COMPUTERS & SECURITY 76 (2018) 295–310

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process

D. Polverini [a], *F. Ardente* [b,*], *I. Sanchez* [c], *F. Mathieux* [b], *P. Tecchio* [b], *L. Beslay* [c]

[a] *European Commission, DG Internal Market, Industry, Entrepreneurship and SMEs, Brussels, Belgium*
[b] *European Commission, DG Joint Research Centre, Directorate Sustainable Resources, Ispra, Italy*
[c] *European Commission, DG Joint Research Centre, Directorate Space, Security and Migration, Ispra, Italy*

ARTICLE INFO

Article history:
Available online 12 December 2017

Keywords:
Enterprise servers
Resource and energy efficiency
Privacy
Cybersecurity
Data protection
Ecodesign requirement
Reuse

ABSTRACT

Decreasing the environmental impacts of Information and Communication Technologies (ICT) devices, whilst at the same time contributing to ensure the data protection and cybersecurity of devices and infrastructure, could seem, at first sight, a difficult challenge. By means of a bottom-up approach, we show with scientific evidences that policy actions at product level have the potential to solve the apparent conundrum. The research is based on a case study related to the implementation of the European Union Ecodesign Directive to enterprise servers and data storage devices. The article proposes a novel approach to combine resource efficiency and data protection and cybersecurity issues, taking a preventative "by design" focus. This is built on the identification and subsequent proposal of solutions of the relevant market failures, i.e. situations in which the allocation of goods and services on a market is not efficient. Potential solutions are then translated into potential Ecodesign requirements for enterprise servers concerning: provision of information on the operation at high temperatures; availability of secure data deletion functionalities; availability of firmware updates to third parties; and design for disassembly of the product. We qualitatively and quantitatively assessed these requirements, in terms of energy and greenhouse gases emission savings, improved reusability, waste reduction, improved protection of personal data and security of the devices. The article concludes that a synergy between the environmental impact and the data protection and cybersecurity of these products – and the systems where they are installed (i.e. the data centres) – can be successfully achieved. Although the research work focused on a specific case study, the paper discusses finally how a similar approach could be applied to several other product groups characterised by similar market failures.

* *Corresponding author.*
E-mail address: fulvio.ardente@ec.europa.eu (F. Ardente).
https://doi.org/10.1016/j.cose.2017.12.001

1. Introduction

Because of the strong development of digital services worldwide, information and communication technology (ICT) devices and infrastructure are more and more subject to cybersecurity and privacy threats, as an increasing number of services require high levels of data protection and the need of a reliable ICT infrastructure. At the same time, the computing power and storage capacity requested from the market are growing at a very fast pace. These trends in the production and use of ICT devices can affect not only the energy efficiency during operation, but also material efficiency (i.e. the use of materials per unit of services), management of waste ICT and, overall, the environmental life cycle impacts of the whole sector. The way in which the ICT market will evolve in the upcoming years will be certainly influenced by issues related to cybersecurity, privacy and environmental impacts. The role of legislative measures in this framework will be of paramount importance, to direct the market towards specific solutions. The challenge is, to ensure cybersecurity, data protection and privacy, whilst also addressing the environmental impacts.

1.1. *Legislative context*

At European Union (EU) level, one of the most renowned legislative tools to reduce the environmental impacts at product level is the Ecodesign[1] Directive (European Union (EU), 2009a), which requires product manufacturers to improve the environmental performance of their products by meeting minimum energy efficiency requirements, as well as other environmental requirements. The legislative framework which builds upon the synergic effect of the Ecodesign Directive and the Energy Labelling Directive (European Union (EU), 2010a) has been up to now of paramount importance to improve the energy efficiency of products and to remove from the market the worst-performing ones.

In December 2015, the European Commission (EC) adopted a Circular Economy action plan (European Commission (EC), 2015a), consisting of legislative proposals on waste and an action plan covering the whole life of products and materials. It is foreseen that the actions proposed in this legislative package will contribute to "close the loop" of product lifecycles, through improved reuse and recycling. The rationale consists in surpassing the "take, make, use and throw away" approach, typical of the linear economy, and to stimulate a deep transformation of the way the EU economy works by shifting to a circular model, to retain precious resources and fully exploit all the economic value within them. In the Circular Economy action plan (European Commission (EC), 2015a) a relevant role is attributed to the Ecodesign policy, which is considered as a suitable legislative tool to develop resource efficiency requirements for products.

[1] Here and in the remainder of the text, Ecodesign is written with the first uppercase letter, to highlight that we refer to the Ecodesign Directive; in many other contexts, ecodesign (with the first lowercase letter) means, more in general, an approach to design with special consideration for the environmental impacts of the product during its whole lifecycle.

Although Ecodesign measures are mostly focused so far on energy efficiency aspects, the scope of the Directive is sufficiently broad to cover all the key aspects of material efficiency, such as durability, reparability, reusability, recyclability, and the ability to disassembly/dismantle critical components (Bundgaard et al., 2017). More systematic integration of material efficiency aspects under Ecodesign will also be enhanced by the on-going development of horizontal standards on material efficiency as discussed by Tecchio et al. (2017).

Even though data security issues were not specifically mentioned by the Ecodesign Directive, the latter generically states that the setting of requirements requires a "proper consideration of the health, social and economic impact of the measures envisaged" and in particular it "must be consistent with the economic and social dimensions of sustainable development". Data protection and cybersecurity could therefore represent an element of interest for the implementation of the Ecodesign Directive, where they would be recognized as characterising the functionality of a certain product.

In May 2016, Regulation 2016/679 (European Union (EU), 2016a), on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, entered into force. This regulation, known as the General Data Protection Regulation (GDPR), repeals the former data protection directive 95/46/EC and shall apply from 25 May 2018. One of the key principles introduced by the GDPR is that of the "data protection by design and by default". This principle defined in article 25 of the GDPR is closely related to the "privacy by design" principle (Hustinx, 2010), which establishes that privacy should be taken into account throughout the entire engineering lifecycle of a product or service, in particular during the design phase.

The EU cybersecurity strategy (European Commission (EC), 2013) followed by the EC Communication on resilience, deterrence and defence (European Commission (EC), 2017a) represent a solid commitment to protect the digital security of citizens, products and services. The Digital Single Market (DSM) strategy (European Commission (EC), 2015b) acknowledges cybersecurity and trust as key factors for the success of the DSM initiative. The 2016/1148/EU Directive on security of network and information systems (European Union (EU), 2016b), known as the NIS Directive, entered into force in August 2016 becoming the latest addition to the European cybersecurity legislative framework. More recently, the EC has adopted a cybersecurity package (European Commission (EC), 2017b) that seeks to complement existing measures and further improve the EU cybersecurity resilience and response. Similarly to the related principles in the data protection domain, "security by design" and "security by default" are recognized as key principles to improve the level of cybersecurity in products and services.

The EC, following these 'by design' principles, has the objective to embed cybersecurity in new policy initiatives since their inception. This paper presents the result of the practical application of these principles in the implementation of the Ecodesign Directive. The objective of the research was precisely to take into consideration cybersecurity and data protection in synergy with energy and material efficiency aspects of the products.

1.2. *Scientific and technical literature*

Hinchliffe and Akkerman (2017) argued that more time and more efforts must be devoted to new aspects, such as material efficiency aspects in product policies, so that resource efficiency can be weighed up against energy efficiency and other parameters. Indeed, although ecodesign of products has a long tradition in industries and academic research (Allenby, 1991; Ardente et al., 2003; Ashley, 1993; Brezet and van Hemel, 1997), the analysis of the potential connections between ecodesign practises and policies is relatively recent (Ardente and Mathieux, 2014a, 2014b; Dalhammar, 2014). Several product groups have been thoroughly analysed from a material efficiency perspective and policy options have even been proposed, for example for electronic displays (Ardente and Mathieux, 2014a; Ardente et al., 2014), for washing machines (Ardente and Mathieux, 2014b), vacuum cleaners (Bobba et al., 2016) and PC/laptops (Talens Peiró et al., 2017). However, very few formal requirements on material efficiency came into force in EU regulations. Bundgaard et al. (2017) identified a possible transition from an "energy efficiency" focus towards a more general resource efficiency approach in policies, although this transition is still in its early phase and far from the full exploitation of its potential. According to Dalhammar (2016) whilst European manufacturers have become increasingly positive towards policy measures for energy efficiency, their attitude is still sceptic towards policy measures related to reusability and end-of-life (EoL) of products.

Scientific literature exploring the link between ICT security and privacy, on one hand, and environmental issues and sustainable development, on the other hand, is mostly limited to the study of aspects related to: a) energy efficiency and trade-off between power consumption and system performance (Castiglione et al., 2012; Guo et al., 2011; Hassanzadeh and Stoleru, 2013; Makri and Konstantinou, 2011; Oracevic et al., 2017; Razaque and Rizvi, 2017; Virvilis et al., 2015), b) security of critical infrastructure for energy and environmental functions (Lopez et al., 2013; Nazir et al., 2017; Theoharidou et al., 2010), and c) development of security and privacy solutions suitable for resource-constrained devices (Chifor et al., 2017; Hassanzadeh et al., 2016; Kumar et al., 2017; Zonouz et al., 2013).

Further study of the intersection between these topics requires approaching them from additional multidisciplinary angles. Indeed, one of ten "deadly sins" of information security, identified by von Solms and von Solms (2004), is "not realizing the fact that information security governance is a multi-dimensional discipline" that is going beyond the "personal dimension" and the "policy/legal dimensions", but involving more and more the "environmental dimension". However, very little research has been carried out on how different aspects of the environmental dimension are connected with security and privacy protection. This is, for example, the case of the management of ICT devices at their end of life to promote good practises in terms of their reusability and recyclability, whilst still granting a sufficient security of the reused devices and the adequate handling of private data stored by former users.

