Autor:	James Chang, James G. Gatto, Meighan E. O'Reardon	**Quelle:**	Verlag Dr. Otto Schmidt, Köln
Dokumenttyp:	Aufsatz	**Fundstelle:**	CRi 2013, 70-74

Mobile Privacy Practices

Recent California developments indicate what's to come

James Chang, *James G. Gatto*, *Meighan E. O'Reardon*[*]

The use of mobile applications has seen huge growth in the past few years. As the use of apps becomes increasingly commonplace, social concerns such as the privacy of app users will increasingly need addressing. California is taking the lead in regulating this important issue. This article provides an overview of mobile privacy (I. and II.), a summary of California's stance on how to address the issue, an overview of the state's principles regarding privacy (III.), its best tips for complying with its principles (IV.), and an examination of the privacy related laws outside of California (V.).

I. Introduction to Mobile Privacy

The use of mobile applications ("apps") continues to grow at a staggering rate. According to a recent press release, as of May 2013 users of Apple's App Store have downloaded over 50 billion apps.[1] This marks a significant increase since crossing 40 billion downloads at the beginning of 2013.[2] Furthermore, according to Apple, nearly 20 billion of the 40 billion downloads occurred in 2012. Apple's App Store first opened in July 2008; thus, users downloaded nearly the same number of apps in 2012 as they did in the prior two and a half years combined. Similarly, Google recently reported that users of its app store have downloaded over 48 billion apps.[3] To meet this demand, developers are responding with a large selection of apps. Apple recently disclosed that its App Store hosts over 850,00 apps.[4]

Despite widespread use and adoption, mobile apps are particularly problematic from a privacy perspective. The privacy risks posed by apps are significant; by their nature mobile devices are portable, and apps provide easy access to vast amounts of personal information including user location information. This combination is risky. Furthermore, users are often multi-tasking or distracted while navigating through content on their mobile devices, and small screens make it difficult to detect malicious activities that expose personal information.

As the use of mobile applications continues to grow, and the risks of use abound, it is important to consider the legal requirements of creating and releasing apps. Significantly, app developers must not only conform to the relevant law in their own jurisdiction, but they must also consider the law in the jurisdiction of the users of their apps as well. The need to focus on these issues is even more compelling and timely in light of the fact that newly appointed FTC Chair, Ms. Edith Ramirez, has announced that she will specifically focus on Children's Online Privacy Protection Act (COPPA), regulating mobile apps, and Internet privacy.

II. Summary of California's Approach to Mobile Application Compliance

California has traditionally been at the forefront of U.S. privacy developments, and the state's recent enforcement of its privacy laws against mobile app developers signals increasing regulatory attention in this market. Within the last year, the California Attorney General's Office established a Privacy Enforcement and Protection Unit to ensure that information collected on the state's residents conforms to statutes such as the California Online Privacy Protection Act (OPPA).[5] The Enforcement Unit's mission is to protect Californians' right to privacy, which the unit does by enforcing state and federal privacy laws, and developing programs to educate consumers and businesses on privacy rights and best practices. In late 2012, the Enforcement Unit and California's Attorney General specifically began targeting mobile app developers and operators.

Similar to websites and more traditional online applications, mobile app developers and operators collecting the personal information of California residents must have a conspicuously posted privacy policy that describes clearly and completely how personal data is collected, used, and shared. Without such a privacy policy in place, mobile app developers and operators could face fines. Additionally, to better assist developers, the Attorney General has published a set of privacy guidelines highlighting best practices.[6] These guidelines provide a general framework of the steps a developer can take to conform with California's requirements.

III. California's Joint Statement of Principles and Enforcement

California is poised to play a significant role in the mobile space given that it is home to many of the corporations leading the mobile revolution and has stringent consumer protection and privacy laws. Because of the number of app developers in the mobile space, California has opted to address deficiencies in mobile privacy by pursuing a strategy with the key app platforms. On February 22, 2012, the Attorney General of California reached an agreement with the six leading mobile application platforms – Amazon, Apple, Google, Hewlett-Packard, Microsoft, and RIM[7] – to create a statement of five principles to foster innovation in privacy protection, promote transparency, and facilitate compliance with privacy laws in the mobile arena (the "Joint Statement of Principles").[8] On June 22, 2012, the Attorney General expanded that agreement to include social applications when it announced that Facebook became the seventh company to sign on.[9]

The Joint Statement of Principles affirms the premise that if an app collects personal information, the app must have a privacy policy. Perhaps most significantly the Joint Statement of Principles makes it practically possible for app developers to comply with California's requirements. The Principles provide for mechanisms on each app platform to (i) allow developers to load their privacy policies into the app store, and (ii) provide users with the opportunity to review app privacy policies prior to downloading the app in question. Previously, users would often need to hunt within applications, already purchased and virtually impossible to "return," just to find the applicable privacy policies.

