Social acceptance is key in exercising the right to privacy

The informational social contract, or social license for the treatment of personal information, needs to be clarified in a new social, economic, security and technological context to protect privacy. By **Chantal Bernier** of Dentons' Global Privacy and Cybersecurity Group.

Social License to Operate, or SLO, refers to the social acceptability a business enjoys to function. It is most germane to the mining sector. In that context, SLO is usually contingent upon public consultations, benefit sharing and impact assessment. The critical difference between SLO and ethics is that an ethical stance is self-proclaimed. SLO is bestowed or withdrawn.

Applying it to privacy law pursues three objectives: i) to create a common ground for regulators and organizations to interpret privacy law in a socially relevant and therefore effective manner, grounded in the expectation of privacy; ii) to recognize that, since personal information is the currency of the digital economy and the material of public policy, users are "funders" and therefore the arbiters of legitimacy in privacy law; and iii) to meet the test of human rights law to limit privacy only as demonstrably justified in a free and democratic society.

While the right to privacy is a fundamental, universal right, immutable and unalienable, its modalities of exercise are a social construct. Throughout centuries and cultures, social mores have evolved as to what is acceptable to reveal or query. When Mark Zuckerberg pronounced in 2010 that "Privacy is no longer a social norm", he was contradicted on the assertion, but no one contested his reference point: social acceptance as legitimacy for the application of the right to privacy.

In "Forming the Social Contract for the Information Society", Richard Mason lays the ground for an SLO lens on privacy:

"The modern social contract is based on an emerging Faustian bargain in information. In return for the knowledge and pleasure that new information provides us there are important new human costs which must be paid. Negotiating this bargain is perhaps the most pressing public and organizational policy issue of our times. As the social contract is renegotiated, information policy will become its most critical feature. No member of society – corporate executive, public leader or ordinary citizen – can escape its impact."[1]

Hence, compliance with privacy law must be guided by seeking fairness of digital dividend and social acceptance in exercising the right to privacy.

The tech giants have understood that and we have seen them struggle for SLO particularly since the Snowden revelations: in December 2013 eight tech giants wrote an open letter to President Obama calling for an urgent review of surveillance methods, distancing themselves from the NSA's indiscretions; more and more telcos are voluntarily issuing transparency reports on the number of law enforcement access requests they receive, hence re-directing

social opprobrium to the "requesters"; in the Microsoft Ireland case[2], the company stood up to the US Government on the extraterritorial reach of warrant access to personal information;[3] and who can forget Apple staring down the FBI on personal data encryption, with the support of several companies, on access to the iPhone owned by the San Bernardino couple responsible for a terrorist attack on December 2, 2015. More recently, WhatsApp, owned by Facebook, announced end-to end encryption on its app, standing up publicly to the Brazilian authorities in 2016 and meeting the wrath of the United Kingdom government after the London attack in February 2017.

Without discounting the genuine commitment of these companies, it is fair to assume that all had their sights on SLO.

Perhaps the most telling sign of a shift towards SLO as the test for privacy compliance and enforcement is the 2016 call by both Apple's CEO Tim Cook and then Director of the FBI James Comey for a legislative and societal debate about the issue of law enforcement access to personal data. Calling it a "societal issue". It was their one point of agreement: the informational social contract, or social license for the treatment of personal information, needs to be clarified in a new social, economic, security and technological context to protect privacy.

So how does this point to the future of privacy regulation? This is how the Fair Information Protection Principles could be applied through an SLO lens.

Accountability: De facto disempowerment of users

User behaviour surveys tell us that users by themselves are too overwhelmed by the complexity of information technology (IT) to hold organizations accountable. We all have read the statistics that, frankly, are repetitive:

- 52 percent of Americans online do not fully understand what a privacy policy is (Pew Research Center 2014) – these same people trust that privacy policies reflect that the personal information they provide to an organization will be held secure.
- Only 16 percent of users read privacy policies (Global Internet User Survey 2012).
- User concern about the protection of personal privacy has increased from 42 percent in 2012, 52 percent in 2014, to 57 percent in 2016 (Office of the Privacy Commissioner of Canada, OPC, 2016 Survey of Canadians on Privacy).

People are, at the same time, massively enjoying digital dividends and increasingly overwhelmed by the complexity of digital technology. This creates an imbalance of power between organizations and users, whether in government or business, that calls for an architecture of mediated accountability.