Starting from 2012, standards have been issued by the European Commission (EC) (2012a, 2012b) to facilitate the EoL treatment of waste of electric and electronic equipment (WEEE). The relevance of data security in WEEE has been identified by the draft standard EN 50614 on "Requirements for the preparing for reuse of WEEE" (CENELEC, 2016). This document states that personal data and other data that have been specifically licensed to a user stored within data-bearing equipment or components (e.g. disk drives, memory chips) shall be eradicated in accordance with a documented and recorded procedure (CENELEC, 2016).

The importance of secure data erasure in sanitization of storage media prior to reuse or disposal has been subject of study in Hughes et al. (2009) where the authors focus on the use case of disks and tapes and discuss the sanitization techniques described in National Institute of Standards and Technology (NIST) standard 800-88 (Kissel et al., 2014). This standard defines media sanitization of data as "the process that renders access to target data on the media infeasible for a given level of effort".

Essentially, the literature describes four levels of sanitization of media. The first one refers to the discard of media without any specific sanitization measure beyond the deletion of files in the operating system. This is the most insecure way to dispose media, as user content can be easily recovered by third parties even if it appeared as deleted in the operating system. The forensic techniques to recover data not securely deleted from storage are well known (Alherbawi et al., 2013; Burghardt et al., 2008; Garfinkel and McCarrin, 2015) and there are a plethora of open source tools that implement them.

The second level refers to the usage of generic techniques to digitally overwrite all storage space, such as the low-level blocks overwrite (Gutmann, 1996; Wright et al., 2008). These techniques are often implemented by third party software and can operate on a wide range of storage hardware. Whilst these techniques offer a good degree of security in the erasure of data in traditional hard-drives, they are not so effective in newer storage devices. In Wei et al. (2011) the authors demonstrate how these techniques do not effectively erase all user content from Solid State Drives (SSDs) given the way these devices work internally.

The third level of sanitization of media is represented by the in-drive erasure functionality implemented in the Advanced Technology Attachment (ATA) and Small Computer System Interface (SCSI) standards. Compatible drives can receive the respective ATA or SCSI and execute a secure erasure of all data following the implementation chosen by the manufacturer (Wei et al., 2011). The main advantage of this method is that the process can be very effective as the manufacturer of the storage device is in the best position to implement it properly (e.g. by selecting the most adequate overwriting pattern). The second advantage is that the process is usually faster, as it is implemented in the firmware of the storage device. However, studies (Wei et al., 2011) have found that whilst this approach is definitively more effective than the ones previously described to render the data unrecoverable, in some cases manufacturers have failed to implement it properly.

The fourth level of techniques is composed by the most extreme techniques that target the very hardware of the storage device with the aim of destroying the stored information. The classic technique is the degaussing of discs, which essentially generates a strong magnetic field that destroys the magnetically encoded information. It is worth noting that this

technique does not work with SSD drives, as demonstrated by Wei et al. (2011). Other more extreme techniques involve the total destruction of the storage device (e.g. by shredding).

Data protection and cybersecurity in electric and electronic equipment are also linked to the availability of firmware updates. Firmware attacks have become more and more common the last decade (Costin et al., 2014; Zhou et al., 2009), leading to a re-evaluation of the role of firmware and its lifecycle when considering the improvement of cybersecurity in products and services. Although firmware vulnerabilities are not new, traditionally they have been cause of concern mostly in embedded devices. However, in the last years we have seen how firmware vulnerabilities in server components could be abused to compromise the system and the services it supports. A recent example of this is discussed by Intel (2017), showing that a vulnerability in the management of firmware of certain enterprise servers can lead to a remote compromise of the equipment. Firmware security in servers is often overlooked and the distribution of patches might not be as effective as in the case of operating system software and tools. It is worth noting that in this particular example, the firmware vulnerability affects a wide range of server models manufactured between 2010 and 2017. The literature review also reveals that the firmware is often the preferred choice for the deployment of backdoors (Ang et al., 2013; Gorobets et al., 2015; Sacco and Ortega, 2009; Zaddach et al., 2013). Due to the nature of these backdoors and the way the firmware operates with respect to the hardware and the operating system, traditional operating system security controls are not effective in detecting malicious code in firmware (Rao and Nayak, 2014). There are also numerous reports of backdoors found hidden in the firmware of consumer devices (Skorobogatov and Woods, 2012).

Firmware security is particularly important in the growing market of "Internet of Things" (IoT, objects and people interconnected through telecommunication) and home automation. With the proliferation of connected smart home devices, such as home security systems, fridges, stoves, televisions and other appliances with remote operation capabilities (von Solms and van Niekerk, 2013), concerns about the protection of personal data have been raised by many experts (Alcaide et al., 2013; von Solms and van Niekerk, 2013; Vermani, 2016). As these types of products are a relatively recent addition to the market, only a limited amount of them have reached EoL and their reuse and recycling treatments have been not investigated yet. In many cases, reuse or recycling operators that we interviewed ignored that new generations of large household appliances (e.g. washing machines, fridges, dishwashers) could be affected by potential data security issues. No studies on the topic have been conducted so far.

Although material and energy efficiency (both related to sustainable development), on one hand, and cybersecurity and privacy protection, on the other hand, have been individually analysed in some literature, we have found no references tackling both topics simultaneously. A notable initiative concerns the special issue of Computers in Industry "Emerging ICT concepts for smart, safe and sustainable industrial systems" (Trentesaux et al., 2016) that compiles 13 papers concerning ICT enabled smart industrial systems and also addressing either safety in the broad sense (including security, reliability and availability) and/or sustainability. Although sustainability was also looked at broadly (addressing environment, economy and society), no scientific work tackling simultaneously safe and sustainable industrial system was presented in this special issue and editors called for intensified research efforts to enable a convergence of smart, safe, and sustainable industrial systems.

1.3. *Aims and structure of the paper*

The present paper describes the research that we have conducted on the relationship between material and energy efficiency issues for energy using products and "privacy and security by design" aspects of these products. Our research is based on the analysis of a specific ICT case study: the development of Ecodesign measures for enterprise servers and data storage products (the most commonly installed ICT products in data centres/server rooms), launched in 2013 within the policy framework of the EU Ecodesign Directive. The aim of our research is to identify potential "preventative" (i.e. by design) solutions to decrease the environmental impacts of servers and data storage devices, whilst contributing to ensure the data protection and cybersecurity of devices and infrastructure. Options for regulatory solutions through the Ecodesign Directive are in particular analysed.

The paper follows a bottom-up approach, starting from considerations derived from the specific case study within the mentioned policy process and then generalizing conclusions valid for a wide range of different products. Its novelty is in the innovative analysis of the connections between resource efficiency and cybersecurity, privacy and data protection considerations, which were never tackled with such synergic approach.

The paper is structured in six sections. It starts by presenting the research approach and the choice of the specific case study (Section 2). Subsequently (Section 3) the focus is on the most relevant market failures affecting enterprise servers and data storage devices, which can hamper the diffusion of resource efficient products and can affect security and privacy aspects during their life cycle. Then, some potential solutions to overcome these problems are proposed and discussed in depth (Section 4). Finally, Section 5 discusses the potential extension of the research approach to different product groups, and Section 6 summarizes the main findings.

2. Presentation of the research approach

The present research follows a bottom-up approach, based on the analysis of a concrete case study: the development of Ecodesign requirements for enterprise servers and data storage products. After the analysis of the product group, and following the commitment of the EC to mainstream cybersecurity and data protection in EU policies (European Commission (EC), 2017b), we analyse how potential product requirements in the Ecodesign policy initiative could contribute to improve the level of data protection and cybersecurity both at product (i.e. server or data storage product) and at system (i.e. data centre) level.

The research approach is articulated according to the following steps:

- identification of certain market failures for the resource efficiency of the case study products, and analysis of potential connections with cybersecurity aspects. This step, as discussed in Section 2, is based on the analysis of information in the literature and on information collected from EoL operators.
- drafting and progressive revision of potential product requirements for enterprise servers and data storage products to increase their resource efficiency, privacy and security. This step is fed by extensive discussions with relevant stakeholders (i.e. policy makers, industries, EoL operators, associations of consumers, market surveillance authorities);
- assessment and discussion of potential benefits related to the identified product requirements;
- analysis of the potential extension of the research to other product groups. This step also includes an analysis of potential strengths and the limitations of the research approach.

2.1. *Reasons for the selection of the case study*

Concerning the ICT products, there are currently Ecodesign implementing measures affecting electronic displays (European Union (EU), 2009b) and domestic computers (European Union (EU), 2013). A further group of ICT products is currently under analysis by the EC, i.e. the enterprise servers and the data storage products. These products were included in the Ecodesign working plan 2012–2014 (European Commission (EC), 2012a, 2012b) as a potential product group for which to investigate the feasibility of Ecodesign measures aimed to decrease their environmental impact in a cost-effective way. Enterprise servers and data storage products represent the highest share of IT products in data centres/server rooms; their annual electricity consumption is estimated (European Commission (EC), 2017c) to be 53 TWh in 2015, corresponding to 2% of the total consumption in the EU, and this figure is estimated to continuously increase: trends such as the IoT, the "Industry 4.0" (the trend of automation and data exchange in manufacturing technologies), and "Cloud Computing" (distribution of computational work and data storage on a number of sites connected in the Internet) are growing at a very fast pace, requiring more and more computing power and storage capacity.

In such an overall context, it is expected that Ecodesign requirements for enterprise servers and data storage products could grant large energy savings (European Commission (EC), 2017c). To date, the typical Ecodesign implementation process (Polverini and Tosoratti, 2016) is on-going for these products and a so-called "preparatory study" (a techno-economic-environmental analysis on the feasibility of Ecodesign requirements) was concluded in September 2015 (Berwald et al., 2015). The preparatory study envisaged some potential Ecodesign requirements, both at hardware level (such as the efficiency of the internal power supply unit), as well as at product performance level (such as the power consumption in idle state). The preparatory study was complemented by another technical study (Talens Peiró and Ardente, 2015), which examined in depth the material efficiency aspects of enterprise servers and data storage products. In both these studies, data security and privacy issues were partially raised, as characterising the product functionality, but not investigated in full detail.

