Privacy matters: issues within mechatronics

Watt, Steve
Milne, Chris
Bradley, David
Russell, David
Hehenberger, Peter
Azorin-Lopez, Jorge

This is the accepted manuscript © 2016, IFAC (International Federation of Automatic Control)

The published article is available from doi:
10.1016/j.ifacol.2016.10.641
Privacy Matters – Issues within Mechatronics

Steve Watt*, Chris Milne*, David Bradley**, David Russell***, Peter Hehenberger****
Jorge Azorin-Lopez*****

* University of St Andrews, St Andrews, Fife, KY16 9AJ, UK (email: ciso@st-andrews.ac.uk & c.milne@st-andrews.ac.uk)
** Abertay University, Dundee DD1 1HG, UK (email: dbonipad@gmail.com)
*** Penn State Great Valley, Malvern, PA 19355, USA (email: drussell@psu.edu)
**** Institute of Mechatronic Design and Production, Johannes Kepler University, Linz, Austria
(email: peter.hehenberger@jku.at)
***** Computer Technology Department, University of Alicante, Alicante, Spain
(email: jazorin@dtic.ua.es)

Abstract: As mechatronic devices and components become increasingly integrated with and within wider systems concepts such as Cyber-Physical Systems and the Internet of Things, designer engineers are faced with new sets of challenges in areas such as privacy. The paper looks at the current, and potential future, issues associated with privacy legislation, regulations and standards and considers how these are likely to impact on the way in which mechatronics is perceived and viewed. The emphasis is not therefore on technical issues, though these are brought into consideration where relevant, but on the soft, or human centred, issues associated with achieving user privacy.

Keywords: Privacy, Users, Big Data, Security, Mechatronics, Cyber-Physical Systems, Internet of Things.

1. INTRODUCTION

While at its fundamental level mechatronics remains a need to reinforce privacy issues through a combination of structured around the integration of the core technologies of legislation, regulation and standards, including in the US the mechanical engineering, electronics and information potential for a “Privacy Bill of Rights”. The introduction of technology, the nature of the systems within which such legislation will impact upon the design processes for mechatronic components and devices and their use in association with Cyber-Physical Systems and the Internet of Things, and hence on the relationships with system users.

Additionally, many of the resulting participatory systems, structured along the lines of Fig. 2, are associated with aspects of data collection, often involving personal or user data, and with the creation of larger data sets resulting from the aggregation of data from and across multiple users. This aggregation of data then has implications for the privacy and security of both individual users and aggregated users across all data collected [Patton 2014; Borgohain 2015; van der Sloot 2014].

To date, emphasis in relation to the safeguarding of personal data has largely been on the ‘hard’ aspects of system security and less on the ‘soft’ issues associated with the privacy of individual users. However, recent studies, as for instance by the US Government [Executive Office 2015], have suggested

![Fig. 1. Increasing abstraction from Mechatronics to Cyber-Physical Systems and the Internet of Things.](image1)

![Fig. 2. A participatory system.](image2)
Drawing on research by the authors in areas such as engineering design, smart systems; including smart homes, domotics and smart grids, eHealth and manufacturing as well as experience in managing the day-to-day operation of large information systems and in engineering education, the paper also considers how privacy issues can be translated into future, user-oriented, systems.

2. MECHATRONICS, CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS

Referring again to Fig. 1, within the context of the paper the relationship between mechatronics components and devices, Cyber-Physical systems and the Internet of Things may be summarised as follows:

**Mechatronics** Smart components and devices characterised by an integration of technologies and a transfer of functionality from the mechanical to the electronics and software domains. In illustration, many vehicle systems from drive train management to environmental control can be considered as essentially mechatronic in nature.

**Cyber-Physical Systems (CPS)** These are formed by an aggregation mechatronic (or other) components through the medium of a smart network supported by and associated with intelligent software to manage the contribution of the individual components to the CPS, and to the CPS in its entirety. Thus, a vehicle could be considered as a CPS structured around an aggregation and assembly of mechatronic components and devices [Shi 2011].

