Crabtree, Andy (2016) Enabling the new economic actor: personal data regulation and the digital economy. In: IEEE 2nd Workshop on Legal and Technical Issues in Cloud Computing and Cloud-Supported Internet of Things, 4-8 April 2016, Berlin, Germany.

This is author's version of the work published by the IEEE in IC2EW DOI: 10.1109/IC2EW.2016.18

Enabling the New Economic Actor

Personal Data Regulation and the Digital Economy

Andy Crabtree
School of Computer Science
University of Nottingham
United Kingdom
andy.crabtree@nottingham.ac.uk

***Abstract*—This paper offers a sociological perspective on data protection regulation and its relevance to the design of digital technologies that exploit or 'trade in' personal data. From this perspective, proposed data protection regulations in Europe and the US seek to create a new economic actor – the consumer as personal data trader – through new legal frameworks that shift the locus of agency and control in data processing towards the individual. The sociological perspective on proposed data regulation recognises the reflexive relationship between law and the social order, and the commensurate need to balance the demand for compliance with the design of tools and resources that *enable* this new economic actor; tools that provide both data protection to the individual *and* allow the individual to exploit personal data to become an active player in the emerging data economy.**

Keywords—sociology; personal data protection; individual control principle, local control recommendation, utility model, human data interaction.

I. INTRODUCTION

Slogans such as "Big Data" and the "Internet of Things" (IoT) herald a new economic market predicated on the trading of "personal data" – i.e., data that pertains to identifiable human beings. McKinsey Global estimate that Big Data could generate from $3 to $5 trillion in value every year [13], and Gartner forecast $1.9 trillion aggregate benefit from the sale and use of IoT technology by 2020 [15]. Personal data is rapidly becoming the "new currency" [9] in the digital economy, though not without comment. A steady drip of media stories detailing the misuse and abuse of personal data is complemented by large-scale leaks, all of which combine to create broad societal concern and engender what the World Economic Forum (WEF) describes as a "crisis in trust" [21]. It is a crisis that motivates new data protection regulation in a bid to rebuild consumer confidence.

The traditional view of data regulation, and one that would seem to underpin many legal perspectives, is that it is there to protect the individual from the misuse and abuse of data that pertains to them, whether it is generated by the individual and used by other parties or it is generated by other parties and is about an identifiable individual. The view offered here is that the new data protection regulations that are being put forward in Europe and America are *also* about enabling a new kind of economic actor: an actor who is an active player in, rather than a passive victim of, the digital economy in general and the emerging data economy in particular. From this point of view, proposed data protection regulations can be seen to promote the data economy by creating legal frameworks that shift the locus of agency and control in data processing *towards the individual*.[1]

This alternative perspective on data protection regulation reflects a sociological understanding of the law. From this point of view the law is not 'simply' a system of rules devised to regulate action, a mechanism of social control as it were; the system is reflexively tied to the social order. Seen from this perspective, efforts to define new regulation are not restricted to defining data protection measures and compliance procedures. They can also be seen to be concerned with creating a *new social order,* one that enables the widespread and even global trade in personal data. The sociological perspective is of consequence to the design of new technologies. It shifts the focus of technology development from a matter of compliance to a matter of (also) envisioning how this new economic actor might be *enabled through design*, i.e., through the building of computational infrastructures, services, applications and devices that enable the individual to become a player in the data market; someone who is empowered through technology and not the victim of it.

This is not to dismiss a concern with compliance, clearly the law places binding requirements on design and it is important that developers build technology with respect to them. It is however, to recognise that focusing on compliance alone is not sufficient to ensure the manifold social and economic benefits that are tied to the trade in personal data. Building in data protection needs to be balanced then with the building of tools and resources that enable personal data to be exploited *by individuals*. The final part of this paper considers one approach towards achieving this balance: Human Data Interaction or HDI [16]. This approach is gaining currency in design, being a cornerstone of DARPA's Brandeis program [6]. If successful it will bring the sought after shift in agency and control about, enabling both the individual privacy protection *and* the personal data trading that is key to the digital economy.