The research described in the present paper further investigated the data security and privacy aspects of the case study products and specifically led to a novel formulation of Ecodesign requirements.

3. Identification of relevant market failures of a typical ICT product group: Enterprise servers and data storage products

The research question, which represented the starting point of the present article, is the following: how to identify solutions to decrease the environmental impacts of servers and data storage devices, whilst contributing to ensure data protection and cybersecurity in devices and infrastructure along their life cycle? The problem was characterised in its multi-faceted nature (as it affects resource efficiency as well as data protection and security of devices), with the aim of identifying its underlying causes.

Under a neoclassical microeconomic perspective (Bukarica and Tomšić, 2017), the observed deviations from perfectly competitive behaviour of markets led to the identification of the relevant market failures affecting enterprise servers and data storage devices. A market failure occurs when a market fails to work efficiently to produce goods in a way that optimizes benefits to society (Dennis, 2006) i.e. to increase the social welfare. As it will be shown in the remainder of this section, market failures for enterprise servers and data storage devices mainly concern imperfect (incomplete) information (Dennis, 2006), i.e. when customers and other stakeholders which play a role throughout the product lifecycle, such as repairers or recyclers, are given neither sufficient nor good-quality information for their purchase (in the specific case of customers) and behaviour decisions (e.g. about the optimal operating temperature, or the way to dispose the product). The reasons for imperfect information vary from case to case, being linked e.g. to lack of standardised methods (such as in the case of energy consumption) or to overcautious end-of-life practises (as in the case of the sanitization of HDDs). Specifically in the case of the (lack of) availability of firmware updates, which will be described in detail in the remainder of this section, this can be considered as a market failure concerning "market power" (the ability of a firm to profitably raise the market price of a good or service over marginal cost).

Once the specific market failures (in the case of enterprise servers and data storage devices) are identified, the most effective regulatory solutions – in terms of Ecodesign requirements – were hypothesized. The present section concerns the presentation of the market failures, whereas the next section is related with the potential regulatory solutions.

3.1. *Market failure concerning energy consumption and reliability aspects*

As evidenced in one of the preparatory documents (European Commission (EC), 2017c) linked to the work on potential Ecodesign measures for enterprise servers and data storage

products, there can be a "non-optimal economic behaviour" of the customers of these products. Enterprise servers and data storage products are perceived by customers as products for which service availability, performance and security still have priority over energy (and resource) consumption. This is also linked to the fact that the lack of information on the energy consumption specifically linked to enterprise servers and data storage devices, coupled with the absence of standardised methods to measure their energy efficiency, can still be a barrier for a conscious and optimal choice of the customers when purchasing the products (in the case of companies whose ICT equipment is located in a dedicated room or space inside the company's premises) or choosing the service provider (as in the case of companies relying, for the ICT services, on an external data centre). Furthermore, these products are typically operated at temperature in the range of 20–22 °C (El-Sayed et al., 2012), as discussed more in detail in the next sections. As proved by Berwald et al. (2015), more information on the energy consumption and reliability of enterprise servers and data storage at higher operating temperature would therefore be highly beneficial, as significant energy savings could be attained at data centre level when working at higher operating temperatures, due to the decreased need of a refrigeration load.

3.2. *Market failures concerning material efficiency, cybersecurity and data protection aspects*

Despite the relevance of reusing products being largely stated by both the legislation (e.g. by the European waste Directive (European Union (EU), 2008) and the scientific community (e.g. by Graedel and Allenby, 1995 and Lindahl et al., 2006), the actual reuse levels are still relatively low. To some extent, policy objectives could also mismatch, since concerns linked to data protection policies could incentivise the physical destruction of data bearing components, whilst this is making impossible the reuse of the component and, in some case, of the whole equipment.

According to recent European statistics, reuse of ICT in the EU28 was around 4% of the WEEE collected in 2014 (Eurostat, 2014), although this figure is an average value referring to all product groups belonging to this category. A certain variability of the reuse rate of ICT is also observed across different European countries, varying from 0% to 8% (Eurostat, 2014). There are evidences that, especially for business-to-business products, the reuse rate for enterprise servers is much higher (quantitative information on the data storage products was not available). For example, statistics of the treatment of professional IT and telecommunication equipment in France in 2013 accounted for reuse of equipment (including spare parts) up to 27% (Berwald et al., 2015). According to a reuse operator in the UK contacted in 2015, 38% of the servers received in their facility were reused as whole, 26% were harvested for spare parts whilst the remaining 36% was sent to recycling (re-tek, 2015). In particular, concerning reused spare parts, around 48% of HDDs and 40% of the memory cards from servers were yearly reused (re-tek, 2015).

More optimistic values on reuse have been claimed by a European association of electronic industries, suggesting that reuse rates of enterprise servers and storage can vary from 31% up to 88% (Berwald et al., 2015). However, higher values can probably be related to best performances in the market and specifically for some types of contract, such as leasing of products (Berwald et al., 2015). On the other hand, few studies on servers considered that, although recycling and recovery rates are generally very high (up to 90%), reuse rate were very low or null (Fujitsu, 2010; Stutz, 2011).

These figures show that reuse of enterprise servers is a developed practise occurring in Europe, with rates largely higher than for other ICT. However, reuse rates are affected by a large variability, depending on the model of servers, type of commercial contract with the client, and the geographical area. It is also considered that reuse of servers has still a potential for improvement. Moreover, compared to the reuse performed by original manufacturers, reuse rates that are achievable by independent reuse operators are generally lower.

In order to identify the reasons concerning potential market failures for reuse, authors of this paper conducted in the last years several personal visits to facilities for the reuse and recycling of WEEE. It was observed that, compared to other ICT, EoL of enterprise servers and data storage have been characterised by some good practises in terms of take-back schemes and flows of reused devices. However, some important barriers to the reuse have also been identified during these visits, such as: data deletion issues in used equipment; limited accessibility to firmware updates, when reuse was conducted by operators other than the Original Equipment Manufacturers (OEMs); and insufficient design for disassembly of the equipment.

3.2.1. *Market failure on data privacy aspects in reused products*

Concerning data deletion issues, there are an increasing number of cases in the literature concerning personal data found in second hand components, like HDDs put back on the market (El Emam et al., 2007; The National Association for Information Destruction (NAID), 2017; Garfinkel and Shelat, 2003). These events are cause of serious concern to the data protection community, as they constitute events of personal data breaches, in case personal data could be recovered from the device. In these cases, the GDPR requires that the breach is notified to the competent authorities and, unless certain conditions are met, to the affected individuals. In this scenario, the Data Controller of the personal data (i.e., as from the GDPR, the person or public authority which determines the purposes and means of the processing of personal data) is responsible for the breach.

In the context of reuse of enterprise servers, reuse operators need to grant the deletion of personal data contained in WEEE before their further treatment. Data protection concerns, along with the lack of specific guidance and, as mentioned before, user empowerment, have led more customers to ask end-of-life operators to ensure that their devices have been (physically) destroyed after their first use in order to avoid the threat of any potential access to personal information. In other cases operators are specifically paid by their clients to certify the destruction of data bearing equipment (e.g. by the physical destruction of the equipment). Alternatively, when such request did not occur, operators developed specific procedures to grant the sanitization of data bearing equipment. This generally occurs by running dedicated data deletion software that is aligned to existing standards (as the

NIST standard 800-88, mentioned in Section 1.2), or by applying in-house developed methods.

The physical destruction of the data storage device is considered as "extreme" and is not specifically requested by Data Protection authorities, who also encourage other environmental friendly options, such as the reuse of the device. In this opinion on the Proposal for a Directive of the European Parliament and of the Council on WEEE (European Data Protection Supervisor (EDPS), 2010), the European Data Protection Supervisor (EDPS), aware of the risks, highlights the importance of considering the protection of the stored personal data in the reuse of equipment and advices that "Best Available Techniques" for privacy, data protection and security in this area should be developed. It is worth mentioning that the EU data protection regulatory framework emphasises a risk assessment based approach to the protection of personal data. Following this risk assessment approach, the proper sanitization of the storage media could in many cases suffice to ensure the proper erasure of personal data in the device.

From the above, it can be concluded that the (quite often) overcautious end-of-life practises for data storage devices are a case of market failure due to imperfect information.

3.2.2. *Market failure on cybersecurity aspects in reused products*

With respect to the cybersecurity dimension, software vulnerabilities continue to be one of the main factors that determine the security risk in digital services. The classical golden rule for mitigation of vulnerabilities is to keep the software updated. At a first sight, it might seem that, in the context of reuse, a complete reinstallation of the operating system and software utilities in the reused server with the latest updated versions would be an effective application of this rule. However, software installed in the hard-drive of the servers is not the only software that exists in a corporate server. The firmware that drives the operation of many of the components of the server, such as the Basic Input-Output System (BIOS), HDD or network cards, can also contain critical vulnerabilities that, if left unpatched, could be used by threat actors to compromise the server and the service infrastructure that it supports (see Section 1.2 for more information).

The application of security patches in the firmware in the form of firmware updates is the most effective way to combat this risk. The growing number of security vulnerabilities in firmware has started to raise concerns regarding the ability to apply security patches and updates in the firmware of reused devices. The unavailability of firmware updates for buyers of second hand equipment does not only impact their interoperability with other hardware and software, but also endangers the security of these devices and the digital services that they support.