This mediated accountability is structured around the sphere of control of each actor. In other words, each actor is accountable for the privacy protection that is within its control:

- Governments are in control of the legislative framework, public policy, law and order, and public good; consequently, they are accountable for effective legislative regimes to protect privacy, including establishing an independent and effective Data Protection Authority (DPA) and public education about privacy rights and recourses.
- DPAs are in control of ensuring compliance with the legislation; hence, they are accountable for exercising their powers to hold organizations accountable on behalf of individuals, monitoring organizations to exercise the due diligence that users do not have the capability of applying, and informing the public to guide them in their privacy choices and assist them in protecting their rights.
- Organizations are in control of privacy protective management of the personal information in their custody. Consequently, their accountability therefore includes complying with relevant legal requirements, demonstrating such compliance, informing users of risks and protective measures on their platforms and providing proper privacy controls for users to implement their risk management choices, including ready access by users, erasure or correction to ensure accuracy and effective remedies as needed.
- Individuals are in control of the IT platform and privacy settings they choose, and the information they share. Their accountability therefore includes understanding the privacy implications of sharing information on digital platforms and exercising the corresponding controls.

That is the realistic model for accountability for compliance, taking into account social realities. The European Data Protection Supervisor uses an environmental analogy by referring to a "big data protection ecosystem"[4] to insist upon a multi-level approach of coordinated action according to reality of control.

An SLO approach makes the DPAs mediators of accountability on behalf of users. This is necessary to correct the growing power imbalance between users and organizations in view of the complexity and invisibility of the Internet operating systems.

The obligation to identify purposes – in a few words

Again, taking a picture of relevant social trends and social acceptance will guide interpretation or modernization of the law on this point:

- Since 2014, mobile has exceeded PC Internet usage – hence, identifying purposes has to occur on a small screen, within a short time.
- The issue has been addressed for some time as in the OPC, British Columbia OIPC and Alberta OIPC 2012 guidance 'Seizing Opportunity: Good Privacy Practices for Developing Mobile Apps'; the challenge is defined as "conveying meaningful information about privacy choices (…) with a small screen and intermittent user attention."
- Intermittent user attention may explain why 58 percent of the respondents to the OPC 2016 Privacy survey answered that they did not read privacy polices before downloading an app.
- And yet, 82 percent of the respondents expressed at least some concern about privacy and reputation, particularly in relation to postings and photos.

A social picture emerges from these statistics: privacy policies need to be relegated to the background because they have no real social relevance; and the essence of their content must move

to a pop up with a Privacy Policy link and consent button, at the user's choice. This addresses the transparency paradox where the more information an organization provides about its privacy policies, the less users read.

Based on social acceptance, we know that users do not want their information used for purposes other than the ones they bargained for. But we also know that they do not read privacy policies because they simply do not fit the Internet environment. An SLO approach would entail that: i) privacy information be written as a warning before going further; ii) the user have just enough information to exercise a choice but, iii) with an option to learn more. Going back to accountability, this quick identification of purposes and consent would be buttressed by increased monitoring by DPAs.

Consent

Again, thanks to the 2016 OPC Privacy Survey, we know that 48 percent of respondents felt they have lost control over the collection of their personal information by organizations. The most recent survey of the Pew Research Center buttresses the importance of control:

- 74 percent say it is "very important" to them that they are in control of who can get information about them; and
- 65 percent say it is "very important" to them to control what information is collected about them.

Autonomous collection of personal information (e.g. beacons and geolocation) gives reason for concern. In this context, the notion of consent appears essentially set aside. And yet, that would be socially unacceptable. Since the right to privacy is the right to determine what will be disclosed about us, consent is of the essence of privacy. We either consent individually — for example when we download an app or buy on line — or collectively when we accept the collection of personal information for the greater good — for example when we file our income tax or participate in a medical research trial.

An SLO approach elevates the notion of consent from strictly individual to collective: social acceptance, or adherence to an informational social contract, creates a context for what is reasonable to expect an individual to understand before providing consent. This entails applying a deferential lens to user choices. Provided all the information is accessible to base valid consent, that user controls are sufficient to exercise it, and that DPAs have the resources to monitor its compliance, user consent alone provides legitimacy of collection, use and sharing of personal information. It does not mean anything goes with consent. But it does mean that anything goes with informed consent, commensurate user control and regulatory oversight. With SLO, there is no second guessing the user, or judgment of what is reasonable to consent to.

Limiting collection, use, retention and disclosure

Again, grounding our analysis on social acceptance, surveys will serve as our proxy to define it with respect to the legitimate limits of collection, retention and disclosure. These are the relevant results of the 2016 survey of the US National Telecommunications and Information Administration (NTIA):

- 23 percent backed away from online activity due to unwanted data collection by online services; and
- 22 percent did the same for fear of loss of control over the use of their personal data.

