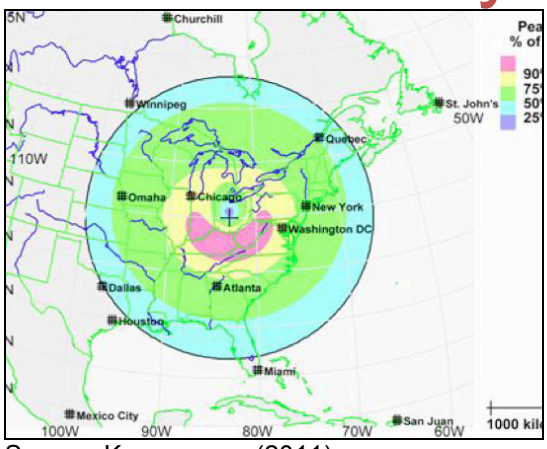
Practicality, Security, War, Terrorist or Cyber-Attack



Source: Kappenman (2011).

High-Altitude Electromagnetic Pulse (HEMP)

This term is often used for EM signals created from a nuclear detonation interacting with the Earth's upper atmosphere.

EMP can cause "*temporary upset and even catastrophic failure to modern electronics and electrical systems over considerable geographic areas of the Earth*" (NATO 2011).

It is often seen as impracticable to protect wireless systems (such as used in Smart Meter systems? – *present author's comment*) against EMP attack. The US National Security Working Group (NSWG 2011), notes "… *vintage type electronic systems are much more robust and tolerant to EMP effects. The bad news is that these systems are growing old and must be replaced, and they will be replaced with modern versions that are inherently more vulnerable to EMP."*

In the USA, Dr Peter Vincent Pry, former Director of the US Nuclear Strategy Forum and President of EMPact America states "… *given our current state of unpreparedness, within 12 months of an EMP event, about two-thirds of the U.S. total population… would perish from starvation, disease and societal collapse*."
No figures appear available for the UK or Europe.

"*A serious national commitment to address the threat of an EMP … can lead to a national posture that would significantly reduce the payoff for such an attack …*"
William R. Graham, Chairman of the US Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack.

It appears sensible to at least delay the rollout of Smart Meter technology till after the passing of the forthcoming solar maxima. This might also allow time for additional system improvements to be undertaken.

Source Region Electromagnetic Pulse (SREMP)

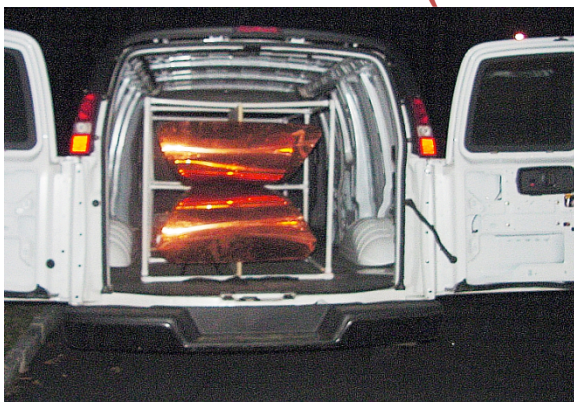
These are caused as a result of nuclear detonation, such as can be created by an air-burst EMP cruise missile, interacting with the Earth's and its adjacent atmosphere.

A single SREMP event could cause irreparable damage to most electronics within a 30 km (18.6 mile) area (Powerwatch 2010). Power supplies for large areas of a smart grid could be easily disabled by such devices unless suitable precautions are taken.

The vulnerability of electronic Smart Meters to such events appears far greater than that of the electromechanical rotating-disk meters they are designed to replace which are unlikely to be damaged.

UK Smart Meters are also being designed so they can be disconnected remotely (Anderson & Fuloria 2010). This may be a major design flaw. As a matter of best practice such meters should be designed to fail in a "supply on" mode (Powerwatch 2010).

Non-Nuclear EMP (NNEMP)



NNEMP Level EMP Source. Source: Kappenman (2011).

Non-Nuclear EMP (NNEMP) is also known as Intentional ElectroMagnetic Interference (IEMI) and is labeled as the "*Intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, … disrupting, confusing or damaging these systems for terrorist or criminal purposes*," (IEC 2005).

Extremely powerful portable radio transmitters (*which can be mobile and coordinated*) can be built to create NNEMP. The effects of

NNEMP/IEMI are similar to solar threats and HEMP but are usually more localised, unless a coordinated attack is undertaken (where they could create effects far larger than those achievable by large nuclear EMP pulses).

