Holistic Governance and Policy Project

Introduction to the HGP Framework

29 October 2015

Summary

The Internet of Things (IoT) exposes the multiplicity and complexity of data flows and data uses. It also exposes the challenges of today's data protection mechanisms and highlights a shift in the balance of power in the information governance ecosystem from individuals to organisations. This shift, however, does not suspend the objectives for data protection and privacy law. Those objectives have always been the free flow of data for productive uses and the protection of individuals as that data is collected and used. Furthermore, data protection law has always combined the rights of individuals, the obligations of data users and the oversight of protection agencies. So this shift in power suggests that three questions need to be rethought:

1. Who should have what obligation(s) with respect to data about an individual and its use,
2. What level of participation is practical for an individual to have, and
3. When should individual participation occur?

In short, what is an effective information governance ecosystem that allows all participants to realise the benefit creating potential of data while providing more meaningful ways to appropriately use and protect this data?

An Illustrative Example

An IoT ecosystem contains many participants and relationships, including the end user (individuals or groups of individuals) and organisations. According to Cisco, by the end of this decade, there will be over 50 billion connected objects – approximately six objects for every person on the planet.[1] The growing wearables industry is representative of this increasingly complex ecosystem.

Vandrico reports[2] the deployment rate of wearable technology [3] is currently at 21 percent and is forecasted to reach over 50 percent by 2016. An explosion of medical wearable devices that are designed to assist doctors with diagnosing diseases is expected. Medical professionals will be able to obtain continuous data by monitoring basic vital signs, such as heart rate, blood pressure, skin temperature and blood oxygenation. Perhaps, more significantly, a continuous recording of data will give the medical industry a greater understanding of the effects of prescribed treatments. Patients also will be able to observe concretely how their lifestyle choices affect their overall health. The addition of gamification or other custom behavioural software can assist in improving the lifestyle choice of a user.

---

[1] Endler, Michael (2013), "Cisco CEO: We're All In On Internet Of Everything", InformationWeek, http://www.informationweek.com/software/information-management/cisco-ceo-were-all-in-on-internet-of-everything/d/did/1108801.

[2] Vandrico (2014), "Vandrico Wearables Market Insights – Q1, 2014", http://vandrico.com/cdn/vdc_wrpt_2014_q1.pdf.

[3] Data does not include Smartphones.

Currently, more than half of the devices in the Vandrico database contain inertial measurement units (IMUs), which include accelerometers, gyroscopes and/or magnetometers. Large portions of these devices are using IMUs to track activity levels and infer the number of calories burned. Vandrico expects these components to become standard for fitness monitors, currently also a large class of wearable devices.

Wearables, such as fitness monitors, will soon throw off a constant stream of data points about the device and the user or owner. More connectivity means more opportunities to use, as well as abuse, the resulting flow of information. Soon, manufacturers, brands and even employers and insurance companies could have unprecedented access to previously unavailable information about individuals.

A test was conducted using a specialised type of fitness monitor (e.g., a Smart Shirt, coupled with big data analytics) to monitor the vital signs of long-distance truck drivers in order to determine fatigue levels. The Vandrico research suggests that such a wearable device will serve multiple purposes. It will be a personal device for the driver for multiple applications, and it will collect and provide data for the purpose of fatigue monitoring by the truck company.

There are many participants who have **benefits, risks and interests** in this wearables supply chain of data. For example:

Participants	**Benefits/Risks/Interests**
Highway transportation administration (or equivalent)	Reduction of fatigue related accidents and the associated devastating outcomes (e.g., school bus accidents)
Truck company	Reduction of risks (e.g., employee relations and legal compliance) and costs (e.g., better scheduling)[4] and creation of better employee relations
Driver	Benefits of better scheduling and perceived risks of "monitoring"
Regulator	Enforcement of applicable law[5]
Employee Union	Perceived risks of employee monitoring

[4] The test market analysing this data was able to pinpoint that one source of driver fatigue was due to company scheduling. Russell, C.A., J.A. Caldwell, D. Arand, L.J. Myers, P. Wubbels, H. Downs (n.d.), "Validation of the Fatigue Science Readiband™ Actigraph and Associated Sleep/Wake Classification Algorithms", http://static1.squarespace.com/static/550af02ae4b0cf85628d981a/t/5526c99ee4b019412c323758/1428605342303/Readiband_Validation.pdf.

