

Mobile App Privacy — You're Doing It Wrong

(and so am I)

Graham Lee, Smartphone Security Boffin,
Fuzzy Aliens Limited

Desktop
Server
Telecom CO
Particle Accelerator

UX
Requirements Eng
Dev Ops
Source Control
...

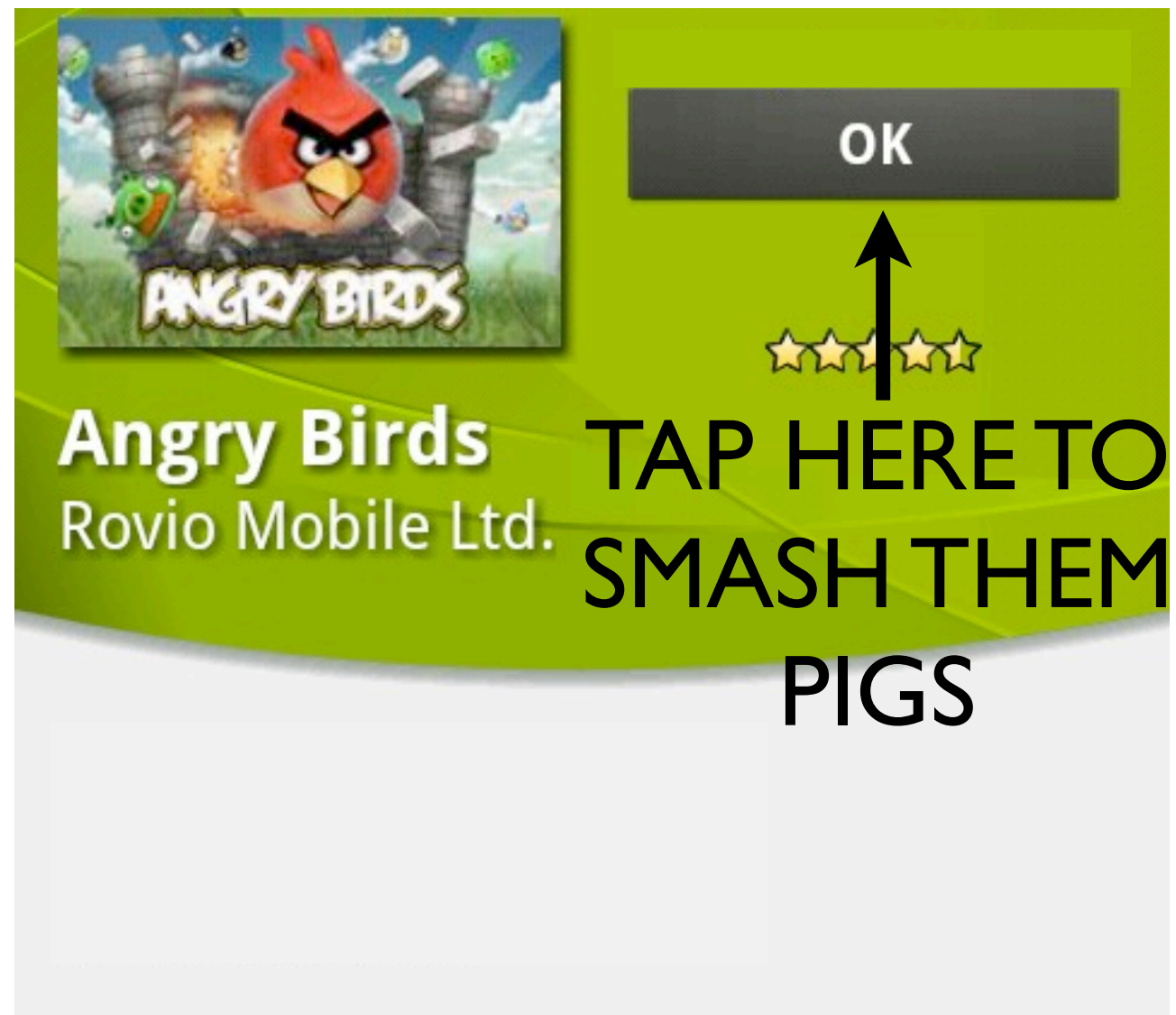


Pre-intro Disclaimer

Introductory Story

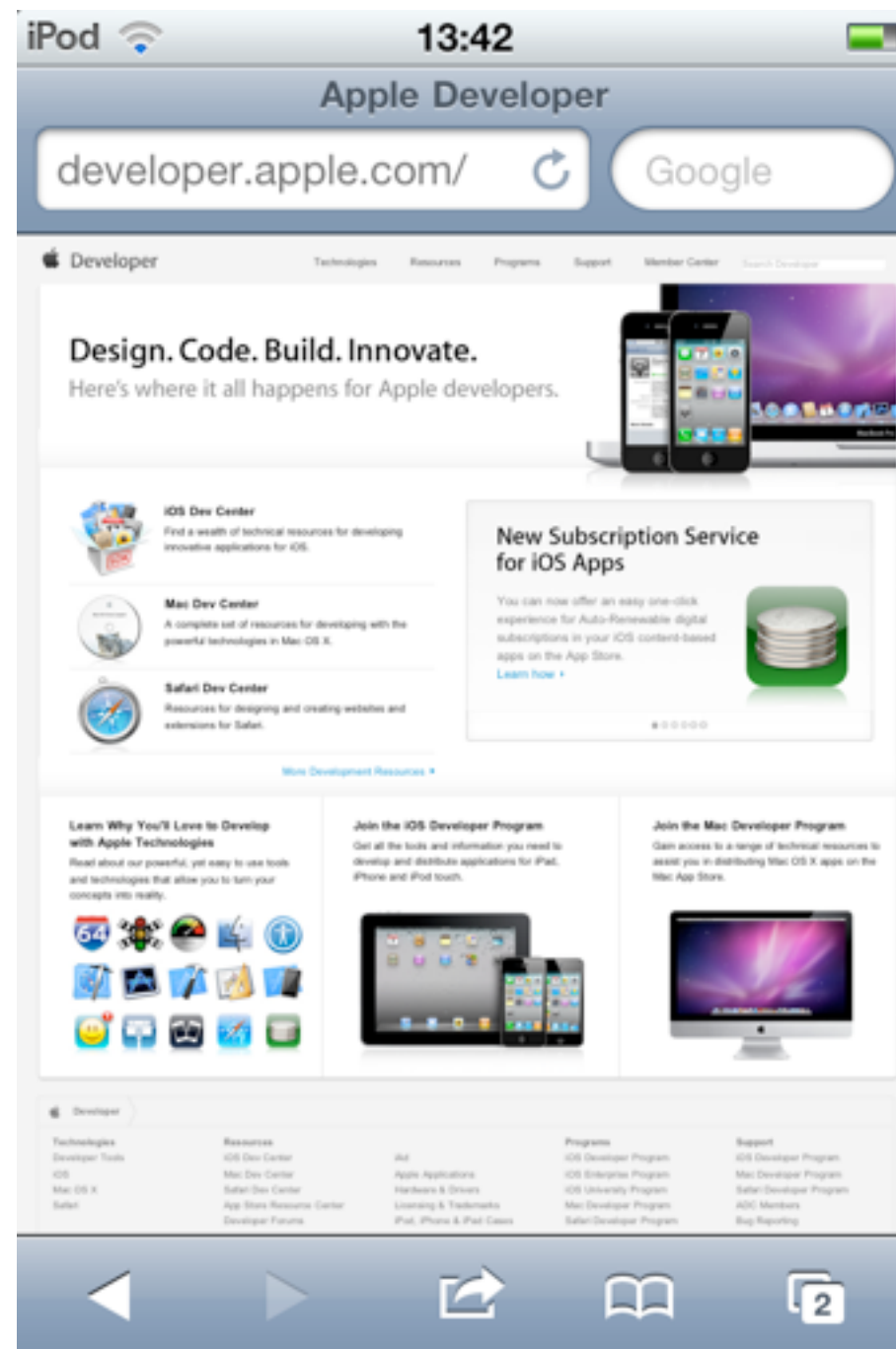
- I can't explain why I did what I did
- It's not just hard to explain the rules, I don't know them
- Ask me, I'll not only give the wrong answer, I'll do something different
- My original plan got replaced at run-time **in the face of new inputs**





Erm...privacy?

iOS Example



Historical Example



“ The Platform for Privacy Preferences Project (P3P) enables Websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents. P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. **Thus users need not read the privacy policies at every site they visit.** ”

What can we draw from this?

- People are capricious
- We can't tell you what information we'll use to make any decision
- A rational choice made earlier can be overridden by novel changes in environment

Spammers and phishers know this

Therefore, give users an
easily-digestible amount
of pertinent
information AT
DECISION TIME

Just-in-time information

Account Name:

Enter the account name associated with this keychain item.