**Internet of Things (IoT)** The IoT provides access to information, context dependant and otherwise, as well as sourcing a range of software, platforms and infrastructure services and functions. In many cases, these will be sourced on demand without necessarily any a priori knowledge as to their origins or structure.

Thus, individual vehicles may communicate with each other to establish traffic flows and determine optimum routing as well as with other systems and agencies, for instance to adjust home based environmental control systems based on estimated arrival times.

3. SECURITY v PRIVACY

Though issues of security and privacy are closely linked, and indeed sometimes seem to be considered as the same, in the context of the paper, security is considered as being conventionally associated with those ‘hard’ elements such as encryption and firewalls which are intended to protect against intrusion while privacy deals with the ‘soft’, or people oriented issues such as the ownership of data and its use. That implies that there is a synergistic relation between security and privacy in which the relationship may well be determined by function.

Consider the instance of the integrated vehicle systems outlined in Section 2. Here, the autonomous flow of data between individual vehicles and, say, a home system can support enhanced traffic management resulting in reduced energy consumption (and of associated CO₂ levels), but also has the potential to provide information at the level of the individual which could, for instance, be used to indicate whether a house is currently occupied.

A shift in emphasis at the level of the individual towards privacy as opposed to security implies that the emphasis of the associated protocols also moves away from providing a hard, or impenetrable, security boundary, to more function based strategies to ensure privacy. In that context, the interest in using techniques such as the blockchain database structures [BBC News 2016; Sweeney 2002; Harrison 2015] is potentially of significance.

Perhaps therefore it is no coincidence that the annual World Economic Forum Risk Report [WEF 2016] has consistently over a period of over 10 years identified cyber security and associated factors such as privacy of the individual as a major, and high impact, risk area.

3.1 The Role of Big Data

The term big data is generally applied to large and complex data sets for which conventional data processing methods and techniques are inadequate. Such sets are often structured around personal data, as for instance health related data, and can be added to, often at the moment without the knowledge of the individual using the device, by devices such as those used to measure exercise levels. The following provides some indication of the types of data sets, and the numbers, involved.

- A study suggests by McKinsey suggests that retailers who fully leverage big data could see an increase in operating margins of as much as 60% [Court 2015].
- IDC1 estimate that in 2015 Financial Services worldwide spent $114 billion on mobility, cloud, Big Data & analytics [IDC 2015].
- Forbes suggest that the Advanced and Predictive Analytics (APA) software market is likely to grow from $2.2 billion in 2013 to $3.4 billion in 2018 [Columbus 2014].

The analysis of such data sets has resulted in the evolution of methods such as predictive analytics, knowledge discovery and data mining as a means of extracting information, and hence knowledge, from such data. However, the ability to extract such knowledge also carries with it privacy implications for those individuals whose data is incorporated into the overall data set [Ekbia 2015; Kambatla 2014].

In recognition of this potential conflict between the individual and the potential use of Big Data, in the US, the President’s Council of Advisors on Science and Technology (PCAST)  

---

1 International Data Corporation
produced a report in 2014 dealing with issues of individual privacy in relation to the growth of Big Data [PCAST 2014]. This report concluded that:

- Encryption is not a perfect solution for securing data, it is however a valuable component of a comprehensive privacy strategy.
- Third parties would create privacy profiles for consumers who would then select their profile such that data holders would be required to differentiate data use between users based on the user’s adopted privacy profile.
- Anonymisation and de-identification have limited relevance as linked data points tend to take on other identifiable attributes.
- Deletion and non-retention policies are not effective means of protecting individual privacy.

It went on to recommended that:

- Concentration should be on data use rather than collection and analysis.
- Policies and regulations should be expressed in terms of intended outcomes and not technological solutions.
- Research into privacy technologies should be strengthened.
- There is a need for more education and training in the area of privacy protection.
- There is a need for policies that stimulate the introduction of practical privacy protection policies.