[5] In locations where privacy laws have been enacted.

This wearables example illustrates the types of complex questions a new information governance ecosystem will need to address:

- How should IoT data, like data related to fatigue monitoring, connected to a cloud service (for example, a single service provider rather than a device specific manufacturer), be considered?
- What are the appropriate uses of this data (for example, could other data created through an analytical discovery process be used in aggregate to apply to insurance rate setting at a group or at an individual level)?
- How should policy and governance guidance and a workable framework that can distinguish between the different uses that leverage the same data be established? If using wearables to determine big-rig driver fatigue becomes an infringement of individuals' interests in control over their own information, are there other fundamental and societal interests, such as the safety of children that may outweigh the individuals' autonomy interests? While other interests, such as insurance company risk rankings, may not overcome these individual interests?
- While the data from this wearable may not be identifiable, it is plausible to make it identifiable by matching it with other data. What should the governance be around such uses?
- How should multiple interests be reflected and governed by society, the organisation and the individual?

The multiplicity of participants, the complexity of the data flows and uses, the wide variety of data combinations, the benefits and risks in the data life cycle, and the identifiability and sensitivity of the data in the wearables example demonstrate the limitations of the current model and the need for a new model.

The Limitations of the Current Model

Today, the wearables industry is virtually unregulated in many parts of the world and does not benefit from well-established participant, industry or ecosystem information governance guidance to help responsibly manage and innovatively use data. Who should have access to what data for what purposes are questions currently not answered in either law or industry codes of conduct. These are questions that need to be addressed.

Today's notice and choice regime, where individuals can opt in or out of the use of their information, is under challenge and is unlikely to be sustainable in the long run as a mainstay of data protection. Also under challenge are the many times and places where participants, other than the end user, should be responsible for many types of obligations, including ones where additional re-engagement with the end user is appropriate. This should also accommodate where the use of the data should not have to involve the end user, but instead should be subject to other obligations, such as security or data retention control**.**

A Simple Example Illustrates These Limitations

Light bulbs increasingly have sensors and have the ability to capture large amounts of data such as household usage patterns. When coupled with advanced analytics, this data can create new insights that could then be acted upon in a way that has an impact on an individual. In this scenario, many business participants could be involved in data analysis, insight generation and application of these insights. It could be the light bulb manufacturer or the utility company. It could be a third-party research firm or the mobile application provider associated with the utility company acting as an independent participant, or it could be a completely different third party.

In today's model, while the light bulb company may have a privacy notice that covers all of this collection and use, it is unreasonable to expect an individual to look at this notice, since it is unlikely there is a direct relationship between the light bulb company and the individual. Where data analysis and data use involves multiple entities, it is unreasonable to expect an individual to look at all of the applicable privacy notices. As this loss of control becomes increasingly common, there are many risks involved (for example, loss of customer trust and/or reactive changes to existing public policy and possible regulatory action). These risks could shut down data-driven business strategies that are truly appropriate and valuable. In addition, left unchecked, public policy confusion combined with inadequate assessment tools will create more "reticence" risk; information simply not being used because decision drivers are unclear.

The fatigue monitor example illustrates the challenges of information use and the multiple sets of interests at issue. The light bulb example illustrates the challenges of meaningful participation, including notice and choice.

What might a new model look like?

In an age of big data, where the goal is the realisation of information-driven economic and societal benefits of information use, effective data protection is more essential than ever. An effective data protection regime incorporates the benefits that information use can create while recognising the risks of data use from a 360-degree perspective.

