Technology Regulation 2.0?

Andreas Mitrakas

Technology regulation 2.0?

Andreas MITRAKAS

Abstract. This paper discusses future ways to regulate technology effectively in an ever accelerating speed of technological development. The current rate of response of legislation to technological evolution is unlikely to allow law keeping up pace with and responding to the needs of society for technology regulation. This is likely to create a rift between on one hand the perceived need of society for technology regulation and on the other, the ability of the legislative to deliver in line with expectations. While the demand for more technology regulation in unlikely to subside, self -regulatory means and tools are likely to increase in prominence, especially if combined with technology in terms of automation. Societal value could be developed in a way that allows legislation to retain its important role in meeting the need for greater control of the evolution of technology. The approach proposed in this paper could be of use to those involved in the governance, service provision or use of technology regulation.

Keywords: Information technology, strategy, regulation, cost benefit analysis, standards, policy, soft law, contracts

1. Introduction

Technology, which is the outcome of creative and innovative mental processes, requires regulation to become usable in society and the economy. Regulation in many ways has provided the safe haven for human ingenuity to thrive, protected, and expand further. In spite of its shortcomings, intellectual property regulation, has provided the ground upon which technology advancements of the industrial and post-industrial ages have come about. In the information age, technology has been driven by private sector initiatives, that seek to penetrate global markets or markets that present comparable features across multiple jurisdictions. Regulating for technology has challenged and often deluded operators, users and legislators alike due to the complexities involved in grasping the often far-reaching consequences of technological innovation. There is an obvious lag between what the legislator sees and believes that technology can do and what technology actually does as it is put to work in a performance driven economic environment. This is no easy rift to bridge and in response Law has sought for decades to restore balance by having Courts interpreting apparently obsolete legislation to render it fit for new purposes. There is no shortage in examples of technology regulation that become obsolete as a result of innovation. This paper reviews some examples of innovations that are credited for the state of art of technology services it then seeks to present an approach on how regulation could evolve to accommodate the emerging needs of technology regulation.

2. Background

Future is determined by such elements as, nascent and emerging technologies the impact of which on society and the economy is not quite appreciated at the time of their emergence. The impact of technology is related to the interaction of emerging technologies with existing ones, the standing need to regulate and the need to organise regulation in a meaningful way that maximises societal benefits from the introduction of technology. However as the pace of technology picks up, the regulation of technology has to follow suit; and this remains a challenge that has yet to be tackled. Current legislative review cycles last long and it is not uncommon that from one "generation" of regulation to the next 20 years lapse; this lag has consequences, as the use of technology under innovative business models eludes the judicial that has to

resort on interpretations to accommodate change. The far reaching consequences of technology are often not understood well enough when a technology is launched or when a technology is put under legislative scrutiny. When applying "dated" laws on new use cases sometimes more space for interpretation is permitted than what is actually needed.[1]

The past two decades have allowed for the fusion of information technology with an array of other technologies accelerating the pace of technology expansion to unprecedented levels. In 1965, Moore's law described a pattern for the exponential growth in complexity and in capacity of integrated semiconductor circuits. Moravec extrapolated Moore's Law to future forms of technology, such as robotic agents.[2][3] Kurzweil suggests that the pace of technological expansion might accelerate further and become the key feature of technological development as early as in 10-15 years.[4]

In the 1960s and through to the 1980s the promise of expert systems gave new impetus to what machines could accomplish to replace humans in carrying out intelligent tasks. Realising that law had a formal as well as an empirical set of attributes that cannot be represented in the same way brought about a break through. Empirical knowledge was brought under the spotlight and it was added as a feature to the requirement of formalised knowledge when seeking to automate legal procedures as it was the case of legal expert systems for example.[5]

Automation in business transactions became yet another frontier to explore. The evolution and widespread use of formalised data structures, i.e. electronic data interchange in select business-to-business processes made automation and exchange of structured business data widespread leading to significant efficiencies marked in terms of costs and working methods. The opening up of telecommunications networks led to the gradual but increasingly more accelerated later pace to develop new products and services. The emergence of the commercialised World Wide Web allowed for further