The Joint Statement of Principles specifically states:

- 1 *Privacy Practice:* Where applicable law so requires, an application ("app") that collects personal data from a user must conspicuously post a privacy policy or other statement describing the app's privacy practices that provides clear and complete information regarding how personal data is collected, used and shared.
- 2 *Transparent Availability:* In an effort to promote greater transparency and to increase developer awareness of privacy issues, the Mobile Apps Market Companies will include, in the application submission process for new or updated apps, either

- (a)an optional data field for a hyperlink to the app's privacy policy or a statement describing the app's privacy practices or
- (b)an optional data field for the text of the app's privacy policy or a statement describing the app's privacy practices.

For developers who choose to submit a hyperlink or text in the available data field, the Mobile Apps Market Companies will enable access to the hyperlink or text from the mobile application store.

- 3 *Whistleblowing:* The Mobile Apps Market Companies have, or will implement a means for users to report to the Mobile Platform Companies apps that do not comply with applicable terms of service and/or laws.
- 4 *Response to Non-Compliance:* The Mobile Apps Market Companies have or will implement a process for responding to reported instances of non-compliance with applicable terms of service and/or laws. Any action that a Mobile Apps Market Company takes with respect to such an application will not limit

law enforcement or any other regulator's right to pursue an action against a developer for alleged violation of applicable law.

- 5 *Best Practices Review:* The Mobile Apps Market Companies will continue to work with the California Attorney General to develop best practices for mobile privacy in general and model mobile privacy policies in particular. Within six months the participants will convene to evaluate privacy in the mobile space, including the utility of education programs regarding mobile privacy.[10]

Following the release of the Joint Statement of Principles in the fall of 2012, the Office of the Attorney General of California sent letters to mobile application developers that failed to satisfy California's privacy laws and offered a thirty (30) day time period to comply. Specifically, the Attorney General sent out letters to the 100 most popular non-compliant apps at the time. The letters were the first step to enforce the California Online Privacy Protection Act against mobile app developers. Under OPPA, mobile app developers and companies are faced with fines of up to $2,500 each time a non-compliant app is downloaded.

On December 6, 2012, the Office of the Attorney General of California filed a lawsuit against Delta Airlines after Delta failed to comply with the terms of the letter from the Attorney General. The complaint alleged that Delta's mobile app could be used to check-in to a flight, view reservations, re-book cancelled or missed flights, pay for checked baggage, track checked baggage, access frequent flyer accounts, take photographs, and save a user's location. Despite collecting information such as a user's name, telephone number, email address, frequent flyer account number, pin code, photographs, and location; the app did not have a privacy policy, let alone one that was conspicuously posted.[11] Within a short period of time after filing suit, Delta published a mobile privacy policy for its app. The lawsuit was subsequently dismissed by the court because the Airline Deregulation Act prevents states from regulating airline services. Because Delta's app allowed users to, amongst others things, check-in to a flight, the court agreed with Delta that the California statute could not regulate its use. Although Delta was able to have the lawsuit dismissed on these grounds, most app makers should not count on being able to make a similar argument. Furthermore, the Attorney General's suit against Delta indicates California's willingness to enforce its privacy laws against app developers and owners.

IV. Privacy on the Go

In a further development related to mobile app privacy in California, in January 2013 the Attorney General of California published "*Privacy on the Go: Recommendations for the Mobile Ecosystem*". The report is directed toward app developers, app platform providers, and advertising networks and provides suggestions for best practices to help developers comply with California law.[12] The recommendations are meant to align with the widely accepted Fair Information Practice Principles (FIPPs), which form the basis for many privacy codes and laws around the world, including the federal Privacy Act of 1974 and

the California Information Practices Act of 1977; these principles include: transparency, purpose specification, collection limitation, use limitation, individual participation, data quality, security, and accountability.

The Attorney General's report aligns with the industry best practice of "privacy by design." The overarching themes of the report include:

- (i)minimizing surprises to end users, and
- (ii)sharing accountability between developers and third parties with access to users' personal information.

The guide recommends that an app's privacy policy be short and easy to understand. Furthermore, apps should include features which not only display a privacy policy, but give users alerts when their information is being used, and control over how data is used. The report also recognizes that protecting user privacy is not a task left solely to an app developer, but the decisions and actions of third parties are also key to protecting users' privacy.

