ESTABLISHED 1987

UNITED KINGDOM REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

AI-powered Onfido one of first selected for the ICO's Sandbox

Onfido, an identity verification company, will research how to identify and mitigate algorithmic bias in machine learning models used for remote biometric identification. By **Ali Vaziri** of Lewis Silkin LLP.

In the digital economy, identity is the key to unlocking access to services widely relied on in order to participate in society. Since in-person interaction is no longer always required of, or expected by, users, the challenge faced by many online organisations is how to know a person wanting to access their services is who they claim to be, and in a

Continued on p.3

Smart-home study weighs the privacy risks involved

Martin Kraemer and **William Seymour** at the University of Oxford report on an ICO-funded research project investigating how 'smart' doesn't have to mean invasive.

Studies and media reports about smart home technologies and smartphone apps show that consumers have little awareness of the information they expose to companies, advertisers, and other cohabitants when they use these services. These thought processes of how devices (and the information economy more generally) work can leave users feeling

Continued on p.6

Future PL&B Events

- *Asian data privacy laws*, 30 October, Linklaters, London
- *New Era for US privacy laws: California and more*, 14 November, Latham & Watkins, London.
- *Balancing privacy with biometric techniques used in a commercial context*, 29 January 2020, Macquarie Group, London.
- *PL&B's 33rd Annual International Conference*, St. John's College, Cambridge 29 June to 1 July 2020.

privacylaws.com

Issue 105 **SEPTEMBER 2019**

UNITED KINGDOM
report

ISSUE NO 105 **SEPTEMBER 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
Ali Vaziri
Lewis Silkin LLP

Martin Kraemer and William Seymour
University of Oxford

Charlotte Reddish, Jenai Nissim and Alison Deighton
Hello DPO

Emma Hughes and Nicola Fulford
Hogan Lovells

Lore Leitner and Christopher Foo
Wilson Sonsini Goodrich & Rosati

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

Data protection issues on and around Brexit

It has not been discussed much in the general media what a detrimental impact a no-deal Brexit would have on data transfers and international business, even if it was recognised as one of the top issues in the negotiations between the EU and the UK. However, in the Operation Yellowhammer papers, the government also highlights the worst possible scenario for data flows; it warns that an adequacy assessment could take years, and law enforcement data and information sharing between the EU and UK will be disrupted.

A leaked government document suggests that the prime minister has instructed government departments to share data they collect about usage of the GOV.UK portal, without informing individuals. This data would feed into Brexit preparations.

A government spokesperson has told Buzzfeed, which broke the story (www.buzzfeed.com/alexspence/boris-johnson-dominic-cummings-voter-data), that "individual government departments currently collect anonymised user data when people use GOV.UK. The Government Digital Service is working on a project to bring this anonymous data together to make sure people can access all the services they need as easily as possible. No personal data is collected at any point during the process, and all activity is fully compliant with our legal and ethical obligations."

In this issue we report on work that Friends of the Earth has done to make sure that its privacy policy is understandable to everyone (p.8) and why Onfido has embarked on the ICO's Sandbox programme (p.1). Another ICO initiative is its grants programme – read on p.1 about privacy issues with smart homes.

The ICO's new cookies policy has raised some questions (p.16) – not least among international business as there are some differences between that and guidance from France's regulator, the CNIL.
Our correspondents also look at issues about consent, contractual necessity and legitimate interests when using AI (p.20) and how to assess data protection risk (p.12).

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.

Smart homes ... from p.1

exploited and powerless. At the same time, a lack of awareness about the data protection rights afforded to individuals – such as those under the GDPR – helps perpetuate the status quo.

The GDPR also introduces the concept of "data protection by design and by default" (DPbD) as a legal obligation for data controllers. In practice an extension of the existing privacy-by-design paradigm, this new requirement is supported by a growing body of DPbD guidelines and methodologies such as those provided by the ICO. As with any change to the regulatory landscape, this presents complex challenges from a product design and development perspective that companies will need time to adapt to.

Smart devices pose a particular problem in the context of data protection by design for two main reasons. Unlike passive technology in homes (e.g. traditional light bulbs or heating), they have the ability to act, react, and adapt by sensing their environments. But smart devices are almost always connected, and this combination means that sensitive data about activities in the home is often unexpectedly shared, not only with third parties outside the home, but also between inhabitants. Understanding where and why data is being collected can also be difficult, as it is often used for multiple purposes, such as service provisioning or profiling for targeted advertising.

