

A view-only version of the paper published on *Nature Energy* can be accessed [here](#).

## **Protecting data privacy is key to a smart energy future**

Carissa Véliz\*

Uehiro Centre for Practical Ethics  
Faculty of Philosophy  
University of Oxford

Philipp Grunewald  
Environmental Change Institute  
School of Geography and the Environment  
University of Oxford

**The ability to collect fine-grained energy data from smart meters has benefits for utilities and consumers. However, a proactive approach to data privacy is necessary to maximize the potential of these data to support low-carbon energy systems, and innovative business models.**

Recent data misuse by Facebook and others have cast a shadow over ‘smart data’. Many users expressed unease and shock about the kind of personal data Facebook holds and shares, and the company is now facing a class action lawsuit for logging text messages and phone calls via its apps <sup>1</sup>. The use of personal data harvested from Facebook by Cambridge Analytica for political campaigns also raised widespread concerns. Google is similarly facing a lawsuit for unlawfully harvesting personal data from iPhones <sup>2</sup>. Unethical data practices can undermine public trust in businesses and institutions, and could hinder the uptake of many potentially helpful data-based solutions, including smart energy services.

The planned deployment of smart meters brings with it unprecedented insights into energy use behaviour. For utilities, advantages include more effective billing, remote disconnection, and avoidance of fraud. For customers, smart meters promise fewer inaccurate bills and the chance to better manage energy use and expenditure. Smart meters are also an enabler for new business models and tariffs using variable or time dependant rates, and could lead to demand reduction through feedback <sup>3</sup>. Indeed, much hope rests on smart data to aid the decarbonisation of our energy systems. A proactive engagement with privacy challenges in this domain is needed to prevent scandals akin to Facebook and Cambridge Analytica. Transparency and best practices can build and maintain users’ trust in the companies they rely upon, which in turn will enable new business models to take advantage of the power of these data in ethical ways. The timely arrival of the European General Data Protection Regulation (GDPR), which came into force on 25 May 2018, could change the way energy service providers engage with their customers. This is a unique opportunity to enhance trustworthiness (the commitment and competence to treat users fairly and protect them from harm) and build trust (the

confidence felt by consumers that energy service providers are trustworthy), which could be vital prerequisites for innovative future business models.

## **Privacy risks for energy data**

The promise of smart meters lies in the fact that they can continually monitor, record, and respond to energy use data. However, energy is abstract and invisible <sup>4</sup>, making it difficult for users to fully appreciate what energy data reveals about them. The link between activities and their energy consumption is often poorly understood, making data derived from energy use even more abstract and imperceptible than energy itself. This degree of invisibility raises questions about individuals' ability to give informed consent for the use of such data.

At least four privacy-related complications arise from energy data and its abstract nature.

*Inference of sensitive information.* The level of insight that can be gained from energy data varies depending on the temporal resolution with which it is collected. With sub-second resolution, many individual appliances can be identified <sup>5</sup>. It is theoretically possible to detect which television channel is being watched based on load variations related to picture brightness. Even at lower resolution of 10 or 30 minutes, common for most smart meters, occupancy and activity patterns can be inferred <sup>6</sup>. Spouses could use such data to uncover infidelity (when the partner claimed not to be at home), and a property may be at risk of robbery if it is known to be unoccupied <sup>7</sup>.

*Discriminative customer segmentation.* Temporary offers could tempt users to share data only to find that they can be used for segmentation in future. High peak time users, for instance, may suddenly find themselves being offered less favourable tariffs. While such cost-reflective discrimination may be defensible from an economic perspective, the manner in which the process is kept transparent could be crucial for developing trust.

*Multi-person data.* Smart meters often collect data from households with shared occupancy. The bill payer may claim ownership of consumption data, but if insights into cohabitants are exposed, their consent for sharing data should be required, too. The balance of power in such arrangements could easily result in members of a household being monitored without their consent.

*Data aggregation.* The most powerful insights can emerge through linking with other data sources, such as loyalty cards, social media, or data from other smart devices sharing data as part of the 'the internet of things'. Even data analysts may not be able to predict what their machine learning algorithms might infer from these combined data sources. This unpredictability makes it practically impossible to inform data subjects about potential future insights and uses of their data.

These points demonstrate how illusive the concept of informed consent can be in the context of energy data. If users are not aware that a footprint of their activities is embedded in the energy data they are sharing, it stands to reason that appreciation of the power of energy data to infer sensitive information cannot be assumed. Consent for

data use may be given too lightly. Consequently, consent should not be considered informed, but should rather be seen as an expression of trust in the utility provider.

Consent is necessary to protect consumers whose data is being collected, but it may not be sufficient. If consent is an expression of trust, reciprocating by being trustworthy is only appropriate. Trustworthiness has to be earned and maintained through ethical practices<sup>8</sup>. Neither trust nor trustworthiness on their own are enough to avoid privacy scandals—both are needed. Consumer trust and corporate untrustworthiness amounts to misplaced trust—for instance, when an energy service provider is thought to collect data for better billing, but shares these data for marketing purposes. Conversely, corporate trustworthiness and consumer mistrust can amount to privacy misunderstandings—for example, if users refuse to share data with energy service providers because they suspect they will get sold to third parties when in fact they will only be used to provide a better service. Transparency can function like a bridge that allows users to recognise corporate trustworthiness, which in turn will contribute to consumer trust.

### **Data hoarding**

The common approach of collecting as much data as possible and keeping it for as long as possible is the result of the perception that data is an unconditional good—the more one has, the better. Even if the uses of data are not yet clear, they might be useful in the future, according to this view.

