Every company is a data company

A common thread across the business sector is the value of the personal data held and processed. **Stewart Dresner** reports from Privitar's In:Confidence Conference on 4 April in London.

The traditional criterion for business success is profitability. But now many tech companies, for example, Uber, are "worth" billions of dollars even if they have never made a profit. In April, Uber officially declared that it might never make a profit.[1]

How does this conundrum work for more conventional companies? Every company is a data company to a greater or lesser extent. The data on people, however, now represents the value of the company. While companies increasingly provide more personalised advertising and services, and everyone likes "free" stuff, *Jason du Preez*, Privitar's CEO, stated that "data can be weaponised under the guise of personalisation…our decisions can be influenced in this way." The cost of not using personal data in a trustworthy way is a missed opportunity.

What kind of decision-making should be handled by machines? "Humans and machines should work together doing what they each do best" Two examples are pilots flying planes, and monitoring in nuclear power stations. "There is a risk of humans overtrusting technology," explained *Dr. Hannah Fry*, (an Associate Professor in the Mathematics of Cities at the Centre for Advanced Spatial Analysis at University College, London) at the same conference. The driverless car is a concept for the future, but partnership between humans and technology is everywhere in the form of assisted driving, such as cruise control and warnings to prevent a crash. Volvo and Toyota are good models in this field.

She continued to emphasise that algorithms are human constructions. There is a danger when asking a machine to be part of our lives. We have to consider the consequences of using people's data and algorithms. There is always a risk from market pressure to quickly deploy a new or modified algorithm. When will a product or service be ready for the market? There is generally a new version being developed.

Algorithms can provide benefits which outweigh the harms, as in the area of diagnostics via health apps. But we should avoid blind faith in machines. Humans need to retain qualities of empathy to assess a situation for factors which may not be written into the coding.

The great majority of smart phone users and website users "voluntarily" disclose their personal data to a huge number of companies, often not realising the full implications of what they are doing as they are focused on the usefulness or entertainment value of the app or website they are using. As a result, companies increasingly use algorithms to collect, analyse and take decisions on the basis of personal data. Even if location data is in principle, de-identified, it takes fewer than four data points in 95% of cases to re-identify people and can do much harm, said *Charlie Cabot*, Research Leader, Privitar. Companies should pay more attention to the risks of re-identification.

Future surveillance of the population is likely to be based more on facial recognition. People will not be aware of its extent, and if they were aware, would not consent to it. *Ed Vaizey* MP, and former Minister of State for Culture and the Digital Economy, gave his perspective that politicians will wait for popular sentiment to increase before taking action. *Ade Adewunmi*, a technology consultant at Think Big Analytics, responded with her view that governments will take advantage of personal data which has been collected.

Vivienne Artz, Chief Privacy Officer, Refinitiv, stated "Privacy is the new normal" and presented her Top 5 present data protection law related challenges:

1. Staffing (they do not need to all be lawyers).
2. Budgets are halving as the drama of the GDPR appears to some top managers to be past its peak.
3. More and evolving European Data Protection Board requirements – even if the UK leaves the EU – as the UK will have to keep its policies consistent with them.
4. Greater customer and vendor awareness.
5. Enforcement.

She also gave her top future issues including: Brexit; the EU ePrivacy Regulation when it is adopted; US and other national laws; Artificial Intelligence and automation; Ethics; and cyber threats and data breaches.

The GDPR is a high standard and continues to provide challenges for companies, for example:

1. Consent which is only one of the legal bases for processing of personal data.
2. The role of the Data Protection Officer
3. International transfers and data localisation
4. Different definitions of personal data and individual rights
5. Conflict of laws.

Steven Hamblin, CTO, Sensyne Health, asserted "Total anonymization is a myth." This is credible when the current average of seven connected devices in the home is forecast in a few years to go up to 70+ according to *Jason Perkins*, Head of Data & Analytics Architecture, BT. Connected devices in a "smart home" give a detailed picture of the living patterns of its residents. BT takes steps to protect the privacy of its customers by deploying data/digital "watermarking" which means that managers can "trace everyone in the organisation who touches the data."

Jason McFall, CTO Privitar, explained that there is a tension, and this creates a trade off between privacy and utility. To achieve

privacy once there is an innovative idea, one has to bring the code to the data. "We don't need the data itself." For example to calculate commuting time, analysts do not need to know where all the data subjects live. Analysts need to analyse the functions not the original data. "Deep learning, machine learning is about extracting data and knowing what to do about it" he concluded.

INFORMATION

Privitar's In:Confidence Conference was held at Printworks in London on 4 April 2019
www.privitar.com/inconfidence19-recap

REFERENCES

1 www.reuters.com/article/us-uber-ipo/uber-unveils-ipo-with-warning-it-may-never-make-a-profit-idUSKCN1RN2SK
2 www.marketingweek.com/2018/02/12/unilever-threatens-pull-ad-spend-platforms-breed-division/
3 www.marketingweek.com/2019/04/12/procter-gamble-new-media-supply-chain/

MAJOR CONSUMER GOODS COMPANIES CITE PRIVACY IN AVOIDING DAMAGING CONTENT

Unilever[2] and separately, Procter & Gamble's Chief Brand Officer, Marc Pritchard, have announced that they do not want their companies' advertising to be placed next to damaging content on websites and social media. Pritchard said: "I'd like to offer a new approach. It's time to invest our brainpower into an ecosystem that builds in quality, civility, transparency, privacy and control from the very start."