Understanding data protection in Smart Homes

In order to ease the transition, the ICO has funded a project at the University of Oxford investigating the future of data protection by design and default in smart homes. The project, led by Professors Ivan Flechais and Max Van Kleek, will begin with a longitudinal study of smart homes to understand how people build connected technologies into their daily lives. Looking in detail at what data families believe is worth protecting, we hope to explore the influence of privacy preferences and choices as our participants develop habits and preferences that will last much longer than individual pieces of technology.

But what use are privacy preferences if you can't put them into practice? To this end the second stage of the project focuses on developing new mechanisms to safeguard the information that users consider the most sensitive whilst still enabling the advanced features that consumers expect from the devices of the future. As well as involving current users of smart devices, we will also be working with industry practitioners and compliance officers to make sure that solutions satisfy existing business requirements and would be practical in a commercial setting.

Problems of Design in everyday use

A frequent problem that we encounter in our work is that contemporary devices are often designed to be used by a single person, in much the same way as a smartphone (or a toothbrush). But previous research conducted at Oxford and other universities shows that the social dynamics of the home contain complex factors that are not addressed by this single-user-per-device model. As a space shared between family members (or long/short term lodgers and even guests), the social order of the home is apt to be disrupted by technology that does not respect existing social arrangements. While responsibilities and resources are generally shared in our home, the extent to which that applies to digital devices differs largely. The everyday use of digital devices in our households then warrants more specific consideration.

This seems like a familiar problem; during a fight over what to watch, your TV does not distinguish between parent and child when changing the channel. With smart devices, the tensions caused by this lack of contextual awareness will now be much more pervasive, be that due to ordering something through someone else's Amazon account via Alexa, or using the companion app to one's smart light bulbs to see if the children have come home during the day.

These examples also highlight the lack of privacy provided by the single user model. It is not difficult to imagine a situation where the contents of searches or purchases made through Alexa might be sensitive, or the use of connected devices to track others' activities could constitute stalking or other forms of harassment (already acknowledged as a problem with smart phones and apps[1]).

On a more prosaic level, although we have found that cohabitants often do consider each other when introducing, configuring, and using devices, there is much more that technology design can do to facilitate and enable the process. Of primary concern for us is how data protection by design and by default can offer a solid foundation to build on as smart devices find new applications in our homes. It is currently difficult enough for individuals to align their preferences for data collection with the behaviour of their own devices (indeed, most cannot), let alone in situations with devices owned by others or in shared spaces, potentially operated by landlords or employers.

While design patterns for data protection over multiple users do exist, the larger challenge emerges when users act on behalf of others. This might be to give guests access to systems in the home, or perhaps to assist friends and relatives to retain their independence (e.g. ageing in place; remaining in your own home for the later years of your life). These users are likely to have vastly different levels of technical skill and familiarity with the technology at hand, meaning that we need strategies to ensure that users have the knowledge, as well as the tools, to make decisions about their own data.

Vox ex Machina

A major development that has marked a new era in personal technology comes in the way we interact rather than what the technology does. Voice interfaces are now more robust and usable than ever before, but they represent more than just a novel way of ordering a take-away.

Pioneering work in the nineties also showed that a number of phenomena normally associated with human interaction also apply to interactions with computer voice interfaces; we gender computers based on their voices, and our social responses to computers (e.g. saying thank you) are often automatic and unconscious. Speech activates the same centres in the brain regardless of whether it originates from a home assistant or another person, presenting

an array of functional and ethical challenges when designing voice-controlled systems.

Ongoing research by the Human Centred Computing group at Oxford is investigating the extent of these effects, focusing on how giving voices to technology changes the way that we think and behave around them. Participants sometimes describe voice assistants as having the same physical 'presence' as a person would, and other cutting-edge research demonstrates that this feeling of social presence is associated with higher rates of disclosure of personal information.

The many faces of privacy

In the context of the smart home, privacy is crucial: Western culture places the home as the most private space in one's life, and householders rightly expect a measure of control over what information goes into and out of their homes. As discussed above, complex household and family dynamics also come into play, acting as forces that shape dynamic privacy preferences that can change from one day to the next.