They pose a serious threat to medium and high voltage transformers and smart grids. Technical solutions are being created to address such threats (Birnbach 2011, Radasky & Savage 2010).

If EMP vulnerabilities remain unaddressed they present increased invitations for attack (Graham et al. 2011).

NNEMP/IEMI present a comparable risk scenario likelihood to that of Cyber Attack (Kappenman 2011).

Power surges

A recent sustained power surge in California appears to further indicate the increased susceptibility of Smart Meters to EMP over the conventional analogue meters they replace (Dremann 2011).

In that incident 80 PG&E SmartMeters caught fire and burned out after the power surge, causing some residents and utilities officials to question their safety. The surge, which lasted 80 minutes, affected 200 homes and businesses. None of the analog meters were affected.

"*The idea with SmartMeters is to make the customers' and the utility's life better, but this is a good example of how sometimes the old way is the good way*."
Debbie Katz, spokesperson for Palo Alto utilities.

Katz further commented that the advantage of the analog meter over its intended 'smart' replacement is that it does not have internal electronics which can be shut down or disrupted by power surges (Dremann 2011).

It is now intended that Paolo Alto city officials will undertake additional research and investigative work to ensure Smart Meter shortfalls and glitches are resolved before investing further in them.

Measures should be taken to ensure that Smart Meters are robust enough to withstand such events. In the meantime, till such matters are addressed, delaying their rollout till after solar maxima subside in 2014 may prove beneficial – *present author's comment.*

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.

Birnbach, C. (2011), Understanding the problem: Nuclear and Non-Nuclear EMP. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Dremann, S. (2011), Power surge raises questions about SmartMeters: East Palo Alto electricity surge burnt out digital meters, Palo Alto Online News, http://www.paloaltoonline.com/news/show_story.php?id=22378

EIS (2010), EIS Summit Summary Report, Electric Infrastructure Security Summit, 20 September 2010, Westminster Hall, Parliament, UK.

Graham, W.R. et al. (2011), Commission to Assess the Threat from High Altitude Electromagnetic Pulse (EMP): Overview. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

IEC (2005), International Standard IEC 61000-2-13 ed1.0, Electromagnetic compatibility (EMC) - Part 2-13: Environment - High Power Electromagnetic (HPEM) Environments - Radiated and Conducted, International Electrotechnical Commission, Switzerland. Quoted by Koepke (2010).

Kappenman, J.G. (2011), An Overview of ElectroMagnetic Threats to Electric Grids – Space Weather, EMP & IEMI. Round Table presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Koepke, G. (2010), Highlights of Connectivity Week 2010: EMC and Smart Grid, http://www.emcs.org/acstrial/newsletters/summer10/EMCStandards.html

NATO (2011), Electrical and Electromagnetic Environmental Conditions: AECTP-250 Edition 2, Allied Environmental Conditions and Test Publication, NATO International Staff, Defence Investment Division.

Powerwatch (2010), Smart Meters - smart idea - not so smart implementation http://www.powerwatch.org.uk/news/20101018_smart_meter.asp

Pry, P.V. (2011), Dr. Peter Vincent Pry President, EMPact America Statement Before The Congressional Caucus On EMP The Capitol Room HVC 200 February 15, 2011, http://www.empactamerica.org/pry-statement-to-emp-caucus.pdf

Foster, J.S. Jr. (2008), Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures. Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack, http://www.bibliotecapleyades.net/archivos_pdf/empc02.pdf

NSWG (2011), National Security Working Group, Weekly National Security Working Group Update, Republican Study Committee http://rsc.jordan.house.gov/UploadedFiles/NSGW_041311_Update.pdf

Radasky, W. & Savage, E. (2010), Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid. Report prepared by Metatech Corporation for Oak Ridge National Laboratory. 53 pp.