Pritchard outlined how P&G has already taken steps to move to this new media supply chain. On quality, it will only buy media from places where content quality is "known, controlled and consistent with its values".

P&G is now choosing to advertise only on 'safelisted' channels and is pivoting to more precise placement, as well as forming partnerships with new platforms that prove from the start their content is "safe and under their complete control". And Pritchard called out platforms that defend brands appearing alongside illegal content, saying they must take responsibility.[3]

ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Using car journey data with consent and pseudonymisation

wejo, a software business that analyses data from car journeys, says that privacy is at the heart of its platform. **Laura Linkomies** reports.

Connected cars collect a vast amount of data which can be used in several ways, for example to improve traffic flow or enhance the safety of drivers or passengers. However, is the average consumer aware of data collection and the uses of their data?

wejo, a software company with its headquarters near Chester, wants to keep data collection and analysis as transparent as possible. The company has a strategic partnership with a global car manufacturer for data sharing and analysis of car data, a landmark deal that includes a

Continued on p.3

Relaxed restrictions? The ICO view on international transfers

Nicola Fulford and **Paul Maynard** of Hogan Lovells analyse the ICO's position on restricted transfers that somewhat differs from that of European colleagues.

The ICO's 'Guide to the GDPR' contains a section on international transfers of personal data which presents a novel approach to applying the rules set out in Chapter V of the GDPR on transfers of personal data outside the European Economic Area (EEA).

The ICO explicitly states that the restrictions in Chapter V only apply where a transfer of personal data is made to a controller or processor in a third country (or to an international organisation) which is not itself

Continued on p.5

Issue 103 **May 2019**

UNITED KINGDOM
report

ISSUE NO 103 MAY 2019

PUBLISHER
Stewart H Dresner
stewart.dresner@privacylaws.com

EDITOR
Laura Linkomies
laura.linkomies@privacylaws.com

DEPUTY EDITOR
Tom Cooper
tom.cooper@privacylaws.com

REPORT SUBSCRIPTIONS
K'an Thomas
kan@privacylaws.com

CONTRIBUTORS
Jenai Nissim and Alison Deighton
HelloDPO

Robin Smith
Lifeboat Foundation

Ros Foster
Browne Jacobson LLP

Nicola Fulford and Paul Maynard
Hogan Lovells

Peter Church and Christina Mysko
Linklaters

Corinna Harris and Graham Mitchell
Clyde & Co (Scotland) LLP

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* United Kingdom 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 2047-1479

comment

Privacy protection should be based on ethics and trust

The research and advisory company, Gartner, named digital ethics and privacy as one of its top 10 strategic technology trends for 2019. In this issue, we look at the use of Artificial Intelligence in the health sector (p.14).

The protection of children's data is another area where ethics should play a major role. The ICO is now consulting (until 31 May) on its Age Appropriate Design Code, something that was added to the UK Data Protection Act 2018 at the last minute. It will have a statutory status and compliance, or non-compliance, is expected to be important evidence in the courts. Companies that are found non-compliant may face regulatory action – ultimately GDPR-style fines. The Code will apply to providers of information society services and has many of the usual data protection principles, but also many good practical examples of how to ensure children's privacy. More about this code in the next issue.

Car data analysis is big business – I talked to software company, wejo, to find out how they comply with the GDPR in this fast moving environment (p.1).

FOI practitioners will be able to draw useful compliance advice from three recent FOI cases which take a stance on costs and vexatiousness (p.10). We also bring you an analysis of a recent Subject Access Request (SAR) case which shows that there is a wide margin for data controllers to strike a balance when aiming to limit the burden of SARs (p.7), and another one on the approach to disclosing the identity of recipients (p.17). Those involved in international transfers will no doubt find useful our correspondent's analysis of a seldom discussed topic – the differences between the ICO and European Data Protection Board views on restricted data transfers (p.1).

Stewart Dresner and I attended the ICO's Data Protection Practitioners' Conference in April. The main message from Elizabeth Denham was that we are now at a critical stage with the GDPR – the crucial change in the law is about accountability but not all organisations embrace that (p.8). See her and 65+ other speakers from 15+ countries at *PL&B's* 32nd Annual International Conference www.privacylaws.com/ac

Laura Linkomies, Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you wish to contribute to *PL&B UK Report*? Please contact Laura Linkomies, Editor (tel: +44 (0)20 8868 9200 or email: laura.linkomies@privacylaws.com) to discuss your idea, or offer to be interviewed about your organisation's data protection/Freedom of Information work.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

PL&B's United Kingdom Report will help you to:

Stay informed of data protection legislative developments.

Learn from others' experience through case studies and analysis.

Incorporate compliance solutions into your business strategy.

Learn about future government/ICO 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 keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

4. Back Issues
Access all the *PL&B UK Report* back issues since the year 2000.

5. Events Documentation
Access UK events documentation such as Roundtables with the UK Information Commissioner and *PL&B Annual International Conferences*, in July, Cambridge.

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

To Subscribe: www.privacylaws.com/subscribe

"I particularly like the short and concise nature of the *Privacy Laws & Business* Reports. I never leave home without a copy, and value the printed copies, as I like to read them whilst on my daily train journey into work."

Steve Wright, formerly Data Privacy & InfoSec Officer, John Lewis Partnership

Subscription Fees

Single User Access

UK Edition **£450 + VAT***
International Edition **£560 + VAT***
UK & International Combined Edition **£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 International Report.
www.privacylaws.com/int