University of New South Wales Law Research Series

DATAVEILLANCE REGULATION: A RESEARCH FRAMEWORK

ROGER CLARKE AND GRAHAM GREENLEAF

UNSWLRS 84

UNSW Law
UNSW Sydney NSW 2052 Australia

E: unswlrs@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Dataveillance Regulation: A Research Framework

Roger Clarke and Graham Greenleaf

7 November 2017

Abstract

Dataveillance is the systematic creation and/or use of personal data for the investigation or monitoring of the actions or communications of one or more persons. It emerged in the 1980s, initially as a set of tools for exploiting data that had already been collected for some other purpose. Developments in information technologies, combined with a voracious appetite for social control among government agencies and corporations alike, has seen dataveillance practices diversify and proliferate.

The regulatory frameworks that enable and control dataveillance activities appear not to have attracted a great deal of attention in the literature. Data privacy measures, usually referred to as (personal) data protection, have been the subject of a great deal of activity in legislatures, resulting in many countries having data protection oversight agencies and a modest level of jurisprudence. On the other hand, provisions that enable rather than constrain dataveillance are voluminous, both pre-dating data protection laws, and passed subsequently and hence often qualifying or over-ruling them.

This paper presents an initial survey and structuring of the field of dataveillance regulation in a manner intended to facilitate the conduct of research in the area. Its scope extends well beyond legislation to encompass all forms of regulatory mechanism. It identifies ways in which the effectiveness or otherwise of regulatory schemes can be evaluated. It suggests a classification scheme that can be applied to dataveillance regulation through technology and by law. This lays, we believe, a foundation for the analysis of the regimes in particular jurisdictions whereby dataveillance practices are regulated, for comparisons among jurisdictions, and for comparative evaluation of degrees of freedom and of authoritarianism.

Contents

1. Introduction

The practice of dataveillance as a means of social control was identified and named over 30 years ago, although examples of the practice have a longer lineage. It has been actively documented, studied and discussed since then. However, there is a only a limited literature on its regulation, even by the more formal kinds of regulatory measures. This paper provides a preliminary review of this as-yet under-researched area. We use the term 'dataveillance regulation' for all measures that have the intended or even incidental effect of influencing dataveillance practice, and the term 'dataveillance law' to refer to legislation, and other aspects of law, that, whether by design or otherwise, have a regulatory effect on the conduct of dataveillance.

A clear understanding of dataveillance is needed for the analysis of relevant regulatory arrangements in any particular jurisdiction, to enable comparisons among jurisdictions, and for evaluation of the degrees of freedom and of authoritarianism respectively enjoyed and suffered by residents of different countries as a result of dataveillance practices. This paper's primary purpose is to establish a framework for the field of dataveillance regulation which will facilitate the conduct of research in the area, by ourselves, and by others.

The paper commences with a discussion of the meaning of the term 'dataveillance', and the various kinds of dataveillance practices. It then outlines the various forms that dataveillance regulation may take, and summarises the characteristics of an effective regulatory regime. Because of its significance, regulation by dataveillance law is then discussed in greater detail. A small set of modalities is defined, and examples are provided. The classification scheme is at this stage provisional, and more a typology of 'ideal types' rather than a formal taxonomy. Some examples are provided from jurisdictions with which the authors are familiar. The final section considers the value that can be derived from a deeper understanding of dataveillance regulation generally, and dataveillance law in particular.

2. Dataveillance

Dataveillance was originally defined as the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons (Clarke 1988). The analysis distinguished personal dataveillance (of an individual known to be of interest) from mass surveillance (whose purposes include to identify individuals of interest).

Since 1988, the theory has been extended in several directions. An important underlying concept is the 'digital persona'. This refers to "a model of an individual's public personality based on data and maintained by transactions, and intended for use as a proxy for the individual" (Clarke 1994a, Karnow 1994, Clarke 2014a). Whereas physical surveillance has its focus on the individual's body and its behaviour, dataveillance watches the shadow that the person casts as they conduct transactions, variously of an economic, social or political nature. Arguments have been made for control by the individual of the digital persona used to represent them (Gowder 1999).

Other extensions to the theory of dataveillance have included deeper consideration of specific techniques such as profiling (Clarke 1993), data matching (Clarke 1994d) and the monitoring of search-terms (Zimmer 2008), articulated models of identification (Clarke 1994c, 2009b) and of location and tracking data (Clarke 2001, Clarke & Wigan 2011,

Michael & Clarke 2013), analysis of dataveillance's support for authoritarianism (Clarke 1994b), the challenges it creates for law (Froomkin 2000) and for political freedom (Clarke 2008), and the impact of the 'big data' movement (Wigan & Clarke 2013). Michael & Michael (2010) have charted the integration of dataveillance within the broader notion of überveillance. Meanwhile, Brin (1998) has proposed protection through transparency rather than secrecy, in particular by ensuring that people who conduct monitoring of others are themselves subject to monitoring; and Mann et al. (2003) has argued that the antidote to unchecked surveillance (of the weak by the powerful) is the conduct of 'sousveillance' (of the powerful by the weak), desirably at a similar level of intensity, which Mann refers to as 'equiveillance' (Mann 2005).

