

University of New South Wales Law Research Series

ELEMENTS OF ZUBOFF'S SURVEILLANCE CAPITALISM

GRAHAM GREENLEAF

(2019) 160 *Privacy Laws & Business International Report* 29
[2019] *UNSWLRS* 99

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>

Elements of Zuboff's surveillance capitalism

Graham Greenleaf analyses Shoshana Zuboff's book which argues that surveillance capitalism and its social engineering is profoundly undemocratic and exploitative.

Shoshana Zuboff's *The Age of Surveillance Capitalism* (Public Affairs, New York, 2019, 690 pp.) has, in the six months since its publication succeeded in familiarising the term "surveillance capitalism", coined by her in 2015¹ to describe a new stage of capitalism. Most users of the term may not appreciate the complexity of the 600 pages of argument that it encapsulates. The book is the most ambitious analysis of the dominant form of post-industrial capitalism that has emerged since the turn of the century. It aims at the scale of analysis that Adam Smith, Karl Marx and others applied to industrial capitalism in all its dimensions: moral, economic and political. It is also a call to arms: an exhortation to rise up against and destroy this mutant version of information capitalism before it destroys us, but without attempting a blueprint for how this is to be done, or what should replace it. While others have analysed threats and mechanisms of the "digital surveillance economy" (another apt, but arguable too limited, conception),² Zuboff's analysis of both is at the more radical end of the spectrum.³

The purpose of this brief article is neither to endorse nor critique Zuboff's analysis. A web search will find an abundance of both critiques and endorsements. My purpose here is simply to explicate what I see as key points of her analysis, and the sometimes unfamiliar concepts and terminology she utilises. Any quotes below are from Zuboff's book. Otherwise I have interpreted or paraphrased her argument, except where I expressly indicate that what is said is my opinion. Zuboff's opening chapter already provides a compelling chapter-by-chapter overview and introduction. I have taken a different focus.

THE LOGIC OF SURVEILLANCE CAPITALISM

Zuboff sets out⁴ a series of largely

sequential steps or stages to explain how "surveillance capitalism" emerged and changed over time, which probably explains the concept better than any short definition.

The origins of surveillance capitalism are traced to the discovery (by Google in 2001) of behavioural surplus, "ready made" as data exhaust in the digital environment. This stems from the realisation (originally the context of operation of a search engine) of the significance of "two texts", one public-facing and the other its shadow. The "public-facing text" is largely created by and accessible to individuals – articles, emails, news stories, photos, videos etc – though not necessarily by those it is about. The hidden text or shadow text accompanies each public-facing text, and is essentially (what we now call) all the metadata about each public-facing text; it is "hidden from public view, 'read only' data for surveillance capitalists". "Behavioural surplus" is the otherwise unused part of the shadow text generated by a particular digital transaction/service (e.g. conducting a search) which is not needed in order to deliver or improve the transaction/service. This "surplus behaviour", the unnecessary "data exhaust", turned out to be of enormous value for unrelated purposes such as selling advertisements (which could be totally unrelated to the operation of a search engine).

Analytics were required and developed to combine behavioural surplus into prediction products, which then "ignited new markets in future behaviour", initially through targeted advertisements which Google could sell. Google's pioneering role in surveillance capitalism was followed by Facebook in 2003, and subsequently by Amazon, Microsoft and others. Other capitalist firms became customers of surveillance products such as targeted ads, or purchased surveillance products to use in their own businesses (in relation to customers, staff or others).

The "extraction imperative" is the necessity to obtain greater volumes of behavioural surplus, because volume increases quality of prediction products. The effects of Facebook's 2009 implementation of the "Like" button, when they found it to be "a powerful source of surplus behaviour", were, in Zuboff's view its "single most momentous innovation in social engineering".

The extraction imperative was justified by the logic of conquest applied to human experience. Google is claimed to have made six "declarations" (perhaps metaphorically), by analogy with colonial conquerors, by which it claimed the "right to expropriate human experience". Each of these builds on and depends upon its predecessors: (i) human experience is "raw material free for the taking", irrespective of "individuals' rights, interests, awareness or comprehension"; (ii) a right to translate it into behavioural data (rendition); (iii) a right to own the behavioural data; (iv) a right to know what it discloses; (v) a right to decide how to use this knowledge; and (vi) culminating in "rights to the conditions that preserve these rights". These are the foundations of surveillance capitalism, on which its justification depends.