The report provides practical recommendations for app developers to develop sound privacy practices including by: (1.) using data checklists, (2.) identifying privacy practices, (3.) drafting a clear privacy policy, and (4.) implementing certain enhanced privacy measures.

1. Data Checklists

If possible, privacy considerations should be made at the start of the app development process. As with most aspects of application development, it is easier to implement functionality at the onset, rather than revising existing code or functionality. The first step to ensure that privacy is taken into account at the beginning of the development process is to create a list of potential information that will be used in the app. With a checklist in place, developers should be better equipped to anticipate issues with data use.

2. Privacy Practices

An app owner's specific privacy practices will depend largely on the functionality of the app in question; however, conforming to general privacy principles helps to balance the needs of the consumer with the needs of the business. Transparency to end users as well as limited storage and collection of personal information are two such principles detailed in the report.

Customers appreciate transparency. In this information age, users have become accustomed to instantly finding information when and where they want it. Furthermore, transparency about privacy practices helps users become more comfortable with an app. One way to promote transparency is to make an app's privacy policy accessible from the app delivery platform before a user even downloads the app to their mobile device. In addition, once downloaded, the privacy policy should also be accessible from anywhere within the app. Finally, keeping in mind that many users begin using apps without

first reading a privacy policy, apps should draw users' attention to how their data (especially sensitive personal information) is being used.

It is recommended that apps should limit the amount of data collected and stored. In today's economy, information collected about users is a very valuable resource; however, users may reject an app if they feel that their information is being stored and used without their consent. It is also important to remember that personal information may be subject to differing laws and user expectations. When data deals with minors or sensitive information, developers must be especially careful to limit what data is collected. Furthermore, where possible, users should be granted granular control over their data, including by programming default settings that protect personal information.

Users expect developers to keep information safe from both external and internal threats. As a general principle, developers should limit access to personally identifiable information to just those employees

that need the information. Furthermore, information should be encrypted so that even if a network is compromised, the data is still protected.

3. Drafting a Privacy Policy
Once a developer has decided on the best practices for their app, a policy should be created to provide an overview of the practices adopted. California recommends that the policy be

- (i)easy to find for both existing and potential users, and
- (ii)easy to comprehend.

There are different ways that a privacy policy can be written so that it is user friendly. For example, one method is to have a layered approach with different versions of the policy, depending on how much detail a user is seeking, ranging from a broad overview to a detailed explanation of each provision. Another approach is to categorize the contents of the policy by the type of personal information that is collected (*e.g.*, biographical information, photos, location, etc.). It is also important to consider that mobile app privacy policies will often be read on mobile devices, and must be formatted accordingly.[13]

Besides making the policy accessible, the policy should also describe how personal information is used in a more concrete manner. Users appreciate clear definitions of information collected by an app, as well as the policy for retention of that information. If an app allows third party use of any information, the policy should describe how, why, and under what circumstances that information is available to the third party.

Finally, since privacy considerations are ever changing, privacy policies should be updated as the needs of the business and consumer change. Be sure to describe how consumers may contact the developer with concerns about the privacy policy as well as how the business will contact the consumer about any changes to the policy.

4. Implementing Enhanced Measures

Privacy concerns do not end with the publication of a sound privacy policy. Consumers will often skip past reading a privacy policy, yet expect robust protection of their data and control over how their information is used. One of the best ways to address this expectation is by providing notice of privacy practices while the user is navigating through the app. Alerts embedded within the app's functionality serve to direct users to specific data collection practices. Such an alert not only makes the user aware of the app owner's privacy practices, but it sets user expectations as to how information will be used. For example, after a form that collects personally identifiably information is completed, and before clicking send/submit, the user may be prompted with a message explaining how the information from the form will be used and with whom it will be shared. Finally, if a user does not agree with how their information will be used, they should have the option, at that point in time, to choose to stop using the app or specifically control how their information is used.

V. Beyond California

California's recent activity in the mobile space is significant from an enforcement and guidance standpoint; however, both domestically and internationally, other regulators are also working to introduce privacy standards to the mobile apps market.