A constant challenge to research in this space is the multifaceted nature of privacy as a catch-all term. Increasingly cited as a goal or requirement of new technologies, its meaning is subjective, contextual, negotiable, and cultural, presenting a significant challenge when it comes to developing the type of "best practice" for building privacy-respecting systems that this research project hopes to deliver.

Our project takes a different approach, following the understanding that considerations of privacy take many different forms in everyday life and as such cannot be seen in isolation[2]. Our design ethnography[3] of communal privacy practices allows us to clarify how household members account for their actions and how they do so in considering others. The idea of implementing social translucence[4] is one example. It encapsulates making transparent the needs and preferences of others using digital devices in relation to an individual's own intention when using digital devices[5].

Current progress

As of September 2019, the longitudinal study is well under way, featuring six households from around Oxfordshire. This will run until March 2020, documenting the experiences of these households as they slowly become more familiar with a range of different smart home devices. Their experiences allow us to observe communal privacy practices as they evolve and change over time, an understanding pivotal to the development of the types of data protection mechanisms and safeguards described above.

After the initial results from the longitudinal study have been analysed, work will begin on developing and prototyping smart home devices that integrate DPbD from the ground up. This work will build on the results from the longitudinal study, aiming to clarify the wants and needs of our participating households.

Early findings from this project have already helped shape a design technique for usable security and privacy which we are currently evaluating with product design and compliance teams. If you would be interested in learning more or participating in evaluations, please get in touch with the research team. The project will run until July 2020.

AUTHORS

Martin Kraemer and William Seymour are DPhil researchers at the University of Oxford Department of Computer Science.
Emails: martin.kraemer@cs.ox.ac.uk
william.seymour@cs.ox.ac.uk

INFORMATION

The project, Informing the Future of Data Protection by Design and by Default in Smart Homes was awarded £81,290 in the ICO's grants' programme.
Building on previous research, the project will conduct a study of six smart homes to study current privacy preferences and to prototype new tools, interfaces, and approaches to smart home privacy. See digiwell.web.ox.ac.uk/informing-future-smart-homes

REFERENCES

1 Freed, Diana, et al. ''A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology.' Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, 2018.
2 Dourish, P., & Anderson, K. (2006). Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction*, 21(3), 319–342.
3 Crabtree, A., Rouncefield, M., & Tolmie, P. (2012). *Doing Design Ethnography*. London: Springer.
4 Refers to designing digital systems that support coherent behaviour by making participants and their activities visible to one another.
5 Dourish, P., & Anderson, K. (2006). Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction*, 21(3), 319–342.

Join the Privacy Laws & Business community

The *PL&B United Kingdom Report*, published six times a year, covers the Data Protection Act 2018, 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 privacy and data protection law issues and tech developments that will affect your compliance and your reputation.

Included in your subscription:

1. Six issues published annually

2. Online search by keyword
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.

3. Electronic Version
We will email you the PDF edition which you can also access via the *PL&B* website.

4. Paper version also available
Postal charges apply outside the UK.

5. News Updates
Additional email updates keep you regularly informed of the latest developments in Data Protection, Freedom of Information and related laws.

6. Back Issues
Access all *PL&B UK Report* back issues.

7. Events Documentation
Access UK events documentation such as *PL&B Annual International Conferences*, in July, Cambridge.

8. 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.

privacylaws.com/reports

"Given the rate of change in law, regulation and business practice, it is essential to have concise and up to date information. *PL&B* is always relevant and continues to offer great value."

Adam Green, Chief Risk Officer, Equiniti

International Report

Privacy Laws & Business also publishes *PL&B International Report*, the world's longest running international privacy laws publication, now in its 33rd year. Comprehensive global news, currently on 165+ countries, legal analysis, management guidance and corporate case studies on privacy and data protection, written by expert contributors

Read in more than 50 countries by regulators, managers, lawyers, and academics.

Subscriptions

Subscription licences are available:

- Single use
- Multiple use
- Enterprise basis
- Introductory, two and three years discounted options

Full subscription information is at privacylaws.com/subscribe

Satisfaction Guarantee

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