Password:

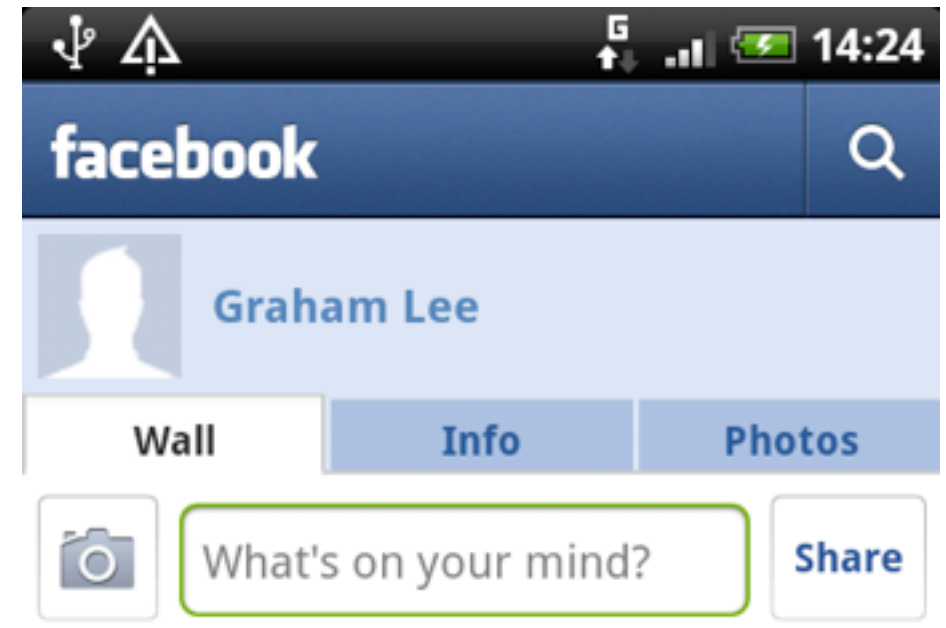
Enter the password to be stored in the keychain.

[Password Strength: Weak](#)

← what I'm trying to do

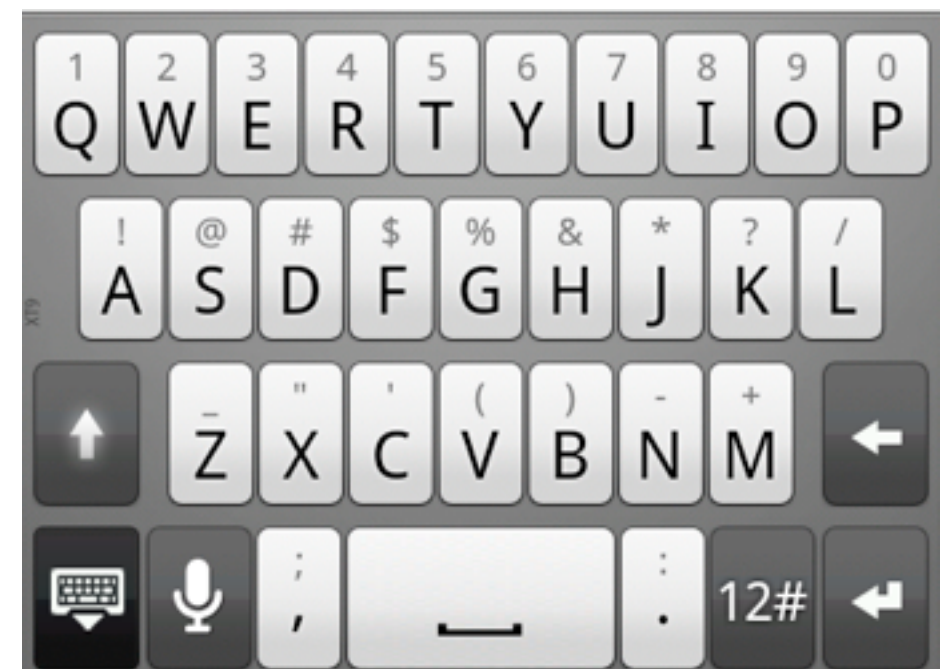
← how it's going

Social Media

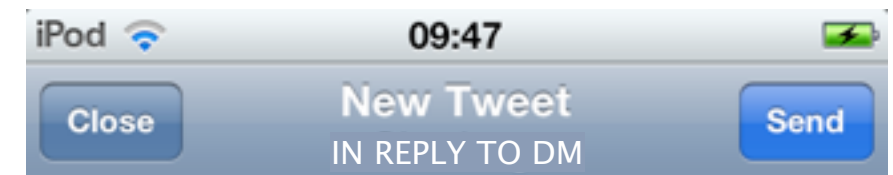


Your mum can read what you post!

