating a blackout. They also state that such outages would "cascade to other parts of the grid, expanding the blackout," with no-one being able to predict the possible scale of such damage (Meserve 2009).

"As a result of the remote off-switches currently specified for ... Smart Meters, 'blackout attacks' could be carried out by rogue nations, terrorists or criminals unless appropriate countermeasures are taken. One of these is the option that Smart Meters are designed to fail in the 'on' mode - human rights laws in Europe stop defaulters simply being disconnected (Anderson & Fuloria 2010)."

There is a high cost to blackouts, the Northeast Blackout of 2003 in North America cost $3 billion (£1.86 billion). A coordinated attack on the grid "could lead to even more significant economic damages" (ICFC 2003).

"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." UK Defence Secretary, the Rt. Hon. Dr. Liam Fox MP (Fox 2010)."

Article 8 - Right to respect for private and family life

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

- Privacy. The UK government presently wishes access to all UK metering information, with gas and electricity meter readings to be taken ... every half hour. However, this is inconsistent with EU privacy law and, as mentioned previously, has already been successfully contested in the Netherlands (Anderson & Fuloria 2010)."

This would also seem to hold true with regard to private matters and operations undertaken by non-domestic customers.

The Government fails to adequately address human rights privacy issues related to both domestic and non-domestic customers. It dresses up its highly intrusive and unwarranted "big-brother" wish to obtain and retain fine-grained data on everything customers do within individual smart metered premises as *"a commitment to amending the roll-out licence conditions to ensure that non-domestic customers with smart meters had a minimum right of access to data from smart meters - half-hourly for electricity, hourly for gas."* This would reveal to it, and other third-parties, whatever was happening in any such metered premises in real time (as well as through collected and retained historical data of energy usage.

In the Draft Communications Data Bill (2012), it is declared that *"it is well established that ... communications are covered by the notion of private life and correspondence ... The case of Malone v UK (1984) 7 EHRR 14 ... provides some limited guidance on the application of Article 8 [of the Human Rights Act 1998] to State activities concerning communications data."* It then goes on as follows: *"... a meter check printer registers information that a supplier ... may in principle legitimately obtain [data]"* and claims that *"... 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."*

However, when regulations are changed (and the use of new technologies proposed) so that metering data can become so fine grained that utility companies *"have the technology to record ... (energy consumption) every minute, second, ... more or less live ... From that we can infer how many people are in the [building], what they do, whether they're upstairs, downstairs, ... when you habitually get up, when did you get up this morning, when do you have a shower: masses of private data ..."* (Martin Pollock of Siemens Energy, quoted by Wynn (2010)); it can be reasoned that access to such data, which could provide huge

amounts of personal information on all individuals' past and present private lives (and kept in perpetuity) is actually undesirable, unjustified, illegitimate and illegal.

Consumers should be allowed to maintain their privacy by default. They should also be allowed to have any historical fine-grained data collected by smart meters and AMI related to their properties, lifestyles, work practices, equipment usage and appliance types, deleted from all records if they so wish, with only the most basic of billing data being retained. The requirement in the industry technical draft for Britain's smart meters in 2011 to provide real-time information every 5 seconds is particularly worrying (SMDG 2011).

Article 12 - Right to marry

"'Men and women of marriageable age have the right to marry and to found a family, according to the national laws governing the exercise of this right," (HRA 1998)."

Claims may be brought if the emissions from technology being employed in some Smart Meters and related technology are proven to reduce human fertility and increase risk of miscarriage thereby hindering individuals' right to found a family.

Article 14 - Prohibition of discrimination

"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).

It may be contested by some – particularly those with EHS – that the widespread introduction of some types of RF/microwave emitting Smart Meters (and related wireless emitting technology) may be discriminatory, as it would interfere with their basic rights and freedoms.

The First Protocol
Article 1: Protection of property

"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).