Preventing EMP catastrophes

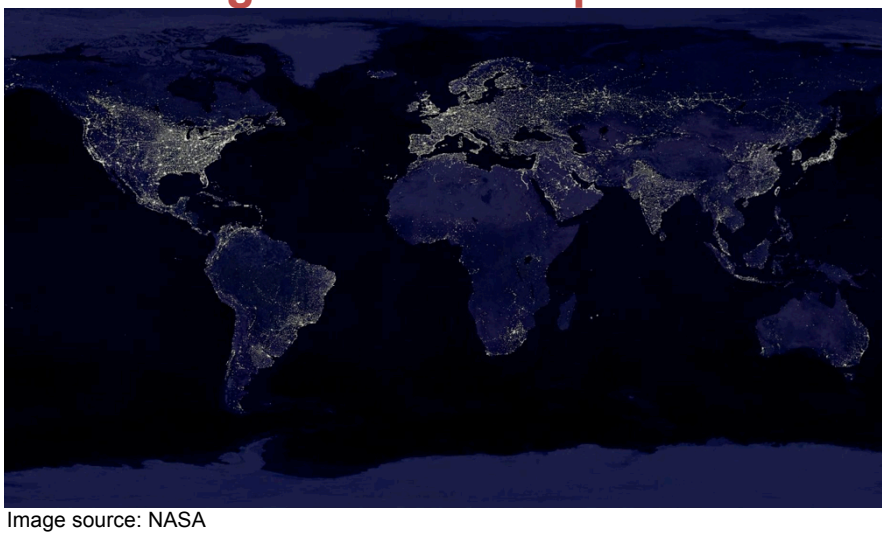


Image source: NASA

Smart grids create more potential points of failure than traditional grids. Ideally, protection should be considered early in the brief. Cost effectiveness is essential (EMPrimus 2011, Koepke 2010).

It is possible with robust planning to prevent EMP catastrophes. Action is required sooner rather than later for smart grids and smart devices, and could create numerous opportunities for investment and the development of new sustainable technologies.

At present there are no procedures to "perform *"black start" [restoring a power station to operation without requiring use of using the external power grid] under severe damage scenario,"* as these require energy and telecom transport that are power dependent (Graham et al. 2011).

Smart grids, Smart Meter systems and related technology should be hardened where practical to prevent adverse effects from EMP.

"*The technology to protect critical infrastructures from natural or malicious electromagnetic threats now exists.*

Implementation costs are estimated at less than 0.01% of GNP. For example, costs for protection of the U.K. electric grid are estimated at approximately £ 0.1B.

The corresponding estimate for the U.S. would be approximately $1B," EIS (2010). … "*Since much of this cost would in any case be incurred for normal periodic upgrade and modernization, the net costs are even lower*," Arbuthnot et al. (2010).

The UK National Security Council recognises cyber-attacks as a Tier One threat – *the highest priority for UK national security* (HMG 2010).

Recommendations (partial listing) – *various authors*

- Adhere to the Electric Infrastructure Security Council (EIS) International Infrastructure Security Roadmap (EIS 2011).
- Determine grid and network level vulnerabilities & prioritise actions.
- Improved forecasting required for EMP events.
- Protect important infrastructures and "high value" assets through appropriate design measures - *including hardening*.* "High value" assets include essential government operations and those of other national institutions.
- Grid-level protection systems should be installed to protect against EMP threats to transformers.
- Harden Smart Meters, smart grids and related technologies against EMP risk.* *(This creates a new level of safety – much like fitting seat belts in automobiles).*
- Delay rollout of additional Smart Meters till after main period of solar risk if unhardened.
- Develop regional and national smart grid restoration plans.
- Provide Government endorsement & tax incentives for required work.
- Undertake "controlled" power cuts when necessary to protect grid.
- Identify & address regulatory gaps that preclude effective mitigation.

*If budget does not stretch to automatically protecting Smart Meters in this way, allow individuals to purchase upgrades that allow them to be hardened.

Recovery periods are shortened as level of grid protection increases (Birnbach 2011). Significant, affordable improvements can be made to prevent, prepare, protect and recover from EMP events (Graham et al. 2011).

It is anticipated that the costs of EMP Protection may in part be compensated by reduced insurance costs (Birnbach 2011).

"*If addressed, our reduced vulnerability helps deter attack, enhances infrastructure resilience and confers added protection against cyber threats and damaging geosolar storms*." Commission to Assess the Threat from High Altitude EMP (Graham et al. 2011).

Certain measures, such as a widespread changeover to fibre-optic data and signal cabling, may greatly increase system robustness to EMP threats (Cikotas & Kappenman 2011), and also open up other streams of revenue (Fehrenbacher 2009) – *the hardening of such systems will further increase their attractiveness to investors*.

References

Arbuthnot, J. et al. (2010), EIS Summit: Electric Infrastructure Security Summit. The First World Infrastructure Security Summit, - London, 20 September 2010, Westminster Hall, Parliament, UK.

