Smart Buildings: Law and Ethics

Cyril Holm

1 Introduction

This paper addresses research issues with regard to law, ethics and *smart buildings*. The background is the research project *Digitalization of the Construction Industry*,[1] a project that primarily aims to investigate *legal* and *ethical* aspects of smart buildings, i.e. houses that optimize performance based on analysis of data, including data that residents produce as they go about their everyday life.

Smart buildings that enhance their performance using technology is not a fundamentally different field of inquiry as compared to other areas affected by the development of technology. What makes buildings interesting, though, is that roughly ten percent of a country's GDP derives from construction.[2] Further to this, approximately thirty percent of a country's energy consumption, and forty percent of its carbon dioxide emissions, derive from construction and buildings in the Northern hemisphere.[3] Hence, research on smart buildings may lead to substantial cost savings and resource efficiency.

Another aspect that makes residences interesting from a legal and ethical perspective is that we in the shelter of our home act on a presumption of being entitled to privacy. As the things we do privately often can be more revealing, as compared to situations in which we are aware of being observed, this information has a potentially high commercial value. All this raises questions about law and ethics. With regard to law, The General Data Protection Regulation (GDPR) is of relevance, because it imposes a rigorous framework on how to process personal data. As for ethics, the issues revolve around how the rights of the individuals are balanced against the social advantages regarding e.g. energy consumption and public health.

2 What is a Smart Building?

Smart buildings are "smart" because they are adaptive. That is to say, they may adjust their functions based on data, e.g. about weather conditions and variations concerning how the building is being used. Adapting the functions of a building may result in optimized energy consumption, more efficient use of resources and improved health of its residents.[4] Data about when residents are at home is for

1 A research project financed by Formas and undertaken jointly by The Swedish Law and Informatics Research Institute, LivinLab a research test bed for "smart houses" at The Royal Institute of Technology, The Department of Philosophy at The Royal Institute of Technology, Akademiska hus, and HSB.

2 *See*, for instance, "www.sverigesbyggindustrier.se/statistik-byggmarknad/bygginvesteringar__6907".

3 Marco Molinari and Olga Kortas, *ICT in the Built Environment: Drivers, Barriers and Uncertainties*, (forthcoming), p. 1.

4 Jonas Vogel, Andreas Novak, and David Bohn Stoltz, *KTH Live-In Lab: Testbädd för boende- och byggrelaterade miljöinnovationer* [KTH Live-In Lab: Test Bed for Environmental Innovations in in Residential housing construction], *Bygg & Teknik*, vol. 5 (2017), pp. 14-17.

example useful for deciding to what extent a house need to be ventilated or heated. Other potential benefits of this research is understanding of how to construct more sustainable buildings, improved logistics regarding utilities, environmental benefits, etc.

Many things will be "smart" in a not too distant future and in a home there are ample opportunities to gather data about the persons living there. In this respect, data on sleeping habits, nutritional intake, contents of human rest products – such as exhaust air, perspiration, secretion, discharge, urine, and faecal matter – can be useful in order to prescribe, or suggest, health-related life-style changes.[5] The use of all types of the aforementioned data must, however, be balanced against possible privacy intrusion, stigmatization, data security breaches, and restricted autonomy. In the privacy of our homes we also do things that may have commercial value as it reveal data that can be used in profiling and predicting consumer demands. This in turn raises legal questions regarding manipulation and discrimination.

2.1 Data Privacy and Security: Overview of GDPR

GDPR is a manifestation of a European tradition of making distinct the sovereignty of the individual. In broad outline, this tradition goes back to Greek philosophy, and hasbeen transplanted into the present *ius commune* through Roman law, and the Catholic Church.[6] GDPR is both in form and substance very much part of this tradition. This inventory of legal issues related to smart buildings, is in part made in light of this tradition.

GDPR is a European-wide (EU-) legislation that aims to fence off information on individuals by giving the individual person a property right to such information,[7] and by laying down strict requirements for the lawful "processing" of "personal data" by others than its owner.

"Personal data" in GDPR is understood as any information that alone, or in combination with some other information, may identify a person.[8] Already from this definition, we understand that this piece of legislation takes a very broad view on its area of application. Evident examples of "personal data" include are personal number and name. Less evident examples include IP-address, GPS

5 *See*, for instance, the research project funded by Horizon 2020, *GoodBrother*; proposal reference: OC-2018-1-23059.