A framework for the analysis of all forms of surveillance is provided by Clarke (2009a). Of particular importance is what that paper refers to as the 'dimensions' of surveillance: What? for Whom? by Whom? Why? How? Where? and When? Consideration of the last question of When? enables important distinctions among categories of dataveillance to be drawn, including the temporal aspects discussed below.

At the time the term 'dataveillance' was first exposed at a conference in 1986, the focus was on the appropriation of data that had already been collected for some governmental or business purpose. During the intervening three decades, dataveillance technologies have proliferated, the costs of conducting dataveillance have declined, and the application of dataveillance techniques has greatly increased. As a result, the demand for data to which they can be applied has spiralled upwards, and many new data gathering activities have emerged.

It is therefore now more accurate and useful to adopt a modified definition of dataveillance by referring to personal data rather than to the systems that process it, and by including explicit reference to data gathering. The revised definition is:

Dataveillance is the systematic creation and/or use of personal data for the investigation or monitoring of the actions or communications of one or more persons.

To give a sufficient indication of the extent of dataveillance in current societies, we need to consider its temporal aspects, and its relationships to other forms of surveillance.

There are four temporal aspects of dataveillance (Clarke 2009a, Table 3B). The timeframe in which surveillance is conducted may be: ephemeral; across a single span of time; across recurrent spans (such as a particular span within each 24-hour cycle); or scattered across time (e.g. triggered by particular conditions detected in published text, uttered words and recorded behaviour). The intensity with which surveillance is conducted may be once-only, repeated, continual, or continuous. The persistence of consequences of surveillance may be ephemeral, because it is limited to observation; short-to-medium term, because it is recorded; or long-term or permanent, because it is archived. The time-period within which surveillance is applied may be: the present, through real-time use; the past, through retrospective use; or the future, through prospective or 'predictive' use. A full understanding of any particular instance of surveillance requires that it be considered against these four temporal dimensions.

There are many forms of surveillance (Clarke 2009a), which can involve observation but not necessarily recording. This applies to physical observation, including audio and video streaming to another location, communications surveillance (e.g. 'wire-taps', where messages are intercepted), location surveillance (where geographical coordinates are

streamed to another location), experience surveillance (e.g. where a person's reading patterns are observed, or streamed to another location), and bodily surveillance (where measures of a human are displayed, or streamed to another location).

These forms of surveillance can be correlated with the various dimensions of privacy which have been identified, usually such that each dimension of privacy has one form of surveillance primarily correlated with it. Analyses propose five (Clarke, 1997), or even nine (Koops et al 2017) dimensions. Analyses propose between five 'dimensions' – privacy of the person, and of personal communications, data, behaviour and experience (Clarke 1997) and nine 'types' – bodily, spatial, communicational, proprietary, intellectual, decisional, associational, behavioral and informational privacy (Koops et al 2017). A reconciliation among four such proposals shows that the analyses' focal points are variously privacy interests, harms, rights and protections (Clarke 2017a).

Where these other forms of surveillance do give rise to recorded data that may be identifiable, they constitute dataveillance and fall within-scope of this discussion. Such dataveillance arising from other forms of surveillance is particularly important and increasingly pervasive, as can be seen from these examples:

- physical surveillance that results in recording of audio, image or video that may be able to be associated with an individual
- communications surveillance that expresses ephemeral messages as recorded data, (as occurs with email messages including logs and archives, recordings of telephony intercepts, etc.), or records metadata about messages (as occurs with telephony 'call data' and ISPs' logs including under 'data retention' schemes)
- behavioural surveillance that results in recorded data, such as recorded CCTV images, and logs and recordings of the electronic activities of such categories of people as employees and students
- location surveillance that results in recorded data, such as automated number plate recognition (ANPR) systems, where the scheme not merely enables actions in relation to the very small percentage of apparently infringing drivers and vehicles, but also results in logs of vehicle movements
- experiential surveillance that results in recorded data, such as search-terms used, web-pages fetched, reading materials downloaded, and reading materials read
- bodily surveillance that results in recorded data, such as measures of human characteristics, including 'biometrics', whether of the nature of identification and identity authentication measures, or physiological indicators such as heart-rate, and signals transmitted by embedded and otherwise closely associated eObjects (Michael & Michael 2014, Manwaring & Clarke 2015)

The concept, technologies and practices of dataveillance are therefore multi-facetted, and substantial bodies of research exist. Without considering synonyms such as ‘data surveillance’ or ‘information surveillance’, since being coined in 1988 the term ‘dataveillance’ was used in only 584 papers (37 p.a.) from 1988-204, but then in over 3,400 papers (250 p.a.) from 2005-17, with a peak of about 450 in each of 2016 and 2017 (all figures from Google scholar). The citation history of the original 1988 paper on dataveillance is also indicative, having averaged 9 citations per year until 2004, but averaging 40 p.a. since then, peaking with about 50 in each year 2013-17, despite being almost three decades old. Dataveillance is therefore a concept which is of substantial and increasing interest.