But keeping data bears risks. The longer data is kept, the greater the chance of misuse, either accidentally or maliciously. The fitness app Strava published data of its users running routes without anticipating that, months later, the location of secret military bases would be inferred and published<sup>9</sup>. In other cases, data can change hands in unexpected ways, for instance as part of a business liquidation, in which customer data can become valuable assets. The data practices of the new owner may differ substantially from those originally consented to<sup>10</sup>.

Security expert Bruce Schneier argues that data is a “toxic asset”<sup>11</sup>, given how hard it is to keep secure, and how many people want it—including national and foreign governments, corporations, would-be employers, personal adversaries, and criminals.

Energy service providers may find themselves at a crucial junction. They are collecting more data than ever, with all the risks that entails, at a time when the public is getting increasingly concerned about their privacy and the overreach of technology in their lives.

### **Privacy and the future of energy**

The new European General Data Protection Regulation (GDPR) enshrines citizens’ right to know what data is being held about them and how it is used, as well as to request its deletion (the right to be forgotten). It further mandates explicit consent for the collection of data, and that this consent may be withdrawn as easily as it was given. Penalties for non-compliance can be as high as €20 million or 4% of global revenue, whichever is higher.

Even though the GDPR is a law designed to protect European citizens, it is already having global ramifications. Companies introducing improved privacy protections across all customers avoid double standards and conflicts between regions. Businesses falling short of these standards might soon experience a loss in customer trust.

The GDPR constitutes a first blueprint for good practices and other countries may soon follow with stricter regulation. After a period of naiveté about the dangers of the data economy, followed by a period of carelessness, both citizens and regulatory bodies are waking up to the need for better data practices <sup>12</sup>. The Wild West of the World Wide Web may be nearing its end.

Energy service providers can respond in one of four ways: avoid the GDPR by withdrawing from the EU market; fail to comply and risk fines; comply with minimal effort (for example, observing the letter of the law, while looking for loopholes and other ways to minimise changes to their data practices, akin to tax avoidance); or embrace privacy pro-actively. By choosing the last option and thoroughly protecting data subjects, energy service providers can lay the foundation for future business models that rely on trust. Rather than solely focusing on gaining customers' trust, it is more important for energy service providers to become trustworthy. Marketing strategies may temporarily gain customers' trust, but without the ethical underpinning that is required for trustworthiness, a scandal could undermine this trust for the entire sector.

Although regulators play an important role to ensure users' trust is not misused, regulation may not be enough. For instance, it has been argued that the GDPR is still lacking in the regulation of data collection, as opposed to data use <sup>13</sup>. Energy service providers have an opportunity to stay ahead of the law by observing best practices and collecting only the data that is necessary to provide good services. Many energy customers are unaware of the types of data that may be collected from them. To avoid erosion of trust, it would be best if they did not learn about it as part of a privacy scandal. Indeed, research has shown that customers who have control over their data and who have been kept well informed are more forgiving in case of a data breach. Transparency and control also result in customers feeling less violated from big data practices <sup>14</sup>. Users should therefore be informed about what data is being held about them, how and where it is secured, who may gain access to it, how long it will be kept for, what kind of insights it may yield, and why it is necessary to collect/keep it. The default should be to collect and share as little information as necessary, with additions as 'opt-in'. This would allow consumers to choose their privacy over other benefits, if they so wish.

Energy service providers themselves have a lot to gain from trustworthiness. Energy retail markets have long suffered from lack of competition. Energy as a product is indistinguishable between providers. In many countries, utilities suffer a lack of customer trust. It is conceivable that trustworthiness could introduce a new dimension of competition into these markets. The most trustworthy organisation may hold a licence to engage in more innovative and cost-effective smart solutions. Future energy business models will heavily depend on data access. To ensure that customers are willing to collaborate, a proactive attitude towards privacy could be vital.

If energy companies succeed in protecting their customers' privacy, they will not only avoid stiff penalties and build up vital trust capital for innovative and data dependant future business models. They will also contribute to building a low carbon energy system

that can take greater advantage of big data opportunities while respecting data subjects' rights. Ethical practices are thus not only valuable as a way of doing what is right—they can also be good for business.

## References

- 1 Gibbs, S. in *The Guardian* (11 May 2018).
- 2 Ruddick, G. in *The Guardian* (30 November 2017).
- 3 Darby, S., Liddell, C., Hills, D. & Drabble, D. *Synthesis report, Department of Energy and Climate Change* (2015).
- 4 Burgess, J. & Nye, M. *Energy Policy* **36**, 4454-4459 (2008).
- 5 Armel, K. C., Gupta, A., Shrimali, G. & Albert, A. *Energy Policy* **52**, 213-234 (2012).
- 6 Stanokvic, L., Stanokvic, V., Liao, J. & Wilson, C. *Applied Energy* **183**, 1565-1580 (2016).
- 7 McKenna, I., Liu, E.C., & Thomson, M. *Energy Policy* **41**, 807-814 (2012).
- 8 O'Neill, O. in *BBC Radio 4* (7 December 2012).
- 9 Hern, A. in *The Guardian* (28 January 2018).
- 10 Singer, N. & Merrill, J. B. in *The New York Times* (28 June 2015).
- 11 Schneier, B. in *CNN* (1 March 2016).
- 12 Butterworth, T. in *Vox* (26 March 2018).
- 13 Stallman, R. in *The Guardian* (3 April 2018).
- 14 Martin, K. D., Borah, A. & Palmatier, R. W. *Journal of Marketing* **81**, 36-58 (2019).

Carissa Véliz's work has been supported by a Wellcome Trust Grant (203132/Z/16/Z).