AQuA
App Quality Alliance

AQuA Round Table

Developer guidelines and tools: are they helping or causing confusion?

The outcome of a Round Table with parties interested in app quality, held at the GSMA offices in London in February 2015.

Introduction

Privacy had been a hot topic at the first Round Table held with the BBC 12 months prior to this event, and was voted the number 1 area in which you said you needed further clarification and guidance. With that in mind, we developed our second Round Table (this time with GSMA) taking a look at the various regulations, tools, frameworks and guidelines available on the subject of Privacy, and make sense out of them with participants' input.

Also, we wanted to discuss attendees' views on other guidelines and tools. It's clear that although guidelines looking at different issues relating to app development have been produced by many industry bodies and commercial organisations over the past 5 years to help developers to help developers address various issues, do these guidelines help or confuse? How much are they used and valued?

On the day of the Round Table issues of privacy were currently very much in the news: an article had appeared on the BBC News site referencing Samsung's voice-activated connected TVs passing recorded voice data to an external server for analysis, and proposals had been made for a new app to allow parents to see everything their children do on their phones.

Privacy Guidelines Discussion

GSMA Privacy Guidelines and UK Information Commissioner's Office

The first set of guidelines we looked at was the **GSMA** Privacy Guidelines. The GSMA had proposed and produced a set of Privacy Design Guidelines for Mobile Application Development and had sought feedback from a range of industry stakeholders, regulators and civil society. They are generally-accepted to be the first set to be developed and helped inform others such as those developed by the Californian Attorney General, the Federal Privacy Commission of Canada and others.

The GSMA's aim was to develop common guidelines that would be relevant globally. Many companies had engaged with the GSMA on this project, some publicly, some privately. They felt they were now at the stage where more developers should be engaged, and there should be more requirements from regulators around the world to be met. The objective is to promote practices that would improve privacy.

It was felt by the GSMA that privacy is not generally publicised to the smaller developers in the large platform providers' ecosystems. Although network operators can exert control over the small part of the ecosystem that they control and ensure compliance, outside of that

narrow area awareness is generally low. GSMA is in dialogue with the bigger players, who are mainly concerned with meeting actual legal requirements in their users' market areas.

UK Information Commissioners Office had also produced guidance to help app developers comply with the UK Data Protection Act 1998 and ensure users' privacy. The guidelines have been well-covered in the press. As with the discussion regarding the GSMA Guidelines, it was felt that developers may be more concerned about meeting app store guidelines than meeting legal requirements, as the former have an immediate effect on whether users are even aware of their app, whereas privacy compliance is a deferred risk that may not become an issue, at least in their eyes.

The comments below sum up the views of the Round Table attendees on the subject of the GSMA and ICO guidelines and privacy in general:

- It was quoted that App Permissions were possibly prone to being used incorrectly: an example quoted was that the top 10 flashlight apps each used between 10 and 20 permissions, when they actually only need one.

- It was asked, why privacy should be any different to other consumer protections, and agreed that privacy should not have to wait for user complaints before it is considered.

- Consumers seem to send out mixed messages, saying that they are worried about privacy but accepting applications that do the things they are concerned about. Both poor explanations of data use and excessive privacy warnings can lose user installs of an app.

- Users who have privacy concerns may still end up accepting permission requests they don't like. It's possible that users perform a mental trade-off between their concerns and the app capabilities they want to have.

- In many cases there is no clarity for the user regarding why permissions are requested by an app. Data that is collected may be passed to multiple unknown analytical companies, and the user will not be aware of this. Developers may also not be clear about why their apps are requesting some permissions.

- Guidelines were created to enable developers to attempt to be compliant in multiple jurisdictions, to encourage good practices and demonstrate good intent. Some regulators may give developers credit for meeting known industry guidelines, even when regulations may not have been fully understood or correctly followed.

- Some bodies may be adopting elements of guidelines as needed. Because of funding and resource limitations, companies may only react to compliance issues after a significant non-compliance event focuses everyone's attention on a problem.

- The Future Privacy Forum (FPF) and the Centre for Democracy & Technology (CDT) have jointly put together a short and simply-worded document which looks at

principles rather than detailed guidelines, in an attempt to reduce the burden of understanding compliance.

- Big brands will have considerable legal resources, but this can also lead to a blinkered approach. Developers or app commissioners who only treat privacy as an issue for legal compliance can miss concerns that may create customer issues.

- When projects are poorly controlled, privacy weaknesses can be introduced. Poor control can allow more drift in multiple delivery cycles, particularly if developers are not comfortable with privacy issues and avoid examining them in depth unless constrained to do so by requirements.

- One major carrier has moved from having a company privacy policy to having seven principles that drive their approach. It was asked whether we should as an industry be looking at reducing the volume of compliance advice in the same way.