When taken together with other analysis of the links between the Internet of Things and Big Data as established above, a number of issues can be identified (FTC 2013), including:

- It is no longer adequate to rely on hard methods such as technology and encryption to protect privacy.
- It is the responsibility of everyone involved in the data chain to manage and ensure privacy.
- In protecting privacy, the use to which the data is to be put is more significant than its collection and analysis.
- Education and training have important roles to play in increasing awareness of privacy issues and solutions at all levels from design to implementation.

Referring to Figs 1 and 2 it is suggested that the role of mechatronics within the general context of Big Data is most usually associated with the collection and onward transmission of source data. Thus by applying the structures outlined in Section 2, a mechatronic device within the home such as washing machine can be connected as part of a smart network within the home, a configuration which might of itself be considered as constituting the home as a basic Cyber-Physical System, which then forms part of a smart grid or cluster formed by and involving a number of such homes.

This cluster then communicates with utilities, transport hubs and other wider networks and systems through the medium of the Internet of Things.

At each stage of this process, user specific data can be gathered and integrated with other, similar, data from other users. Thus the mechatronic system is in many instances functioning as a data source for the wider networks, which in turn has implications for both component and system operation and design to ensure the privacy of the user(s).

4. PRIVACY CONSIDERATIONS


Article 5 of the latter requires that public communications providers such as Internet Service Providers and telecoms companies are required to take technical and organisational measures to:

“ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services.”

Article 6 then requires that providers of Web services that transfer messages from Web servers to Web browsers via text files (cookies) must inform users that these are being used, describe their use and secure consent before a cookie can be stored on a user’s device.

As those legislative provisions play a lesser role in privacy protection in comparison with the EU Privacy Directive, assessment of the legislative frameworks to protect privacy in the development and use of the IoT focuses on the EU Privacy Directive, and the forthcoming Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU Data Protection Regulation) [COM(2012) 11 Final].

Though these are European regulations, their reach is not restricted to the geographical boundaries of the EU and device manufacturers based outside the EU will fall within the scope of the directive when their devices are used for the processing of personal data within the EU. Thus, a US manufacturer who produces a fitness monitoring device such as a pedometer which then transmits data relating to the device owner to a social media feed will, when the device is used within the EU, fall within the scope of the legislation.

Indeed, EU Data Protection Regulation provides specific provision in Article 23 that:

“[Privacy by design] give incentives to [data] controllers [organisations that decide how an individuals’ personal information are to be used] to invest, from the start, in getting data protection right (such as data protection impact assessments, data protection by design and data protection by default). The proposals place clear responsibility and accountability on those processing personal data,
throughout the information life cycle.” [Article 29 Working Party 2012]

Thus the legislation will require that [legal] entities who collect and determine the purposes for which personal data will be used, must proactively respond to EU privacy legislation by adopting data protection by design².

4.1 Trust, Sensitivity and Market Success

Data, notably personal data, is increasingly becoming a critical market asset driving the development of applications, services, products and business processes and is an increasingly significant contributor to economic growth. However, consumer concerns as to whether organisations can be trusted to safeguard their personal data are growing [Roeber 2015].

These concerns are not limited to organisations which use personal data to drive product development. Many organisations also derive competitive advantage from [big] data mining and analysis to deliver insights that are then used to drive business and organisational decisions. [Bradley J 2013; Xiaoni Zhang 2015].

Treacy and Breuning [Treacy 2013] in their assessment of the interface between the IoT and the Data Protection Directive, conclude that:

“Organisations wishing to take their products and services to the next level [the IoT] will need to identify the privacy risks and work to mitigate these before embarking on such projects.”

Further, the EU Article 29 Working Party holds the view that for commercial success, organisations must address consumer privacy concerns, commenting that [Article 29 Data Protection Working Party 2014]:

“Indeed, empowering individuals by keeping them informed, free and safe is the key to support trust and innovation, hence to success on these markets. The Working Party firmly believes that stakeholders meeting such expectations will hold an exceptionally strong competitive advantage over other players whose business models rely on keeping their customers unaware of the extent to which their data is processed and shared and on locking them into their ecosystems.”