II. THE SOCIOLOGICAL PERSPECTIVE, IN BRIEF

The sociological perspective on the law may be viewed as new and provocative, and it may well be so in this particular

[1] New regulation is also being proposed in Japan [18]. The emphasis here is on enabling the "utilization" of personal data in order to "revitalize the economy". The proposed regulation posits the introduction of an "independent third-party authority" in order "to gain trust from consumers".

venue, but it is really a very old one that reaches back to the beginnings of the discipline in the 19th century [7]. In many respects it reminds us, as [2] puts it, of something that we all take so much for granted that we tend to *forget* it. The sociological perspective reflects common-sense reasoning [22] and thus puts what anyone knows about law and society, and not just the learned opinions of legal experts, on the agenda. What anyone knows is that the law is an integral part of the social order, not simply in the sense that it is key to maintaining order but that it reflects in its writing, rewriting and use the social order that is to be maintained. Thus, in sociological terms, the law 'functions' (in contestable ways) to define and shape the social order [8], which in the developed world at least is essentially capitalist in nature.

Capitalism, as any kind of social order, manifests itself in different ways in different societies, with these being reflected in a historical sequence of unique local laws. In the UK, for example, capitalism can be seen to emerge over centuries through, and arguably despite of, a succession of statutes regulating labour. The decline of feudal social order in the early part of the 14th century was marked by statutes, such as the Ordinance of Labourers 1349 and the Statute of Labourers 1351, that sought to prohibit increases in wages and the free movement of workers, not that they were particularly effective. Nevertheless, the same laws were still being reformed two hundred years later, as reflected in the Statute of Artificers 1562, and it would be another century until the feudal social order was finally dispatched by the Tenures Abolition Act 1660. Such examples demonstrate the reflexive relationship between law and the social order, revealing its role in maintaining order, reshaping it, and creating it anew.

The old order was replaced by "a new division of labour", which underpinned the wealth of nations and the common man [17]. With it a new economic actor – one long in the making – was born; an actor whose labour was premised on a contractual relationship rather than one's relationship to the feudal estate. In turn, the law came to encode this new actor and the new social order in regulation. The Employers and Workmen Act 1875 dissolved the Master and Servant Act 1823, which made breach of contract by a worker into a criminal matter. The Truck Act 1887 abolished payment in goods rather than money. The Trade Boards Act 1909 introduced minimum wage criteria, and the Representation of the People Act 1918 and the Equal Franchise Act 1928 eventually enfranchised the economic actor in Smith's "new" social order. Thus it continues, with an ongoing series of historically situated and locally unique laws not only regulating the social order but also, at the same time, reflexively shaping and reshaping it. This reflexive relationship between the law and social order is consequential for technology development.

The consequence turns upon setting the legal preoccupation with the meaning of the law to one side and asking instead what is its sociological function? When viewed from this perspective the debate about what the law requires of design with respect to privacy and the processing of personal data shifts from a matter of understanding data protection measures and compliance procedures to understanding the social organisational arrangements the law seeks to bring about. This, to reiterate, is not to set a concern with data protection and compliance aside. It is to ask *what kind of social order does the law seek to create?* It is this foundational matter that we all too often take for granted and lose sight of when considering matters of law, especially when we turn to the legal profession in a bid to interpret the law and arrive at a definite sense of its meaning. Nevertheless, it is a matter that concerns us here.

III. The Legislative Perspective, Sociologically Construed

While the nomenclature varies from state to state data protection regulation generally focuses on the obligations of what is often referred as the 'data controller' – i.e., the party who determines the purposes for which and the manner in which personal data is processed – and regulates the act of 'data processing', which may be carried out by another party on the controller's behalf. It also specifies the rights of 'data subjects' – i.e., a living individual to whom personal data relate. There is much about the obligations of data controllers and processors in proposed European and American regulation. However, in both cases, it is clear that regulation is not 'simply' concerned with data protection. Just as it does in Japan, the *economy* looms large in EU and US draft legislation.

In draft European legislation [10] the need to revise data protection regulation is firmly *premised* on economic considerations. The explanatory memorandum prefacing the proposal outlines the concerns that motivate the introduction of the new data protection framework. Thus, it is explained that "heavy criticism", "particularly by economic stakeholders", motivates the need to "adapt" the existing framework due to "fragmentation" in the ways in which data protection is currently implemented across the Union, and the need for "increased legal certainty" and "harmonisation of rules" across international borders given the "rapid development of new technologies". These concerns "constitute an obstacle to the pursuit of economic activities" and "distort competition".