The NTIA drew this conclusion from its survey that directs us to an SLO approach:

"It is clear that policymakers need to develop a better understanding of mistrust in the privacy and security of the Internet and the resulting chilling effects."[5]

It is fair to extend this comment to all organizations: collection, use, retention and disclosure of personal information should be guided by concern for user benefit and control, albeit at the expense of corporate objectives. The three tenets of SLO – public consultation, benefit sharing and impact assessment – apply here. The idea is to increase consideration of social acceptance as a decisional factor in the collection, use, retention and disclosure of personal information for both organizations in determining their practices, and regulators in assessing compliance with privacy law.

Accuracy, access and remedies

The right to accurate personal information is most challenged in the digital economy with respect to the permanence of the Internet, where it lasts long past the accuracy of personal information, and with respect to profiling through algorithms that may draw a very detailed, possibly inaccurate, profile of a user.

The internationally coordinated investigation of Global 24h, where the site was deliberately posting embarrassing legal information about individuals, is illustrative of addressing an issue on the basis of social acceptance. The OPC Report of Findings relied upon the Model Policy for Access to Records in Canada (Policy), developed by the Judges' Technology Advisory Committee of the Canadian Judicial Council (CJC) following public consultations where consensus was found as follows:

- Permitting unrestricted e-access to court documents may be harmful;
- Bulk search of electronic court documents by the public should not be permitted;
- Where public access is allowed, information should be de-identified;
- Data-mining of electronic court documents should be prohibited; and
- Remote public access to all court records is not desirable[6].

The public consultation by the CJC infers that a permanent posting on the Internet, beyond its relevance, is inaccurate and socially unacceptable.

The other new privacy risk of the Internet relevant here is profiling for advertising. It occurs and yet may be accurate or not, accessible or not, and remediable or not. *The Economist* reflects social consensus with an article on advertising and technology entitled 'Stalkers Inc'[7]. The article refers to that social consensus:

"Relevant ads are probably more useful to consumers than irrelevant ones. But any business based on covert surveillance is vulnerable to a backlash."

SLO would be met with the broadening of existing mechanisms that provide ready access to a profile (for e.g. Google Ad Preferences), and direct access to correction and elimination. This requires organizations to alert

users to the constitution of a profile with implied consent for non-sensitive personal information and low expectation of privacy, or with express consent for sensitive information in a context of high expectation of privacy with ready access to consult, correct and challenge as the case may be.

Safeguards

In the last NTIA survey, mentioned above, 45 percent responded that privacy and security concerns deterred them from performing at least one common online activity over the previous year such as financial transactions and purchasing goods or services. The reality of incessant and virulent attacks has impacts on social scrutiny of organizations. While every breach creates an uproar and financial loss (an average of $4M per breach according to Forbes 2017), SLO is only lost upon evidence of negligence in safeguarding the information or in responding to the breach. By way of example, that made the difference between the LinkedIn and the AdultFriendFinder (AFF) breaches.

The LinkedIn breach occurred in June of 2012. LinkedIn immediately notified the public, users and regulators, and remedied the situation. It responded with demonstrable care for users' data, integrity and transparency. It has doubled its users since then, showing that the diligence with which it responded to the breach may have, in fact, enhanced its SLO rather than reduced it.

In contrast, in the AFF breach in 2015, experts found evidence of lacks in safeguarding with inadequate cybersecurity. Users were offended by its delayed response to the breach. Risk to SLO was directly raised by David V Forte:

"How can a company salvage or maintain the trust of its customers after so easily losing the private information of 3.5 million accounts; let alone against supposedly a single hacker operating out of a small, foreign country across the world? Consumers may see this as a lack of interest in the safety of their personal information."[8]

The two examples show that an SLO approach to safeguards refocuses the obligation from outcome to diligence. Consequently, organizations must continue to address 100 percent of identifiable risks and document them, and regulators need to focus on due diligence in prevention and response rather than impact of breach.

Conclusion: Applying SLO lens to privacy law

Organizations and regulators have a common ground to apply privacy law: social acceptance. It puts the power where the right to privacy bestows it: with the user, not the letter of the law.

Organizations, private or public, protect privacy not as a mere regulatory framework but as a matter of social responsibility as trustees of users' personal information.

Regulators ensure compliance with privacy law on behalf of users, not in place of them, which means taking into account the dynamics of social acceptance rather than only the static rules of privacy law in a formal, bureaucratic manner.

AUTHOR

Chantal Bernier is Counsel at Dentons' Global Privacy and Cybersecurity Group, and former Interim Privacy Commissioner of Canada.
Email: Chantal.bernier@dentons.com

REFERENCES

1 Mason, Richard O, Forming the Social Contract for the Information Society, (1980) ICIS 1980, Proceedings, 17, aisel.aisnet.org/icis1980/17/
2 *Microsoft v. United States*, No. 14-2985 (2d Cir. 2016)
3 *Microsoft Corp. v. The U.S. Department of Justice, et al.*, No. 2:16-cv-00538, W.D. Wash.). (Opposition to dismissal motion available. Document #97-160922-019B.)
4 Opinion 4/2015 Towards a New Digital Ethics p.9
5 Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NTIA Office of Policy Analysis and Development May 13, 2016.
6 https://www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_Synthesis_2005_en.pdf,
7 September 11, 2014 at www.economist.com/news/leaders/21616953-surveillance-advertising-industrys-new-business-model-privacy-needs-better
8 www.linkedin.com/pulse/impact-adult-friend-finders-data-breach-dario-v-forte

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Germany's new DP Act: Big news or business as usual?