We conclude that it is time that closer attention was paid to the means by which laws and other regulatory measures both enable and control dataveillance.

3. Categories of Dataveillance Regulation

Dataveillance is subject to many different influences, which may variously stimulate or constrain its use. Constraints are of many kinds, including preclusion of practices, the setting of pre-conditions in the absence of which dataveillance cannot be used, and the setting of post-conditions that apply to its application. This section briefly reviews the various forms of influence that are of a regulatory nature. The term 'regulation' refers to the exercise of control or governance over activities (Baldwin & Cave 1999, Braithwaite & Drahos 2000). It accordingly encompasses all forms of constraint and extends to enablement in the passive sense of permission, and possibly in the more positive senses of encouragement and even stimulation.

Clearly, law is one major form of regulation. A narrow interpretation of law is that it is rules imposed by a politically recognised authority. In the categorisation used by Clarke & Bennett Moses (2014), for example, law corresponds primarily to only the first of four forms of regulatory mechanism: formal regulation ('government'); co-regulation; industry self-regulation; and organisational self-regulation ('governance')

An expansive interpretation of law, on the other hand, might recognise a much broader set of phenomena, including the 'soft law' in the third category here:

- **Law made by the State**, including legislation, both primary & delegated (such as regulations); treaties that bind the State; decisions by courts and tribunals, which influence subsequent decisions (depending on the jurisdiction and on court hierarchies); and, in principle at least, 'meta-regulation' (Gupta & Lad 1983, Parker, 2007), whereby the regulatee is subject to a requirement to satisfy some broad regulatory principles
- **Law made by Private Entities**, but endorsed and enforced by the State including contracts, co-regulation, and perhaps binding self-regulation
- **Quasi-Legal Instruments** that are customarily observed by at least some organsations, but which lack enforceability. Possible examples include MOUs between local and international enforcement bodies, Guidelines published by oversight agencies, and, even less convincingly, industry self-regulation, corporate self-governance, and 'soft meta-regulation', e.g. in the *Privacy Act 1988* (Cth): "a media organisation is exempt ... if ... [it] is publicly committed to observe standards that ... deal with privacy ... and ... have been published" (s.7B).

Co-regulation is a cross-over point between self-governance and external governance (Hepburn 2006). It involves the establishment of a Code or Standard within a legislative context that makes the requirements enforceable. However, organisations that are to be subject to the regulatory measure have significant input to the requirements, in some cases to the point of writing them. Advocates for the nominal beneficiaries of the measures may or may not be invited to participate, and may or may not have material influence in the drafting of the document.

Mechanisms other than law also have regulatory influence on dataveillance. In more general contexts such as cyberspace regulation, they have been categorised in varying ways, including in Lessig's well-known categorisation of code, norms and markets (Lessig

1999a, 1999b and drafts from 1995), but also by other proposed categories such as 'intrinsic controls' (Clarke 1995) or 'natural controls' (Clarke 2014b).

The category of regulatory activity that Lessig referred to as ‘code’ ('West Coast Code', to distinguish them from formal laws or 'East Coast Code'), is better described as the architecture and infrastructure of cyberspace, and consists of considerably more than software including standards, protocols, hardware and in some instances biometrics (Greenleaf 1998). Architecture/infrastructure has very significant effects on regulating dataveillance, both by enabling it, and by intentionally or incidentally placing limits on its practice or effectiveness by such mechanisms as default settings, message encryption, pseudonymous identities and obfuscatory routing.

The regulation of dataveillance by architecture and infrastructure can be further categorised into a number of modalities. In Table 1, we provide a tentative set of such modalities. These encompass technologies that do and do not enable dataveillance, technologies that only enable dataveillance if the individual takes some particular action, and technologies that enable dataveilllance unless the individual performs an action of the nature of denial or circumvention. The following section adopts a related but somewhat different approach to regulation by 'dataveillance law'.