[1] See, Vernor v. Autodesk, Inc. (555 F. Supp. 2d 1164), that addressed the applicability of the first-sale doctrine to software sold under the terms of "shrinkwrap licensing." The First Instance Court ruled that the transfer of software to the first acquirer that bore the characteristics of a sale gave right to reselling the software under the first-sale doctrine. In appeal, the US Court of Appeals for the Ninth Circuit, (decision of 10/09/2010), reversed the first sale doctrine ruling remanding for further proceedings on the misuse of copyright claim. In a more recent development the Librarian of the Library of the Congress applied this principle on the jail breaking practice concerning smart phones, rendering it illegal under the Digital Millenium Copyright Act (DMCA - Pub. L. 105-304, Stat. 112 Stat. 2860 (1998)), unless the operator agrees to it. This is a development that the legislator of the DMCA, that aimned at protecting the intellectual property rights of content providers, could hardly foresee in 1998.

[2] See, Moore, G.E. (1965). Cramming more components onto integrated circuits. Electronics, 38:8

[3] Moravec, H. (1998). Robot: Mere Machine to Transcendent Mind, OUP,

[4] Kurzweil, R., (2006). The Singularity is Near. Gerald Duckworth & Co Ltd.

[5] Leith, P. (2010). The Rise and fall of the legal expert system. European Journal of Law and Technology, 1:1

inroads in terms of automation and decision support and commoditisation of information. Intelligent agents have been able to collect preferences, make suggestions and support decisions made by consumers in large applications environments for electronic commerce. Large scale reputation systems profiled users enhancing the sense of trust that consumers and business users alike can show in a transaction. In a case regarding transactions with private and public bureaucracies, an intelligent agent would fetch information from various sources, i.e. libraries to present it to the requestor according to a predefined set of presentation rules and help the requestor accomplish an organisational goal.

On the regulatory side the need to protect personal data from undue breaches led to the adoption of data protection legislation. While the first concrete piece of European legislation on data protection was voted in 1995, in January 2012, the European Commission proposed a sweeping reform of the EU data protection rules of 1995. The 1995 rules had been interpreted differently by the 27 member countries, which led to inconsistent enforcement. The new proposal suggests a single law that will apply to all members of the EU. This proposal is now under legislative scrutiny by the European Council and the European Parliament before becoming a final law in 2015.

In another instance of proposed regulation, the Proposal for a Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market claims a technology-neutral approach, an objective which is largely attained to throughout. This proposal however addresses specific technologies used in relation to electronic identification and trust services for electronic transactions in the internal market. These services include but are not limited to, electronic signatures, electronic delivery, web site authentication etc.

3. Technologies of the day after tomorrow

Various technologies are likely to play a key role in the years to come, and shake the current technology pattern by providing a breakthrough. Obviously the technology landscape will not only be influenced by technology. It is likely, however that a small number of them might change pre-determined patterns, shifting social and regulatory interactions related to these technologies. The impact of these technologies is such that unless grasped early enough by the legislator with a view to re-evaluate its regulatory strategy, they are going to be disruptive in a way that regulating them becomes dysfunctional.

Big data

Big data is extremely large sets of data related to consumer behaviour, social network posts, geo-tagging, sensor outputs, and other types of tags and meta-tags that associate human behaviour with data.[6] On the outset big data is the output of devices and sensors that consumers, organisations and devices use across the globe to go about their lives and business. Data is generated due to human or machine activity; it is recorded by means of information systems that are hosted typically in large data centres on the cloud. Big data is an extended representation of human activity and behaviour in all walks of digital life and beyond. Leveraging on big data broadens the ability of individuals and organisations to interact, as well as monitor, control and evaluate such

[6] Johnson B.D. (2012), Big data; Still to come? The Futurist. 46:4.

interactions. It is likely that big data will pose such challenges as access to data, privacy, data formatting and challenges for security.