"This is why it is time to build a stronger and more coherent data protection framework in the EU, backed by strong enforcement that will allow the digital economy to develop across the internal market, put individuals in control of their own data and reinforce legal and practical certainty for economic operators and public authorities."

The economic imperative is similarly marked in draft US legislation. The proposed Consumer Privacy Bill of Rights [4] seeks to extend the reach of the Federal Trade Commission's Fair Information Practice Principles (FIPPs). While FIPPs is not enforceable, it does form the basis of laws regulating the use of personal data in specific sectors (e.g., health, education, finance). The proposed bill "carries FIPPs forwards" and seeks to apply it through self-regulation enforced by the FTC Act (Section 5) prohibiting "unfair or deceptive acts or practices" to "the interactive and highly interconnected environment in which we live and work today." Although adopting a different approach to data protection, the concerns that motivate the proposed bill are similar to those in Europe. Thus the proposed bill of rights seeks to address the problems occasioned by a fragmented "sectorial" environment, provide "greater legal certainty" to companies, and "create interoperability between

privacy regimes" in order to "promote innovation" and "drive the digital economy".

Evidently the purpose of proposed legislation is not 'simply' to lay down data protection measures and spell out compliance procedures. It does this of course, but to a social rather than a legal end: to engender individual or consumer *trust*. Furthermore, as the following extracts make clear, the purpose of proposed regulation is not to engender trust per se, but to engender trust *in the digital economy*; an economy that increasingly relies upon the trade in personal data.

"Preserving trust in the Internet economy protects and ***enhances substantial economic activity****. Online retail sales in the United States total $145 billion annually. New uses of personal data in location services, protected by appropriate privacy and security safeguards, could create important business opportunities. Moreover, the United States is a world leader in exporting cloud computing, location- based services, and other innovative services. To preserve these economic benefits, consumers must continue to trust networked technologies. Strengthening consumer data privacy protections will help to achieve this goal."* [4]

"The scale of data sharing and collecting has increased dramatically … Building trust in the online environment is ***key to economic development****. Lack of trust makes consumers hesitate to buy online and adopt new services. This risks slowing down the development of innovative uses of new technologies. Personal data protection therefore plays a central role in the Digital Agenda for Europe, and more generally in the Europe 2020 Strategy."* [10]

Where is the proposed new economic actor in all of this, the individual or consumer as data trader and thus lynchpin of the data economy? The proposed EU regulation explicitly seeks to *"put individuals in control of their own data"*. This is to be achieved through the implementation of "appropriate technical" as well as organisational "measures" at the time of "the design of processing" and at the time of "the processing itself." These measures should provide for informed consent "at the time of collection or within a reasonable period" and informed choice through the implementation of "certification mechanisms and data protection seals" that allow individuals to "quickly assess the level of data protection" offered by digital products and services. Furthermore, individuals should be able to "obtain a copy of the data concerning them" and "transmit those data" from one automated application into another one to "further strengthen the control over their own data" [10].

The US Consumer Privacy Bill of Rights seeks to provide "consumers who want to understand and control how personal data flows in the digital economy with better tools to do so." The issue – indeed "principle" – of individual control looms large in the proposal, being the first of seven key "rights" laid out in the draft bill.

"Consumers have a right to exercise control over what personal data companies collect from them and how they use it."

The "Individual Control principle" has two key aspects to it: one "providing consumers with easily used and accessible mechanisms" with which to exercise control, and two "consumer responsibility", which recognises that the use of personal data turns upon the individual's decision to share data with others. "Control over the initial act of sharing is critical." It turns upon consumers having the tools and mechanisms to hand to make informed decisions and exercise control. The draft bill suggests that "innovative technology can help to expand the range of user control" and cites examples such as "detailed privacy settings", "do not track" and "opt out" mechanisms. However it also goes so far as to say that while such mechanisms "show promise" they "require further development" [4].

It might be argued that this is a thin legal basis on which to ground the claim that proposed regulation seeks to enable a new economic actor. We are not, however, making a legal argument but a sociological one. From this perspective the need to enable *individual control over the flow of personal data* in the digital economy is evident in both EU and US proposals. It is on this basis that we say proposed legislation seeks to shift the locus of agency and control in data processing towards the individual. The measures proposed to affect the shift are not purely legal in nature – not 'simply' a matter of specifying data protection measures and compliance procedures - but reach out to "technical measures", "tools", "easily used and accessible mechanisms" and "innovative technologies" to *enable* the actor's participation *in* the digital economy.