Table 1: Modalities of Dataveillance Regulation by Architecture and Infrastructure

1.	sion	**'You can not'** Design features that, whether intentionally or incidentally, do not support dataveillance activities, and may even prevent them
2.	Participation	**'You can not, unless'** Design features that, whether intentionally or incidentally, do not support dataveillance activities, and may even prevent them, unless the individual who is, or whose devices or traffic are, subject to dataveillance takes some action to enable it
3.	t Participation	**'You can, unless'** Design features that, whether intentionally or incidentally, support dataveillance activities, unless the individual who is, or whose devices or traffic are, subject to dataveillance takes some action to disable it
4.		**'You can'** Design features that, whether intentionally or incidentally, support dataveillance activities

The number and definitions of other categories of regulation – norms/morality, intrinsic/natural limits, markets/economics – and the boundaries between them, are more contested. Examples within such categories include the obviousness of the activity, the degree of 'creepiness' that the activity generates among the relevant public, the extent to which it excites social countermeasures, the relationship between costs and benefits, and the scope for over-intrusiveness to lead to the loss of customers. It might be the case that the combination of such controls are sufficiently effective, and the residual risk sufficiently limited, that active regulatory measures are unnecessary. A fully-developed framework for

the analysis of dataveillance regulation will require a more précised demarcation of these categories and the modalities through which each operates, but that has not been attempted here. Surveillance is in itself a significant form of regulation (Foucault 1975) including in cyberspace (Greenleaf 1998), and so is dataveillance. However, whether this regulatory role is as part of other categories of regulation, or should be treated as a separate category of regulation, is not considered here.

4. Evaluation Principles for Regulatory Schemes

To be of maximum utility, a study of dataveillance regulation needs to extend beyond the descriptive to embrace the normative. How we can know whether any particular regulatory scheme is good, bad or indifferent? Other general approaches to regulation will be necessary for evaluation of elements of dataveillance regulation unrelated to data privacy (Baldwin and Cave 1999; Drahos and Braithwaite, 2000).

Generic approaches to evaluating regulation can be applied to dataveillance regulatory schemes (e.g. Baldwin & Cave 1999, Drahos & Braithwaite, 2000). A comprehensive set of evaluation criteria is proposed in Clarke & Bennett Moses (2014). This encompasses process factors (clarity of aims and requirements, transparency, participation and reflection of stakeholder interests), aspects of the resulting regime (comprehensiveness, parsimony, articulation, educative value and appropriate generality and specificity), and the outcomes of the process (oversight, enforceability, enforcement and review).

In the area of privacy and data protection laws, evaluative frameworks based on responsive regulation theory are relevant (Greenleaf 2014, Chapter 3), as are approaches documented in Wright & de Hert (2016). APF (2013) consolidates widely-recognised expectations of assessment procedures for significant policy proposals, including both pre-conditions (conduct of an evaluation process, consultation, transparency, justification and proportionality) and post-conditions (safeguards and mitigation measures, controls to ensure that they are in place, and audit).

Once dataveillance regulatory measures in any particular segment or jurisdiction have been identified and documented, such evaluation criteria can be applied in order to determine the extent to which the regulatory framework appears to be in place, effective, efficient, flexible and adaptable. An example of such an analysis is Clarke (2016).

5. Dataveillance Law: Modalities and Examples

All forms of dataveillance regulation are in need of closer attention than they have been given to date. However, formal regulation by law plays a special role within the overall regulatory framework. This is because it carries the imprimatur and the power of the state, and sets a framework within which other regulatory forms operate. It accordingly warrants deeper treatment, to provide a firm foundation for subsequent research into formal regulation in particular.

Dataveillance law comprises formal regulatory mechanisms that affect the practice of surveillance involving data about people. Research published to date addresses specific questions, such as the extent (if any) to which the data protection law in a particular jurisdiction represents a regulatory measure in relation to particular forms of dataveillance. On the other hand, broader questions are less often considered, and the suggestion of a framework within which broader questions can be considered appears to be novel in the surveillance and privacy literatures. No publications have yet been found whose purpose is to explain the relationship(s) between dataveillance (or data surveillance), on the one hand, and regulatory regimes generally, and law in particular, on the other. Recent

compendia on surveillance do not address such questions (e.g Ball et al. 2012), nor do overviews of the field (Lyon, 2007). While we cannot provide any detailed theory of such relationships here, we suggest a framework within which such theories can be developed.

As discussed in Part 3 above, there are many forms of law, ranging in their degree of authority and effectiveness, including legislation, case law, contracts and codes, and thus different forms of dataveillance law. In addition to this multiplicity of forms, dataveillance law performs a number of different functions in relation to dataveillance practices. We have adopted the term 'modalities' to refer to those functions.
At one extremity, a law may mandate the performance of a particular dataveillance practice, and at the other extreme, a law may absolutely prohibit it. The functions of a great many laws, however, lie somewhere between these modalities of mandation and prohibition. Care is needed to distinguish the intermediate modalities in a manner that is both logical and a useful basis for analysis.

Table 2 presents a set of 6 modalities. As with the categorisation for dataveillance regulation in Table 1, the set will no doubt be further refined once it has been applied in a variety of jurisdictions and sectors. It is important to distinguish 'pre-conditions', which are threshold tests that result in permission or otherwise for a particular dataveillance activity to be performed, from 'post-conditions', which apply to those dataveillance activities that do proceed. Any satisfactory set of criteria for evaluation of dataveillance regulation needs to maintain that distinction.