Agent driven identification and authentication technologies

In the draft European Regulation on electronic identification and authentication services legal persons are afforded the ability to sign independently of the natural persons involved in their management, like a general manager representing the organisation for example.[7] In view of the explicit permission for legal persons to sign an additional extension could be considered to legally permit intelligent agents to sign for the purpose of non-repudiation. If intelligent agents are not explicitly permitted to sign with an electronic signature and bind for example a natural person, would it be within reach to incorporate an intelligent agent and have it sign on behalf of the incorporating company, which as legal person is allowed to sign on its own.

This is a theoretical argument for the time being of course, but in the course of the next few years leading to implementation of this Proposal, signatures for intelligent agents are likely to become a necessity.

As technologies become ubiquitous in the next 2-5 years that is the period in which this Proposal will be voted and its implementation will be launched it is likely that the next legislative action in the area of electronic identification and authentication will be in a period shorter that the 15 year that that Directive 1999/93/EC claimed from launch as a proposal till sunset. It is likely that legal capacity of agents to conclude legally binding acts might be challenged, especially in view of possible combinations with other provisions such as incorporating an intelligent agent. Further to the capacity to act, other areas might include the validity of a legal act signed by an agent, the evidence required to prove an act and the value of such evidence. Information security and privacy aspects are likely to become of importance too as accessing the data storage of the intelligence agent might reveal patterns related to natural persons.

Coming to terms with the law of accelerating returns

According to Kurzweil "an analysis of the history of technology shows that technological change is exponential, contrary to the common-sense "intuitive linear" view. So we won't experience 100 years of progress in the 21st century — it will be more like 20,000 years of progress (at today's rate). The "returns," such as chip speed and cost-effectiveness, also increase exponentially. There's even exponential growth in the rate of exponential growth.'' Within a few decades, Kurzweil claims, machine intelligence will surpass human intelligence allowing a merger of biological and non-biological intelligence."[8] In an era of unanticipated technological developments, assessing the capacity to transact of new types of human intelligence might be required.

4. Towards regulating potentially disruptive technologies

[7] Proposal for a Regulation of the European Parliament and of the Council on Electronic identification and trust services for electronic transactions in the internal market (COM(2012) 238).

[8] See, http://www.kurzweilai.net/the-law-of-accelerating-returns (visited on 30/01/2013).

Even before the notion of exponential technological growth was introduced, the impact of technology had been typically disruptive due to the new and sometimes uncalculated elements that it introduced in society, as it was applied. Disruptions might not be visible to the unaware observer from one stage to the next however the impact technology has other societal expressions has a dramatic effect. New business ideas that rely on technology appear and old ones that are based on obsolete or concurrent technologies become extinct. It is quite challenging to have new technologies rooting as viable business ideas especially as they seek to compete with other established ones that in terms of business cycle they resonate well with the users. Some aspects of the economic perspective of regulation, that seeks to address the governance, social and economic order beyond regulating rights and obligations of parties involved is further presented.

The efficiency of a proposed regulatory solution can be analysed on the basis of the Coase theorem that provides us with the notion of what efficiency means when making an agreement.[9] Coase suggests that a contractual solution must take into account three factors: transaction costs, the efficiency of the outcome and the legal framework.[10] By considering these variables a solution can be reached. The efficiency of a contract also depends upon factors such as the social context, the transaction costs and the legal reality of the environment in which the legal solution is applied. If the cost of obtaining information in order to draw up a service agreement concerning information security services is too high, other solutions should be sought instead.[11] If we apply this theorem in the regulatory area for technology we can consider that regulation is preferred when unfettered access to information is available; i.e. access to access to all possible future uses of technology is clearly described, sufficiently understood and anticipated before the regulation is proposed.

In a mature technology environment, where a broad selection of technologies and regulatory instruments are available, several factors influence the final regulatory outcome. These factors include negotiation power of the key actors, the expertise they have, access to resources, the timetable to fulfil the desired level of implementation, etc. In general to decide on whether regulation is required the regulatory burden (RB) of legislating, monitoring compliance and enforcing should be calculated and pondered against the perceived market distortion costs (MDC) due to the associated with the lack of regulation. The relationship could be presented as follows:

$$RB<MDC$$

In regulating technology, law has experienced long return cycles that allowed for consolidated views to emerge, consensus with regard the proposed legislative arrangement to emerge, those who could potentially disagree to drop out of grace or be taken over or having their views represented by others who sought the proposed legislative solution. There are numerous examples of legislation that even in the more

[9] Posner, R., (2003) *Economic analysis of Law*, New York: Aspen Publishers.