6 *See*, Franz Wieacker, *A History of Private Law in Europe*, trans. Tony Weir, forward by Reinhard Zimmermann (Oxford: Clarendon Press, 1995), Part 1, in particular Chapter 2. For further on this, see J.M Kelly, *A Short History of Legal Theory* (Oxford: Clarendon Press, 1992); and Randall Lesaffer, *European Legal History: A Cultural and Political Perspective* (Cambridge: Cambridge University Press, 2009).

7 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).Chapter 3; and preamble Article 7.

8 GDPR Article 4.1.

position, partly given credit card numbers, electronic keys, and travel passes tied to a specific individual.

The "processing" of "personal data" in GDPR means "any operation or set of operations which is performed on personal data, whether or not by automated means, such as collection, organisation, structuring, storage, and alteration".[9]

GDPR stipulates that personal data shall only be collected for legitimate and explicitly specified purposes; that the collecting of personal data must be minimized; that personal data must be accurate, and immediately corrected if false; that personal data is de-personalized as soon as the purposes of the processing admits; that the personal data must be secured against loss, destruction, and theft by organizational and technological means.

If "personal data" is processed according to all of the above general principles, lawful processing must also fall under at least one on the legal bases for such processing as set out in Article 6 of GDPR. These legal bases are: consent, performance of a contract, compliance with a legal obligation, protecting the vital interests of the owner of the personal data, performing the duties of public authorities, or in the public interest, securing the legitimate interests of someone other than the owner of the personal data.

GDPR also contains provisions concerning "sensitive personal data", such as racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, information on health, genetic information, biometric information, sex life, or sexual orientation. Processing of "sensitive personal data" is by default prohibited, although there are a number of significant exemptions,[10] for instance when the owner of the sensitive personal data give consent, or in situations involving employment or social security. The exemption for processing sensitive personal data on the basis of consent is particularly important when it comes to research on smart buildings and such areas of functionality as biometric keys and health optimizations based on data on genetics and overall health.[11]

2.2 GDPR and Commercial Aspects of Smart Buildings: Areas of Functionality

In this section, three aspects of smart buildings are addressed: (i) energy, (ii) security, and (iii) health.[12]

---

9 GDPR Article 4.2.

10 GDPR Article 9.2.

11 It should be pointed out that it is far from clear that consent applies in all possible situations, as the inequality between the parties may diverge to a great extent.

12 These three areas were chosen based on the current developments in research and technology. However, with break-through technologies what are considered the most promising areas of functionality is likely to change. Regardless of such changes, though, the important aspect here is to use areas of functionality to illustrate how they drive the data creation, and how that data relates to The GDPR. In addition, these areas of functionality, are in line with this inter-disciplinary research project, and with Katarina Backlund's Ph.D. project on "smart

2.2.1 Energy consumption

A standard application in a smart building is to measure the level of carbon dioxide in indoor air to be able to determine when residents are present.[13] That knowledge allows for optimisations such as decreasing heating and ventilation when no one is home. If such "smart" functionality is employed, and if the heat given off by residents, and the appliances they use, is used as sources of heat contributing to heating a living space, one can even out the lows and highs in indoor temperature. The result is greatly reduce energy consumption, especially when combined with solar energy and heavy insulation.

Other energy optimisations concern hot water and electricity.[14] Having information on the pattern of consumption one can store pre-heated hot water in insulated tanks, and electricity in batteries, to be used during spikes in demand. Such optimisation based on user patterns can be fine-tuned for individual households. Pricing can also be used to further distribute demand over a typical 24-hour consumption cycle, or over the yearly seasons; buying at "off hours", storing locally for peak consumption.

On the other hand, it is necessary to ask what kind of personal data these optimisations requires. If we start with the example of measuring the level of carbon dioxide in the indoor air, that information tells us when someone is home. Given that this somebody is the resident, that information is "personal data" according to GDPR, because it identifies a person. This information may be seen as innocuous in itself, but taken together with other pieces of information, it may be revealing of aspects of a person that that person wants to keep private. Information about the levels of carbon dioxide further gives information on how many are present in a residence. This may be sensitive for a number of reasons, such as tenancy law, or otherwise.

Further to this, information on the use of electricity may give information on what kinds of appliances are used, and at what times. This information may seem innocuous, but parsed and combined with other information; it could give a picture of private matters individuals may want to keep private.