1. USA
On a national level, the Federal Trade Commission (FTC) has recently released a series of recommendations outlining ways to improve mobile privacy disclosures. In December 2012, the FTC released its report *"Mobile Apps for Kids: Disclosures Still Not Making the Grade*" directly addressing considerations for mobile apps targeted toward children.[14] Significantly, the February 2013 FTC report titled *"Mobile Privacy Disclosures*" echoes many of the same themes outlined in California's guidance.[15] In addition to a wealth of other guidance in the report, the FTC specifically recommends that app developers should:

- *Privacy Policy:* Have a privacy policy and make sure it is easily accessible through the app stores;

- *Availability & Consent:* Provide just-in-time disclosures and obtain affirmative express consent before collecting and sharing sensitive information (to the extent the platforms have not already provided such disclosures and obtained such consent);
- *In-App Third Party Services:* Improve coordination and communication with ad networks and other third parties that provide services for apps, such as analytics companies, so the app developers can better understand the software they are using and, in turn, provide accurate disclosures to consumers. For example, app developers often integrate third-party

code to facilitate advertising or analytics within an app with little understanding of what information the third party is collecting and how it is being used.
- *Selfregulation:* Consider participating in self-regulatory programs, trade associations, and industry organizations, which can provide guidance on how to make uniform, short-form privacy disclosures.[16]
- In addition, in early May 2013, Georgia Congressman Hank Johnson introduced the Application Privacy, Protection and Security (APPS) Act 2013 which, if enacted, would require app developers to display privacy policies and obtain consent to those policies before the app is even used, allow users to decide the fate of data that has been collected on them after no longer wanting to use an app, and regulate app developers' data storage policies.

2. European Union

Internationally, the European Union Article 29 Working Committee has also been actively examining the issues around mobile app privacy. In February 2013, the Article 29 Working Committee adopted an Opinion on Apps on Smart Devices (the "Opinion") that outlines the legal framework for processing personal data in apps and the necessary consent.[17] The Opinion concludes that responsibility for mobile app privacy rests with multiple parties including app developers, app stores, operating system and device manufacturers and other third parties who use collected data.

3. Conclusion

California is playing a leading role, but is not alone in its efforts to enforce existing privacy laws against mobile app owners and developers. California's guidance to app developers seems to be consistent with similar guidance from the FTC and even the Article 29 Working Committee in Europe. Therefore, California's actions in the last year signals activity yet to come in other jurisdictions, and developers should pay attention to the state's guidance to anticipate potential mobile app privacy issues. It is important to ensure that you have worked with experienced legal counsel in this area to avoid being the next company against which an enforcement action is brought.

Fußnoten

*) James Chang/James G. Gatto/Meighan E. O'Reardon, Washington. Further information about the authors on p. 96.

1) Press Release, Apple, App Store Marks Historic 50 Billionth Download (May 23, 2013), available at *http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html.*

2) Press Release, Apple, App Store Toes 40 Billion Downloads with Almost Half in 2012 (Jan. 17, 2013), available at *https://www.apple.com/pr/library/2013/01/07App-Store-Tops-40-Billion-Downloads-with-Almost-Half-in-2012.html.*

3) John Koetsier, 900M Android Activiations to date, Google says, Venture Beat, May 15, 2013, available at *http://venturebeat.com/2013/05/15/900m-android-activations-to-date-google-says/.*

4) *Press Release*, *Apple*, *Apple's App Store Marks Historic 50 Billionth Download (May 23*, *2013)*, *available at http://www.apple.com/pr/library/2013/05/16Apples-App-Store-Marks-Historic-50-Billionth-Download.html.*

5) Press Release, State of California Department of Justice, Office of the Attorney General, Attorney General Kamala D. Harris Announces Privacy Enforcement and Protection Unit (July 19, 2012), available at *http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-privacy-enforcement-and-protection.*

6) State of California Department of Justice, Office of the Attorney General, Privacy on the Go, Jan. 2013, available at *http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.*

7) D.B.A. BlackBerry.

8) State of California Department of Justice, Office of the Attorney General, Joint Statement of Principles, Feb. 22, 2012, available at *http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.*

9) Press Release, State of California Department of Justice, Office of the Attorney General, Attorney General Kamala D. Harris Announces Expansion of California's Consumer Privacy Protections to Social Apps as Facebook Signs Apps Agreement (June 22, 2012), available at *http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-announces-expansion-california%E2%80%99s-consumer.*

10) State of California Department of Justice, Office of the Attorney General, Joint Statement of Principles, Feb. 22, 2012, available at *http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf.*

11) Complaint, *People v. Delta Air Lines Inc.*, No. CGC-12-526741, (Cal. Super. Ct. Dec. 6, 2012).

12) State of California Department of Justice, Office of the Attorney General, Privacy on the Go, Jan. 2013, available at *http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.*

13) See, for example, Google's Privacy Policy (May 23, 2013), available at *http://www.google.com/policies/privacy/ which formats itself according to the device it is accessed from*.