Table 2: Modalities of Dataveillance Law

1.	**Prohibition**	**'You must not'** Laws that formally proscribe organisations from carrying out particular dataveillance activities.
2.	**Conditional Prohibition**	**'You must not unless'** Laws that proscribe dataveillance activities unless particular pre-conditions are satisfied'. Where the pre-condition is satisfied, the permission may also be subject to the requirement to at least consider, and possibly the requirement to actually satisfy, post-conditions, viz. safeguards and mitigation measures, controls and audit.
3.	**Silence**	**'It's up to you'** No relevant law mandates, permits or prohibits, whether with or without conditions applied; which is equivalent to an implied permission (in most legal systems).
4.	**Conditional Permission**	**'You may, provided that'** Laws that provide formal permission for dataveillance activities (negating possible claims of illegality) or provide capacity to organisations to do so, but contingent on some pre-condition(s) being satisfied. The permission may be subject to the requirement to at least consider, and possibly the requirement to actually satisfy, post-conditions, viz. safeguards and mitigation measures, controls and audit.
5.	**Permission**	**'You may'**

		Laws that provide unconditional permission for dataveillance activities (negating possible claims of illegality) or provide capacity to organisations to do so. The permission may be subject to the requirement to at least consider, and possibly the requirement to actually satisfy, post-conditions, viz. safeguards and mitigation measures, controls and audit.
6.	**Mandation**	**'You must'** Laws that formally require organisations (public or private sector) to carry out particular dataveillance activities. The mandation may be subject to the requirement to at least consider, and possibly the requirement to actually satisfy, post-conditions, viz. safeguards and mitigation measures, controls and audit.

Some examples of each modality are provided below, drawn from legislation with which the authors are familiar, from the Australian federal and State jurisdictions, but not purporting to represent a systematic examination of Australian jurisdictions. Their purpose is in part to illuminate the abstract definitions proposed in Table 2, and in part as a preliminary test of the comprehensiveness and effectiveness of our proposed classification scheme and associated definitions.

There are remarkably few obvious instances of (1.) Prohibition, but one is the Queensland Criminal Code s.227A criminalisation of observation or visual recording made for the purpose of observing or visually recording another person's genital or anal region.

A few examples are found of (2.) Conditional Prohibition. Very weak provisions in the *Surveillances Devices Acts* (Vic, WA, NT) prohibit the use of visual and aural surveillance devices for recording, but only if the person under surveillance has a strong case for expecting the behaviour would not be observed, transmitted or recorded. An only marginally stronger feature of the *Telecommunications (Interception and Access) Act* (Cth) provides a general prohibition on interception (s.7(1)), but is subject to s.7(2), which creates a dozen exceptions.

Category (3.) Silence is, by definition, characterised by the absence rather than the presence of evidence. However, some examples can be found in the form of types of organisations and of data that are exempted from data protection legislation. In the case of Australian data privacy law, the many exemptions from the law include personal data handling by most small businesses (*Privacy Act 1988* (Cth) s.6C), individuals in a non-business capacity (s.7B), and personal data held for personal, family or household affairs (s.16). Dataveillance activities by these organisations or persons (in such circumstances) are therefore permitted unless prohibited by other laws.

For category (4.) Conditional Permission, pre-conditions must be satisfied. An example is a provision in the *Telecommunications (Interception and Access) Amendment (Data Retention) Act* (Cth) s.110A (TIAA). This authorises an extensible list of 14 enforcement agencies and security authorities to demand data that is mandatorily retained by carriers and carriage service providers / ISPs. However, under s.110A, the extensibility to additional agencies is conditional on a declaration by the Minister. This is an example of delegated legislation creating a form of control that may or may not have any meaningful regulatory effect. The apparent safeguard of a short list of agencies has in any case

proven to be a red herring. It has come to light subsequent to the provision's passage that scores of agencies have demand powers in any case, and do not need a s.110A declaration (Duckett 2017). The agency that sponsored the legislation would have been well aware of this 'feature', but failed to declare it during the public and parliamentary debates. Some of the many agencies that do not need a s.110A declaration may be subject to pre-conditions, and possibly to post-conditions as well.

The notion of (5.) Permission encompasses dataveillance that is authorised by law, but may be subject to post-conditions. For example, the Data-Matching Program (Assistance and Tax) Act (Cth) authorises agencies to match data, but subject to a number of safeguards contained in the Act and supporting 'guidelines'. Some of the many agencies that do not need a TIAA s.110A declaration in order to access ISPs' data may not be subject to pre-conditions, but may be subject to some post-conditions.

In the case of (6.) Mandation, instances are more readily found. An example that involves the co-option of very large numbers of private sector organisations into state surveillance activities is the *Anti-Money Laundering and Counter-Terrorism Financing Act* (Cth) – commonly referred to as AML/CTF, which requires financial institutions, but also many other kinds of business enterprises, to report suspicious and other transactions to a government dataveillance agency (Austrac), and to comply with a substantial set of AML/CTF measures.