Today, more and more organisations seek to create benefits from information, and more and more consumers are expecting benefits from information through more connected, "always on" devices and services. If the utility of the resulting information is to be leveraged and the benefits that big data is already making possible are to continue to be enjoyed, better, faster and more scalable public policy and related governance mechanisms need to be evolved. Doing so will help achieve more effective data use and protection and new ways for organisations to demonstrate that scalable public policy models can be implemented through accountable governance systems. As the European Data Protection Supervisor stated in his recent opinion, "Towards a New Digital Ethics", new business models are placing the principles of data

protection under strain, and fresh thinking is required as to how these principles can be applied.[6]

If meaningful protection of personal data and benefit to society are to be achieved from the increasing power of data and analytics, governance models need to evolve to keep pace with the growing uses of big data. This evolution must retain the benefit of individual participation, including appropriate transparency, as part of effective data protection, while providing for the role of accountable organisations in a holistic information governance framework enabling appropriate information use.

In early 2015, the Information Accountability Foundation (IAF) launched the Holistic Governance and Policy Model Project (HGP Project) to delve more deeply into how this challenge might be addressed and to design a more evolved governance approach. Given the complexities of today's information flows and use, the question to be answered is: what would a more practical and meaningful governance system look like?

The IoT Ecosystem

The chart that follows shows the categories of participants in an IoT ecosystem. Individuals and organisations in the ecosystem have complex data exchange relationships with each other. Some of these relationships are direct and exist between the user/individual and a business participant, and other relationships are indirect and may or may not be initiated by the user. In addition, relationships can start, end and re-start between multiple participants as new uses of data are envisioned.

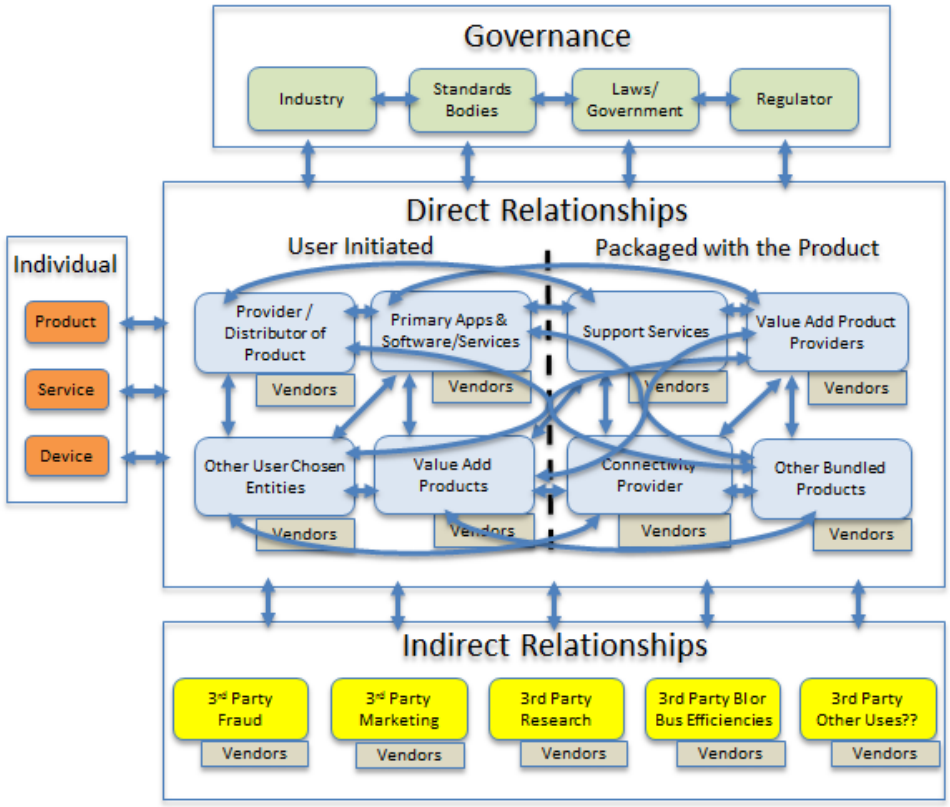
To add to the complexity, new uses and new exchanges of data can trigger questions on the "sensitivity" of the data, even if by classification the data was not originally sensitive. At the same time, if sensitive data is used for operational reasons, such as securing the ecosystem, then different and even fewer obligations by a participant should apply.