14) Federal Trade Commission, Mobile Apps for Kids: Disclosures Still Not Making the Grade, Dec. 2012, available at *http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf.*

15) Federal Trade Commission, Mobile Privacy Disclosures, Feb. 2013, available at *http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.*

16) Federal Trade Commission, Mobile Privacy Disclosures, Feb. 2013, at ii, available at *http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.*

17) Data Protection Working Party, Opinion 02/2013 On Apps on Smart Devices, Feb. 27, 2013, available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.*

recherchiert von: **Ulrich Gasper** am 05.07.2013

Dokument-typ:	Sonstiges	**Quelle:**	
		Fundstelle:	Verlag Dr. Otto Schmidt, Köln CRi 2013, 96

About the Authors

James Chang is an associate in Pillsbury Winthrop Shaw Pittman's Los Angeles Office. As a member of the firm's Intellectual Property practice, Mr. Chang performs various tasks relating to patent prosecution, litigation, and general IP needs of Pillsbury's clients. Prior to joining Pillsbury, Mr. Chang served as an endowed research fellow at UC Irvine School of Law, where he researched the legal basis for virtual property. Mr. Chang's industry experience includes work at software development studio, Blizzard Entertainment. Pillsbury is a full-service law firm with a keen industry focus on the energy and natural resources, financial services, real estate and construction, and technology sectors.

James Gatto is a partner at Pillsbury Winthrop Shaw Pittman and the creator and leader of the firm's Social Media & Games team, leader of the Virtual Worlds and Video Games team and leader of the Open Source team. He leverages his unique combination of over 25 years of IP experience, business insights and attention to technology trends to help companies develop IP and other legal strategies that are aligned with their business objectives. His practice focuses on all aspects of intellectual property, internet and technology law, including patent, trademark, copyright, trade secret and open source. Pillsbury is a full-service law firm with a keen industry focus on the energy and natural resources, financial services, real estate and construction, and technology sectors.

Christophe Gronen is partner at BMH Avocats in Paris. He is a member of the Paris bar as well as of the Munich bar and his legal expertise focuses on commercial law, insolvency and restructuring and intellectual property law. He can be reached at *cgronen@bmhavocats.com*.

Dr. Mathias Lejeune works a**s** attorney at law in Munich. He is a member of DGRI (German Association of Law and Information Technology), speaker of the DGRI committee for contract law and a member of the editorial team of the law magazine "Der IT Rechts-Berater" ("The IT-Counselor"). He has published books and articles in the field of the international software contract law for many years, especially concerning the US law.

Professor Ian Lloyd, Research Fellow in ILaws at the University of Southampton and a visiting professor at the Open University of Tanzania. Ian is author of a number of textbooks in the field of IT Law including works on Information Technology Law, the sixth edition of which was published in 2011 and Telecommunications Law, Both books are published by Oxford University Press. Ian is also Consultant Editor for the Communications Law Title of Halsbury's Laws of England and, together with Professor Steven Saxby, is working on a further title for Halsbury on the topic of Information Technology Law. Together with Professor Saxby, Ian is responsible for the distance learning based LLM course in Information Technology and Telecommunications Law.

Annelies Moens is the Immediate Past President of the International Association of Privacy Professionals in Australia/New Zealand. She is the Head of Sales and Operations at Information Integrity Solutions P/L, a global privacy strategy consulting company based in Australia. A former Deputy Director of

Compliance at the Australian Privacy Commission, Annelies has degrees in Law, Computer Science and an MBA. Email: *amoens@iispartners.com*.

Meighan O'Reardon is a senior associate in Pillsbury Winthrop Shaw Pittman's Global Sourcing group, where she currently focuses on technology transactions, including information technology and business process outsourcing transactions; software licensing and development arrangements; intellectual property contracts; and other related corporate transactions. Ms. O'Reardon also regularly advises clients on data use and privacy matters including data breach response, privacy policies and terms of use, and international data transfers of personally identifiable information. Pillsbury is a full-service law firm with a keen industry focus on the energy and natural resources, financial services, real estate and construction, and technology sectors.

John Selby is a Lecturer at Macquarie University in Sydney, Australia. An expert on Internet law, his research applies an interdisciplinary approach to studying the various modalities through which the Internet may or should/should not be regulated so as to maximise its benefits to society whilst minimising its negative externalities. In 2009, he was a Postel Center Fellow at the University of Southern California and in 2006 he was recognised as one of Australia's New Voices in Technology and International Relations. For correspondence about this article, email: *john.selby@mq.edu.au*.