In the context of the paper, data can generally be linked to usage activities, which may then be recorded and/or transmitted, much of the data being personal data. The Article 29 Working Party is very clear on this point, stating that [Article 29 Data Protection Working Party 2014]:

“IoT stakeholders aim at offering new applications and services through the collection and the further combination of this data about individuals – whether in order to measure the user’s environment specific data “only”, or to specifically observe and analyse his/her habits. In other words, the IoT usually implies the processing of data that relate to identified or identifiable natural persons, and therefore qualifies as personal data in the sense of article 2 of the EU Data Protection Directive.”

In September 2014 the Article 29 Working Party issued an opinion that identified the main privacy risks, within the framework of the Data Protection Directive, and recommendations for addressing those risks and went on to state that [Article 29 Data Protection Working Party 2014]:

“The recommendations offer a practical view of what IoT stakeholders should consider when developing and marketing their products in compliance with not only the current EU data protection framework, but also taking into account [successor legislation] the upcoming EU General Data Protection Regulation.”

In the US, similar arguments were presented by the United States Federal Trade Commission (FTC) in its staff report: Internet of things – Privacy and security in a connected world [FTC 2013].

Though the Working Party and the FTC share much common ground in their assessment of the nature of privacy risks, a consensus has yet to emerge on how privacy rules may be applied to encourage and stimulate innovation while protecting consumer privacy.

Here Corbet [Corbet 2014] comments that:

“…. core privacy principles such as transparency, consent and data minimisation should apply in an IoT ecosystem.”

A significant difference between the US and the EU lies with the fact that federal data protection laws only exist in European Member States. Not only is the Data Protection Directive well established, this legislative framework will shortly be extended with a single Data Protection Regulation, requiring the exploration of frameworks within which stakeholders can work to ensure proportionate responses to consumer privacy concerns throughout the entire lifecycle of a device and the associated processing and transmission activities.

As privacy jurisprudence develops and evolves it is likely that more specific guidance on establishing privacy as a core component of product and service by design will emerge. It is fundamental that such future thinking in this space emanates from and engages in a multi-disciplinary focus in which technologists and privacy/information governance practitioners come together, otherwise innovation will become stifled.

Table 1. Stakeholder responsibilities

<table>
<thead>
<tr>
<th>Stakeholder Role</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device manufacturers</td>
<td>By defining the functionality of a device and creating the ability for it to operate a device manufacturer will determine what data is captured and the subsequent modes of processing/operation, which can include the onward transmission of data to another device or</td>
</tr>
</tbody>
</table>

² Also referred to within the legislation as “Privacy by Design.”
Hence in responding to privacy as a core functional design element, an understanding the legal basis for processing personal data is fundamental. Before personal data can be used, stakeholders who provide devices and/or services (where the provider qualifies as a data controller) must ensure that their devices/services are capable of fulfilling at least one of the 6 requirements of Article 7 of the EU Data Protection Directive [Directive 95/46/EC 1995], itself due to be superseded by the General Data Protection Regulation [COM(2012) 11 Final].

Critically, products and services must be designed and managed so that they are capable of successfully engaging those requirements.

It is in this context that Table 1 sets out the relevant stakeholder roles.

The key requirements of the legislation are then summarised in Table 2 while associated areas of concern are set out in Table 3 along with the privacy requirements of users as Table 4.

It is therefore clear that those who seek to take their products and/or services into the IoT eco-system will need to understand the fundamental concepts of privacy legislation, and work to mitigate privacy concerns as a core element of product and/or service design.

### 5. PRIVACY BY DESIGN

Privacy by design emerged in 1995, from the joint work of Information and Privacy Commissioner of Ontario, Canada and the Dutch Data Protection Authority on “privacy enhancing technologies” and the principles of “data minimization” which:

> “explored a new approach to privacy protection, with a number of case studies to show that systems with no personal data—or at least with much less personal data—could have the same functionalities.”

Work to develop the concept of privacy by design continued, culminating in 2009 with the publication of a statement of 7 foundation principles [Privacy by Design 2009] set out in Table 5. The third principle “Privacy Embedded into Design” demonstrates how the concept is an approach of systems engineering, where privacy requirements are considered and addressed throughout the whole of the engineering process:

> “Privacy is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that it becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.”

