US State legislatures are active on privacy issues

Several states aim to legislate on cyber security and drones, and there are plans to widen the definition of "personally identifiable information". **Bob Belair** reports from Washington DC.

When the international privacy community thinks about privacy in the US, they focus, quite understandably, on the Trump Administration and the Congress. What the Trump Administration and the Congress have done (mostly said, rather than done) and what they may do are critical. We discussed the Trump Administration's privacy posture in our last article (*PL&B International* December 2016, p.1) and, undoubtedly, we will do so in future articles. But, as privacy experts know, there's another important source of US privacy policy – state legislative action.

From January through March and into April, almost every US state legislature is in session (some, like New York and California, stay in session almost all year and a few states have adopted other schedules. Texas, for example, meets only twice a year). Historically, about five percent of all legislation considered by state legislatures each year relates in one way or another, and to one degree or another, to the protection of personal privacy. That continues to be true in this cycle. More specifically, we are seeing significant volume in both introduced legislation and legislation reaching the state Governors' desks in the following areas:

1. Expanding the definition of "personally identifiable information" (PII);
2. Enhancing protections for sensitive categories of PII including:
   - Education
   - Health
   - Biometric;
3. Enhancing protections with respect to certain types of both state government and non-government surveillance and, specifically, a flood of bills regulating the collection of PII by unmanned, aerial devices (drones); and
4. Enhancing cybersecurity and data breach protections.

Expanding definition of PII

Historically, the Federal Trade Commission (FTC) has been the leader in attempting to expand the definition of "personally identifiable information". In an April 2016 blog post, former FTC Consumer Protection Bureau Director, Jessica Rich, said: "We now regard data as personally identifiable when it can be reasonably linked to a particular person, computer or device." This is consistent with the position that the FTC took in its 2012 Privacy Report and in its Children's Online Privacy Protection Act Rule. The FTC's April 2016 blog post labels "persistent identifiers, such as device identifiers, MAC addresses, static IP addresses, and retail loyalty card numbers" as PII.

The states have taken note. California has already characterised log-in credentials as PII in connection with data breach notice requirements. Florida, North Dakota, Nevada and Wyoming have followed suit. Effective in January 2017, Nebraska, Rhode Island and Illinois also defined email addresses or usernames in combination with a password as PII.

Privacy protections for sensitive types of PII

Student information: In this legislative cycle, the states are particularly interested in enhancing protections for student related PII. The federal Family Educational Rights and Privacy Act already provides baseline confidentiality and other privacy protections for PII in records held by educational institutions. This year the states are doing more.

Two jurisdictions have already enacted new protections. The District of Columbia has enacted legislation which extends privacy protections to any student-related data that can be de-aggregated or reconstructed to identify an individual student. The new law also prohibits schools and other educational agencies from compelling students to provide their social media passwords or configurations.

On the other side of the country, the Wyoming legislature has also acted to require the state Superintendent of Education to develop standards for school districts for protecting student privacy including collection, student access, security and use of student data by school districts.

In addition, several other states are poised to enact new student privacy legislation. Arizona, for example, is expected to enact legislation to require third parties that have access to student PII to maintain comprehensive security procedures and to delete student information when requested by the school from which they obtained the information.

Illinois is also expected to enact legislation enhancing protections for student privacy including regulating contractors' access to, and use of, student information.

The Virginia legislature has passed a bill that is currently awaiting the Governor's signature to require school service providers to assure that students and, in the case of minor students, their parents have access to student records in a user-friendly format.

Three other states – Connecticut, Idaho and Rhode Island – are actively working on legislation that would enhance student data privacy including a bill in Rhode Island that would limit school officials' ability to monitor and search a student's "take-home technology devices".

What we are seeing in the education space is state legislatures seeking to enhance cybersecurity; address social media and new technology issues; and extend privacy protections to vendors and other school contractors.

Health PII: In this cycle, state legislatures have also moved to enhance privacy protections for health data. The Health Insurance Portability and Accountability Act (HIPAA) already provides comprehensive privacy

protections for health information originated by, or in the possession of, health care providers, payers and clearinghouses. Most of the state legislative activity is aimed at extending health privacy requirements to the health insurance regulatory environment (Arkansas and Washington State); providing additional security protections for health PII (Pennsylvania and Massachusetts); and enhancing penalties for data breaches involving protected personal health information (Massachusetts).