The extraction imperatives' "need for scale drove a relentless search for new high-volume supplies of behavioural surplus", with new competitive dynamics, as surveillance capitalism's leaders "aimed at cornering these supplies of raw materials and seeking lawless undefended spaces in which to prosecute these unexpected and poorly understood acts of dispossession." To me, this seems to be much the same mechanism by which the logic of industrial capitalism, particularly the inevitable decline in profitability in existing markets, required it to invent new and more profitable types of markets such as "education", "entertainment", "fashion", "sport" and "warfare", encompassing aspects of human

behaviours which were previously regarded as part of the domestic sphere or that of the state. This was in addition to the geographical expansion of markets in industrial capitalism made possible by colonialism and by international trade, which has its analogies in the surveillance capitalist's evangelism to "connect" the whole world, and to unsuccessful attempts to facilitate low cost Internet access throughout the developing world.

The "prediction imperative" arises because "[m]ore powerful prediction products required economies of scope as well as scale", so this involved the increase in extension of surveillance across many new activities, plus expansion in the "depth of predictive detail" of the behavioural surplus obtained through surveillance, in addition to mere volume.

To satisfy this prediction imperative required the development of techniques for "rendition of all aspects of human experience" into behavioural digital data. Rendition is where surveillance data crosses the boundary directly into the real world, and is no longer only dealing with the virtual world. "Rendition" is the same as "datafication" in big data theories.

"Economies of action" is Zuboff's expression to describe practices which involve going beyond predicting behaviour "in order to intervene in the state of play and actively shape behaviour at the source" in the real world. Economies of action were initially most vividly illustrated by the success of the Pokemon Go in causing people to act as predicted and desired in the real world, and most dangerously by the actions of Cambridge Analytica to cause people to change voting behaviour.

In relation to both the virtual and real worlds, "elaborate new means of behaviour modification" have been developed "to shape ... behaviour in ways that continuously improve their approximation to guaranteed outcomes". "Guaranteed outcomes" is a key but particularly confusing term, since the aim is only to obtain a closer approximation to a desired behaviour, not to obtain it with complete certainty ("guaranteed"). The methods and ideologies of behaviour modification are discussed further below.

"Surveillance capitalists are now locked in a cycle of continuous intensification of the means of behavioural modification", and presumably of each prior stage. It is not clear why they are "locked in", and what would happen to a surveillance capitalist that tried to change direction (as Zuboff considers Amazon, and perhaps even Microsoft, might still do).

Although Zuboff is insistent that the invention and pursuit of surveillance capitalism by its initial proponents was contingent (other choices could have been made), there is a strongly deterministic element in that each stage after the first two is regarded as following "necessarily" from the preceding steps.

'HOW DID THEY GET AWAY WITH IT?'

Zuboff identifies 16 reasons why surveillance capitalism has been able to get away with developing this audacious new "market form", and consolidating it in little over 15 years. Some of the most important need to be mentioned. Like totalitarianism in the 1930s, it was so unprecedented in what it was doing that understanding lagged behind implementation. The various declarations of rights to expropriate human experience disarmed opponents, allowing Google and others to move swiftly. The timing (2001) created an environment of "surveillance exceptionalism". "The dispossession cycle" by which "audacious incursions" (such as StreetView) were followed by retreat when resistance was met, then gradual habituation and PR to accustom the public to the general idea, and some adaptation of the concept, followed by even greater expansion, was repeated in many contexts. Ignorance of the true nature of surveillance capitalist practices is compounded by the dizzying speed at which they change. Dependency on free services by consumers has become close to addiction, fed by anxieties of loss of inclusion. Hero-worship of the innovative geniuses of Silicon Valley created authority for them, supported by powerful PR machines, and close ties to Washington, resulting in perceptions of the inevitability of the present situation. A huge variety of

"fellow travellers" participated at the margins of surveillance capitalist practices, or held shares dependent on their continuing success. And in the US, the dominant location where this played out, both data privacy and consumer protection laws are very weak, and the enforcement of competition laws stayed frozen since the turn of the century.