2.2.2 Security

Traditionally our home has been a place to seek shelter from the outside world; a place where we can experience comfort, trust, and privacy, all of which most people are keen to protect. The law traditionally secures the home as a place of

buildings" and The GDPR, a project that is conducted together with the partner of this Research project, Akademiska hus.

13 Vogel, Novak, and Bohn Stoltz, *KTH Live-In Lab: Testbädd för boende- och byggrelaterade miljöinnovationer* [KTH Live-In Lab: Test Bed for Environmental Innovations in in Residential housing construction], p. 14.

14 Ibid., p. 14.

utmost significance in a person's life, and a place that is so significant as to stop government to entry by force, without undue legal basis.[15]

Modern "smart" security devices, such as biometric keys (keys that operate on finger prints or face recognition), allows you to determine exactly who used the lock at what time to enter a house. A CCTV camera placed at an entrance to a building allows you to see who is at the door. Smart alarms that can be monitored from afar, and allow you to see the interior of a home on your cell phone, is another feature that is already popular.

Also in this case the utilised personal data may be sensitive and the processing must be in accordance with the GDPR.[16] Information on when you enter the house, can be damaging when paired with other information. Cameras at entrances reveal a lot of data on individuals, as does camera surveillance inside the residence. Data may e.g. reveal gender, ethnicity, religious practices, or the disobedience of religious practices and so forth.

2.2.3 Health

Health is a rapidly growing sector, not least in terms of "smart" technologies that support a healthy life.[17] In addition, the steady growth of knowledge about how to prevent welfare diseases such as obesity, diabetes, coronary conditions and cancer with adjusting the way we live; by eating less and more nutritious, and by exercising, we can substantially change the probability of those diseases. Because a residence is a place that we can accommodate to our personal lifestyle, and because we spend much time there, smart buildings can "nudge"[18] us to better chances of more good years by technology.

Many use technology in phones to monitor daily exercise, heart rate and so forth. Many also have tools for exercise in their homes in addition to exercising outdoors. However, there are a number of things you can do in a smart house that are difficult to accomplish outside the house. For instance, one can monitor the quality of sleep, as poor quality of sleep, especially snoring can be an indicator of other health related issues. Further, one can monitor the contents of exhaust air from humans and take a reading of the contents. A final example is to monitor the contents of urine and faecal matter to look for indicators of potential poor health.

It goes without saying, that monitoring of this kind generates personal data, in most cases sensitive personal data. Many of us would also have a great interest in utilising the data, if basing our eating habits and exercise regimes on it nudge

15 *Cf*, the standard constitutional provisions that the government need a decision by a court to a law for the search of someone's home.

16 GDPR Article 9.1.

17 *See*, for instance, the research project funded by Horizon 2020, *GoodBrother*; proposal reference: OC-2018-1-23059.

18 Richard H. Thaler and Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth and Happiness* (London: Penguin, 2008).

us to increasing the probability of more good years in our life span. It is however also information that most of us understand to be very private.

2.3 GDPR and Research on Smart Buildings

The research project, "Digitalisation in the Construction Industry", for which this inventory of legal and ethical issues with regard to smart buildings is made, is concerned not only with commercial aspects of smart buildings, but also with how research on such buildings may be conducted.

As we saw in the previous section, smart houses may generate sensitive personal data, as defined by the GDPR. Because regulation of research in GDPR is partly delegated to national parliaments, this is a regulatory field that currently is somewhat unclear as national parliaments are not done legislating in this field. However, three areas should be closely observed: research involving "personal data", research involving "sensitive personal data", and research involving databases.

Research on "personal data", then, must be undertaken with a legal basis found in Section 6 of GDPR, as it involves "processing" of such data. As consent is a legal basis[19] that has been largely excluded from use in situations when the inequities among the parties to a consent is too large, (as they could be in a situation when a government body asks for a consent from an individual), the legal basis must instead be "public interest", Section 6.e, which, in turn, must be further corroborated in national legislation.

According to the Government investigation SOU 2018:36, public interest is secured as a legal basis in Swedish law because in Chapter 2, Section 18 of *Högskoleförord-ningen* [Swedish Ordinance on Higher Education][20] it is clear that such a legal basis exists for research conducted by a public university, or other public research institute. However, if you are a private research entity, the legal basis of public interest is not viable. You must instead apply for their research to be approved by an ethical review board, in line with the Ethical Review Act.[21].

Moreover, if the research uses "sensitive personal data", it has to be approved by an ethical vetting board, regardless whether the research entity is public or private.