6. Practical Utility of the Analysis

Distinguishing 'modalities' of dataveillance regulation generally, and of dataveillance law in particular, might well be seen as an intellectualisation with limited practical application or implications. On the other hand, such analyses, when applied in particular contexts, may provide valuable insights into the manner in which dataveillance regulation operates. Combination of an analysis of the modalities in Tables 1 and 2 against a preferred set of evaluation criteria for regulatory regimes could throw a great deal of light on the tensions between regulatory measures in the data protection laws and other relevant subject areas. Further, analyses of this kind may enable consistent and comprehensive critiques of the tensions between regulatory measures facilitating dataveillance and those purporting to limit it (‘data protection’), across modalities, technologies and jurisdictions.

Perhaps more comprehensive surveys of dataveillance laws will in due course find moderate numbers of instances of the nature of (1.) Prohibition, comparable to the high count already evident in the case of (6.) Mandation and the intermediate modularities. If not, then the paucity of such outright prohibitions on dataveillance could suggest a political history of dataveillance that reflects dominance of the interests of social control and authoritarianism over the interests of individual freedoms.

The analytical framework proposed in this paper has potential value beyond individual jurisdictions. It may assist with the recognition of precedents for particular features of dataveillance regulation. It may also facilitate comparisons among related provisions in different jurisdictions, and the identification of pre-conditions and post-conditions applied to particular forms of dataveillance in different jurisdictions. The framework might even provide a basis for generating scores measuring countries' intrusiveness into human freedoms.

Disciplined analysis of dataveillance law, of the kinds proposed here, also has application to broader questions. For example, a 'surveillance state' can be characterised as a nation in which pervasive surveillance is critical to the ruling regime's survival. The criteria could

be operationalised as a jurisdiction that places few prohibitions or conditions on state dataveillance activities necessary to control political power. In other words, modalities 5-6 dominate, with some use of modalities 3-4, and very little of 1-2.

A 'surveillance society', on the other hand, can be seen as one in which it considered normal for almost all human activities to be subjected to dataveillance, and where many organisations apply it extensively. Hence, in operational terms, a surveillance society places few prohibitions on non-state dataveillance activities, and conditions involving data subject control are ineffective, so modalities 3-6 dominate, with little use of modalities 1-2.

The modalities analysis is also applicable to notions of more recent origin. During the last few decades, the digitisation revolution – the process of expressing data in machine-readable form (generally as a series of bits), or converting analogue data into digital form – has been all-but completed. This has laid the foundation for 'digitalisation', or ‘datafication’, which involves a shift of the interpretation and management of the world from human perception and cognition to processes that are almost entirely dependent on digital data.

A current manifestation of digitalisation is the ‘digital surveillance economy', which refers to that segment of the private sector in which revenue and profit are dependent on the expropriation and exploitation of personal data (Clarke 2017b). An even broader critique of contemporary society and polity is embodied in the notion of 'surveillance capitalism' – "information capitalism that predicts and modifies human behavior as a means to produce revenue and market control" (Zuboff 2015). A deep understanding of the digital surveillance economy and of surveillance capitalism, and the roles that regulation plays within them, requires analysis of the kind outlined in this paper.

7. Conclusions

The purpose of this paper was to present a framework to assist in the study of dataveillance regulation. Section 2 provided a definition of dataveillance, discussed the various dimensions across which dataveillance practices vary, and the various sources of the data on which the practices depend. It identified multiple characteristics of dataveillance related to the time(s) when and the period during which it is performed. Section 3 distinguished a range of different forms of regulation. Section 4 discussed a number of approaches to evaluating a regulatory regime, including against indicators of its effectiveness, efficiency, flexibility and adaptability. Because of the particular significance of formal regulation by law, Section 5 extended the framework, by considering the various roles performed by dataveillance laws. It proposed a set of 6 'modalities' that reflect different points on a scale from mandation of the performance of dataveillance, via four intermediate points, to the other extremity of prohibition. Section 6 argued that our approach has practical utility, including for the study of surveillance states and surveillance societies.

Technological developments, economic incentives to corporations, and national security 'imperatives' have resulted in societies and polities being under serious threat from rampant surveillance. Much deeper insight is needed into the means whereby societies and polities exercise control (or fail to exercise control) over dataveillance. This paper has provided a framework within which further research can be undertaken into dataveillance regulation as a whole, and dataveillance law in particular.

The analysis presented here is a first foray into the new field of dataveillance regulation, and hence all elements of the analysis are at this stage provisional, requiring further consideration from both theoretical and practical perspectives. The proposed sets of four and six modalities need to be applied to particular contexts and in particular jurisdictions, in order to establish whether they achieve sufficient disjunction among the categories and sufficient ease of use, and whether they provide sufficient insight into the nature of regulatory frameworks.