When products become data-generation platforms, individuals inevitably will be more aware of the worth of their own data. This awareness requires that control or "autonomy" be made more meaningful or practical and be supplemented by obligations on other participants.

The obligations of business participants should be determined by the combination of the data, the use of the data, the participant that is using the data and additional factors like the identifiability and sensitivity of the data.

[6] EDPS (2015), "Opinion 4/2015: Towards a New Digital Ethics", https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-09-11_Data_Ethics_EN.pdf.

Chart 1: Ecosystem of Participants



The Proposed Framework

Today's information flows and uses need a re-balancing of responsibilities, the introduction of new obligations and a new way to think about obligations for each participant. The fundamental approach is to focus individual participation where it is meaningful and impactful but eliminate it where it is not and to expand business risk assessment, transparency and accountability obligations so that regulators are more informed about business practices and more effective in their enforcement. The objective is to better align responsibilities while improving overall data protection effectiveness.

Such an effective information governance system, given the 21st century ecosystem and data use, should include these inter-related components:

- Individuals should have meaningful, contextual and flexible engagement where there is genuine choice that facilitates control over information about them. A new data use that could impact the individual and one where some choice is either expected or desired could require additional user engagement. Conversely, a new but compatible use may not require additional user engagement.

- Business users of information would determine the extent and type of individual engagement and other appropriate obligations through a risk assessment process covering the data, its use and other mitigating factors. Such a risk assessment looks at both any immediate risks as well as implications of the information use over time and implements appropriate risk mitigations (for example, de-identification of the data).
- All business participants would provide an accessible, transparent notice covering their policies and practices relating to information collection and use. Such a notice would constitute the legally binding obligations a regulator looks to regarding compliance oversight. While this disclosure would be accessible to individuals and regulators, individuals would not be required to read or acknowledge it. This disclosure should explain the organisation's information governance processes, including its risk assessment process. While this transparency obligation may include engagement with individuals relative to their choice(s), transparency mechanisms and individual engagement approaches could be separate, providing they are consistent.

These obligations are – in addition to other foundational business obligations – applicable to all data about individuals that a business processes or exchanges, some of which are already in place (for example, the security of the data), other legal requirements, and/or contractual obligations (upstream and downstream).

There has been much debate over the past few years about the current governance structure and the emphasis on data collection and purpose specification. Some have argued that a shift in focus more on the "use" of data would provide better control and protection for the individual. The HGP Project recognises that BOTH collection AND data use are important and should be part of a more mature and effective governance structure.

Moreover, while data collection and initial purpose specification are important, subsequent uses of data derived from analytical driven insights coupled with the growing number of business participants in evolving ecosystems means a focus on data use and other factors is equally important. This proposed approach does not suggest that the current governance model, consistent with today's legal requirements, does not contemplate "data use". Rather, it suggests that this historical model, when it was developed, did not and could not have envisioned today's myriad of data use models and that a re-balance of obligations is required.

In fact, there are many uses of data where there need not be active engagement with the end user/individual. Use of data for securing the ecosystem, operating the product or fraud prevention are examples where no meaningful choice or control over the use of data is common. These uses of data, however, should carry obligations, such as security, that should be transparent. However, they do not have to be part of a meaningful individual engagement obligation.

Conclusion

Under the Proposed Framework, the obligations of the business participant using an individual's data should be determined for each participant using the data by the combination of the data itself and the use of the data, along with additional factors like the identifiability and the sensitivity of the data. In short, a more balanced, fluid and contextually flexible set of obligations can achieve today's information governance objectives. This represents a fresh, new way to achieve the application of the fundamental data protection principles.

Next Steps

Over the coming months, the IAF plans on further developing, testing and socialising this Proposed Framework. This will be accomplished through dialogue with multiple stakeholders who all share the same goals of enabling the generation of wonderful opportunities and benefits from information while effectively protecting individuals and considering a broad range of interests relative to its use.

Peter Cullen, Jennifer Glasgow and Stan Crosley are the principle authors. They received input and editorial assistance from many project participants for which they are grateful. They remain responsible for any errors.