ReedSmith

Global Regulatory Enforcement

If you have questions or would like additional information on the material covered in this Alert, please contact one of the authors:

Paul Bond
Partner, Princeton
+1 609 520 6393
pbond@reedsmith.com

Christopher Cwalina
Counsel, Washington D.C.
ccwalina@reedsmith.com
+1 202 414 9225

Amy Mushahwar
Associate, Wasington, D.C.
+1 202 414 9295
amushahwar@reedsmith.com

Nick Tyler
Associate, London
+44 (0)20 3116 3695
ntyler@reedsmith.com

Christine Nielsen
Associate, Chicago
+1 312 207 6459
cnielsen@reedsmith.com

…or the Reed Smith lawyer with whom you regularly work.

Department Of Commerce Steams Ahead With Privacy Regulatory Blueprint: What You Need To Know

I. Introduction: Overview of the Document, Process and Political Context

A. Although the Commerce Data Privacy Report does not have legal effect, class action attorneys can use reports like this to inform a complaint. *Example*: Flash cookie claims in Arkansas – Class action attorneys referenced the FTC and Commerce reports from December 2010 that served no legal effect as the reports were still in draft form.
The Department of Commerce report takes a very business friendly tone, which will be in opposition to the report that will soon emerge from the Federal Trade Commission. This tone is keeping with the approaches Commerce and the FTC have taken on other issues, most recently the Google Privacy Policy integration changes.

1. Commerce General Counsel Kerry stated Google had been "very transparent" on its privacy practices.
2. FTC Chairman Jon Liebowitz states the privacy policy forces consumers to make a "brutal choice."

B. Public Comments are being requested by the Department of Commerce on this white paper.
C. FTC Privacy Report will be published soon and will emphasize Privacy by Design, greater online transparency, and greater consumer choice (i.e., Do Not Track).

II. Consumer Bill of Rights: Consumer Control, Transparency, Respect for Data Context, Secure Handling of Data, Access & Correction, Data Minimization and Accountability

A. The principles in the Bill of Rights emerge from the FIPPS.

1. Principles are meant to be flexible.
2. Affirms set of consumer rights and emphasizes the importance of context.
3. Appendix to the report includes a comparison of the Consumer Privacy Bill of Rights to other statements of FIPPS.

B. Scope is expanded to include some identifiers that have not previously been thought of as "personal information."
C. Principles

1. Consumer Control
   a) Any company that collects data about individuals must give consumers appropriate choices about the data it collects irrespective of whether the company uses the data itself or discloses to third parties.
   b) Different level of choices for consumer facing companies and non-consumer facing companies.
      (1) Consumer facing: simple, persistent and scalable, from the consumer's perspective
      (2) Non-consumer facing: companies should seek innovative ways to provide effective consumer choice
   c) Consumer Responsibility – Need for companies to provide consumers with an opportunity to withdraw consent.
2. Transparency
   a) Mobile – Provide disclosures in manner that accounts for the mobile device.
3. Respect for Data Context
   a) The most important point is the relationship the company has with a consumer. That relationship distinguishes the levels of notice and choice that must be provided to consumers.
   b) Context distinguishes personal data

March 2012
reedsmith.com

c) Business processes necessary to provide services
d) Companies should limit the use of the data for relationship they have with consumers and the context consumers originally disclosed the data.
e) If the company's use is for purposes outside of the original purpose, heightened transparency and choice should be provided.
f) Age/sophistication of consumer needs to be taken into account – minors, for example.
g) Commonly accepted practices v. Non-commonly accepted practices
(1) An example of a commonly accepted practice is the disclosure of customer name and address to fulfill orders.
(2) Another example is for a game application on a mobile device – company collects unique device number for purposes of saving the game. But, if the unique identifier is used for another purpose, the company should provide notice to the consumer and allow them to prevent that disclosure. The second use of the data is a non-commonly accepted practice.

4. Secure Handling of Data: Assess security risks and data practices.
5. Access & Correction
a) Consumers should have the right to access and correct personal data in a matter that is appropriate with the sensitivity of the data.
b) Report extends the right to access and correct data outside of existing sectors that already require it – like HIPAA and FCRA.
c) Level of access and opportunity to correct is dependent on the scale, scope and sensitivity of the data collected, as well as the likelihood that data, if exposed, will cause financial, physical, or other material harm.
6. Data Minimization
a) Companies should collect only as much data as they need to accomplish the task.
b) Wide data collection may be essential for some services, but not others.
7. Accountability
a) Three ways a company is accountable:
(1) Companies should be accountable to enforcing authorities and consumers for adhering to principles.
(2) Need to hold employees responsible for adhering to the principles and provide training.
(3) Where appropriate, companies should be conducting personal information audits.
b) Third parties – if you disclose data to third parties, affirm that the third parties are under enforceable contractual obligations.