The availability of firmware updates has been also highlighted by reuse operators as a crucial aspect for the reuse of servers. The benefit of getting new technologies to market is more valuable than the prospect of facing the risk of some bugs in the firmware, which can be finally fixed in an acceptable time when they will raise. This is why when an error occurs the OEM's labs are developing bug fixes to correct the flaws during the period they support the product. Up to 2010 it was usual for OEMs to make these fixes available for free to all end-users. This practise has become a standard in all industries, especially in the automotive industry. It is commonplace for a car manufacturer to recall vehicles to apply modifications for safety for instance. However, in the last decade OEMs decided to restrain the access to firmware updates for some ICT products only for the benefit of the end-users who were signing a maintenance agreement with them. This practise of restricted access to firmware can hinder the reusability of products as enterprise servers and data storage products. The difficulty for third parties dealing with maintenance, reuse and upgrading of enterprise servers and data storage products to access the market of reused and refurbished products is the reason for which the market failure concerning the (lack of) availability of firmware updates has been classified as concerning the "market power", by also taking into account that the enterprise servers and data storage products market is a highly concentrated one (e.g. in 2013, 78% of the market was covered by the top five international vendors (Berwald et al., 2015)).

Furthermore, the limited availability of firmware updates is generally related to ICT security issues, as discussed in Section 1.2.

3.2.3. *Market failure on disassembly operations and related privacy aspects*

Disassembly is intended as the "non-destructive taking apart of an assembled product into constituent materials and/or components" (British Standardisation Institute (BSI), 2009). Repair and EoL operators generally identified the "ease of disassembly" of WEEE as an essential prerequisite for their reuse. WEEE needs to be disassembled to permit their checking and to allow the repair and replacement of faulty and/or obsolete components. Barriers to disassembly have been observed mainly in household products (e.g. computers, tablets, and smartphones) and related to different aspects as: the use of welded or glued components; the use of several different fastening techniques (e.g. the used of several different screws and snap fits); the use of proprietary fastening systems (e.g. special screws that necessitate of special tools); and in general the low visibility or accessibility of certain fastening (e.g. screws that are covered by labels). Some disassembly difficulties have been also observed for enterprise servers, especially when their disassembly is performed by independent reuse operators, who do not know exactly the architecture of the server and the required disassembly procedures. That is why this market failure can be considered as a case of imperfect information. The ease of disassembly of servers relates to data privacy issues, since the extraction of data bearing components (e.g. HDDs and SSDs) is, in some cases, necessary to grant their proper sanitization or destruction.

3.3. *Conclusion on the need to conciliate market failures*

As analysed in the previous parts of this section, Table 1 summarizes the four market failures concerning the market of enterprise servers and data storage products, and stemming from the novel conjoint analysis of resource (energy and material) efficiency and data security and privacy aspects.

All these market failures seem to go against several fundamental European policy orientations on energy efficiency

Table 1 – The market failures stemming from the conjoint analysis of resource efficiency and data security and privacy aspects.

N	Issue	Type of market failure	Environmental impact aspects	Cybersecurity aspects
1	Higher operating temperature	Imperfect information	Energy efficiency	Reliability
2	Difficulties for data deletion	Imperfect information	Material efficiency-reuse – end of life	Data privacy
3	Availability of Firmware updates	Power market	Material efficiency-reuse	Data security
4	Difficulties in the disassembly	Imperfect information	Material efficiency-reuse – end of life	Data privacy

(European Commission (EC), 2015c), material efficiency (European Commission (EC), 2015a) and data protection (GDPR Regulation and Regulation (EU) 2016/679). Therefore our research aimed to identify and analyse, through an adapted and well-structured bottom-up approach, the potential policy options to solve these market failures.

4. Integration of resource efficiency, data privacy and security aspects into ecodesign of products

On the basis of the approach described in Section 2, we propose a novel formulation of potential Ecodesign requirements that could solve market failures as in Table 1. Table 2 lists those requirements which provide suitable legislative solutions to the challenges – highlighted in the form of market failures – emerged from the analysis in Section 3. Compared to the suggestions formulated in Berwald et al. (2015) to which the authors of this paper had previously contributed, the requirements presented here have been improved and sharpened following intense interactions with stakeholders since 2015.

Each requirement of Table 2 will be analysed in the remainder of this section. The first part (Sections 4.1 to 4.4) discusses the rationale and the feasibility of the requirements, as well as a qualitative discussion of potential benefits in terms of environmental, privacy, data protection and cybersecurity aspects. Finally, Section 4.5 provides a quantitative estimation of the expected environmental benefits stemming from the implementation of the potential requirements.

4.1. *Information on the product energy consumption and reliability at higher operating temperature*

The Ecodesign requirement consisting in the compulsory presence of information on the product energy consumption and reliability at higher operating temperature is expected to foster the increase, when feasible, of the operating temperature of data centres and server rooms. Based on existing literature (El-Sayed et al., 2012), it can be approximated that enterprise servers and data storage products are typically operated at temperature in the range of 20–22 °C as any systematic (i.e. not only due to temporally limited variations) temperature increase is seen as potentially problematic concerning reliability issues. Despite this, some big companies explicitly declare higher temperature values (up to 29.4 °C inlet temperature (Data Center Knowledge (DCK), 2016), proving that a proper thermal management of the data centre allows such solutions.

The Ecodesign requirement could consist of two reporting obligations: the first one the idle power consumption at high operating temperature, and the second one on the declared operating condition class, i.e. a temperature range in which the

Table 2 – Potential Ecodesign requirements to solve the market failures of Table 1.

Product requirement	Content and potential formulation	Rationale
1) Information on the consumption and reliability at higher operating temperature → *in reply to market failure 1*	Information on the idle state power consumption and the declared operating temperature range of the enterprise server at higher operating temperature shall be provided with the product	The compulsory presence of information on the idle state power consumption and the declared operating temperature range is expected to help solving the market failure related to the perceived lack of focus by customers on methods to decrease the overall energy consumption at data centre level (in particular by increasing, when feasible, the operating temperature)
2) Secure data deletion built-in function → *in reply to market failure 2*	Secure data deletion of potentially reusable data storage devices (i.e. HDDs, SSDs, memory cards) shall be ensured by providing a data deletion function with the product	The compulsory presence of a secure data deletion function is expected to boost the reuse rate of data storage devices and, overall, of whole enterprise servers and data storage products
3) Availability of firmware updates to reuse operators → *in reply to market failure 3*	The latest version of firmware for the enterprise server/data storage product shall be made available to third parties dealing with maintenance, reuse and upgrading of servers	The compulsory availability of the latest version of firmware is expected to facilitate third parties dealing with maintenance, reuse and upgrading of enterprise servers and data storage products to reuse and refurbish products with higher security levels
4) Design for disassembly of key components → *in reply to market failure 4*	The following types of components (when present) shall be identified, accessible and removable by hand or with commonly available tools: (a) HDDs and/or solid state devices (b) memory, (c) processor, (d) motherboard, (e) expansion cards/graphic cards, (g) power supply	The improvement of the design for the disassembly is expected to help solving the market failure related to the difficulties encountered in the disassembly by third parties dealing with maintenance, reuse and upgrading of servers

product (either an enterprise server or a data storage product) is expected to reliably perform its operations. Concerning the latter aspect, the temperature ranges classification of the ASHRAE guidelines for data centres (ASHRAE Technical Committee 9.9, 2015) could provide the necessary standard "language".

In terms of servers reliability, quantitative analyses (ASHRAE Technical Committee 9.9, 2015), performed by means of the "time weighted x-factor" (a parameter which represents the relative failure rate of a single server at a certain inlet temperature), show that there is not a significant increase in failure rate, even in unfavourable geographical locations[2]. Moreover, previous research (El-Sayed et al., 2012) proved that the effect of higher operating temperatures is smaller than often assumed, in particular because failure rates seem to be dominated by factors others than temperature, such as, in particular, poor handling procedures. For these reasons, it can be concluded that data centre equipment (not only servers, but also data storage products, networking and other equipment) are nowadays normally able to run under A1[3] conditions without any restrictions in terms of reliability. It is highlighted here that ensuring the reliability of the operations is an essential prerequisite to grant the security of the information from the perspective of server's customers.

4.2. *Secure data deletion built-in function*

The requirement on the availability of a built-in function for the secure erasure of data tackles directly the market failure that relates to the issue of sensitive and personal information in reused equipment. This requirement is aimed at facilitating the deployment of reuse practises and at empowering the customer and the Data Controller in taking the most appropriate decision regarding media sanitization, following a risk based approach. Literature shows that built-in functions for data sanitization offered in many storage devices (ATA and SCSCI standard) are capable of providing a fairly strong assurance in the process, suitable for many typical scenarios of risk.

The main impediment in the practical application of this approach seems to be the need to find compatible software to trigger the process. This is the reason why in the requirement of built-in function for secure erasure of data, the approach hereby presented is aimed at empowering the customer by mandating the existence of a ready-to-use function in the product that could drive the process.

It is expected that the reuse of enterprise servers and data storage products will increase if such secure data erasure function, capable of securely erasing all data with a selectable degree of assurance, is ready and can easily be used by customers for each equipment.

This secure data deletion function will also allow a boost for resource efficiency of enterprise servers and data storage. In particular, embedded options for secure data deletion will stimulate the decision towards erasure instead of destruction, so a progressive change in the aptitude of users and EoL operators is expected for a wider acceptance of product reuse.

4.3. *Availability of firmware updates to third parties*

According to servers reuse operators, the number of failures due to firmware issues, regardless of the technologies used by the manufacturers, is increasing within the last decades. Not performing firmware updates can result in slowing down or even stopping operations, with a potential loss of data. The restricted access to firmware updates has been identified by reuse operators as one of the major barrier to reuse servers. Practically, if firmware updates are not available the server is generally discarded even if potentially reusable, or alternatively, harvested for spare parts.

The requirement on the availability of firmware updates aims at enhancing the development of reuse practises by improving the compatibility and interoperability with components.