Finally, research on smart buildings will most certainly involve creating databases. A public research entity can manage a database on the legal basis provided in the *Högskoleförordningen*. Private research entities must acquire such a legal basis by getting an approval by an ethical vetting board.[22] Such approval by an ethical vetting board, is conditioned on the consent of the research subject. Consent must be voluntary, explicit, specific, and documented. Further to this, the consent is only valid if the research subject is informed about

19 GDPR Article 6.1.a

20 Regulation of higher education SOU 2018:36, p. 243.

21 SOU 2018:36, p. 245.

22 SOU 2018:36, p. 243-45.

the research on the following topics: plan, purpose, methods, possible consequences and risks, identity of research body, that it is voluntary to participate, and that there is a right to cease to participate.

2.4 Property Rights to Personal Data in Commercial Real Estate and Research on Smart Buildings

The personal data that is generated in commercial and research aspects of smart buildings intuitively belongs to the person that the data is about. That is, it is intuitive that the individual about whom the data is about, and the individual that in some sense "produces" the data, has the property right to that data. This intuitive idea is expressed in GDPR as the idea that the individual from whom personal data emanates, owns that data[23] and can depose of it a way he or she sees fit. However, it is worthwhile to see on what grounds one can argue for such ownership. This is of interest partly because the idea of legal ownership is hard to separate from some morally based idea that it is morally right that someone has a right in something. It is also of interest when we discuss moral issues related to commercial uses of personal data by others than its owner. This because commercial entities form a picture of someone's identity from many different data-points that taken in isolation are of scant interest, but processed together may be very intimately telling about someone's life, and as such be of high commercial value.

In view of this, one can ask what right commercial entities have to commercialise data owned by the individual from whom it emanates. I shall not go into different lines of argument on individual property rights here, but just note that there are several traditions on this issue. In the theory of libertarianism the idea is that the individual has a right to self-ownership and this right is so powerful that it prohibits the state or other coercive apparatus to infringe upon it,[24] and because individual volitions are free, rights is freedom.[25] If we think of the personal data in the sense of GDPR, it seems clear that the individual has a property right to that data. There are also additional analysis available of legal rights in terms of legal privileges, claims, powers, and immunities, that can be used to further highlight different aspects of data in GDPR.

2.5 Privacy

Over time, the law gradually has come to include not only the physical protection of person and property, but also the immaterial and abstract aspects of persons and property. In line with this development, Samuel D. Warren and Louis D.

23 GDPR Chapter 3; and preamble Article 7.

24 Robert Nozick, *Anarchy, State, and Utopia* (New York: Basic Books, 1974), p. ix., Cf. G. W. F. Hegel, *Outlines of the Philosophy of Right* (Oxford: Oxford University Press, 2008), p. 26.

25 Ibid., p. 46.

Brandeis in an 1890 paper famously argued that the right to privacy in the broadest sense is derived from the inviolability of personhood.[26]

In 1960, William Prosser continued the discussion on the need for the law to defend the right to privacy, and made an inventory of cases since the time of 1890 and concluded that the right to privacy had branched off into four distinguishable torts, namely, (i) intrusion into the plaintiff's privacy, (ii) public disclosure of embarrassing facts about the plaintiff, (iii) publicity placing the plaintiff in a false light to the general public, and (iv) appropriation of the plaintiff's name for the advantage of the defendant.[27]

In 2006 Daniel Solove, argued that the concept of privacy as previously developed is wholly inadequate for understanding the possible breaches of the right to privacy in the age of information technology.[28] Taking a broader view of privacy, extending beyond the focus on tort, Solove argues that privacy also includes wrongs such as incivility, lack of respect, and causing emotional angst.[29] However, Solove is not arguing for rights in absolute terms, but follows the tradition of viewing rights as the tools of a legal order to protect the socially valuable, in this case the easement of the friction of society on the individual.[30] Solove identifies four broader actions that potentially involve privacy breaches:[31] information collection, information processing, information dissemination, and invasions.

Under these four headings, he goes on to list a number of privacy breaches. These privacy breaches are: [information collection] surveillance and interrogation;[32] [information processing] aggregation, identification, insecurity, secondary use, and exclusion;[33] [information dissemination] breach of confidentiality, disclosure, exposure, increased accessibility, blackmail, appropriation, and distortion;[34] [invasions] intrusion and decisional

26 Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, vol. 5 (1890) Harvard Law Review, p. 205.