[10] Mitchell Polinsky, A., Shavell, S. (2010). *The Uneasy Case for Product Liability*, Harvard Law Review

[11] A. Mitchell Polinsky, S. Shavell, *The Uneasy Case for Product Liability*, forthcoming, Harvard Law Review (forthcoming), 2010, pp. 31-34.

recent past of rapid technological growth required return cycles of fifteen years to pass from one generation of legislation to the next.

There is little doubt that the role of technology is likely to expand further and penetrate yet new levels of human activity in the society. Further regulation will remain a requirement. However in view of the accelerating pace of development it is doubtful that in a few years from now there will be sufficient time to effect regulatory evolution the way we are used to do. Those long review cycles are likely to be reduced to a few months or weeks, reducing the capability of the legislator to respond, or deeply understand the implications of both technology and regulation. This alone would not be the problem of course; the issue is related with the societal impact that the inability of the legislative process to bring about regulatory impact will have. While large swaths of technological activity would remain under regulated or outside regulatory scope the impact of the lack of regulation would be stark denying business and citizens protection from abuse and the ability to enforce rights.

The remainder of this paper presents an overview of possible approaches that are likely to alleviate the innovation pressure on societies that not necessarily in need.

5. Seeking to regulate in the age of exponential growth

The pace of regulation is not likely to take a recess; however the way regulation is promulgated is likely to face new challenges with the advent of ever shorter technology cycles that bring disruptions along with them.

The accelerating disruption cycles paradox

It is also likely that the need to govern the cross-border impact of technology as well as the countering of threats to society that are brought about by technology will also pick up pace. Therefore a paradox is likely to emerge being that from an ever narrower window of opportunity due to the accelerating disruption cycles more regulation will be demanded; this is likely to impact future regulatory strategies. This situation is unlikely to be sustained, should the legislator resort on currently available methods and means. A combination of efficient means is likely to emerge to facilitate the legislator in bringing about regulatory change and following the pace of technological development.

The remainder of this paper reviews some models that could bear fruit when seeking to invoke self-regulatory elements in information technology without necessarily resorting to new legislative instruments. While the legislative impetus on information technology is likely to pick up further in the future, concurrent approaches could help reducing the effect of the long legislative process on trade partners.

Commoditising valuation models

The valuation of goods and services is likely to be more in demand. In case of civil wrongdoing, like when a contract is breached it is essential to reckon what has been the value of the wrongful act done. The answer very much depends on the value that the goods or services had at the time the wrongful act occurred. There is a direct relationship between the goods or services in question and the markets in which these values are measured. If A is involved in a car accident with the 10-year old car that belongs to B, clearly A owes damages to B, however those damages will be discounted

in a way that reflects the net present value of the car at the time of the accident, rather than the value of the car when new. Is B is unhappy with its valuation because of the emotional value that this good carries for him, additional elements might have to be inserted in the calculation to satisfy B (the answer cannot be to damage something of emotional value to A); this of course might be a difficult calculation, as the only objective way to value that car is to base it on a market calculation.[12]

If the goods at risk are intangible, the example might have a different outcome. Home videos on a memory stick have to be transferred to different media in a shop; the clerk pays attention but somehow the home videos are lost. If the possibility to lose a video is 1/1000 then how would these videos be valuated? The photo shop clerk offered to deliver the videos in a steel box and never lose them against an extra fee of 100 Euros. The client is faced with the dilemma of insuring against a non-valuated item. Suppose the client decides to pay the premium then the valuation he attaches to it is 100 * 1000 = 100 000 Euros.