Moreover, firmware updates can also contribute to a global risk mitigation strategy based on securing the identification and development and deployment of security patches. The ability of devices contained in a corporate server to allow the deployment of firmware updates is crucial to achieve an effective mitigation of the security risk by enabling the deployment of security patches. Against this reasoning, it could be argued that, by doing so, the door might also be left open for third parties to abuse the update mechanism and deploy malicious code into the firmware (such as a firmware rootkit). Whilst conceptually correct, the benefits of enabling the possibility to update firmware to both tackle security flaws and enable new functionalities are far greater than the risks. As a matter of fact, experience in software updates for the operating system shows that the risk can be mitigated effectively by applying the right techniques such as the digital signature of the binary updates and subsequent validation during the updating process.

Our analysis concluded that, in order to promote the reuse of corporate server equipment, the reused server should be capable of providing equal level of protection against cybersecurity threats with the existing one before the reuse took place. By ensuring that any firmware update will also be available for reused equipment, customers can be reassured that, should a vulnerability be identified in the firmware of one of the components, the security update will not be made available to the original customers only.

4.4. *Design for disassembly of key components*

The objective of this requirement is to stimulate manufacturers to implement a "design for disassembly" of a selected list of components, including relevant data bearing components as HDD, SSD, memories and processors. Thanks to this requirement, operators (including repair and reuse centres) can access the selected components and disassemble the product for checking, repair and/or replacement.

This design allows benefits in terms of increased reusability and reparability of used enterprise servers, otherwise discarded and sent to recycling facilities.

[2] As an example, a town with a tropical climate such as Miami would have a time-weighted x-factor of 1,26, against the value 1 at the baseline temperature 20 °C.

[3] A1 is the first range of environmental classes for data centres (ASHRAE Technical Committee 9.9, 2015), and prescribes a recommended temperature range between 18 °C and 27 °C.

The requirement also allows a higher data security level, since data bearing components can be more easily accessed and disassembled for data deletion process, or for destruction, when specifically requested by the client. Also in this last case, components to be destroyed could be easily replaced by new ones, allowing the reuse of the remaining server's parts.

4.5. *Quantification of the potential environmental benefits*

The following sections provide a qualitative and, when possible, quantitative assessment of potential environmental benefits related to the proposed requirements.

4.5.1. *Benefits related to the operating conditions*

To estimate the savings deriving from the information requirements on higher operating temperatures, the analysis also included the survey of manufacturers and users on potential expected behaviours once these requirements would be in force, to understand how the market would react. More in detail, it has been hypothesized that, as an effect of the Ecodesign information requirements on the product energy consumption and reliability at higher operating temperature, a 30% of customers would actually adopt higher operating temperatures. Under this hypothesis, the effect (in terms of energy saving) stemming from these Ecodesign information requirements would account for more than 60% of the overall projected 9 TWh annual savings (European Commission (EC), 2017c), which makes these requirements of great importance, despite their informative (and not based on minimum threshold values) nature. More in detail, the expected annual energy savings should be of 5,7 TWh, which equates to a reduced Global Warming Potential (GWP) of 2000 thousands of tonnes (kt) of CO_2 equivalent.

4.5.2. *Benefits related to the improved reuse*

We provide quantitative estimations of potential benefits that can be achieved thanks to the proposed requirements for the only product group of enterprise servers. A similar analysis on data storage products was not possible due to the lack of specific data. In particular, we assumed that thanks to these requirements it would be possible to increase the amount of servers at EoL that can be reused instead. Improving the reuse rate of servers result in an extended useful service of the product, in a reduced need for raw materials, and also in a reduced amount of waste sent to treatments, with consequent reduction of material incinerated and landfilled and related harmful emissions.

Considering the various figures on reuse available in literature, as discussed in Section 3.2, the reuse rate of servers is largely variable and depends on the brand and/or the model of the server, on the type of commercial contract with the client and on the geographical area. Reuse rates of servers can vary from 20% up to 80%. Based on the qualitative analysis of potential benefits and based on the discussion with reuse and recycling operators, it is estimated that 1) the requirement on data deletion could increase the reuse rate by 2%–5%; 2) the requirement on firmware availability could increase the reuse rate by 5%–8%; 3) the requirement on design for disassembly could increase the reuse rate up to 2%, especially concerning the harvesting of servers for reusable spare parts.

The quantitative analysis of potential benefits was therefore focused on the estimation of the material savings and of the reduced environmental impacts. The former is quantified through the additional amount of material that remains in the economy thanks to reuse, instead of being discarded and being directed to EoL processes. The latter is estimated by means of the reduced GWP in the hypothesis that the production of new servers is avoided. The metrics used to assess such benefits were respectively: the mass (t) of materials per year, which is additionally reused instead of being recycled, incinerated or landfilled (with consequent and irreversible losses of materials); and the related reduction of GWP (t CO_2 equivalent) per year.

This quantitative assessment was developed building on recent studies on market trends and environmental analysis of enterprise servers, prepared respectively by Berwald et al. (2015) and Talens Peiró and Ardente (2015). Berwald et al. (2015) provided the figures for shipments in EU-28, over different years, indicating that the overall market is quite stable, with about 1.63 million units yearly shipped. Talens Peiró and Ardente (2015) provided a bill of materials for an average rack server with a mass of 23 kg (excluding packaging), as well as the results of a Life Cycle Assessment (LCA) study. Talens Peiró and Ardente (2015) quantified the GWP for the manufacturing of a case study server, being about 914 kg CO_2 equivalent per unit. Talens Peiró and Ardente (2015) also estimated the quantity of Critical Raw Materials (CRMs) contained in servers, such as neodymium, cobalt, silicon and palladium. CRMs are crucial to Europe's economy and essential to maintaining and improving our quality of life (European Commission (EC), 2014). Approximately 58 grams of CRMs are stored in each server, which means more than 90 t/year, when considering the overall amount of servers yearly sold in the EU-28.

Based on the analysis of Talens Peiró and Ardente (2015), servers that have a potential for reuse are can be diverted from waste flows and addressed to reuse operations. Remaining flows of waste are directed to recycling, with about 74.3% of the material recycled and the remaining 25.7% incinerated with energy recovery or landfilled. Thanks to the requirements proposed in Table 2, a number of improvement scenarios are established, in which the reuse rate of the enterprise servers is gradually increased compared to the current base-case scenario:

- Scenario A (precautious scenario): the reuse rate increases by 2%;
- Scenario B (balanced scenario): the reuse rate increases by 5%;
- Scenario C (medium-high scenario): the reuse rate increases by 8%;
- Scenario D (optimistic scenario): the reuse rate increases up to 15% (large boost achievable thanks to the synergic use of all the requirements).

Fig. 1 presents the variations of mass flows of servers at EoL in the EU-28, according to the increased reuse rate in different scenarios. Taking into account Scenario A, where the reuse rate increases by 2% compared to the base-case rate, an amount of about 753 tonnes of materials per year would be kept

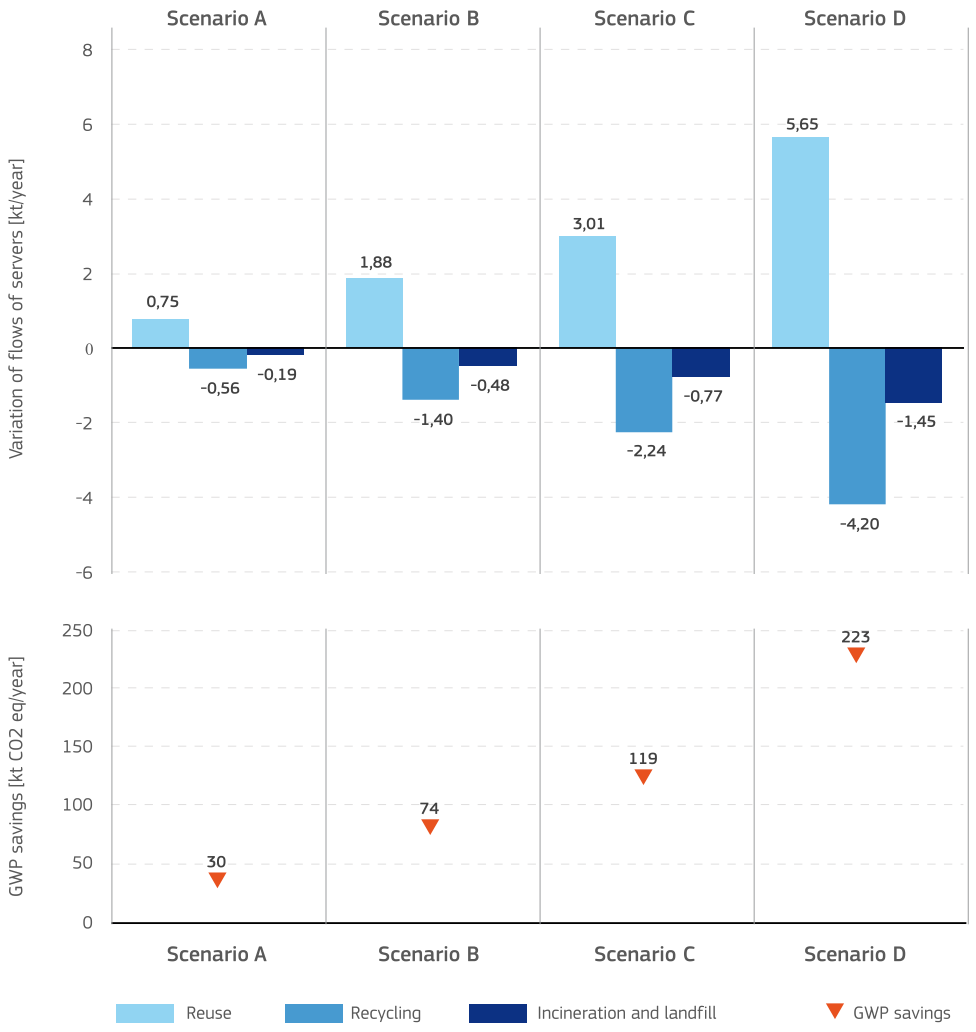

Fig. 1 – Variations of the flows of servers at end-of-life due to different scenarios on the reuse rate in the EU-28, and potential GWP savings (in thousands of tonnes (kt) of CO_2 equivalent per year) in different scenarios: A) increased reuse by 2%; B) increased reuse by 5%; C) increased reuse by 8%; D) increased reuse by 15%; (totals may not agree because of rounding).

functional in the economy instead of being recycled or disposed of. In Scenario D, this amount equals to about 5651 t/year. In other words, these quantities represent an improvement in terms of resource circularity since materials are used longer in the servers with the same function which they were designed for. Otherwise these materials would be processed through a recycling process that requires energy and resources, providing secondary raw materials (not necessarily of the same quality), but also with a significant loss of materials due to incineration and recycling.