HOW DOES ALL OF THIS CHANGE POWER RELATIONSHIPS?

How do these ten steps in the formation of surveillance capitalism, and the sixteen side-steps to support them, change the distribution of power in our societies? The results are three-fold: (i) an asymmetric division of learning in society; (ii) instrumentalism; and (iii) an anti-democratic seizure of social power.

The division of learning: The distinction between public-facing texts and shadow texts, from which surveillance capitalism originated, and the fact that surveillance capitalists monopolise control over the shadow texts, creates "unprecedented concentrations of knowledge and power, surveillance capitalism achieves dominance over the division of learning in society – the axial principle of social order in an information society". "Division of learning" is not defined, but is described as something close to asymmetric accumulation of knowledge, and control over how to acquire it. For Zuboff, the result is that the 'division of learning is ... a hostage to surveillance capitalism's privileged position as the dominant composer, owner and guardian of the texts', producing "unprecedented asymmetries of knowledge and power".

Control over the division of learning can readily be equated, in my view, with control over the division of labour in industrial capitalism. The concept of "behavioural surplus" on which it is based has obvious echoes of Marx's key concept of the "surplus value" of labour as the basis of industrial capitalism and the ultimate source of profit.⁵

Instrumentalism – radical behaviourism: Zuboff argues that an unprecedented form of power is created by surveillance capitalism, which she labels "instrumentarian power". It differs from "totalitarian" power (itself

unprecedented when it arose in the 20th century) in various ways, including: (i) there is no single dictator, nor party, holding this power, it is distributed (unevenly) among competing surveillance capitalists; (ii) it is located primarily in the market, not the state; (iii) it does not rely on physical force, and nor is it aimed against any target “out-groups”; and (iv) there is no prescribed ideology to which individuals must submit (no “engineering of the soul”, in Stalin’s terms), but a more limited aim to achieve conforming behaviour.

“Instrumentarianism” is defined as “the instrumentation and instrumentalization of behaviour for the purposes of modification, prediction, monetization and control,” where “instrumentation” is ‘the ubiquitous connected material architecture’ through which control is exercised (described rather oddly as “the puppet”), and “instrumentalization” is “the social relations that orient the puppet master.” Power was once identified with the ownership of the means of production, but is now identified with ownership of the means of behavioral modification that is “Big Other”. This is Zuboff’s term for the impersonal, indifferent perspective of the pervasive means of behavioural modification through which this power is exercised, and derives from Skinner, not Orwell.

The most important origins of instrumentarianism are in the radical behaviorism of BF Skinner (*Beyond Freedom and Dignity* 1971), which limited the scope of scientific psychology to the study of visible behaviours, described as focusing on the Other One, people solely as their externally observable behavior. Concepts such as “freedom”, “will” and “dignity” are seen as nothing more than ignorance of

the behavioural causes of actions, and democracy similarly. Skinner lacked the tools for the large-scale implementation of his ideas, but Zuboff sees his role as overtaken by modern successors with similar ideology, led by Alex Pentland (MIT Media Lab, Social Physics 2014) who pioneered “reality mining” from phones and wearables, leading to extensions of surplus behaviour beyond data mining into real life.

The resulting ideology is one which sees behaviour modification, in the pursuit of profit (rather than for the purpose of inculcating any set of beliefs), and in the belief that people will cooperate in order to receive the benefits of a completely ordered life, as the main goal of surveillance capitalism. The role of machine intelligence intervening in human life is exemplified by an “Internet of things” (IoT) enabled factory where “the cloud with an intelligent edge” can result in a local machine “anticipate and pre-empt variations from the norm ‘before they happen.’” Humans learning to act more like machines is seen as desirable. The presentations by CEOs of the major surveillance capitalism platforms are shown to often present such views, but the extent to which this ideology is adopted by those involved in its daily operations is not explained fully.