III. Public-Private Partnership to Enact Voluntary Codes in the Absence of Legislation & DAA Support; Potential Impact of Report on Legislative Agenda

A. Public – Private Partnership to Enact Voluntary Codes
1. Both the Department of Commerce and the FTC are going to do what they can right now and will not wait for federal legislation.
2. Commerce will convene industry and privacy advocate stakeholders. This means workshops – companies can have the opportunity to get out ahead of this issue by helping to draft the self regulatory code.
3. Commerce anticipates the FTC enforcement will be a critical component of the self-regulatory framework.

B. Support of the Digital Advertising Alliance's Initiatives
1. DAA initiatives have been lauded as good examples of self regulation. The fact that the

DAA has a strong enforcement mechanism in the Council of Better Business Bureaus is another reason why the DAA's program has this support.

2. Significantly, both the FTC and Commerce identified that the Digital Advertising Alliance's Online Behavioral Advertising and Multi-site standards will be used as the standards to assist browser companies in the development of a Do Not Track header. The details for how the browser-header based solution are still to be ironed out, but it is significant that government and industry have now settled on a standard after years of wrangling about what is the best standard to help consumers recognize opt-outs.

C. Legislation

1. Even though the headline from last week was "we can't wait," legislative proposals are still contemplated in this draft. The Department of Commerce would like to see the following legislative items passed:

a) Codification of the Consumer Bill of Rights;

b) National Breach standard;

c) Direct grant of FTC Enforcement Authority;

d) Safe Harbor to the Consumer Bill of Rights;

e) Greater uniformity of privacy laws on a state level, with the respect that states still have a role (essentially, preempting laws that would be inconsistent, but likely leaving room for states to be more protective)

f) Preserving sector-specific laws (HIPAA, GLB, CAN-SPAM, COPPA, FERPA, CPNI, etc.).

IV. Enforcement (FTC Lead/Safe Harbor Supported/Still Anticipates State Enforcement Role)

A. Enforceable Code of Conduct

1. Multistakeholder process to develop codes of conduct that implement the general principles in the Consumer Privacy Bill of Rights.

2. The Department of Commerce report recommends granting APA rulemaking authority to the FTC to review codes of conduct against the Consumer Privacy Bill of Rights, provide a public comment period on proposed codes, and finalize the codes of conduct through that rulemaking process.

3. Once the code of conduct is complete, companies to which the code is relevant may choose to adopt it.

a) A company's public commitment to adhere to a code of conduct will become enforceable under FTC Act §5.

b) Similarly, a company's public commitment to adhere to a code of conduct will become enforceable under state UDAP laws.

4. Do we need to worry about the states?

a) Maryland Attorney General Doug Gansler, NAAG President-elect, will spearhead a national initiative examining privacy and the internet for the 2012-13 year. AG Gansler takes over as President in June 2012.

b) The states have historically investigated companies for making representations in privacy policies about the protection of personal information and not living up to those representations.

(1) By way of recent example, a multistate AG letter was sent to Google regarding its privacy policy changes.

5. Codified Consumer Privacy Bill of Rights – Legislation that tracks the Consumer Privacy Bill of Rights.

a) Enforcement

(1) FTC

(2) State AGs

b) Safe Harbor. Forbearance from enforcement of statutory Consumer Privacy Bill of Rights.

(1) Commerce also recommends providing forbearance from enforcement of state laws against companies that adopt and comply with Codes of Conduct.

c) Preemption. Commerce recommends enacting legislation that preempts state laws to the extent they are inconsistent with the Consumer Privacy Bill of Rights.

V. International Interoperability

A. Commitment made to "increasing interoperability with the privacy frameworks of the United States' international partners." Three means of achieving this:

1. Mutual recognition
2. Development of codes of conduct
3. Enforcement co-operation

B. The Department of Commerce report alludes to the need for "more flexible, innovation-enhancing privacy models among our international partners" = Europe = 'Elephant in the Room'.

C. The current international landscape

1. January 25, 2012 - European Commission published draft of a proposed Data Protection Regulation to replace the European Data Protection Directive (dating back to mid-1990s). The Regulation is expected to come into force across the European Union within the next 3 years.
2. The intent behind implementation through a Regulation, rather than a Directive, is to achieve greater consistency and harmonization than has been achieved through local national laws implementing the Directive - the 'patchwork quilt'.
3. Optimism that Regulation will achieve this aim tempered - the UK regulator (ICO) concerned that harmonization is not achievable on the basis of entrenched cultural, political and legal differences across the EU. On a more positive note, lawmakers and regulators on both sides of the Atlantic are, at the highest level, speaking the same language.