A growing body of peer-reviewed scientific research (and strong anecdotal evidence) indicates that the microwave emissions from operational smart meters can damage flora and fauna / biological systems at even very low microwave exposures – thereby potentially causing loss of property or diminution of its worth. Furthermore, the increased overall exposure levels caused by the addition of such infrastructure may raise background

RF/microwave exposures to a degree where detrimental biological effects may be seen in situations where they were not previously observed. (This has already been the case in a number of foreign countries where smart meters have now been installed).

References

- AEPN (2010), Cyber Terrorism Escalated To Tier One Risk In The UK, AEP Networks, http://www.prosecurityzone.com/News/It_security/Network_security__routers_and_data_centres/Cyber_terrorism_escalated_to_tier_one_risk_in_the_uk_15519.asp#axzz1QjuniAJI
- 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.
- Bentham, M. (2013), Top judge 'surprised' that controversial EU laws that we blocked are now legally binding. Evening Standard (Published 12 November 2013), http://www.standard.co.uk/news/politics/top-judge-surprised-that-controversial-eu-laws-that-we-blocked-are-now-legally-binding-8934773.html
- CE (2011), The potential dangers of electromagnetic fields and their effect on the environment, Council of Europe / Conseil de l'Europe, Doc 12608.
- Cherry, N. (2000), Safe exposure levels, http://www.whale.to/b/cherry3.html
- 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/actstudyguide.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
- EMFSN (2011), Smart Meter Health Complaints, EMF Safety Network, http://emfsafetynetwork.org/?page_id=2292
- Fox, L. (2010), Keynote presentation at The First World Infrastructure Security Summit, Electric Infrastructure Security Summit, Westminster Hall, Parliament, UK, 2010.
- Havas, M. (2011), Havas Submission to CCST "Report on Smart Meters" http://www.magdahavas.com/2011/01/18/havas-report-on-smart-meters-forccst/
- HMG (2010), A Strong Britain in an Age of Uncertainty: The National Security
- Strategy, HM Government, Presented to Parliament by the Prime Minister by Command of Her Majesty October 2010, The Stationery Office Limited.

- Hoffman, D. & Rowe, J. (2010), Human Rights in the UK (Third Edition), Pearson, London, 466 pp.
- GI (1998) Guerra v Italy (1998) 26 European Human Rights Reports: 357
- HRA (1998), Human Rights Act 1998, legislation.gov.uk, http://www.legislation.gov.uk/ukpga/1998/42/contents
- KCRA 2011, Some SmartMeter Customers Say Devices Make Them Sick, http://www.kcra.com/station/25639450/detail.html
- ICFC (2003), The Economic Cost of the Blackout An issue paper on the Northeastern Blackout, August 14, 2003, ICF Consulting, 3pp.
- IUK (1980), Ireland v United Kingdom (1980) 2 European Human Rights Reports: European Court Cases 25.
- LMRS (1996) LM & R v Switzerland (1996) 22 European Human Rights Reports: European Commission Decision 130.
- 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
- 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
- npower (2013), Standard terms for supplying electricity and gas to domestic customers. July 2013.
- NTSM (2002), Napier v The Scottish Ministers (2002), United Kingdom Human Rights Reports 308.
- OTLB (2011), Shrubs Don't Lie - We Should Listen When They Die, http://stopsmartmeters.org/2011/04/08/shrubs-dont-lie/
- Powerwatch (2010), Smart Meters - smart idea - not so smart implementation, http://www.powerwatch.org.uk/news/20101018_smart_meter.asp
- Schwartz, M.J.(2010), Smart Grids Offer Cyber Attack Opportunities Hackers are likely to exploit the 440 million potential targets researchers predict smart grids will offer by 2015. InformationWeek, http://www.informationweek.com/news/security/vulnerabilities/showArticle.jhtml?articleID=227701134
- 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

- US GAO (2011), Electricity Grid Modernization: progress being made on Cybersecurity Guidelines, but key challenges remain to be addressed. United States Government Accountability Office, Report to Congressional Requesters.
- Wynn, G. (2010), Privacy concerns challenge smart grid rollout, http://www.reuters.com/article/2010/06/25/us---energy---smart---idUSTRE6501RQ20100625