Biometric PII: Many states have recently acted, or are in the process of acting, to make biometric data a trigger for data breach notification requirements and related remedies. Biometric data is customarily defined to include a fingerprint, voice print, retina or iris scan, facial imaging or facial geometry. Illinois recently adopted legislation to broaden the definition of biometric PII to include, "unique biometric data generated from measurements or technical analysis of human body characteristics".

Illinois is also actively considering legislation to amend their biometric information privacy act to prohibit a private entity from requiring a person or customer to provide their biometric identifier or biometric information as a condition for the provision of goods or services.

In addition, Washington State is actively considering legislation that would restrict and regulate the collection, as well as the sale, of biometric information.

Surveillance

With the Trump Administration now in place, no privacy issue has generated more concern, both in Washington and in the state capitols, than surveillance. But what can the states do about it? Not much, given that for a variety of reasons and in a variety of ways, states are stopped from regulating federal surveillance behavior.

But, this has not stopped larger and more privacy protective states – such as Illinois and New York – from trying to address surveillance issues. New York, for example, is actively considering a bill that would create a state Commission on Personal Privacy, "in light of rapid technological advances". New York is also considering legislation that would prohibit the installation, transmission or use of computer software that collects and transmits personally identifiable information without the authorisation of the device's owner. Illinois may enact the "Geolocation Privacy Act" which would prohibit a private entity from collecting, using, storing or disclosing location based information obtained from a person's mobile device unless the entity has first received that person's express affirmative consent.

The states do have authority to regulate non-federal operation of unmanned aircraft systems, otherwise known as drones. Remarkably, in the 2017 cycle, legislatures in 38 states are considering legislation to regulate, and mostly restrict, the use of drones. South Dakota, Virginia and Wyoming have already passed legislation requiring relevant state agencies to develop rules regulating drone use.

Other states are actively considering legislation that would prohibit a private entity from collecting PII from the use of a drone without the express consent of the person whose PII is being collected. Hawaii and Maine, among other states, are considering such legislation. In addition, many states including Kentucky, New Hampshire, New York and Massachusetts either restrict or altogether prohibit state governmental or law enforcement agencies from using drones to collect PII.

Data breach, cybersecurity and privacy enhancements

Many state legislatures are quite active in 2017 enhancing data breach protections; addressing cybersecurity threats; and, more generally, seeking to enhance information privacy protections.

Several states, for example, have added the acquisition of (or collection or access to) health information as a trigger for a data breach. Oregon, Illinois, Nebraska and Nevada all fall into this category. California, the worldwide leader in data breach protection, is considering comprehensive amendments to its data breach legislation to enhance benefits for breach victims.

Many states are also addressing cybersecurity threats. For example, Mississippi, on 10 March, enacted legislation establishing a cybersecurity program to provide comprehensive and coordinated cybersecurity systems, services, policies and standards. Alabama is considering the Information Protection Act of 2017 which would provide enhanced protections for sensitive personally identifiable information. Texas is considering the "Texas Cybersecurity Act" which adds protections to PII held by Texas state agencies.

Many states are also moving to enhance the security and integrity of state-issued drivers licenses. Arkansas, Oklahoma, Alaska, Idaho, Maine, Minnesota, Missouri, Oregon, South Carolina and Washington are all latecomers to complying with federal requirements (and eligibility for federal dollars) by enhancing the security and reliability of the identification features on their state issued drivers licenses.

In a related initiative, several states are moving to restrict the use of automated licence plate readers. Illinois is actively considering a bill that would prohibit the use of, or sharing of, information harvested from automated licence plate recognition systems except where the law enforcement agency has obtained an administrative authorisation. Montana is considering similar legislation.

State privacy enhancements

The US privacy landscape is complicated. The President, several of the federal regulatory agencies, the Congress, the state legislatures and even the state governors and regulatory agencies all have an opportunity to initiate or enhance privacy reforms. The result can be frustrating – even counterproductive. But, the results can also be surprisingly positive.

In a US political environment, where neither the President nor the Congress are looking to enhance privacy protections, the state legislatures, as set out above, are quietly going about developing and/or upgrading a variety of key privacy protections.