VI. Convergence theme

A. Scope of "personal data/information" in the Commerce report is wider – looks more European

B. Appendix B – comparison of Consumer Privacy Bill of Rights and other statements of FIPPS, including OECD Principles of 1980 on which most of 89 and counting global data privacy laws are based.

C. Straightforward exercise to map on to the Consumer Privacy Bill of Rights, some of the core elements of EU Data Protection Regulation: individual control, transparency, focused collection, access and accuracy (which present real practical challenges that EU experience can inform), as well as security equate to well-established EU data protection concepts of fairness, transparency, purpose limitation, data minimization, individual rights of access and correction, and security (including employee training and vendor contracts)

D. New accountability principle – stand-out new element of EU proposal

1. Success of accountability principle in APEC countries and US self-regulation/compliance practice
2. At the root of adoption of binding corporate rules as a solution to EU transborder dataflow restrictions for multi-nationals
3. Essential role of Chief Privacy Officer cannot be emphasized enough.
4. Privacy by Design concept
5. Privacy Impact Assessments as a practical compliance tool

E. Existing US Laws that have been exported to EU:

1. Data breach notification – US criticism of focus on process rather than improving security practices – general concerns expressed by others about practicality of 24 hour timescale for notifying regulators and lack of seriousness threshold for breach notification.
2. Children - EU Regulation's verifiable consent requirement for children was modified at late stage (after US intervention) from age limit of under-18 years to under 13 years, which is more in line with COPPA.

F. Continuing concerns from U.S. and business community about EU proposals for "right to be forgotten," continued restrictions on transfers to 'third countries' including U.S. (will there be a new Safe Harbor?) and international investigations (EU data protection laws seen as blocking statute).

G. Respect for Context

1. Very familiar from UK perspective and concept of purpose limitation and the practice of fair processing. UK approach strongly advocates the importance of adding a layer of practicality, flexibility and common-sense to communicating with consumers about personal information handling practices. Not optimistic that such approach is, or will be, applied consistently across Europe.
2. "In law, context is everything."

VII. Privacy Class Action Litigation; Summation, farewell, and call to action

A. Difference between the 2010 draft version and the 2012 final version:

1. 2010 version – FIPPS backbone
2. 2012 version – FIPPS converted into a Consumer Privacy Bill of Rights
   a) What are consumers being promised about the future of privacy, and what is the practical reality?
   b) Consumer expectations are being ratcheted up.

B. Increase in class action litigation.

1. More suits regarding what companies are doing with personal information.
2. Reassess risk management with respect to privacy litigation and appropriately insure against a rising risk in a volatile area.

About Reed Smith

Reed Smith is a global relationship law firm with more than 1,600 lawyers in 23 offices throughout the United States, Europe, Asia and the Middle East.

The information contained in this Client Alert is intended to be a general guide only and not to be comprehensive, nor to provide legal advice. You should not rely on the information contained in this Client Alert as if it were legal or other professional advice.

Reed Smith LLP is a limited liability partnership registered in England and Wales with registered number OC303620 and its registered office at The Broadgate Tower, 20 Primrose Street, London EC2A 2RS. Reed Smith LLP is regulated by the Solicitors Regulation Authority. Any reference to the term 'partner' in connection to Reed Smith LLP is a reference to a member of it or an employee of equivalent status.

This Client Alert was compiled up to and including March 2012.

The business carried on from offices in the United States and Germany is carried on by Reed Smith LLP of Delaware, USA; from the other offices it is carried on by Reed Smith LLP of England; but in Hong Kong, the business is carried on by Reed Smith Richards Butler. A list of all Partners and employed attorneys as well as their court admissions can be inspected at the website www.reedsmith.com.

© Reed Smith LLP 2012.

All rights reserved.

March 2012
reedsmith.com

ReedSmith

The business of relationships.

NEW YORK
LONDON
HONG KONG
CHICAGO
WASHINGTON, D.C.
BEIJING
PARIS
LOS ANGELES
SAN FRANCISCO
PHILADELPHIA
SHANGHAI
PITTSBURGH
MUNICH
ABU DHABI
PRINCETON
N. VIRGINIA
WILMINGTON
SILICON VALLEY
DUBAI
CENTURY CITY
RICHMOND
GREECE
OAKLAND