References

APF (2013) 'Evaluation Meta-Principles to Reflect Multiple Stakeholder Interests', Australian Privacy Foundation, 2013

Baldwin R. & Cave M. (1999) 'Understanding Regulation: Theory, Strategy and Practice' Oxford University Press, 1999

Ball K., Haggerty K.D. & Lyon D. (eds.) (2012) 'Routledge Handbook of Surveillance Studies' Routledge, 2012

Braithwaite J. & Drahos P. (2000) 'Global Business Regulation' Cambridge University Press, 2000

Brin D. (1998) 'The Transparent Society' Addison-Wesley, 1998

Clarke R. (1988) 'Information Technology and Dataveillance' Commun ACM 31,5 (May 1988) 498-512, PrePrint at http://www.rogerclarke.com/DV/CACM88.html

Clarke R. (1993) 'Profiling: A Hidden Challenge to the Regulation of Data Surveillance' Journal of Law and Information Science 4,2 (December 1993), PrePrint at http://www.rogerclarke.com/DV/PaperProfiling.html

Clarke R. (1994a) 'The Digital Persona and its Application to Data Surveillance' The Information Society 10,2 (June 1994) 77-92, PrePrint at http://www.rogerclarke.com/DV/DigPersona.html

Clarke R. (1994b) 'Information Technology: Weapon of Authoritarianism or Tool of Democracy?' Proc. IFIP World Congress, Hamburg, September 1994, PrePrint at http://www.rogerclarke.com/DV/PaperAuthism.html

Clarke R. (1994c) 'Human Identification in Information Systems: Management Challenges and Public Policy Issues' Information Technology & People 7,4 (December 1994) 6-37, PrePrint at http://www.rogerclarke.com/DV/HumanID.html

Clarke R. (1994d) 'Dataveillance by Governments: The Technique of Computer Matching' Information Technology & People 7,2 (December 1994) 46-85, PrePrint at http://www.rogerclarke.com/DV/MatchIntro.html

Clarke R. (1995) 'A Normative Regulatory Framework for Computer Matching' Journal of Computer & Information Law XIII,4 (Summer 1995) 585-633, PrePrint at http://www.rogerclarke.com/DV/MatchFrame.html

Clarke R (1997) 'Introduction to Dataveillance and Information Privacy, and Definitions of Terms' , 1997 and revisions, at http://www.rogerclarke.com/DV/Intro.html#Priv

Clarke R. (2001) 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications' Information Technology & People 14, 2 (Summer 2001) 206-231, PrePrint at http://www.rogerclarke.com/DV/PLT.html

Clarke R. (2008) 'Dissidentity: The Political Dimension of Identity and Privacy' Identity in the Information Society 1, 1 (December, 2008) 221-228, PrePrint at http://www.rogerclarke.com/DV/Dissidentity.html

Clarke R. (2009a) 'A Framework for Surveillance Analysis' Xamax Consultancy Pty Ltd, February 2009, at http://www.rogerclarke.com/DV/FSA.html

Clarke R. (2009b) 'A Sufficiently Rich Model of (Id)entity, Authentication and Authorisation' Proc. IDIS 2009 - The 2nd Multidisciplinary Workshop on Identity in the Information Society, LSE, London, 5 June 2009, Revised Version at http://www.rogerclarke.com/ID/IdModel-1002.html

Clarke R. (2014a) 'Promise Unfulfilled: The Digital Persona Concept, Two Decades Later' Information Technology & People 27, 2 (Jun 2014) 182 - 207, PrePrint at http://www.rogerclarke.com/ID/DP12.html

Clarke R. (2014b) 'The Regulation of of the Impact of Civilian Drones on Behavioural Privacy' Computer Law & Security Review 30, 3 (June 2014) 286-305, PrePrint at http://www.rogerclarke.com/SOS/Drones-BP.html

Clarke R. (2016) 'Privacy Impact Assessments as a Control Mechanism for Australian National Security Initiatives' Computer Law & Security Review 32, 3 (May-June 2016) 403-418, PrePrint at http://www.rogerclarke.com/DV/IANS.html

Clarke R. (2017a) 'An Instrumentalist's View of Koops et al.'s Typology of Privacy' Notes for a Panel Session, Brussels, January 2017, Xamax Consultancy Pty Ltd, at http://www.rogerclarke.com/DV/PTyp-1701.html

Clarke R. (2017b) 'Risks Inherent in the Digital Surveillance Economy: A Research Agenda' Working Paper, Xamax Consultancy Pty Ltd, September 2017, at http://www.rogerclarke.com/EC/DSE.html

Clarke R. & Bennett Moses L. (2014) 'The Regulation of Civilian Drones' Impacts on Public Safety' Computer Law & Security Review 30, 3 (June 2014) 263-285, PrePrint at http://www.rogerclarke.com/SOS/Drones-PS.html