Birnbach, C. (2011), Understanding the problem: Nuclear and Non-Nuclear EMP. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Cikotas, B. & Kappenman, J. (2011), Options for Protection: Protecting National Electric Grids and Critical Infrastructures. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

Connor, S. (2011), 'Controlled' power cuts likely as Sun storm threatens national grid. The Independent, 13 June 2011, http://www.independent.co.uk/news/science/controlled-power-cuts-likely-as-sun-storm-threatens-national-grid-2296748.html

EIS (2011), EIS Summit: International Infrastructure Security Roadmap, Electric Infrastructure Security Summit - The Capitol Building, US Congress, Washington D.C., 11 April 2011.

EMPrimus 2011, Grid and transformer protection, http://www.emprimus.com

Fehrenbacher, K. (2009), Fiber Have a Role in the Smart Grid? A Tennessee Utility Thinks Sohttp://gigaom.com/cleantech/does-fiber-have-a-role-in-the-smart-grid-a-tennessee-utility

Foster, J.S. Jr. et al. (2008), Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures.

Graham, W.R. et al. (2011), Commission to Assess the Threat from High Altitude Electromagnetic Pulse (EMP): Overview. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington D.C.

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.

Koepke, G. (2010), Highlights of Connectivity Week 2010: EMC and Smart Grid, http://www.emcs.org/acstrial/newsletters/summer10/EMCStandards.html

McClelland, J.H. (2011), Protecting our Critical Infrastructures. Presentation given at The 2nd Annual World Summit on Infrastructure Security, Washington DC

US Homeland Security (2009), Securing the Modern Electric Grid from Physical and Cyber Attacks. Hearing before the Subcommittee on Emerging Threats,. First Session 21 July 2009, Serial No. 111-30, 147pp.

Cyber security

"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 cyber-attack 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 some countries' 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).

The development of appropriate solutions to realistic threats to security of supply should be carried out before large-scale UK smart grid rollouts are undertaken.

"Without securely designed smart grid systems, utilities will be at risk of not having the capacity to detect and analyze attacks, which increases the risk that attacks will succeed and utilities will be unable to prevent them from recurring," (US GAO 2011).

The installation of remote off-switches for Smart Meters would further increase risk to the consumer.

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.

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

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.

ICFC (2003), The Economic Cost of the Blackout An issue paper on the Northeastern Blackout, August 14, 2003, ICF Consulting, 3pp.

Meserve, J. (2009), 'Smart Grid' may be vulnerable to hackers. CNN.com, http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/#cnnSTCText)

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

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

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.

Smart Meter Data

Every electrical appliance has its own energy fingerprint readable by Smart Meters. Those accessing such information have indications of the appliances individuals have and how often they use them.

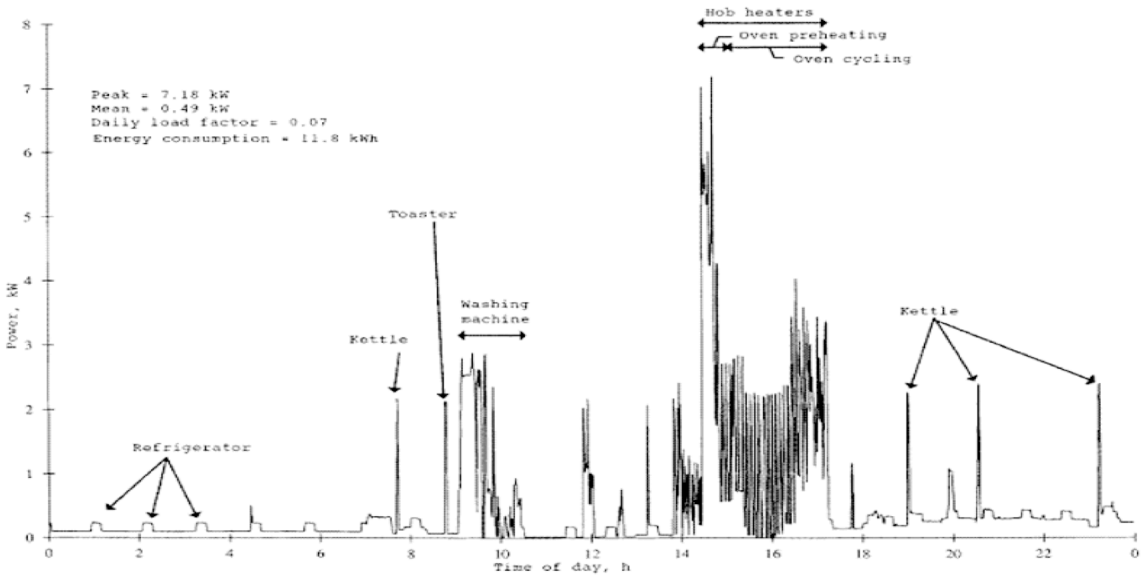


Image source: Newborough & Augood (1999).