The underlying need to enable the new economic actor – the individual as data trader – through technology development can be further apprehended when we turn to those parties tasked with transforming legislation (actual and potential) into best practice guidance; in this case the Article 29 Working Party (WP29), established under the 1995 Data Protection Directive, and the Federal Trade Commission (FTC), tasked with enforcing data protection in the US. Both parties have issued guidance with regards to the Internet of Things (IoT), which is set to be a primary engine of personal data production and distribution, over the last two years. Both parties offer a broad range of recommendations for best practice to industry. Of particular note here are those recommendations that speak to the *Individual Control principle*.

The FTC proposes a number of practical measures to put the individual in control of personal data generated by IoT devices [19]. These include "general privacy menus" enabling the application of user-defined privacy levels (e.g., low, medium, high) across all their IoT devices by default. The use of icons on IoT devices to "quickly convey important settings and attributes, such as when a device is connected to the Internet" and to enable users to quickly "toggle the connection on or off." The use of "out of band" communications to communicate important privacy and security settings to the user via other channels, e.g., via email or SMS. And the use of management portals or "dashboards" that enable users to configure IoT devices and accompanying privacy settings.

"Properly implemented, such 'dashboard' approaches can allow consumers clear ways to determine what information they agree to share."

WP29 also proposes a number of practical measures "in order to facilitate the application of EU legal requirements to

the IoT" [1]. These include providing users with "granular choices" over data collection, including the "time and frequency at which data are captured", and scheduling options to "quickly disable" data capture. Users should also be "in a position to administrate" IoT devices "irrespective of the existence of any contractual relationship" and "easily export their data" from IoT devices "in a structured and commonly-used format." Furthermore, settings should be provided that enable users to distinguish between different individuals using shared devices "so that they cannot learn about each other's' activities." These recommendations may be seen to complement the dashboard approach towards putting the Individual Control principle into practice, insofar as they largely specify *privacy settings* that users can activate. However, the WP29 recommendations go a step further.

*"To **enforce** transparency and user control, device manufacturers should provide tools to **locally** read, edit and modify the data before they are transferred to any data controller."*

*"Device manufacturers should enable **local** controlling and processing entities allowing users to have a clear picture of data collected by their devices and facilitating **local** storage and processing without having to transmit the data to the device manufacturer."*

The *local control* recommendation is radical. It undermines the current approach to privacy being widely adopted by industry – i.e., encryption. This approach puts personal data online for processing *before* making it available to the user. As Winstein [20] puts it,

"Manufacturers are shipping devices as sealed-off products that will speak, encrypted, only with the manufacturer's servers over the Internet. Encryption is a great way to protect against eavesdropping from bad guys. But when it stops the devices' actual owners from listening in to make sure the device isn't tattling on them, the effect is anti-consumer."

The security-based model does not satisfy the Individual Control principle, nor is it sufficient to satisfy end-user privacy requirements, as encryption does not stop device manufacturers from exploiting their personal data. The local control recommendation is also radical because it provides a strong pathway to striking the necessary balance between privacy protection and the need to enable the new economic actor.

IV. Striking the Balance

The sociological perspective on legislation makes it perspicuous that the function of proposed regulation is to engender consumer trust in the digital economy. This raises the issue of balancing data protection with the building of tools and resources that enable a new economic actor. The need to strike this balance is underscored by the WEF, which emphasizes a "lack of empowerment" as a key issue "undermining trust" in the digital economy [21]. The WEF recognises that "the current system reflects an asymmetry in power that broadly favours institutions (both public and private)." This asymmetry is often construed in terms of "notice and consent challenges" and the power that large institutions have to "orient notice and consent agreements to advance their interests." There is, however, another key issue here that concerns "individuals being able to use their own data for their own purposes." It his here where "the power dynamics come into play".

"The dominant principle of the new economy, the information economy, has been to conceal the value of information." [11]

Following Lanier the WEF argues that individuals not only need to be able to "assert more control" but also be able to *benefit* from the ways in which personal data "is leveraged and value distributed". Thus, the WEF proposes as an "alternative model" that enables personal data to "be used as a utility" by the individual, rather than it being something that is simply handed over to others albeit with appropriate data protection mechanisms in place.