Clarke R. & Wigan M.R. (2011) 'You Are Where You've Been: The Privacy Implications of Location and Tracking Technologies' Journal of Location Based Services 5, 3-4 (December 2011) 138-155, PrePrint at http://www.rogerclarke.com/DV/YAWYB-CWP.html

Duckett C. (2017) 'Australian government has no issue with agencies demanding telco data outside metadata laws' zdNet, 9 March 2017, at http://www.zdnet.com/article/australian-government-has-no-issue-with-agencies-demanding-telco-data-outside-metadata-laws

Foucault M. (1975) 'Discipline and Punish: The Birth of the Prison' (trans. Alan Sheridan, 1977), Peregrine, 1979

Froomkin A.M. (2000) 'The death of privacy?' Stanford Law Review 52, 6 (May 2000) 1461-1543, at http://osaka.law.miami.edu/~froomkin/articles/privacy-deathof.pdf

Gowder P. (1999) 'Book Review of 'The Transparent Society' and 'Data Smog'' Harvard Journal of Law & Technology 12, 2 (Winter 1999) 513-532

Greenleaf G (1998) 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21(2) *University of New South Wales Law Journal*, 593, at https://ssrn.com/abstract=2188160

Greenleaf G (2014) *Asian Data Privacy Laws: Trade and Human Rights Perspectives* (OUP, 2014)

Gupta,A. & Lad L. (1983) 'Industry self-regulation: An economic, organizational, and political analysis' The Academy of Management Review 8, 3 (1983) 416-25

Hepburn G. (2006) `Alternatives To Traditional Regulation' OECD Regulatory Policy Division, undated, apparently of 2006, at http://www.oecd.org/gov/regulatory-policy/42245468.pdf

Karnow C.E.A. (1994) 'The Encrypted Self: Fleshing Out the Rights of Electronic Personalities ' J. Marshall J. Computer & Info. L. 13, 1 (1994), at http://www3.cirsfid.unibo.it/asmiur01/area/documenti/Karnow_1994.pdf

Koops B.-J. et al. (2017) 'A Typology of Privacy' University of Pennsylvania Journal of International Law 38, 2 (2017) 496

Lessig L (1999a) 'The Law of the Horse: What Cyberlaw Might Teach' (1999) 113:Harvard Law Review, 501; earliest version was the Stanford Technology Law Review Working Papers 1997, draft at http://stlr.stanford.edu/STLR/Working_Papers/97_Lessig_1/index.htm (no longer available)

Lessig L. (1999b) 'Code and Other Laws of Cyberspace' Basic Books, 1999

Lyon D. (2007) 'Surveilance Studies: An Overview' Polity, 2007

Mann S. (2005) 'Equiveillance: The equilibrium between Sur-veillance and Sous-veillance' Opening Address, Computers, Freedom and Privacy, 2005, at http://wearcam.org/anonequity.htm

Mann S., Nolan J. & Wellman B. (2003) ' Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments' Surveillance & Society 1, 3 (2003) 331-355, at https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3344/3306

Manwaring K. & Clarke R. (2015) 'Surfing the third wave of computing: a framework for research into eObjects' Computer Law & Security Review 31,5 (October 2015) 586–603, PrePrint at http://www.rogerclarke.com/II/SSRN-id2613198.pdf

Michael K. & Clarke R. (2013) 'Location and Tracking of Mobile Devices: Überveillance Stalks the Streets' Computer Law & Security Review 29, 3 (June 2013) 216-228, PrePrint at http://www.rogerclarke.com/DV/LTMD.html

Michael M.G. & Michael K. (2010) 'Toward a State of Überveillance' IEEE Technology & Society 29, 2 (Summer 2010) 9-16, at http://ieeexplore.ieee.org/iel5/44/5475068/05475070.pdf

Michael M.G. & Michael K. (2014) 'Uberveillance and the Social Implications of Microchip Implants: Emerging Technologies' IGI Global, 2014

Parker C. (2007) 'Meta-Regulation: Legal Accountability for Corporate Social Responsibility?' in McBarnet D, Voiculescu A & Campbell T (eds), The New Corporate Accountability: Corporate Social Responsibility and the Law, 2007

Wigan M.R. & Clarke R. (2013) 'Big Data's Big Unintended Consequences' IEEE Computer 46, 6 (June 2013) 46 - 53, PrePrint at http://www.rogerclarke.com/DV/BigData-1303.html

Zimmer M. (2008) 'The Gaze of the Perfect Search Engine: Google as an Infrastructure of Dataveillance' Chapter 6, pp. 77-102, in Spink A. & Zimmer M. (eds.) (2008) ' Web Search: Multidisciplinary Perspectives' Springer, 2008

Zuboff S. (2015) 'Big other: Surveillance capitalism and the prospects of an information civilization' Journal of Information Technology30 (2015) 75-89, at https://cryptome.org/2015/07/big-other.pdf