27 William L. Prosser, *Privacy*, vol. 48, no. 3 (1960) California Law Review, p. 389.

28 Daniel J. Solove, *A Taxonomy of Privacy*, vol. 154, no. 3 (2006) University of Pennsylvania Law Review, p. 480. For more in the issue of privacy and technology, *see* Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social life* (Stanford: Stanford University Press, 2010).

29 Solove, *A Taxonomy of Privacy*, p. 486.

30 Ibid., p. 488. For an application of this view on rights, see Barbro Björkman and Sven-Ove Hansson, *Bodily Rights and Property Rights*, vol. 32 (2006) Journal of Law, Ethics and Medicine, pp. 209-14. For further on this view of rights with a view to private law legislation in the Swedish welfare state, see Cyril Holm, *Bearing and Sharing Risk in the Swedish Welfare State*, in ed. Matthew Dyson, *Regulating Risk in Private Law* (Cambridge: Intersentia, 2018).

31 Solove, *A Taxonomy of Privacy*, p. 490.

32 Ibid., p. 490.

33 Ibid., p. 490.

34 Ibid., p. 490.

interference.[35] As we see, the privacy breaches Solove lists under information collection and information processing directly alludes to what is meant by processing data in GDPR.

2.6 Legal Risk Analysis

As the GDPR is a demanding legislation, and because it is left to national parliaments to determine the exact scope of it, all entities are recommended to safeguard the legal situation by contemplating a legal risk analysis,[36] and by taking measures to lower legal exposure.

The standard way of taking such risk measures is to a conduct *privacy impact assessment*, that is, make an inventory of where an entity is likely to be invading privacy and how to do this in a legal manner; and by conducting a *data security impact assessment*, that is, to make an assessment of where data handled in an organisation is vulnerable from a security standpoint,

Additional measures are to, appoint an *ethical officer* – a person dedicated to overseeing the ethical aspects of privacy and security of personal data, and a *privacy officer* to oversee specific privacy aspects of data gathering – the legal risks are lowered.

3 Ethical Issues

3.1 Introduction

The fact that people will live in smart buildings and produce data, makes ethical issues unavoidable.

In normative ethics – the field in which theories are developed to answer what is morally right – there are several contenders, such as consequentialist theories[37] and rights based theories.[38] On consequentialist theories, it is a question of weighing the good consequences of data, against the bad consequences of data, and the line actions that bring about the best balance of these, is the morally right path of action. Rights-based theories are closely aligned to a legal way of thinking; if an individual has a right, that right is a trump against balancing violating that right in the name of the overall good consequences.

To investigate these theories in view of smart buildings is certainly worthwhile, but it is a far-reaching undertaking and here I will instead focus on saying something about the individual innocuousness of data, why we may not care about such data, but why we perhaps should do so.

---

35 Ibid., p. 490.

36 Peter Wahlgren, *Legal Risk Analysis: A Proactive Legal Method* (Stockholm: Skrifter utgivna av Juridiska fakulteten vid Stockholms universitet, 2013), Chapter 5.

37 *See*, for example, Krister Bykvist, *Utilitarianism: A Guide for the Perplexed* (London: Continuum, 2010).

38 Robert Nozick, *Anarchy, State, and Utopia* (New York: Basic Books, 1974).

3.2 Smart Buildings, Innocuous Data, and Virtual Identities

Smart buildings, as indeed all data hording and surveillance, raise ethical questions. Is it justified to gather this data? Is it justified if there is consent or if data is voluntarily given? Is it justified in terms of the possible positive consequences, such as improved health and energy efficiency?

The issue on how what may seem as innocuous information in fact tells you very much about a person's life, is best illustrated with an example. In the US, Target, a chain of stores, identified from purchases of four items – cocoa-butter lotion, a large purse, vitamin supplements, and a bright blue rug – that the buyer was pregnant, and in the automated customer communication they proceeded to deliver a gratulatory package. The teenage girl, as well as her parents, was caught off guard, as the girl's sex life, as well as her pregnancy status, was revealed.[39]