An anti-democratic “coup from above”: Zuboff concludes her argument by reiterating why surveillance capitalism is a radical departure from classic (industrial) capitalism. First, classic capitalism says market actors must have broad freedom of action because the whole state of the market is unknowable. Surveillance capitalism distorts this because it tries to make the whole of the market knowable (predictable), although only by the

practitioners of surveillance capitalism, while those practitioners retain freedom from regulation: “an unprecedented convergence of freedom and knowledge”. Second, “surveillance capitalism abandons the organic reciprocities with people that have long been a mark of capitalism’s endurance and adaptability”, so ideas of workers also being consumers and thus requiring a living wage, fair housing etc, no longer have a role. Third, surveillance capitalism has a form of “collectivist orientation” toward predictable group outcomes, that does not sit comfortably with market capitalism or market democracy, or even with neoliberalism.

Zuboff therefore characterises surveillance capitalism as “a profoundly anti-democratic social force” ... “a coup from above”, and an “overthrow of the people” by a technological Trojan horse (Big Other). She regards it as a mutation of capitalism which needs to be overthrown, but that this does not entail overthrowing capitalism in general, or some other form of information capitalism. Her book does not dwell on solutions (it is long enough already), although she thinks some must originate with strong enforcement of the EU’s GDPR, and the engagement of NGOs and activists to ensure such enforcement occurs. She endorses Thomas Piketty’s comment “If we are to regain control of capital, we must bet everything on democracy.”

CONCLUSION – READ, DON’T IGNORE

Zuboff is not a fatalist: surveillance capitalism is not a technology, but a market form. Its logic of accumulation is currently dominant, but neither inevitable, nor impervious to

REFERENCES

- 1 Shoshana Zuboff ‘Big Other: Surveillance Capitalism and the Prospects of an Information Civilization’ (2015) 30 *Journal of Information Technology*, 75–89 <https://ssrn.com/abstract=2594754> ; The same title was used in JB Foster and RW McChesney, ‘Surveillance Capitalism: Monopoly-Finance Capital, the Military-Industrial Complex, and the Digital Age’ *Monthly Review*; New York Vol. 66, Iss. 3, (Jul/Aug 2014): 1-31, but is more to do with the relationship between state surveillance and capitalism, a related but distinct issue.
- 2 Clarke R. (2019) ‘Risks Inherent in the Digital Surveillance Economy: A Research Agenda’ *Journal of Information Technology* 34,1 (Mar 2019) 59-80, at doi.org/10.1177/0268396218815559, PrePrint at www.rogerclarke.com/EC/DSE.html
- 3 For criticism that it is not a radical enough critique, failing to consider the whole capitalist structure, see E Morozov ‘Capitalism’s New Clothes’ *The Baffler*, 4 February 2019 thebaffler.com/latest/capitalisms-new-clothes-morozov
- 4 Zuboff, particularly pgs 338-40, plus p179 and following on Google’s ‘declarations’.
- 5 For a defence of the labour theory of value, see Paul Mason *Postcapitalism, A Guide to our Future* (Penguin, 2016, pp. 147-59).
- 6 Clarke ‘Risks inherent ...’ (2019), abstract and text.

ANALYSIS/NEWS

destruction. As Clarke puts it, the digital surveillance economy could sweep away centuries of individualism and humanism; or institutional adaptation may blunt the worst aspects; or rebellion through popular outrage and legal tools may dismantle its apparatus and ideology.⁶

It is not possible to do justice to an

argument elaborated over 600 pages in a mere 2,500 words, but this summary may suffice to convey some of the complexity, novelty and thoroughness of Zuboff's analysis of and case against surveillance capitalism, and perhaps to provide encouragement to read the book. Its arguments and terminology will be with us for some time, and deserve to be.

INFORMATION

For valuable comments, thanks to Roger Clarke, Elizabeth Coombs, and Marc Rotenberg, but responsibility for all content remains with the author.