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 (such as sleep problems*), 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)

*Emissions from some wireless Smart Meters have been reported to be linked to health and sleep problems (EMF SN 2011) – *present author's comment*.

Data provision & privacy/security issues

"*Digital information and communication technology offers the possibility of a new world of freedom. It also offers possibilities of surveillance and control which dictatorships of the past could only struggle to establish. The battle to decide between these possibilities is being fought now*," Stallman (2010).*

**Refer also to Appendix 7*.

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. …
Martin Pollock of Siemens Energy, quoted by Wynn (2010).

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).

Unlike conventional meters that measure total energy use through day and night tariffs (and are normally read four times every year), Smart Meters allow energy use to be read with far finer granularity (typically every half-hour). There is much debate as to what level of information should be provided by Smart Meters and to whom it should be provided.

" *high resolution electricity usage information can be used to reconstruct many intimate details of a consumer's daily life … [there are many ways], that information could be used in ways potentially invasive of an individual's privacy*." Quinn (2009).

A court in the Netherlands (Cuipers & Koops 2008) has already determined that the mandatory collection of non-essential fine-grained Smart Meter data is against Article 8(1) of the European Convention of Human Rights (which the UK is signed up to).

That ruling has led to mandatory Smart Meter installation being halted in the Netherlands (metering.com 2009). It is important to address such potential legal issues as early as possible and ensure that necessary safeguards are put in place.

"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*", as it is their degree of positive acceptance, support and involvement with Smart Meters and related technology that will determine the level of success smart metering achieves.

"*Data protection issues play a very important and even decisive role in the successful implementation of smart metering*," Knyrim & Trieb (2011).

As noted by Berliri & Maxwell (2010):

- 'Privacy by Design' creates opportunities rather than threats for smart grids – *it instills consumer confidence.*
- Consumers concepts of privacy are altering; soon statutory provisions may be inadequate. Privacy should be embedded into the technology.
- There may be competitive advantages for those able to offer the highest levels of privacy protection.

Robust privacy measures and policies are required to cover data usage and distribution if consumers are to be brought onboard and potential security shortfalls addressed.

Smart grid privacy measures			
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	

Source: Sooriyabandara & Kalogridis (2011).

Undertaking robust measures to anonymise Smart Metering data and remove recognisable appliance load signatures can help to address privacy concerns (Efthymiou & Kalogridis 2010, Kalogridis et al. 2010). Such measures may include: Privacy Enhanced Home Energy Management using Elec Privacy algorithms (*to disguise the signatures of electronic equipment*) and Escrow: Data Anonymisation.

Privacy Initiatives

Ontario, Canada

The province of Ontario in Canada is a world leader in embedded privacy protections for smart grids (PBD 2010). Adopting its guidelines may help prevent many claims on Human Rights privacy issues that might otherwise stall or halt rollouts.

1. Proactive not Reactive; Preventative not Remedial

"*Smart Grid systems should feature privacy principles in their overall project governance framework and proactively embed privacy requirements into their designs …*"

2. Privacy as the Default

"*Smart Grid systems must ensure that privacy is the default — the "no action required" mode of protecting one's privacy — its presence is ensured*."

3. Privacy Embedded into Design

"*Smart Grid systems must make privacy a core functionality in the design and architecture of Smart Grid systems and practices — an essential design feature*."

4. Full Functionality — Positive-Sum, not Zero-Sum

"*Smart Grid systems must avoid any unnecessary trade-offs between privacy and legitimate objectives of Smart Grid projects*."

5. End-to-End Lifecycle Protection

"*Smart Grid systems must build in privacy end-to-end, throughout the entire life cycle of any personal information collected*."

6. Visibility and Transparency

"Smart Grid systems must be visible and transparent to consumers - engaging in accountable business practices - to ensure that new Smart Grid systems operate according to stated objectives."