[Change privacy settings](#)



Social Media



Confidential Data



Subject: Conference guest

You asked for contact details for Bob, who you met at our sales conference. I've attached his details from our CRM.

Graham.



Subject: Conference guest

You asked for contact details for Bob, who you met at our sales conference. I've attached his details from our CRM.

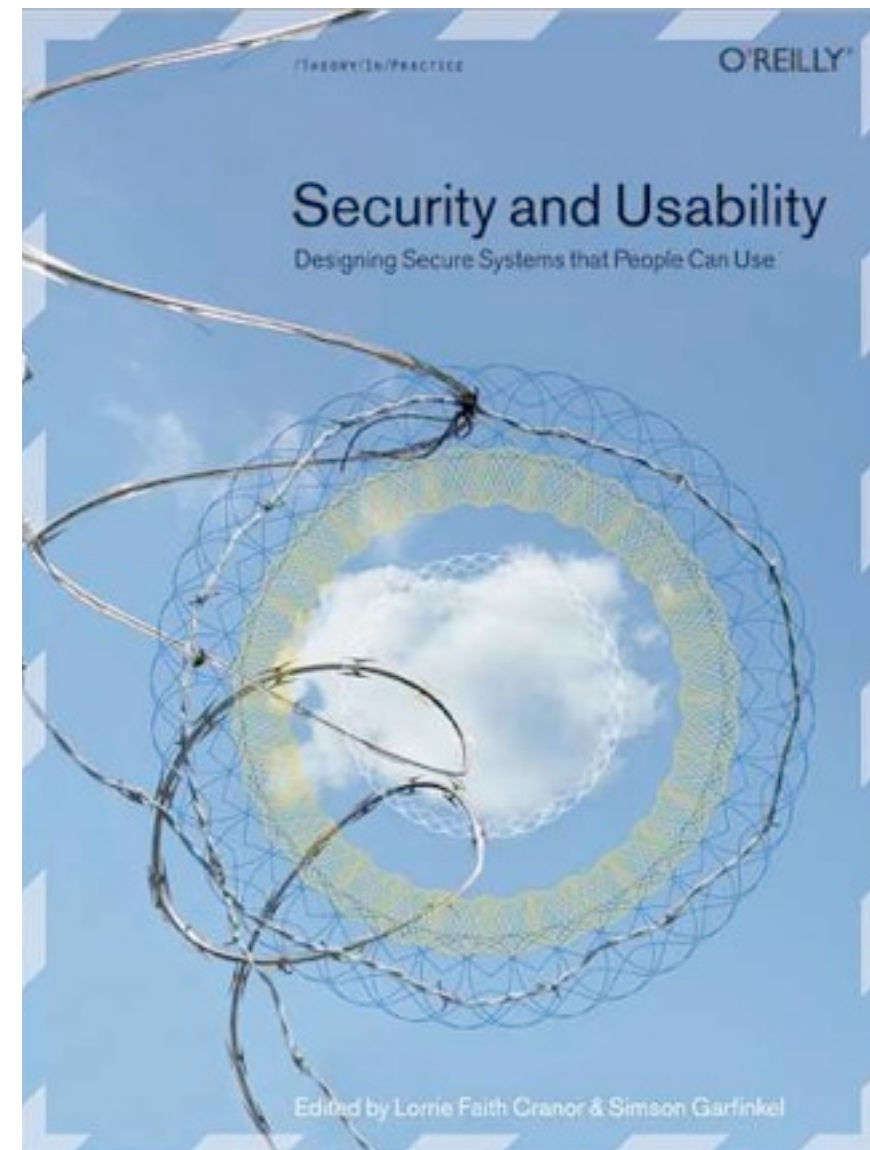
Graham.

Warning: attachment includes credit card data.
[Delete Attachment](#)



Summary

- Users *can* help themselves to privacy...
- ...if app developers do their part and help out
- AFFORDABILITY IS KEY (in everything)
- Read these books ➡



@dianleeg