### Table 2. Requirements of EU Data Protection Directive

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consent</td>
<td>People need to be fully informed as to how their personal data will be used, and by whom. Where a user opts to consent, that consent must be explicitly captured and that fact recorded. Users also have the right to withdraw their</td>
</tr>
</tbody>
</table>
consent, this will have to be managed as part of product and service design. Fundamentally, IoT systems design must provide for robust consent management, where users can continually opt in or out, without any disadvantage, they must retain the right to have full use of the functionality of the system/service that they have paid for (Article 29 Data Protection Working Party 2011).

For the contract to remain valid, there cannot be any creep in the use of personal data. The collection and use of personal data must be clearly understood and defined as part of device and/or service design.

A data controller can process personal data, and share this with a third-party where it is their legitimate interests or those of the third-party as long as the fundamental rights of the data subject are not undermined.

As the privacy concerns of data subjects are fundamental, it is unlikely that a data controller can successfully claim economic interests as a justification to legitimise their processing of personal data.

| Contract | Use of personal data by IoT devices and/or services can be legitimised where there is a contract between the data controller and the data subject. The use of personal data must be necessary to fulfil the contract, requiring “a direct and objective link between the processing itself and the purposes of the contractual performance expected from the data subject.” (Article 29 Data Protection Working Party 2014)

For the contract to remain valid, there cannot be any creep in the use of personal data. The collection and use of personal data must be clearly understood and defined as part of device and/or service design.

| Legitimate Interests | A data controller can process personal data, and share this with a third-party where it is their legitimate interests or those of the third-party as long as the fundamental rights of the data subject are not undermined.

As the privacy concerns of data subjects are fundamental, it is unlikely that a data controller can successfully claim economic interests as a justification to legitimise their processing of personal data.

### Table 3. Areas of concern

<table>
<thead>
<tr>
<th>Privacy challenge</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of control and information asymmetry</td>
<td>Given the ubiquitous nature of the IoT, where a stakeholder processes personal data unknown to the user, people may find that they rapidly lose control of their privacy, where they then become subject to third-party monitoring, notably where their personal data is disseminated to other stakeholders without prior knowledge or consent.</td>
</tr>
<tr>
<td>Quality of user’s consent</td>
<td>It is easy for IoT stakeholders to be invisible. If a user is unaware of the data processing taking place, then consent cannot be relied upon as a lawful basis for processing personal data. Data subjects must be informed that processing is taking place.</td>
</tr>
<tr>
<td>Inferences derived from data and repurposing of original processing</td>
<td>With the increased volume of data generated by the IoT, combined with advances in data analysis and cross-matching, it becomes easier for secondary forms of personal data to be generated and used for purposes beyond those that were originally intended.</td>
</tr>
<tr>
<td>Intrusively bringing out of behaviour patterns and profiling</td>
<td>In the IoT the proliferation of sensors/devices, makes it relatively easy to build up a picture of a person’s life from trivial or even anonymous data. Data harvested from the IoT could be used to predict future behaviours, leading to significant privacy intrusion, where a data controller makes a decision on an individual, based on future profiling.</td>
</tr>
<tr>
<td>Limitations on the possibility to remain anonymous when using services</td>
<td>The nature of the IoT is likely to make it extremely difficult for users to use services anonymously, as the connection between a user and a device will more often than not be inextricable.</td>
</tr>
<tr>
<td>Security risks: security versus efficiency</td>
<td>It may be difficult to implement many security measures on IoT devices such as sensors, where there is a trade-off between hardware based encryption and battery life. Integration of physical and logical IoT components, provided by a range of stakeholders only provides a level of security at the weakest point in the chain. IoT devices that become everyday objects present a new distributed target.</td>
</tr>
</tbody>
</table>