But how can data owners assess their potential damages by themselves, in information security? Although this might sound unusual, it is not; insured parties typically carry out an implicit risk assessment as well as a self-assessment of the value of the insured goods or services before they turn to an insurance broker to get a quotation. A self-assessment of the possible value of the information that is under threat is a first but critical step down the road of securing information. And this is a step that the information owner who is the user of the information security services has to take. There is a discreet benefit in following this approach, as the information owner is likely to have to take two dimensions of the problem into account: the information owner will want to state a low value to keep his insurance premiums down but if he states too low a value, then the value of his intangibles might be deemed to be too low for his overall business valuation.

A different situation arises from a combination of data that serves invariably personal and professional proposes; such is the case of a home office where a professional stores home videos and company data alike. What would the value of the loss of data be in this case? While information security measures can indeed by employed to protect private and professional data alike, it is highly unlikely that the valuation of the loss of data will be identical for both categories of data. When seeking benchmarks, the "willingness to pay" comes forward as a proper measurement to benchmark the situation. Suppose that an airbag costs 100 Euro and that every 10 000 purchases an airbag gets to save one life; in this case 1 million is spent to save one life, which sets the benchmark for a price tag on a life to 1 million. The purchaser is protected from this 1/10 000 chance to lose his life in an accident involving the use of an airbag. If airbags were priced at 1000 Euro and people stopped buying them this would mean that the price on life is below the 10 million mark.

In technology the impact of the loss of information has to be valuated by the client as we are talking about intangibles that typically carry subjective value that might only be of importance to the owner of that information. There is information of course that

[12] Ward Farnsworth, *The Legal Analyst: A Toolkit for Thinking about the Law*, University Of Chicago Press, 2007, location 4364.

serves purposes that can be determined in an objective manner, like it is the case of tax related data held by the tax payer. As cloud service providers proliferate their services it is likely that increasingly more data will flow from proprietary data centres that operate at arm's length to cloud based services. If the jurisdiction of protecting data in transit or at rest has not been determined it is likely that the client might find herself in a challenging situation if data is wrongfully handled, tampered with or outrightly lost.

Valuation models for data are likely to be further developed for the purpose of facilitating trade partners and consumers alike in a way that allows them to better leverage on new business models.

Cost benefit analysis

What are the appropriate organisational arrangements concerning risk quantification that allow the data owner to properly value and assess the value of the data under her control? In the air safety or maritime safety areas, government agencies set the stage of standards and metrics required to meet the safety expectations of the industry. This is a top down approach that has evolved over time and it ensures that benchmark requirements are in place and they are met. An alternative approach is to take a contingent valuation whereby the target group is surveyed as to how much they are prepared to pay in order to avoid a certain result from happening.

Cost benefit assesses the total expected costs against the total expected benefits to obtain the most profitable option. Quantified benefits and costs are adjusted in order to calculate their present value. Economic efficiency is taken as a criterion to assess the relative merits of two situations and then decide which one is the best able to maximize social welfare, after taking into account social costs and benefits. Cost-benefit analysis is developed as a subject in order to be a practical guide to social decision-making by evaluating social costs and benefits with private costs and benefits. It is often the case that the project should go ahead while the benefits to society as a whole from the project are greater than the benefits of any individual pertaining to this project. The efficiency effect of a project is the difference between costs and benefits. In order to calculate the social costs and benefits it is necessary to consider also private costs and benefits as well as externalities.[13] A cost-benefit analysis allows to objectively assessing the benefits deriving from a certain action. However the criteria used in a cost-benefit analysis are typically rigged by the subjective views of the party that carries out such analysis. Cost-benefit analysis refers to assessing, the case for a project, and program or policy proposal for the purpose of supporting decision making.

The highlights on this area include certain aspects that provide assurance to the parties involved. Self-regulatory efforts that can take the form of invariably seeking compliance with the policies and technical standards in the application area; setting out a contractual framework that involves all parties in an information security framework regardless of them being service providers beneficiaries or relying parties etc.

[13] Weixiao Wei, (2008) *ISPs' Indirect Copyright Liability Regime: An Economic Efficient Liability Regime for Online Copyright Protection Shaped by Internet Technology*, Bileta Conference Proceedings.