AUTHOR

Bob Belair is a Partner at Arnall Golden Gregory LLP and will address these issues as a speaker at *Privacy Laws & Business's* 30th Annual International Conference, *Promoting Privacy with Innovation*, 3-5 July at St. John's College, Cambridge see www.privacylaws.com/annualconference/
Email: robert.belair@agg.com

ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

Privacy Shield up and running and surviving initial hurdles

The EU-US Privacy Shield is valid for now but a DPA assessment is due in September. In the meantime, US-based companies are self-certifying and DPAs are preparing to deal with complaints. By **Laura Linkomies** and **Stewart Dresner**.

The Privacy Shield has now been adopted by some 1,800+ US-based companies, and the Department of Commerce is currently reviewing an additional 300+ companies' applications. Half of these companies are Small and Medium Enterprises. So on the US side, the programme is being adopted more widely, and can be seen as successful in terms of take-up. To compare, the EU-US Safe Harbor

Continued on p.3

Argentina to update its data protection law

Argentina's Data Protection Authority has proposed reforms to the current law which the government has accepted, explains its Director, **Eduardo Bertoni**.

Argentina's Data Protection Law (25.326) was passed in October 2000 and entered into force one year later. Technological changes that have taken place during the last 16 years have had an impact on the protection of personal data and triggered new possible violations of the right to privacy. Furthermore, the experience accumulated by the Argentine Data Protection Authority during all these

Continued on p.5

Issue 146 **April 2017**

INTERNATIONAL report

ISSUE NO 146 APRIL 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
Glenn Daif-Burns
glenn.daif-burns@privacylaws.com

CONTRIBUTORS
Bob Belair
Arnall Golden Gregory LLP, US

Eduardo Bertoni
Data Protection Authority, Argentina

Robin Bayley
Linden Consulting, Canada

Agatha Moczulski, Michael Swinson, Patrick Gunning and Kate Jackson-Maynes
King & Wood Mallesons Australia

Nathalie Metallinos
IDEA avocats, France

Hiroshi Miyashita
Chuo University, Japan

Merrill Dresner
PL&B Correspondent

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

GDPR's influence growing even before it is in force

The Commissioner for Justice of the European Commission, Věra Jourová, visited the United States at the end of March to seek assurances about the EU-US Privacy Shield and announced a review in September (p.1). In the meantime, EU DPAs have prepared a complaints form and procedure for Europeans should they need to complain about the processing of their personal data by US companies which are Privacy Shield participants (pp. 4-5).

The European Parliament's Civil Liberties, Justice and Home Affairs Committee (LIBE) voted recently to support a resolution declaring the Privacy Shield to be inadequate. It is expected that the resolution will be voted on by the whole of the Parliament soon.

Argentina is taking a different path by updating its existing law to include some of the elements of the GDPR. Argentina already has an adequacy decision from the European Commission, dating back to 2003, but has now issued a draft law, the Director of Argentina's DPA writes in an article exclusive to *PL&B* (p.1).

In the US, the Republican majority in the US Congress has voted to repeal the Federal Communications Commission privacy protections for Internet users and President Donald Trump has signed it. This could have dire consequences for consumer privacy. On the whole, it seems that privacy friendly initiatives are now limited to state level legislation. One of the issues getting much attention is drones (p.6). States are also passing bills to strengthen consumers' online privacy.

In the UK, Brexit is causing concern to UK data controllers because of the risk of future incompatibility of UK data protection law with the EU DP Regulation, despite the government announcing that the GDPR will apply come May 2018 (p.11). Elizabeth Denham, the UK's Information Commissioner, recently gave evidence to the House of Lords EU Home Affairs Sub-Committee, where she recommended that the best option to guarantee uninterrupted data flows would be for the UK to apply for EU adequacy decision as soon as Article 50 is triggered – so that would be possible now.

DPA cooperation is more important than ever and in Europe it will be an element present in the GDPR. The European Data Protection Board is being set up to replace the EU Art. 29 DP Working Party. It remains to be seen whether the UK can sit at the table. Graham Greenleaf explores the DPAs' networks and channels for their international cooperation (p.14).

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, Chief Privacy Officer, BT Group, UK**"

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