In the hypothesis that a reused server delays the production of a new product, Fig. 1 also depicts the overall reduction in terms of GWP. The reduction is again additional, because referred to the base-case scenario. Therefore, the additional GWP reductions over the four scenarios range from 30 to 223 kt of CO_2 equivalent per year. These results take into account the manufacturing phase of new servers. Impacts of reuse operations (due e.g. to checking, repair, cleaning) have been estimated as 3.4 kg CO_2 equivalent per unit (Talens Peiró and Ardente, 2015). Nevertheless, calculation assumed that energy consumption during the service life would remain constant. Although not quantified here, environmental benefits of reuse could even be larger for other impact categories (e.g. concerning resource consumption) than they are for GWP.

This analysis shows that these environmental benefits brought by improved reuse, expressed as GWP savings, can be added to the avoided greenhouse gas emissions brought by energy efficiency measures, expressed in the same unit. This demonstrates the synergy that can be obtained when coupling resource efficiency and privacy, data protection and security.

5. Discussion

The research presented in this paper is a first attempt to connect resource efficiency aspects of products with privacy, data protection and cybersecurity issues taking a preventative (i.e. by design) focus. The research approach and the outcomes described in the previous sections are novel aspects

not only in the area of product policies but also in the scientific literature.

The research specifically focused on the European Ecodesign policy, which targets the development of requirements that all products in the market should comply with. However, more ambitious requirements (e.g. secure data deletion performed according to more stringent procedures; improved design solution for disassembly; free availability of firmware updates) could be part of voluntary policy schemes (e.g. the European Ecolabel (European Union (EU), 2010b) or Green Public Procurement (European Commission (EC), 2008), or voluntary agreements at industry level or, in general, other environmental and/or security labelling schemes. Hence, benefits presented in this paper for the product groups could even be greater in the future thanks to generalization and deepening of good design practises along all manufacturers.

The research presented in this paper is also affected by certain limitations. First of all, it was developed on a single case study, which could be considered as particularly successful but also not fully representative. Enterprise servers are indeed business-to-business products with already an established market for repair, reuse and data sanitization. Further applications, especially for business-to-consumers, could encounter different problems and obstacles.

The practical applicability of the identified requirements was also questioned by industrial stakeholders (Digital Europe (DiE), 2017), in particular because of the reuse of server being already largely occurring in European market. Moreover, specific criticisms were raised on the potential product requirements discussed previously, for example concerning the characteristics for the data deletion functionality, intellectual proprietary issues for firmware and the disclosure of information on the product to non-authorised personnel.

Concerning the built-in secure data deletion, different options could be in principle feasible to comply with the proposed requirement: the secure data deletion function could e.g. be installed in the BIOS (either the one of the motherboard or the one of the RAID controller, or both), in a bootable CD or DVD, in a software preinstalled in the operating system that comes with the server or in a software freely available from the manufacturer site. Moreover, data deletion could be customer specific. Manufacturers and customers could have different needs in terms of security of data. In this case, the proposed requirement (see Table 2) should be considered as granting a certain level of security for new products put into the market, whilst additional procedures or customized treatments could be still further performed. In specific high security circumstances, such as the financial, medical or military sectors, customers could still require the destruction of the data bearing components or of the whole product. Concerning the firmware updates availability, major concerns regarded that firmware development are related to intellectual property rights and often subject to contractual agreements. In some cases, manufacturers stipulate commercial contracts with the customers for the firmware provision, including also customized options. In this context, the availability of updates should be granted by manufacturers to third parties (especially independent reuse operators), although the possibility of having commercial agreements would not be excluded. Moreover, manufacturers are required to produce clear contracts on what firmware is legally owned by the consumer and is retained by the manufacturer. This distinction is necessary for third party repairers and consumers to stay properly informed of their ownership rights (New York State Senate (NY), 2017).

Concerning the design for disassembly of enterprise servers, it is recognized that a large part of the servers currently produced are already enhanced in this sense. Detailed information on disassembly is also provided by OEM to authorised repairers. However, not all the relevant information is available to independent professional repairers. The objective of the requirement is hence to avoid that certain products, which are difficult to be disassembled, could be introduced in future in the market. Furthermore, such requirement could particularly facilitate independent reuse and repair operators, which contributes to the circularity of the sector.

Concerning the potential Ecodesign requirement on the product operating temperature, the regulatory approach of this paper could positively affect the energy management of data centres and servers rooms, without entailing risks on the system reliability. According to the proposal under discussion, the approach would be not to allow enterprise servers and data storage products to be placed on the EU market only if they comply with minimum prescribed operating temperatures: the proposed requirement on the operating temperature is an information one, i.e. it would be compulsory to declare at which maximum temperature range the product can work (leaving freedom to the manufacturer to choose the temperature range). The proposed solution is, in authors' view, the best trade-off between the aim of solving the identified market failure and a precautionary approach towards the specificities of enterprise servers and data storage products market.

Concerning the reuse aspects, the assessments of potential benefits were mainly based on expert judgements by reuse and recycling operators, which can be affected by different sources of uncertainty as: a) the lack (or discordance) of information concerning the flows of servers currently reused in the EU-28; b) the variability of reuse rates due to, for example, the model of the server, brand, type of commercial contract with the client, and the geographical area; c) the uncertainty in defining future improvement scenarios. Moreover, the environmental assessment was mainly based on figures referred to a single case study. Overall, the assessment of reuse potentials expressed with the GWP indicator should be considered as an indicative estimation of the potential range of benefits that could be achieved for the product group. The additive nature of benefits (expressed as GWP savings) brought both by the increased energy efficiency and the reuse improvements demonstrates that energy efficiency, material efficiency, privacy and security issues can be coupled into effective and synergic policy measures.

Finally, it has to be noted that the requirements hereby discussed are still potential ones at the time of writing this paper. The finalisation of such process could entail some modification to the scope and the form of these requirements, in particular when taking into account key policy aspects such as the enforceability (by the relevant national market authorities) of a legislative measure. The work performed so far and the set of potential Ecodesign requirements envisaged in this

paper however represent, in the authors' view, a novel, suitable and robust proposal.

6. Conclusions and perspectives

This paper elaborates on the challenge of decreasing the environmental impacts of ICT products during their life cycle, whilst at the same time ensuring the privacy, data protection aspects and effective security of devices and infrastructure. It proposes an innovative analysis of the connections between resource efficiency and data protection and cybersecurity. Through the analysis of a case study, related to the implementation of the Ecodesign Directive to enterprise servers and data storage devices, it demonstrates that a synergic "win-win" approach between the environmental improvement and privacy, data protection and security can be achieved. The starting point of the analysis consisted in the identification of the market failures – i.e. situations in which the allocation of goods and services on a market is not efficient. Market failures affecting the market of enterprise servers and data storage devices have been identified. Subsequently, four areas of improvement were identified: 1) (need of) improved information on the product energy consumption and reliability at higher operating temperature; 2) (need of) improved information on data deletion practises; 3) (need of) improved market structure to allow firmware updates by third parties dealing with maintenance, reuse and upgrading; and 4) (need of) improved design for disassembly of the products. The analysis led to a novel formulation of four requirements, potentially applicable in the context of ecodesign policies: a) provision of compulsory information on product performance and consumption at high operating temperatures, b) compulsory presence in products of a built-in secure data deletion function to support the secure deletion of data, c) availability of latest version of firmware for third parties (other than OEMs) and d) compulsory design for disassembly of certain components (such as HDDs and/or SSDs, memory, processor, etc.), and the provision of relevant information on the disassembly. These requirements have still to be considered as proposals, since the policy process and the debate with stakeholders are still on-going.

The article also presented some qualitative and quantitative assessments of benefits that can be brought by these proposed Ecodesign requirements, from energy/material efficiency but also security/data protection perspectives. The expected savings from the product performance and consumption at high operating temperatures have been estimated in the order of 5,7 TWh per year (equivalent to 2000 kt of CO_2 equivalent), whereas the three material efficiency requirements (data deletion function, availability of latest version of firmware and design for disassembly) would prevent around 1900–3000 t/y of materials to be wasted and they would save around 75–120 kt of CO_2 equivalent per year (under some average scenarios). Benefits brought by the energy efficiency and the material efficiency requirements can hence be cumulated.

The presence of a secure data deletion function also contributes to protect the personal data when the product reaches the end of the operation and, overall, it will make customers keener in allowing used servers and data storage products for refurbishing. The availability of firmware updates allows repair/reuse operators to run the upgrading and to test the functionality and compatibility of different components when performing refurbishing operations. Moreover, the availability of updated versions of the firmware will facilitate the effective distribution and application of security patches to vulnerabilities that might have been identified in the original firmware. This research also concluded that policy measures initially conceived in an environmental protection context can be enhanced to purse in synergy also data protection objectives. Promoting resource efficient devices through policies can be even an incentive to ensure data protection and cybersecurity.