ESTABLISHED
1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Issue 160

AUGUST 2019

NEWS

- 2 - **Comment**
Data protection is taken seriously
- 6 - **EU reviews adequacy decisions**
- 9 - **Processor SCCs, video guidelines**
- 10 - **The GDPR after one year**
- 18 - **'Data Free Flow With Trust' at G20**

ANALYSIS

- 29 - **Zuboff's surveillance capitalism**

LEGISLATION

- 14 - **GDPR implementation in Croatia**
- 16 - **Latvia's GDPR-implementing law**
- 24 - **Dubai IFC consults on DP law**
- 26 - **South Africa's POPIA expected to enter into force in 2020**
- 33 - **California's privacy law**

MANAGEMENT

- 12 - **DPO Networks and associations**
- 20 - **Navigating e-Privacy**
- 22 - **AdTech: Consent, legitimate interest and joint controllership**

NEWS IN BRIEF

- 8 - **EU Council reviews the GDPR**
- 13 - **Sweden defines areas of priority**
- 17 - **Spain and Greece face EU action**
- 19 - **Egypt moves towards DP law**
- 19 - **APPA meets in Japan**
- 25 - **Germany amends DP law**
- 25 - **EU work on DP ethics**
- 28 - **Sri Lanka considers DP law**
- 28 - **DPA's act on AdTech complaints**
- 32 - **US FTC fines Facebook \$5 billion**
- 32 - **US FTC action: Equifax settles**
- 32 - **Privacy Shield Ombudsperson**
- 35 - **Portugal adopts new DP law**
- 35 - **CJEU Opinion on validity of SCCs not until December**

Belgium's DPA aims at mediation rather than fines

Previously the DPO for Nielsen, the new Belgian DPA brings both academic insight and a business experience to his regulatory role. **Stewart Dresner** and **Laura Linkomies** report.

Dr David Stevens was appointed as Chairman of Belgium's DP Authority on 28 March 2019, together with the other members of the Executive Committee of the Belgian Data Protection Authority. The delay in appointments was partly due to strict

language requirements; the GDPR implementing Act was adopted in 2018 and entered into force on 5 September 2018 (*PL&B International* February 2019, p.1).

Dr Stevens is an experienced data

Continued on p.3

National approaches to 'legitimate interest' trouble EU

The European Commission's unease over national implementation of the GDPR also encompasses limits to data subjects' rights and 'effective' independence of DPAs. **Tom Cooper** reports.

The European Commission is continuing bi-lateral and group discussions with Member States as it pursues the harmonisation of data protection rules across the bloc. But multi-state operators remain wary of tripping over national

variations in the implementation of the EU General Data Protection Regulation (GDPR). Karolina Mojzesowicz, Deputy Head, Data Protection Unit, European Commission, confronted

Continued on p.4

www.privacylaws.com

Subscribers to paper and electronic editions can access the following:

- Back Issues since 1987
- Materials from PL&B events
- New search function
- Videos and audio recordings

See the back page or **www.privacylaws.com/subscribe**

To check your type of subscription, contact kan@privacylaws.com or telephone +44 (0)20 8868 9200.

PL&B Services: Publications • Conferences • Consulting • Recruitment
Training • Compliance Audits • Privacy Officers Networks • Roundtables • Research

INTERNATIONAL
report

ISSUE NO 160

AUGUST 2019

PUBLISHER**Stewart H Dresner**
stewart.dresner@privacylaws.com**EDITOR****Laura Linkomies**
laura.linkomies@privacylaws.com**DEPUTY EDITOR****Tom Cooper**
tom.cooper@privacylaws.com**ASIA-PACIFIC EDITOR****Professor Graham Greenleaf**
graham@austlii.edu.au**REPORT SUBSCRIPTIONS****K'an Thomas**
kan@privacylaws.com**CONTRIBUTORS****Robert Waixel**
Anglia Ruskin University, UK**Laura Drechsler**
Brussels Privacy Hub, Belgium**Marija Gregorić and Lovro Klepac**
Klepac, Babic & Partners LLC, Croatia**Katrine Plavina**
Vilgerts, Latvia**Wenlong Li**
University of Edinburgh, UK**Frank Madden**
IBM, UK**Will Stern and Sabrina McGraw**
Covington & Burling LLP, US**Dino Wilkinson**
Clyde & Co, United Arab Emirates**Published by**Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom**Tel: +44 (0)20 8868 9200****Email: info@privacylaws.com****Website: www.privacylaws.com****Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753

Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

© 2019 Privacy Laws & Business

“ comment ”

Data protection is taken seriously – also in the US

The \$5 billion fine imposed on Facebook by the US Federal Trade Commission is the largest we have seen for a privacy violation (p.32) and will perhaps influence EU DPAs in their enforcement. However, a ban on certain types of processing may be more effective than any fine when talking about a company the size of Facebook. Europe has yet to see such a large GDPR fine. *PL&B's* interview with Belgium's new Data Protection Commissioner reveals that he in fact regards mediation as more effective than fines (p.1).