WEF goes on to suggest that this alternative *utility model* might be enabled through the development of Personal Data Management Services (PDMS). It notes "there is growing momentum in the area" and that "more than one new personal data service was launched per week" between January 2013 and January 2014 [21]. PDMS, such as MyDex or OpenPDS, tend to be cloud-based and despite growing commercial interest public uptake has been problematic. A recent report suggests that poor uptake is due to "consumer's perceptions of privacy and security risks" [12]. The situation is compounded by the fact that personal data are distributed across a great many silos (e.g., Facebook, Google, Twitter, etc.), with no standard data formats, no standard APIs for access, and no easy way of obtaining a *holistic* overview. Furthermore, as [5] point out, most personal data do not belong to a single individual but are *social* in nature (e.g., communications data), and PDMS solutions have yet to addressed this foundational matter.

Current approaches do not strike the balance then between data protection and control, let alone enable personal data to be used as a utility for individual benefit. An alternative approach – and one that seeks to put the local control recommendation into practice – is offered by the emerging field of Human Data Interaction (HDI). HDI is premised on the recognition that the pervasiveness of computing in everyday life means that "data are also now ubiquitous"; be it data "created *by* us" or data "created *about* us by others" we are in the midst of a "data-driven" society [16]. Data has become a first-class object in computer science, something meriting attention and treatment in its own right, and the notion of HDI denotes this. It also seeks to "empower individuals" to ensure "that people remain the first consideration of a data-driven society". HDI is not 'just' a distinct topic then, it also has an axe to grid or an agenda more prosaically that may be apprehended when we consider the "core themes" that underpin it.

- *Agency*. If people are to be empowered in the use of their personal data they need to be able to exercise agency. Agency sits at the heart of HDI and seeks to move beyond consent to enable individuals to "engage with its collection, storage and use, [and] to understand and modify raw data and the inferences drawn from it."
- *Legibility*. Agency requires legibility, yet our mundane interactions with online data systems are often opaque. HDI is concerned to make data, and the analytics that are applied

to it, both "transparent and comprehensible to people". This will entail surfacing the data that is being collected and making individuals aware of this, and developing tools and resources that enable data and data processing to be reasoned about by individuals.

- *Negotiability*. HDI recognises that "power in the system is presently disproportionately in favour of the data aggregators", and that there is need to enable individuals to engage in a meaningful dialogue with those parties that would leverage their data. Developing tools that enable people not only to reason about but also broker the use of their personal data is key to empowering individuals. [16]

HDI is not confined to the study of data then, but to affecting fundamental social change through technology development in a bid to redress the current imbalance in power between individuals and those who would consume their data. At the current moment in time the affect is confined to the development of the underlying technical infrastructure required to make conceptual instantiations of HDI such as "Dataware" [14] and "Databox" [3] work. The emphasis placed on individual control in these models lends to the view that HDI is essentially concerned with privacy protection.

" ... the key technical problem in supporting an ecology around my data is ... access and control. ... who gathers, processes and distributes my data; when and to what purpose this occurs; and the means by which I can access it and enable processing applications and services to access it on my behalf." [14]

Privacy is an important facet of HDI, key to redressing the asymmetry in power, but HDI recognises that there is more to the matter than that.

"By redressing the extreme asymmetries in power relationships in the current personal data ecosystem, the Databox opens up a range of market and social approaches to how we conceive of, manage, cross-correlate and exploit 'our' data to improve 'our' lives." [3]

HDI is not 'simply' concerned with privacy then, but seeks to "enable voluntary participation in information marketplaces" [16]. This may not sit well with privacy advocates, however 'simply' enabling privacy protection is not sufficient for the sociological function of the law to be achieved. Proposed legislation does not 'merely' posit a raft of data protection measures and compliance procedures; it posits them to "enhance" and "develop" the "digital economy". If the new social order envisioned by law-makers (not lawyers) is to come about – one in which individuals actively engage in the trade of personal data - technologies and tools are required that enable individuals to both protect *and* exploit their data.

HDI not only seeks to support both, and thus strike the balance between protection and utility, but to do so in novel ways that circumvent the problems faced both by current security-based and PDMS approaches in applying the local control recommendation. Thus the latest concrete manifestation of HDI posits a "physical component", such as a "low-energy computing device" or "augmented home router", which is situated in the home and entirely under the local control of the individual or individuals whose data is "collated" by it. This Databox approach enables individuals to control access to both online (Internet) or physical device (IoT) data, can prevent copies of personal data being made by others by running analytics locally to deliver agreed upon results, and provides a high level of security "including turning it off or completely disconnecting it from all networks".