The current rule of appointing a DPO in organisations remains. There is no cap on fines and there is the possibility of a criminal sentence of up to three years. By **Katharina A. Weimer,** Senior Associate, Gowling WLG, Munich.

In the midst of the "winds of change" brought by the General Data Protection Regulation (GDPR), Germany's parliament (the *Bundestag*) and the Federal Assembly (the *Bundesrat*) passed a new bill on data protection (the German Draft), waiting to be signed by the Federal President as the final step of the law-making process[1]. With the German Draft, the German government aims at implementing the

Continued on p.3

EDPS: New e-Privacy law will mean stronger enforcement

The EDPS welcomes the form of an EU Regulation for e-Privacy but calls for stronger protection for metadata, and envisages some flexibility on consent. **Laura Linkomies** reports from Brussels.

The Regulation on Privacy and Electronic Communications is proposed to take effect from 25 May 2018, and aligns with the GDPR on many aspects. In an exclusive interview with *PL&B*, Giovanni Buttarelli, the European Data Protection Supervisor, said that the GDPR will "remain incomplete without this additional exercise." He welcomes the fact that the proposal extends the scope of e-Privacy rules

Continued on p.7

Issue 147 **June 2017**

INTERNATIONAL report

ISSUE NO 147 JUNE 2017

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.thomas@privacylaws.com

CONTRIBUTORS
Scott Livingston
Simone IP Services, Hong Kong

Sophie Lawrance and Noel Watson-Doig
Bristows LLP, UK

Chen Hui-ling and Michael Fahey
Winkler Partners, Taiwan

Katharina A. Weimer
Gowling WLG LLP, Germany

Laura Hall
Allen & Overy, US

Meredith Jankowski and Michelle Anderson
DLA Piper LLP, US

Chantal Bernier
Dentons LLP, Canada

Published by
Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
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

comment

Germany: Milestone reached in GDPR implementation

Germany has issued a new draft law to implement the provisions of the GDPR, and may be the most advanced with its plans within the EU. The draft law, adopted by the Parliament on 27 April is not easy to understand – and is in places stricter than the GDPR. For example, the law introduces the possibility of imprisonment of up to three years (p.1).

The intersection of US litigation and EU Data Privacy Laws means that controllers who may become involved in US litigation should consider potential obligations to retain, review and produce documents when drafting privacy policies and notices (p.15). The extra-territorial reach of the GDPR is a concern for non-EU companies offering goods and services in the region – when does it apply? Our correspondents analyse the situation on p.18.

An example of the global reach of the GDPR is that the US multinational Stanley Black & Decker chooses to follow the GDPR standard across its operations (p.13) in order to simplify its compliance. But companies do not have to worry about just the GDPR – plans to adopt the e-Privacy Regulation are advancing. Read on p.1 what the EDPS, Giovanni Buttarelli thinks of the proposal.

In China, new data export restrictions need companies' attention (p.9), and mean cost implications for companies as well as restrictions on their use of cloud computing. New legislative developments take place in ASEAN countries (p.25). In Taiwan, we see an increase in enforcement action (p.23).

Data protection principles come into question when determining whether a company has a dominant position under competition law, and organisations need to consider the extent to which collusion in relation to privacy policies is an area that competition authorities may investigate (p.20).

To conclude, organisations need a 'social license' to operate – the social acceptability of a business is key in the future privacy landscape, says Canada's former Interim Privacy Commissioner Chantal Bernier (p.28).

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 100+ 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 100+ 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, Denstu Aegis Network**"

Subscription Fees

Single User Access

International Edition **£550 + VAT***

UK Edition **£440 + VAT***

UK & International Combined Edition **£880 + VAT***

* VAT only applies to UK based subscribers

Multi User Access

Discounts for 2-10 users. Enterprise licence for 11+ users.

Subscription Discounts

Introductory 50% discount. Use code HPSUB (first year only) for DPAs, public sector, charities, academic institutions and small and medium companies.

Discounts for 2 and 3 year subscriptions

International Postage (outside UK):

Individual International or UK Edition
Rest of Europe = £22, Outside Europe = £30

Combined International and UK Editions
Rest of Europe = £44, Outside Europe = £60

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