7. Respect for User Privacy

"Smart Grid systems must be designed with respect for consumer privacy, as a core foundational requirement."

That document states that the above principles should be applied to: accountable business practices; Information Technology (IT) systems; and physical design and networked infrastructure for smart grids (PBD 2010).

"… if the data protection rights of consumers are not sufficiently taken into account, then their acceptance of the new technology will be lacking, which could lead to its unsuccessful implementation," Knyrim & Trieb (2011).

Another concern related to 'Privacy by Design' is that present smart grid systems have a life expectancy of 10-20 years, during which time any in-built security they may have risks becoming compromised or outdated.

United Kingdom

The UK is adopting an approach to privacy drawn on international best practice measures and the advice of privacy experts (DECC 2011).

In September 2011, it was announced that the UK Government has established a central data and communications company to administer access to smart grid data to help allay consumer privacy concerns over Smart Metering. The UK Government will also oversee its security (smartmeters 2011).

California, USA

In July 2011, California voted to adopt it's own comprehensive set of privacy and security rules for the three utility companies that provide the majority of Californians with electricity (King 2011).

If consumers wish, they will be able to allow third parties to receive their backhauled Smart Meter data directly from the utilities, as opposed to directly from the Smart Meters in order to support services including demand response, energy advice and energy efficiency. It is important to note that the CPUC declared that "*The utilities … will bear no new liability for the actions of third parties which acquire information via this [mechanism]*."

The CPUC also stated that they will not exercise jurisdiction over third parties who directly receive energy usage data from installed devices that receive data via the HAN interface (King 2011).

It is likely that the Californian and UK initiatives will be a success if they fully take into account Human Rights' privacy issues and the need to anonymise electrical metering data to gain public trust.

Texas, USA

In Texas all meter data on electricity shall belong to the customer (BSM (2011). Texas Utilities Code 39.107(b) states:

"*All meter data, including all data generated, provided, or otherwise made available, by advanced meters and meter information networks, shall belong to a customer, including data used to calculate charges for service, historical load data, and any other proprietary customer information*. …"

References

Berliri, M. & Maxwell, W. (2010) Smart metering, smart grid and privacy by design, Project E-Cube, 21 September 2010.

BSM (2011), Smart Meter Data Belongs to the Customer, http://www.bansmartmeters.com/blog/2011/03/smart-meter-data-belongs-to-the-customer/

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

DECC (2011), Smart Metering Implementation Programme: Response to Prospectus Consultatiion. Supporting Document 1 of 5 Data Access and Privacy. Department of Energy and Climate Change and the Office of Gas and Electricity Markets, 56 pp.

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

Kalogridis, G. et al. (2010), Privacy for Smart Meters: Towards Undetectable Appliance Load Signatures, First IEEE Int. Conference on Smart Grid Communications, Oct. 2010.

King, C. (2011), California PUC adopts consumer data access and privacy rules for smart meters. Smart Grid Watch, eMeter, http://www.emeter.com/smart-grid-watch/2011/california-puc-adopts-consumer-data-access-and-privacy-rules-for-smart-meters/

Knyrim, R. & Trieb, G. (2011), Smart metering under EU Data Protection Law, International Data Privacy Law, 1(2), pp. 121-128.

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.

PBD (2010), Privacy by Design: Achieving the Gold Standard in Data Protection for the Smart Grid. Information and Privacy Commissioner, Ontario, Canada, Hydro One Inc. and Toronto Hydro Electric. 37 pp. http://www.ipc.on.ca/images/Resources/achieve-goldstnd.pdf

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.

Smartmeters (2011), Britain Remains Smart Grid leader. smartmeters, http://www.smartmeters.com/the-news/2584-britain-remains-smart-grid-leader-

.html

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_SmartGridsPrivacybyDesign.pdf

Stallman, R. (2010), Is digital inclusion a good thing? How can we make sure it is?, IEEE Communications Magazine, 48, pp. 112-118.

TUC (2011), [Texas] Utilities Code, Title 2. Public Utility Regulatory Act, Subtitle B. Electric Utilities, Chapter 39. Restructuring of Electric Utility Industry, Subchapter A. General Provisions, http://www.statutes.legis.state.tx.us/Docs/UT/htm/UT.39.htm

Wynn, G. (2010), Privacy concerns challenge smart grid rollout, http://www.reuters.com/article/2010/06/25/us-energy-smart-idUSTRE65O1RQ20100625