V. Enabling the New Economic Actor

This may be a short paper but it presents the parts of a complex argument about the law, its intended outcomes, and how these might be achieved. The aim in conclusion is to pull these together for clarity's sake. The core proposition here is that when viewed from a sociological perspective the law, and proposed data protection regulation in the US and Europe in particular, seeks to foster new social organisational arrangements that enable a new kind of economic actor: the individual as data trader. Seen from the sociological perspective the law has a reflexive relationship to social order. It is not 'simply' a mechanism of social control but, in its writing, rewriting and use is shaped by and shapes the social order itself. Furthermore, the social order is not neutral, but manifest in concrete forms of social life: feudalism, socialism communism, etc. Thus, the law functions to maintain particular types of social order, to reshape them, and create them anew.

Proposed regulation in Europe and the US, like its counterpart in Japan, is shaped by and shapes local versions of capitalism. As such, concerns with the economy – and the digital economy in particular – are writ large in draft legislation. While there is much about data protection and compliance in these documents, the overriding social purpose of legislation is to build consumer trust *into* the digital economy. Thus, from a sociological perspective, the purpose of proposed legislation is to further "develop" and "enhance" the particular type of social order at work in the respective jurisdictions. Furthermore, the lynchpin of legislation is a new kind of economic actor, one "empowered" by legislation to exercise "control" over the "flow" of personal data in the digital economy.

Proposed data protection regulation is not 'simply' or 'merely' about putting protection measures and compliance procedures in place then. It is also, at the same time, about shifting the locus of agency and control to enable the new economic actor, a point made perspicuous by the emphasis placed on individual control in proposed EU legislation and manifest concretely in proposed US legislation through the *Individual Control principle*. It is apparent too that the measures proposed by draft legislation to affect this shift are not purely legal in nature. Enabling the new economic actor is not only a concern for members of the legal profession then, but for technology developers as well, who legislators anticipate will drive innovation and provide the tools and resources that will actually enable the actor to exercise control over the flow of personal data and become an active participant in, rather than a passive victim of, the digital economy.

The need to enable the new economic actor through design is underscored by the best practice guidance offered by official data protection bodies, particularly the FTC and WP29, with

respect to Internet of Things devices and applications. These emphasize the building in of mechanisms that put the Individual Control principle into practice: general privacy menus, device toggles, out of band communications, management portals and dashboards, etc., that enable users to make "granular" choices over data collection. The most radical of these is the *local control recommendation* suggested by WP29, which seeks to allow individuals to locally control data processing entities and view, read, modify and edit data *before* they are transferred to a data controller. The local control recommendation provides a radical alternative to dominant security-based approaches that distribute personal data to manufacturers' servers before making it available to the data subject and which, in doing so, do *not* prevent the ongoing abuse of personal data by industry.

The need to enable the new economic actor is further underscored by the WEF, which identifies the asymmetry in power between individuals and organisations as a key driver of the public crisis in trust in the digital economy. The WEF proposes the adoption of a *utility model* that enables individuals to derive value from the trade in their personal data, and suggests Personal Data Management Services provide a way forwards. However, these suffer from a range of issues that make their uptake problematic, notably their inability to provide a holistic overview of personal data or to manage the fundamentally social nature of personal data. Human Data Interaction (HDI) provides a viable alternative to the troubles occasioned by security-based approaches and PDMS. Conceptual models such as Dataware and Databox implement the Individual Control principle and Local Control recommendation to instantiate a Utility Model that both enables privacy protection *and* the exploitation of personal data for individual benefit. HDI is in its infancy. Nevertheless, in combining the core elements of individual and local control with utility, HDI provides an 'in principle' model capable of meeting the sociological purposes of proposed legislation.

Proposed data protection laws are not 'simply' about protecting our personal data from abuse. The law has a reflexive relationship to the social order and thus, in Europe and the US at least, with the continuing evolution of Smith's "new division of labour". If the sociological function of proposed legislation is to be achieved there is need to strike a balance *in design* between privacy protection and enabling a new economic actor equipped with the tools and resources to actively engage in the digital economy. Barak Obama reminds us that we need privacy "now more than ever" [4], but the words of his Democratic predecessor, Bill Clinton, should also ring in our ears when reading proposed legislation – "It's the economy stupid." This is not said to incite or offend, but to emphasize that implementing privacy protection measures through design is not sufficient to achieve the sociological function of proposed regulation. We also need to enable individuals to *extract value* from their personal data, both economic and social, for without this there will be relatively little to regulate. Enabling the new economic actor is key.