In terms of quantifying liability as such the aspects that can be considered include the calculation of a cost benefit co-efficient that can be used to assess the value extracted from the information security measures employed. Additionally a market valuation should be made available that sets out the value that data represents for the data owner vis-a-vis its market usability; low value personal data can be set with the lowest value, while high value professional data can be assigned with a high value.

Most importantly an assessment of what data represents for the information owner stands at the centre of this approach that aims at determining the liability emanating from loss of data in case of an information security breach.

Standards for self-regulation

Information technology woes are often addressed by means of voluntary frameworks self-imposed by the trade partners themselves. These frameworks include policies and agreements that aim at setting up the conditions for information security safeguards within an organisation, or in transaction frameworks. At a bilateral level, the parties use service level agreements to specify the quality service they seek from their provider and ensure availability rates for their applications. Parties might set up security frameworks, which are activated by means of subscriber agreements executed individually. In this later example the service can be a generic one that does not necessarily allow for a high degree of customisation. Information security assurance can be provided for by adhering to international standards. Regardless of the form information takes, or means by which it is shared or stored, it should always be appropriately protected.

Standardisation in the EU has gradually assumed an approach that contains covers up for limitations emanating from a strict legislative process that can be seen as too narrow to address business and society needs.[14] Technical standards, thus, provide a layer of "soft law" that deviates from a strict legislative approach; in promulgating "soft law" standards, the industry often has a leading role.[15]

Liability assessment tools

A model is further presented hereunder to support the process of assessing liability. The application area of this very model is limited and it presents a calculation model that aims at quantifying liability. This conceptual Information Security Liability Assessment (ISLA) tool aims at easing typical shortcomings associated with the assessment of the value of information in a given operational environment that pose discreet shortcomings to the ability of risk takers to determine and apportion their liability exposure.[16]

[14] Standardisation policy in the EU dates to the *Cassis de Dijon* case in which the European Court of Justice ruled that a product meeting the requirements of one member state should be legally made available in another; allowing the emergence of mutual recognition of technical standards as a matter of significant interest in the EU internal market (ECJ 120/78 of 20/02/79).

[15] Senden, L., (2002). Soft law in the European Community Law. Hart Publishing.

[16] Mitrakas A., (2011) Information security liability: an assessment model, in P. Kleve, P., Noortwijk van, K., Something bigger than yourself: Essays in honour of Prof. R. V. De Mulder, Rotterdam: Erasmus University Rotterdam; See also, Mitrakas,

ISLA: Information Security Liability Assessor	
Assessment criteria	**Representation value**
Own valuation of data	10
Market valuation (market risk co-efficient)	0…+3
Cost benefit	0...+2
Policy (audited and compliant)	+1
Contract	+2
Standards	+1
Worst case	-3 (variable)

The model works as follows: the information owner has to determine the value of the data (DV) that he seeks to protect by means of information security measures. A market value (MV) factor represents the social impact of the data loss. In this case a scale form 0-3 is permitted where 0 denotes strictly personal, no value data and 3 represents the high grade professional data to be protected.

A cost benefit (CB) analysis indicates whether there is need to outsource the task of information security or it makes better sense to carry it out as an in sourced one. Acceptable values range from 0 to +2 to denote the efficiency rate of a solution, with low figures referring to own solutions and a higher figure leading to high risk that are mitigated with high protection alternatives.

There are 3 conditions that could ease things up if properly implemented, and these include, a strict and adhered to policy framework (P), a contractual framework (C) and the implementation of technical standards (S).

It is advisable to remove points if a "worst-case scenario" (WS) has to be provided for, like in case of high risk operations. We then derive the following formula that helps assessing the estimated liability (L) exposure.

$$L=((DV*MV)/CB)*((P+C+S)-WS)$$

The higher the result the more valuable the data asset is assessed, which boosts in return the liability in case of an information security breach. The overall results can be utilised in an operational context to determine the liability of an information security breach.

Clearly this model does not provide an absolute instrument to determine liability and variations or interpretations might be necessary in some cases. Isla can, however be used in a coherent manner when seeking to determine the liability of service providers or users of information security services.