### Table 4. Privacy design requirements for stakeholders

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy impact assessments (“PIAs”)</td>
<td>PIAs undertaken prior to the launch of any IoT entity. PIA methodology recommended for RFID applications should be considered.</td>
</tr>
<tr>
<td>User empowerment</td>
<td>Data subjects rights must be recognised and respected, users must retain control over their data at all times. Data subjects as consumers/users should not suffer any economic penalty or service degradation if they opt not to consent to the use of their personal data. Consent should be granular – focused on specific areas of processing. Data subjects should have the facility to continually withdraw their consent, without having to exit from the service provided. All IoT stakeholders must be able to communicate to ensure that user choices are respected and acted upon. IoT devices and services should operate with a do not disturb function, including the facility to disable and enable sensors.</td>
</tr>
<tr>
<td>Data minimisation</td>
<td>Most IoT stakeholders only require aggregated data. Stakeholders should delete raw data as soon as that data has been extracted for processing. Deletion should take place at the closest point of data collection of the raw data.</td>
</tr>
<tr>
<td>Privacy by design &amp; privacy by default</td>
<td>Principles of privacy by design and privacy by default to be applied by all IoT stakeholders.</td>
</tr>
<tr>
<td>Transparency</td>
<td>Information on the use of personal data by IoT stakeholders should be made available in as user-friendly a manner as possible. Such information should not be confined to general privacy statements that are available from terms and conditions.</td>
</tr>
</tbody>
</table>

### Table 5. Underlying principles of Privacy by Design

| 1 | Proactive | not Reactive; Preventative | not Remedial |
| 2 | Privacy as the Default Setting | |
| 3 | Privacy Embedded into Design | |
| 4 | Full Functionality — Positive-Sum, not Zero-Sum | |
| 5 | End-to-End Security — Full Lifecycle Protection | |
| 6 | Visibility and Transparency — Keep it Open | |
| 7 | Respect for User Privacy — Keep it User-Centric | |

As suggested by Fig. 3, this implies that ownership of, and hence control over, data is transferred from the organisation to the individual.

Working to embed Privacy by Design principles as a foundation of systems analysis and design is likely to involve establishing new interfaces/partnerships, with systems designers, engineers, information governance and privacy practitioners coming together within the product design and requirements specification phases.

For instance, the requirement to advise users as to how their personal data is being processed, which will include how data is collected and transferred to other stakeholders who are data controllers, could be aided by repurposing business data flows/process maps to explain what processing takes place and when to users. This level of analysis can also potentially be utilised to reduce the likelihood of incremental creep in the processing of personal data.
Mapping out the processing and understanding data flows, notably when data can take on new meaning, will assist in establishing processing boundaries. Having determined the process boundaries, these should then inform the design phase, with the view of developing products/services that guard against any drift into illegal uses of personal data, notably where inferences can be derived from data and repurposing beyond the lawful justification for processing. This may mean that data controllers can rely more heavily upon contracts as a legitimising basis to process personal data, reducing the requirement to rely on consent – which could then simplify product and service design.

Fig. 3. The difference between conventional and privacy by design approaches to user privacy issues.

6. CONCLUSIONS

It is clear that meeting the requirements of privacy by design will require the extension of mechatronics’ established practice of multi-disciplinary working at the technical level to encompass within the design process new design procedures encompassing legislation and the associated legal requirements. A fundamental consideration is thus that of how best to bring the relevant multi-disciplinary elements together within the appropriate academic, professional, practitioner and organisational contexts to provide and sustain the required technical and legal innovation that will become increasingly required?

Understanding and recognising when data makes the transition from data to personal data or sensitive personal data will be critical in the design and provision of effective privacy solutions. In that regard, an area where technical and legal innovation can come together is that of developing and integrating anonymization techniques to turn data into a form which does not identify individuals, and where identification is not likely to take place within the design process. This will allow for a much wider use of the information, while mitigating privacy risks for the data subjects. Successfully anonymized data will also fall out of the scope of data protection legislation, which by extension will reduce pressures on IoT stakeholders where the scope of their responsibilities as a data controller can be reduced.

Overall therefore, it is increasingly apparent that privacy issues are likely to have a major and significant impact on the way in which future mechatronic systems are designed, developed, implemented and used.

REFERENCES


Corbet, R. (2014) Internet of Things where are we now?