ACKNOWLEDGMENT

The author acknowledges the support of the Engineering and Physical Sciences Research Council, grant EP/M001636/1.

REFERENCES

[1] Article 29 Data Protection Working Party, "Opinion 8/2014 on recent developments on the Internet of Things", 14/EN WP233, 2014. http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp223_en.pdf

[2] J.A. Barnes, "Durkheim's division of labour in society", in Man, vol. 1 (2), pp. 158-175, 1966.

[3] A. Chaudry, J. Crowcroft, H. Howard, A. Madhavapeddy, R. Mortier, H. Haddadi and D. McAuley, "Personal data: thinking inside the box", in Proc. of Critical Alternatives, pp. 29-32, Aarhus: ACM, 2015.

[4] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, 2012. www.whitehouse.gov/sites/default/files/privacy-final.pdf

[5] A. Crabtree and R. Mortier, "Human data interaction: historical lessons from social studies and CSCW", in Proc. of the 14th European Conference on Computer Supported Cooperative Work, pp. 1-20, Oslo: Springer 2015.

[6] DARPA Brandeis Program, 2015. http://cacm.acm.org/news/184344-darpa-to-pursue-revolutionary-privacy-tools/fulltext

[7] E. Durkheim, *De la Division du Travail Social*, Paris, Presses Universitaires de France, 1893.

[8] V. Ferrari, "Functions of law", in Encyclopedia of Law and Society: American and Global Perspectives, D. Clark, Ed., Thousand Oaks, CS: Sage, 2007, pp. 611-617.

[9] C. Gates and P. Matthews, "Data is the new currency", in Proc. of New Security Paradigms Workshop, pp. 105-116, Victoria, BC: ACM, 2014.

[10] General Data Protection Regulation, COM(2012) 11 Final, 2012. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:en:PDF

[11] J. Lanier, Who Owns The Future?, New York, Simon and Schuster, 2013.

[12] R. Larsen, G. Brochot, D. Lewis, F. Eisma, and J. Brunini, Personal Data Stores, European Commission Digital Agenda for Europe, August 7, 2015. https://ec.europa.eu/digital-agenda/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school

[13] J. Manyika, M. Chui, P. Groves, D. Farrell, S. Van Kuiken and E. Almasi Doshi, Open Data: Unlocking Innovation and Performance with Liquid Information, McKinsey and Company, 2013.

[14] D. McAuley, R. Mortier, and J. Goulding, "The dataware manifesto", in Proc. of the 3rd International Conference on Communication Systems and Networks, pp. 1-6, Bangalore: IEEE, 2011.

[15] P. Middleton, P. Kjeldsen and J. Tully, Forecast: The Internet of Things Worldwide 2013: Gartner, 2013.

[16] R. Mortier, H. Haddadi, T. Henderson, D. McAuley and J. Crowcroft, "Human-data interaction: the human face of the data-driven society", Social Science Research Network, 2014, http://dx.doi.org/10.2139/ssrn.2508051

[17] A. Smith, An Inquiry into the Wealth of Nations, London, Methuen & Co., 1776

[18] Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society, Policy Outline of the Institutional Revision for Utilization of Personal Data, 2014. http://japan.kantei.go.jp/policy/it/20140715_2.pdf

[19] US Federal Trade Commission Staff Report, Internet of Things: Privacy and Security in a Connected World, 2015. www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-thingsprivacy/150127iotrpt.pdf

[20] K. Winstein, "Introducing the right to eavesdrop on your things", in The Agenda Magazine, July edition, 2015. www.politico.com/agenda/story/2015/06/internet-of-things-privacy-concerns-000107

[21] World Economic Forum, Rethinking Personal Data: A New Lens for Strengthening Trust, 2014. www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf

[22] D. Zimmerman and M. Pollner, "The everyday world as a phenomenon", in Understanding Everyday Life, J. Douglas, Ed., Chicago, Aldine Publishing Company, 1970, pp. 80-103.