- Regulations & guidelines can be misused if a narrowly-interpreted justification is used as a "get-out-of-jail-free" card when challenged on adverse activity.

The attendees were divided on the subject of privacy guidelines: some felt that that there might be too many different guidelines to follow, and others were of the view that the greater the number of guidelines by different organisations, the better the chance of a developer being aware of the need for them to ensure they limit their use of customers' data.

The Round Table discussion then moved on to Privacy Tools ....

Privacy Tools Discussion
MEF Privacy Policy Generator and Intuit Short Form Privacy Notice

MEF's Privacy Policy Generator is an online tool that asks developers to answer a few simple questions about how their app handles user data which, in a 10-minute process gives HTML file that can be customised and embedded directly into the developer's application. It educates developers as they fill out the survey by warning when they are likely to come into conflict with regulation or normal user expectations, and is intended to help build trust with users.

In response to the Mobile App Privacy Voluntary Code of Conduct which calls for mobile applications to include a short form privacy notice, **Intuit** in conjunction with the **App Developers Alliance** has created open source code for consumer-friendly short-form privacy notices: simple, easily understandable screens that clearly inform consumers what data the app is collecting and with whom the data is shared. Intuit's Short Form Privacy Notice grew out of the trend in the US for a long, fully-featured privacy notice to be used. The Short Form Privacy Notice instead highlights the essential points, and links back to a detailed notice for the full legal declaration. The Intuit Privacy Notice is not a complete and formal privacy policy, more a way for developers to inform their users. It lists what data is collected and why, along with what is not collected, for incorporation in an app or store description.

The comments below sum up the views of the Round Table attendees on the subject of the above tools and also covers further discussion on the use of Privacy tools and guidelines in general:

- Very broad categories of data on permissions were agreed to be unhelpful: if the data mentioned seems to have no relationship to the normal usage of the app, it will confuse users.

- Attendees identified usage of the just-in-time privacy notice, where you may alert the user to the imminent collection of specific data, with the possibility to opt out.

- There was discussion of the need to have both carrot and stick in regulation. A potential carrot for a developer is being able to identify beneficial effects on the bottom line. Protecting user data does not necessarily adversely affect the business benefit: the relationship between the end user and the company is not a tug of war that only one party can win. There can be willing trade-offs that will benefit both parties. Giving users data management capabilities and building trust with developers and data collectors is needed to improve the situation.

- An area for further investigation is whether users of smart power meters could make any decision about what happens to the collected data, about how widely that data could be disseminated, and for what purposes. As one attendee put it: *"I have a relationship with this company to provide this service, but they are taking my information and selling it off in order to make money, without being connected to the original purpose for which I gave consent"*.

- Revocation of consent and uninstallation could both affect data retention. For one type of application, you might want all the data to be deleted. For another app (e.g. one that takes photos and videos) you might very definitely want to retain data. "Their" data vs "my" data was agreed to be an important, but not always clear-cut, user distinction.

The Round Table then moved on to talk about two other sets of Guidelines and their relevance to today's app development world.

(Please note: the discussion on privacy had been very invigorating, with many thoughts exchanged. As a result, the non-privacy-related guidelines below weren't discussed in as much detail due to lack of time).

Non-privacy-related Guidelines Discussion
GSMA IoT Device Connection Efficiency Guidelines

The GSMA has worked with its ecosystem partners to establish the GSMA IoT Device Connection Efficiency Guidelines looking at how machines should communicate via the mobile network in the most intelligent and efficient way.

Why? Developers using mains-powered PCs may generate power-inefficient code through not having the same constraints as the user. There are many custom platforms at the moment, each of which may require a unique solution to this problem, as there is no common framework. Because there are only a few manufacturers of IoT components at present, the problem is manageable while there are limited routes into the environment. It represents an opportunity to get good practices introduced early on. The objective of developing these Guidelines is to get big players to only engage with developers who follow the Guidelines. As they are backed up with test cases, future accreditation is a possibility.

It was generally agreed that by creating the standards for the evolving IoT now, we can get them accepted before big players promote competing proprietary technologies that may serve their own ecosystems well, but be less helpful for the overall development environment.

AQuA Testing Criteria

AQuA's Testing Criteria for iOS apps and Testing Criteria for Android apps are sets of baseline QA steps that complement functional testing to ensure the app sits well on the device. The Network Performance Testing Criteria help ensure that the app uses data on a mobile network efficiently and doesn't burn the battery.

It was agreed that Testing Criteria were very much regarded as relevant in promoting good practice, and provide a consistent user experience. To grow their usage further, there needs to be dialogue with the brands commissioning apps, to ensure they are mandating the use of the criteria in app development.