It is worth to mention that, although the research focused on a specific case study, analogous considerations and research could be applied to other product groups characterised by similar market failures, as for example computers, tablets and smartphones. Our research intended also to anticipate such risks and propose ICT specific measures that could be implemented in future in a large set of appliances, including large household appliances such as washing machines and fridges. This would become more and more critical with the expected growing of the IoT. Having a built-in function for the deletion of personal data in wearable, mobile and smart home devices, EoL operations would be facilitated in their task and helped in being in line with law requirements.

Finally, the article represents a first concrete experience of the "privacy and data protection by design" concept, i.e. taking into account data protection and cybersecurity aspects already at the design stage of the product. The discussion around the potential requirements contains relevant recommendations on how to improve the data protection and cybersecurity by a better design of the product. In a market more and more oriented towards the IoT, product recommendations here discussed could be extended to several other products, helping to proactively prevent and tackle cybersecurity risks that our society could face in the close future.

Disclaimer

The views expressed in the article are personal and do not necessarily reflect an official position of the European Commission. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use, which may be made of the information contained therein.

Acknowledgement

The authors would like to thank Igor Nai-Fovino for the feedback provided on the manuscript.

REFERENCES

Alcaide A, Palomar E, Montero-Castillo J, Ribagorda A. Anonymous authentication for privacy-preserving IoT target-driven applications. Comput Secur 2013;37:111–23.

Alherbawi N, Shukur Z, Sulaiman R. Systematic literature review on data carving. digital forensic. Procedia Tech 2013;11(Iceei): 86–92.
Allenby B. Design for environment: a tool whose time has come. SSA J 1991;5–10.
Ang C, Costello M, Stolfo SJ. When Firmware Modifications Attack: A Case Study of Embedded Exploitation. NDSS; 2013.
Ardente F, Mathieux F. Identification and assessment of product's measures to improve resource efficiency: the case-study of an energy using product. J Clean Prod 2014a;83:126–41.
Ardente F, Mathieux F. Environmental assessment of the durability of energy-using products: method and application. J Clean Prod 2014b;74:62–73.
Ardente F, Beccali G, Cellura M. Eco-sustainable energy and environmental strategies in design for recycling: the software "ENDLESS". Ecol Modell 2003;163(1–2):101–18.
Ardente F, Mathieux F, Recchioni M. Recycling of electronic displays: analysis of pre-processing and potential ecodesign improvements. Resour Conserv Recycl 2014;92:158–71.
Ashley S. Designing for the environment. Mech Eng 1993;115(3):53–5.
ASHRAE Technical Committee 9.9. Thermal Guidelines for Data Processing Environments, Fourth Edition; 2015.
Berwald A, Faninger T, Bayramoglu S, Tinetti B, Mudgal S, Stobbe L, et al., Ecodesign Preparatory Study on Enterprise Servers and Data Equipment, Luxembourg; 2015, doi:10.2873/14639.
Bobba S, Ardente F, Mathieux F. Environmental and economic assessment of durability of energy-using products: method and application to a case-study vacuum cleaner. J Clean Prod 2016;137:762–76.
Brezet JC, van Hemel CG. Ecodesign. A Promising Approach to Sustainable Production and Consumption. United Nations Publication, UNEP;1997.
British Standardisation Institute (BSI). Standard BS 8887-2 – Design for manufacture, assembly, disassembly and end-of-life processing (MADE). Terms and definitions. 2009.
Bukarica V, Tomšić Z. Energy efficiency policy evaluation by moving from techno-economic towards whole society perspective on energy efficiency market. Renew Sustain Energy Rev 2017;70:968–75.
Bundgaard AM, Mosgaard MA, Remmen A. From energy efficiency towards resource efficiency within the ecodesign directive. J Clean Prod 2017;144:358–74.
Burghardt A, Feldman AJ, Hamilton BA, States U. Using the HFS D. Journal for deleted file recovery, 2008, 5.
Castiglione A, Cattaneo G, Cembalo M, De Santis A, Faruolo P, Petagna F, et al. Engineering a secure mobile messaging framework. Comput Secur 2012;31(6):771–81.
CENELEC. prEN50614. Requirements for the preparing for re-use of waste electrical and electronic equipment. Version; 2016. Available from: https://www.cenelec.eu/dyn/www/f?p=104:110:166511065401301::::FSP_ORG_ID,FSP_PROJECT,FSP_LANG_ID:1258637,58426,25. [Accessed 17 July 2017].
Chifor B, Bica I, Patriciu V, Pop F. A security authorization scheme for smart home Internet of Things devices. Future Gener Comput Syst 2017;doi:10.1016/j.future.2017.05.048.
Costin A, Zaddach J, Francillon A, Balzarotti D. A Large-Scale Analysis of the Security of Embedded Firmwares. USENIX Security Symposium. August 20–22, 2014, San Diego, CA; 2014.
Dalhammar C. Promoting energy and resource efficiency though the ecodesign directive. Scand Stud Law 2014;59:147–79.
Dalhammar C. Industry attitudes towards ecodesign standards for improved resource efficiency. J Cleaner Prod 2016;123:155–66.
Data Center Knowledge (DCK). The Facebook Data Center FAQ (Page 4); 2016. Available from: http://www.datacenterknowledge.com/the-facebook-data-center-faq-newest-page/. [Accessed 20 July 2017].
Dennis K. The compatibility of economic theory and proactive energy efficiency policy. Electr J 2006;19:58–73.
Digital Europe (DiE). Key industry proposals on ErP Lot 9 draft regulation on enterprise servers and storage; 2017. Available from: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2375&language=en-US&PortalId=0&TabId=353. [Accessed 17 July 2017].
El Emam K, Neri E, Jonker E. An evaluation of personal health information remnants in second-hand personal computer disk drives. J Med Internet Res 2007;9(3):e24.
El-Sayed N, Stefanovici I, Amvrosiadis G, Hwang AA, Schroeder B. Temperature management in data centres: why some (might) like it hot. Proceedings of the 12th ACM SIGMETRICS/PERFORMANCE joint international conference on Measurement and Modeling of Computer Systems, pp 163–174; 2012. doi:10.1145/2254756.2254778.
European Commission (EC). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Public procurement for a better environment, COM/2008/0400 final; 2008.
European Commission (EC). M/518 Mandate to the European standardisation organisations for standardisation in the field of Waste Electrical and Electronic Equipment; 2012a. Available from: http://ec.europa.eu/environment/waste/weee/pdf/m518%20EN.pdf [Accessed 17 July 2017].
European Commission (EC). Commission staff working document: Establishment of the Working Plan 2012–2014 under the Ecodesign Directive, SWD (2012) 434 final; 2012b.
European Commission (EC). Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. JOIN(2013) 1 final; 2013.
European Commission (EC). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the review of the list of critical raw materials for the EU and the implementation of the Raw Materials Initiative. COM(2014)0297 final; 2014.
European Commission (EC). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Closing the loop – An EU action plan for the Circular Economy, COM/2015/0614 final; 2015a.
European Commission (EC). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. COM(2015) 192 final; 2015b.
European Commission (EC). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee, the Committee of the Regions and the European Investment Bank. A framework strategy for a resilient energy union with a forward-looking climate change policy. COM(2015)080 final; 2015c.
European Commission (EC). Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. JOIN(2017) 450 final; 2017a.
European Commission (EC). EU cybersecurity initiatives: working towards a more secure online environment; 2017b. Available from: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity. [Accessed 30 July 2017].
European Commission (EC). Environmental impact of enterprise servers and data storage products. Ares(2017)3069227; 2017c.