A., (2011) Assessing liability arising from information security breaches in data privacy, International Data Protection Law Journal, Vol. 1, Issue 2, Oxford: Oxford University Press.

6. Back to the (legislative) future?

When seeking to lay out legal strategy for future legislative action that meets new technology challenges, it is extremely hard to make predictions of course. The legislator has the ability to determine the way it passes legislation anyway, hence this article rather than making predictions seeks to present a snapshot of what is possible. The challenge posed by technology ahead is associated with rapid change. Long legislative cycles are unlikely to survive as a way of addressing the regulatory requirements of technology. Nevertheless, the demand for legislation to regulate technology is likely to increase. Legislation is thus likely to have to be more geared towards a two-tier model, where at the top tier, a broad brush approach based on principles and governance will be adopted. At this level the high level issues such as principles, a governance model and methods are addressed. At a lower level the implementation will be organised around the needs for benefiting from new technologies, quick liability simulations or rapid extra-judicial settlements, by means of automated agents. To support regulatory needs methods that draw their origin from other disciplines are also likely to emerge. At the European level standardisation has been the typical has example that has been leveraged upon to deliver regulation according to predefined models supported by the parties upon which regulation is directed.[17] Other models might include cost benefit analysis, risk assessments and more technology oriented ones such as liability valuation models.

7. Conclusions

The impact of technology on society has led to numerous efforts to address technology governance and transaction risks by means of legislation. The pace of legislation with long review cycles is likely to be affected in the light of technology convergence and the emergence of new technologies that further accelerate the technology life cycle. In the near future it is likely that the legislative process will have to pick up pace to match that of technology. This is a challenging matter. Alternative strategies can be developed to allow for the regulation of technology by reducing that the legislative process has. In this paper we presented an array of instruments that can be seen as a way to regulate technology and user behaviour in a world of accelerating technology cycles.

Note

This paper expresses the author's personal views only and not those of any other party including his employer in any way whatsoever. This paper cannot be associated with any deliverable, report or opinion of the author's employer.

References

Farnsworth, W. (2007). The Legal Analyst: A Toolkit for Thinking about the Law, Chicago: University Of Chicago Press, (Kindle version, location 4364).

Johnson B.D. (2012), Big data; Still to come? The Futurist. 46:4.

[17] Mitrakas A., and Eecke van P. (2005). Commentary on Directive 1999/93 on a Community framework for electronic signatures, in Buellesbach, A., Poullet, Y., Prins J.E.J. (eds.). Alphen aan de Rijn: Concise European IT Law, Kluwer Law International.

Kurzweil, R., (2006). The Singularity is Near. Gerald Duckworth & Co Ltd.

Leith, P. (2010). The Rise and fall of the legal expert system. European Journal of Law and Technology, 1:1.

Mitchell Polinsky, A., Shavell, S. (2010). The Uneasy Case for Product Liability, Harvard Law Review.

Moore, G.E. (1965). Cramming more components onto integrated circuits. Electronics, 38:8.

Mitrakas A., (2011) Information security liability: an assessment model, in P. Kleve, P., Noortwijk van, K., Something bigger than yourself: Essays in honour of Prof. R. V. De Mulder, Rotterdam: Erasmus University Rotterdam.

Mitrakas, A., (2011) Assessing liability arising from information security breaches in data privacy, International Data Protection Law Journal, Vol. 1, Issue 2, Oxford: Oxford University Press.

Mitrakas A., and Eecke van P. (2005). Commentary on Directive 1999/93 on a Community framework for electronic signatures, in Buellesbach, A., Poullet, Y., Prins J.E.J. (eds.). Alphen aan de Rijn: Concise European IT Law, Kluwer Law International.

Moravec, H. (1998). Robot: Mere Machine to Transcendent Mind, OUP.

Posner, R., (2003) Economic analysis of Law, New York: Aspen Publishers.

Senden, L. (2001). Soft law in the European Community Law, Hart Publishing, Oxford, 2004.

Weixiao Wei, (2008) ISPs' Indirect Copyright Liability Regime: An Economic Efficient Liability Regime for Online Copyright Protection Shaped by Internet Technology, Bileta Conference Proceedings.