The question, then, is whether seemingly innocuous information is morally relevant. Adam Henschke, in his book *Ethics in the Age of Surveillance*[40], makes the case that innocuous information should be treated with the same moral care as medical information. With regard to medical information, it is obvious to most of us that privacy constraints apply. This is because that information is directly sensitive as having to do with our identity and person. The case that Henschke makes is that the innocuous data, together with meta-data, gives information about a person that is as sensitive as medical data.[41] More specifically, he argues that anyone using electronic devices, or anyone venturing out of his house, is a target of surveillance, and that this information is innocuous in isolation, but put together by government agencies, or by corporations, they form "virtual identities". These virtual identities, or so Henschke argues, ought to be treated with respect as having moral status.[42]

The ethical aspect here is that information is linked to identity – and identity is perceived to be yours – and not something, someone else has to own or operate. The idea of the individual has traditionally been a sheltered idea in European history, but is it now an idea that is challenged by advances in technology. The trajectory of this development indicates that it is possible to sway peoples' decisions on the bases of their virtual identities, thus shattering

39 Adam Henschke, *Ethics in the Age of Surveillance: Personal Information and Virtual Identities* (Cambridge: Cambridge University Press, 2009), p. 3.

40 Henschke, *Ethics in the Age of Surveillance: Personal Information and Virtual Identities* (Cambridge: Cambridge University Press, 2009. For more on the topic of surveillance, see Stanley Greenstein, *Our Humanity Exposed: Preictive modelling in a Legal Context* (Stockholm: Stockholm University, 2017); Liane Colonna, *Legal Implications of Data Mining: Assessing the European Union's Data Protection Regulation Principles in Light if The United States Government's National Intelligence Data Mining Practices* (Tallinn: Ragulka, 2016); and Elisabet Fura and Mark Klamberg, *The Chilling Effect if Counter-Terrorism Measures: A Comparative Analysis of Electronic Surveillance Laws in Europe and the USA*, in Freedom of Expression: Essays in Honour of Nicolas Bratza (Oisterwijk: Wolf Legal Publishers, 2012), p. 463.

41 Henschke, *Ethics in the Age of Surveillance*, p. 12.

42 Ibid., p. 12.

the keystone of the idea of "one man – one vote", namely the view of man as capable of rational decision-making based on information.

Of course, a home is such that the data gathered in privacy is more prone to be revealing about the virtual identity of a person. This is an important ethical issue to consider – an issue that also branches out into politics as we have seen – when engaging in the commercial aspects of smart buildings.

4 Concluding Remarks

This paper provides an inventory of potential legal and ethical issues with regard to smart buildings, especially relating to personal data and fundamental rights of individuals. Many pieces of information about us seem innocuous when viewed in isolation, but when data is aggregated, the picture may change. A notorious example is Cambridge Analytica's claim that combined with a personality test the company was able to predict a person's decisions.[43] That Facebook and Google, among others – is privy to personal communications around the world; that Russia tampers with elections of sovereign nations; that commercial firms were payed as consultants to sway elections, gives pause. Admittedly, smart buildings and the information involved is a lesser matter, but this overall picture makes us want to think about these issues long and hard, not least because innocuous information in sufficient quantity says a lot about identity.

A final word on ethical risk analysis: Because GDPR is such an ambitious legislation, and because it leaves to national legislators to specify some of its provisions, breaches of the law are likely to occur despite the best of intentions. In addition to a legal risk analysis, then, it may also be a preventive measure to perform an *ethical risk analysis*.[44] Many of the issues discussed, will not be confined to law in the public mind, but to wider issues of the ethical appropriateness of processing personal data, and of exposing such data. To map the ethical issues involved, and in order to be prepared to meet potential inquiries from the media and others, it is wise to consider the ethical implications of realization and research on smart buildings. All this provide strong arguments for further research on the issues addressed here.

---

43 "www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm".

44 As opposed to the traditional risk analysis, which focuses on probability and severity of potential bad outcomes, the ethical risk analysis involves issues of agency and inter-personal relations, issues that ethics are based upon. For further on ethical risk analysis, see Sven-Ove Hansson, *The Ethics of Risk: Ethical Analysis in an Uncertain World* (Basingstoke: Palgrave Macmillan, 2013). On new technologies and ethical risks see, Elin Palm and Sven-Ove Hansson, *The Case for Ethical Technology Assessment (eTA)*, vol. 73 (2006) Technological Forecasting & Social Change, pp. 543-58. For further on how to conduct ethical risk analyses, see Sven-Ove Hansson, *How to Perform an Ethical Risk Analysis (eRa)*, Risk Analysis: An International Journal; An Official Publication of the Society for Risk Analysis, first published 28 February 2018, "doi.org/10.1111/risa.12978".

Administration