Available from: https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3069227_en. [Accessed 21 December 2017].
European Data Protection Supervisor (EDPS). Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE). EC Official Journal; 2010. Available from: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A52010XX1016(02). [Accessed 17 July 2017].
European Union (EU). Directive 2008/98/EC of the European Parliament and of the Council of 19 November 2008 on waste and repealing certain Directives. Off J Eur Union 2008.
European Union (EU). Directive 2009/125/EC of the European Parliament and of the Council of 21 October 2009 establishing a framework for the setting of ecodesign requirements for energy-related products, OJ L 285, 31.10.2009, p. 10–35; 2009a.
European Union (EU). Commission Regulation (EC) No 642/2009 of 22 July 2009 implementing Directive 2005/32/EC of the European Parliament and of the Council with regard to ecodesign requirements for televisions, OJ L 191, 23.7.2009, p. 42–52; 2009b.
European Union (EU). Directive 2010/30/EU of the European Parliament and of the Council of 19 May 2010 on the indication by labelling and standard product information of the consumption of energy and other resources by energy-related products, OJ L 153, 18.6.2010, p. 1–12; 2010a.
European Union (EU). Regulation (EC) No 66/2010 of the European Parliament and of the Council of 25 November 2009 on the EU Ecolabel (Text with EEA relevance), OJ L 27, 30.1.2010, p. 1–19; 2010b.
European Union (EU). Commission Regulation (EU) No 617/2013 of 26 June 2013 implementing Directive 2009/125/EC of the European Parliament and of the Council with regard to ecodesign requirements for computers and computer servers, OJ L 175, 27.6.2013, p. 13–33; 2013.
European Union (EU). Regulation (EC) No 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 (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88; 2016a.
European Union (EU). Directive 2016/1148/EU of the European Parliament and of the Council of 6 July concerning measures for a high common level of security of network and information systems across the Union (NIS Directive), OJ L 194, 19.7.2016, p. 1–30; 2016b.
Eurostat. Statistics on Waste Electrical and Electronic Equipment (WEEE) in 2014; 2014. Available from: http://ec.europa.eu/eurostat/web/waste/key-waste-streams/weee. [Accessed 17 July 2017].
Fujitsu. White paper. Life cycle assessment and product carbon footprint. PRIMERGY TX 300 S5 and PRIMERGY RX 300 S5 server: 1–6; 2010. Available from: http://fujitsu.fleishmaneurope.de/wp-content/uploads/2010/12/Whitepaper-LCA-PCF-ESPRIMO-E9900.pdf. [Accessed 17 July 2017].
Garfinkel SL, McCarrin M. Hash-based carving: searching media for complete files and file fragments with sector hashing and hashdb. Digit Investig 2015;14:95–105.
Garfinkel SL, Shelat A. Remembrance of data passed: a study of disk sanitization practices. IEEE Secur Priv 2003;17–27.
Gorobets M, Bazhaniuk O, Matrosov A, Furtak A, Bulygin Y. Attacking hypervisors via firmware and hardware. Blackhat USA 2015; 2015. Available from: http://www.c7zero.info/stuff/AttackingHypervisorsViaFirmware_bhusa15_dc23.pdf. [Accessed 8 January 2018].
Graedel TE, Allenby BR. Industrial ecology. Englewood Cliffs, New Jersey: Prentice Hall; 1995.
Guo H, Mu Y, Li Z, Zhang X. An efficient and non-interactive hierarchical key agreement protocol. Comput Secur 2011;30(1):28–34.
Gutmann P. Secure Deletion of Data from Magnetic and Solid-State Memory. In: Proceedings of the Sixth USENIX Security Symposium, San Jose, CA, July 22–25, pp. 77–90; 1996.
Hassanzadeh A, Stoleru R. On the optimality of cooperative intrusion detection for resource constrained wireless networks. Comput Secur 2013;34:16–35.
Hassanzadeh A, Xu Z, Stoleru R, Gu G, Polychronakis M. PRIDE: a practical intrusion detection system for resource constrained wireless mesh networks. Comput Secur 2016;62:114–32.
Hinchliffe D, Akkerman F. Assessing the review process of EU Ecodesign regulations. J Clean Prod 2017;article in press.
Hughes GF, Coughlin T, Commins DM. Disposal of disk and tape data by secure sanitization. IEEE Secur Priv 2009;7(4):29–34.
Hustinx P. Privacy by design: delivering the promises. Identity Inf Soc 2010;3(2):253–5.
Intel. About the Intel Manageability Firmware Critical Vulnerability; 2017. Available from: https://www.intel.com/content/www/us/en/architecture-and-technology/intel-amt-vulnerability-announcement.html. [Accessed 17 July 2017].
Kissel R, Regenscheid A, Scholl M, Stine K. NIST special publication 800-88 revision 1 guidelines for media sanitization. U.S. Department of Commerce; 2014.
Kumar A, Zeadally S, Wazid M. Lightweight authentication protocols for wearable devices. Comput Electr Eng 2017;63:196–208.
Lindahl M, Sundin E, Östlin J. Environmental issues with the remanufacturing industry. Proceedings of the 13th CIRP international conference on Life Cycle Engineering, 31st May – 2nd June 2006 Leuven, Belgium, 447–452; 2006.
Lopez J, Alcaraz C, Roman R. Smart control of operational threats in control substations. Comput Secur 2013;38:14–27.
Makri E, Konstantinou E. Constant round group key agreement protocols: a comparative study. Comput Secur 2011;30(8):643–78.
Nazir S, Patel S, Patel D. Assessing and augmenting SCADA cyber security: a survey of techniques. Comput Secur 2017;70:436–54.
New York State Senate (NY). Senate Bill S618B on the sale of certain diagnostic and repair information systems; 2017. Available from: https://www.nysenate.gov/legislation/bills/2017/s618/amendment/b [Accessed 17 July 2017].
Oracevic A, Akbas S, Ozdemir S. Secure and reliable object tracking in wireless sensor networks. Comput Secur 2017;70:307–18.
Polverini D, Tosoratti P. A Regulatory Approach for Potential Energy Efficiency Requirements on Computer Servers, Electronics Goes Green 2016+, ISBN 978-3-00-053763-9; 2016.
re-tek. Reuse and recycling of enterprise servers. Private communication; 2015.
Rao U, Nayak U. Malicious software and anti-virus software. The InfoSec handbook. Apress; 2014. p. 141–61.
Razaque A, Rizvi SS. Secure data aggregation using access control and authentication for wireless sensor networks. Comput Secur 2017;70:532–45.
Sacco A, Ortega A. Persistent BIOS infection. CanSecWest Applied Security Conference; 2009.
Skorobogatov S, Woods C. Breakthrough silicon scanning discovers backdoor in military chip. International workshop on cryptographic hardware and embedded systems. Berlin, Heidelberg: Springer; 2012.
Stutz M. Carbon footprint of a typical rack server from Dell: 4; 2011 Available from: i.dell.com/sites/content/corporate/corp-comm/en/Documents/dell-server-carbon-footprint-whitepaper.pdf. [Accessed 17 July 2017].

Talens Peiró L, Ardente F. Environmental footprint and material efficiency support for product policy – analysis of material efficiency requirements of enterprise servers. Publications Office of the European Union; 2015 doi:10.2788/409022.
Talens Peiró L, Ardente F, Mathieux F. Design for Disassembly Criteria in EU Product Policies for a More Circular Economy. A Method for Analyzing Battery Packs in PC-Tablets and Subnotebooks. J Ind Ecol J Clean Prod 2017;21(3):731–41.
Tecchio P, McAlister C, Mathieux F, Ardente F. In search of standards to support circularity in product policies: a systematic approach. J Clean Prod 2017;168:1533–46. https://doi.org/10.1016/j.jclepro.2017.05.198.
The National Association for Information Destruction (NAID). Report: Personally Identifiable Information Found on 40 Percent of Used Devices in Largest Study To-Date; 2017. Available from: http://www.naidonline.org/nitl/en/consumer/news/5845.html. [Accessed 17 July 2017].
Theoharidou M, Kotzanikolaou P, Gritzalis D. A multi-layer criticality assessment methodology based on interdependencies. Comput Secur 2010;29(6):643–58.
Trentesaux D, Borangiu T, Thomas A. Emerging ICT concepts for smart, safe and sustainable industrial systems. Comput Ind 2016;81:1–10.
von Solms B, von Solms R. The 10 deadly sins of information security management. Comput Secur 2004;23(5):371–6.
von Solms R, van Niekerk J. From information security to cyber security. Comput Secur 2013;38:97–102.
Vermani S. Internet of things: security & privacy threats. Int J Recent Sci Res 2016;7(5):11403–6.
Virvilis N, Mylonasa A, Tsalis N, Gritzalis D. Security busters: web browser security vs. rogue sites. Comput Secur 2015;52:90–105.
Wei M, Grupp LM, Spada FE, Swanson S. Reliably erasing data from flash-based solid state drives. FAST 2011;11.
Wright C, Kleiman D, Sundhar RSS. Overwriting hard drive data: the great wiping controversy. Inf Syst Secur 2008;243–57.
Zaddach J, Kurmus A, Balzarotti D, Blass EO, Francillon A, Goodspeed T, et al. Implementation and implications of a stealth hard-drive backdoor. Proceedings of the 29th annual computer security applications conference. ACM; 2013.
Zhou Z, Fan J, Zhang N, Xu R. Advance and Development of Computer Firmware Security Research, 2(1); 2009.
Zonouz S, Houmansadr A, Berthier R, Borisov N, Sanders W. Secloud: a cloud-based comprehensive and lightweight security solution for smartphones. Comput Secur 2013;37:215–27.

Davide Polverini is a policy officer in the European Commission Directorate General DG Internal Market, Industry, Entrepreneurship and SMEs since 2012, in charge of the implementation of the Ecodesign Directive 2009/125/EC; among others, he is the responsible for the work on computer servers. Davide graduated in Materials Engineering, and holds a PhD in Mechanical Engineering focused on design and industrial engineering methods for innovation on industrial products. His professional experience is in the fields of industry (seven years in the R&D area of the domestic appliances sector) and of photovoltaics (two years at the Joint Research Centre as a scientific officer).

Fulvio Ardente is PhD in Environmental Applied Physics with a dissertation on the application of Life Cycle Assessment (LCA) to renewable energy sources. He was contract professor at the University of Palermo and lecturer of the course on renewable energy sources and environmental sustainability. Since 2010 he is working at the European Commission – DG Join Research Centre (JRC) researching on Ecodesign of energy related products, modeling of resource efficiency of products (durability, reusability, recyclability) and circular economy strategies for resource savings and secondary raw materials production.

Ignacio Sanchez is a European Commission Official at the Joint Research Centre. He works in the Cyber and Digital Citizen Security Unit, within Directorate E on Space, Security and Migration, where he leads several lines of research in the fields of cybersecurity, privacy, data protection and fight against cybercrime. Ignacio holds a PhD and an MSc in computer engineering and has a background of 15 years of experience in the field of information security.

Fabrice Mathieux is research staff in the JRC. He works on resource efficiency and circularity assessment methods and underlying data applied to materials/products/systems, and on their use for policy making (e.g. concerning raw materials, resource efficiency, and circular economy). Fabrice graduated in Mechanical engineering and holds a Master Degree in waste Management and Life Cycle Assessment. His Industrial Engineering PhD Thesis concerned design for recycling of electr(on)ics. Before joining the European Commission, he led research in various universities in France and beyond (e.g. UK, Fiji islands).

Paolo Tecchio holds a Master Degree in Energy Engineering and a PhD in Materials Science and Technology. He worked as LCA expert and as a research fellow at the Politecnico di Torino (Italy), at the Institut National des Sciences Appliquées de Lyon (France) and at the Massachusetts Institute of Technology (USA). At JRC since 2015, he is working on resource efficiency assessments, in support of policies for raw materials and circular economy.

Laurent Beslay is a European Commission Official at Joint Research Centre, within the Directorate on Space, Security and Migration and works as Scientific Project Leader on Law enforcement technologies. He manages research activities on cybercrime and organized crime, biometric systems and privacy safeguards. From 2004 to 2011, he was Coordinator on Security and Technology and scientific advisor of the European Data Protection Supervisor. He previously worked, for six years, for the JRC - Institute for Prospective Technological Studies as a PhD candidate (Electronic surveillance: benefits and risks for the EU) and as a project officer in the field of cybersecurity.