On Internet giants and surveillance capitalism, read Graham Greenleaf's analysis of Shoshana Zuboff's thought-provoking book on p.29.

The European Commission monitors the Member States' implementation of the GDPR, and much work still remains to be done. In some instances, Member States have introduced national requirements on top of the Regulation, in particular, through many sectoral laws. This practice leads to fragmentation and results in creating unnecessary burdens, the Commission says in its recent Communication. Speaking at our Annual Conference in Cambridge in July, Karolina Mojzesowicz, Deputy Head, Data Protection Unit, European Commission, said that the Commission has taken a "very proactive" approach to the implementation of the Regulation, working with Member States to discuss options, possibilities and solutions. It continues to analyse national legislation and to clarify issues in bilateral discussions (p.1).

We follow closely the Commission's work in this field which will result in a report in 2020 (p.10). In this issue, we are pleased to bring you news from two more countries in our series of articles on GDPR implementation at national level; our correspondents from Latvia (p.16) and Croatia (p.14) discuss their countries' laws, which have both been in force since last summer.

Another area of work at the EU Commission is to review the existing adequacy decisions and evaluate any new national applications for an adequacy assessment. With Japan having achieved the mutual adequacy decision, Korea is next in line (p.6). The G20 is discussing an overarching framework that promotes cross-border data flows (p.18), and the next EU-US Privacy Shield review will begin in mid-September.

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Join the Privacy Laws & Business community

Six issues published annually

PL&B's International Report will help you to:

Stay informed of data protection legislative developments in 125+ countries.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Find out about future regulatory plans.

Understand laws, regulations, court and tribunal decisions and what they will mean to you.

Be alert to future privacy and data protection law issues that will affect your organisation's compliance.

Included in your subscription:

1. Online search functionality

Search for the most relevant content from all *PL&B* publications and events. You can then click straight through from the search results into the PDF documents.

2. Electronic Access

We will email you the PDF edition which you can also access via the *PL&B* website. You may also choose to receive one printed copy.

3. E-Mail Updates

E-mail updates help to keep you regularly informed of the latest developments in data protection and privacy issues worldwide.

4. Back Issues

Access all the *PL&B International Report* back issues since 1987.

5. Special Reports

Access *PL&B* special reports on Data Privacy Laws in 125+ countries and a book on Data Privacy Laws in the Asia-Pacific region.

6. Events Documentation

Access International and/or UK events documentation such as Roundtables with Data Protection Commissioners and *PL&B Annual International Conferences*, in July, in Cambridge, UK.

7. Helpline Enquiry Service

Contact the *PL&B* team with questions such as the current status of privacy legislation worldwide, and sources for specific issues and texts. This service does not offer legal advice or provide consultancy.

To Subscribe: www.privacylaws.com/subscribe

“*PL&B's International Report* is a powerhouse of information that provides relevant insight across a variety of jurisdictions in a timely manner. **Mark Keddie, Global Data Protection Officer, Dentsu Aegis Network**”

Subscription Fees

Single User Access

International Reports £560 + VAT*

UK Reports £450 + VAT*

UK & International Reports £900 + VAT*

* VAT only applies to UK based subscribers

Multi User Access

Discounts for Multiple User licence (up to 10) and Enterprise licence (unlimited users).

Subscription Discounts

Introductory discount (first year): 30% off for DPAs, public sector, charities, academic institutions, use code SUB30; 20% off for other organisations, use code SUB20.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition

Rest of Europe = £25, Outside Europe = £35

Combined International and UK Editions

Rest of Europe = £50, Outside Europe = £70

Satisfaction Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.

Privacy Laws & Business also publishes the United Kingdom Report.

www.privacylaws.com/UK