




mobisec the apps co.
WINNERS PLAY IT RIGHT
19/06/17

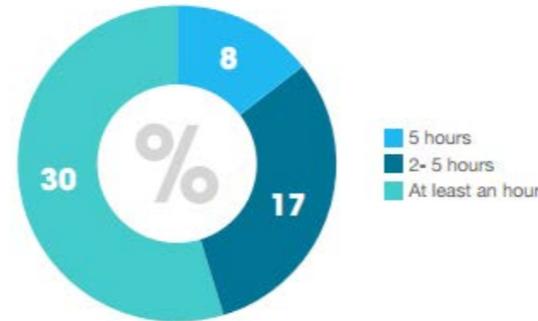


PREMESSE: IL MOBILE,
FUTURO ODIERNO



In 2015 in **UK 55%** of smartphone users spend at **least 1 hour a day**

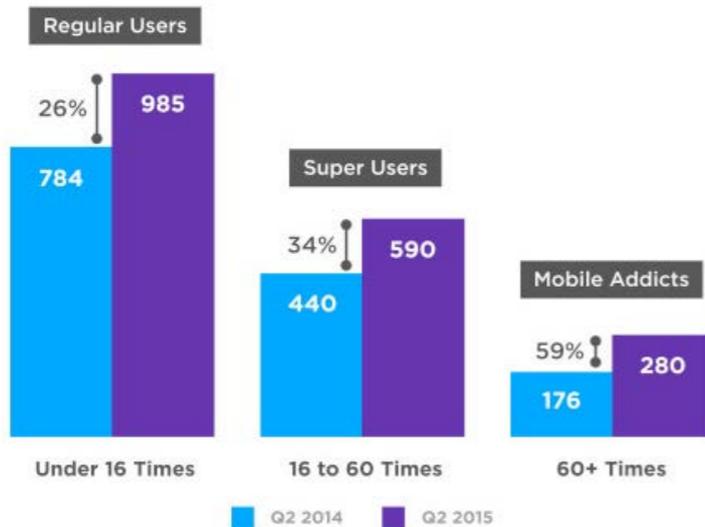
How much time a day are we spending on our mobiles?



In the US the average time spent using apps has exceeded TV watching.

Mobile addiction continue its rise among all user ranges.

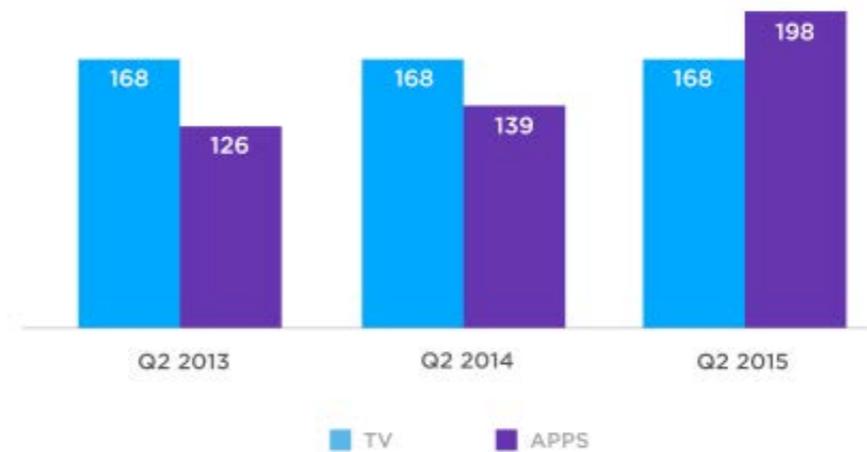
Mobile Addiction Continues to Rise
Worldwide Daily App Usage Distribution (Millions)



Source: Flurry Analytics

Time Spent in Mobile Apps and on TV

US DAILY AVERAGE IN MINUTES



Source: Flurry Analytics, US Department of Labor Statistics

Flurry research into mobile addicts.

Flurry on time spent and revenue on TV vs Mobile

WHAT NOW?

Internet is going Mobile
Business is going Mobile
Risks are going Mobile



RISKS AND SECURITY



DOV'ERA IL DATO SANITARIO FINO A QUALCHE DECENNIO FA?

19/06/17



**nelle strutture
sanitarie**

- **cartelle cliniche cartacee**
- **documenti sanitari presso medici di base sul territorio**
- **laboratori di analisi**
- **cliniche private**
- **SSN**

DOV'È IL DATO SANITARIO OGGI?

19/06/17

nelle strutture
sanitarie

nei datacenter



- **anagrafi sanitarie nazionali**
- **SSN**
- **database internazionali di dati sanitari e ricerca**
- **knowledge base di divulgazione medica**
- **congressi**
- **fondazioni**

DOVE SARÀ IL DATO SANITARIO DOMANI*?

19/06/17



OVUNQUE

- tutto quello che già esiste oggi
- wearable devices
- mobile devices medicali
- knowledge base intergiurisdizionali (assicurazioni / sicurezza pubblica / anagrafe sanitaria internazionale)
- telemedicina (ricerca)
- telemedicina (intervention e pratica medica a distanza)



PRIVACY E PROTEZIONE DEL
DATO SANITARIO



PERCHÉ IL MOBILE È ESPONENZIALMENTE PIÙ PERICOLOSO?

GLI ELEMENTI DELLA PROTEZIONE: C.I.A.

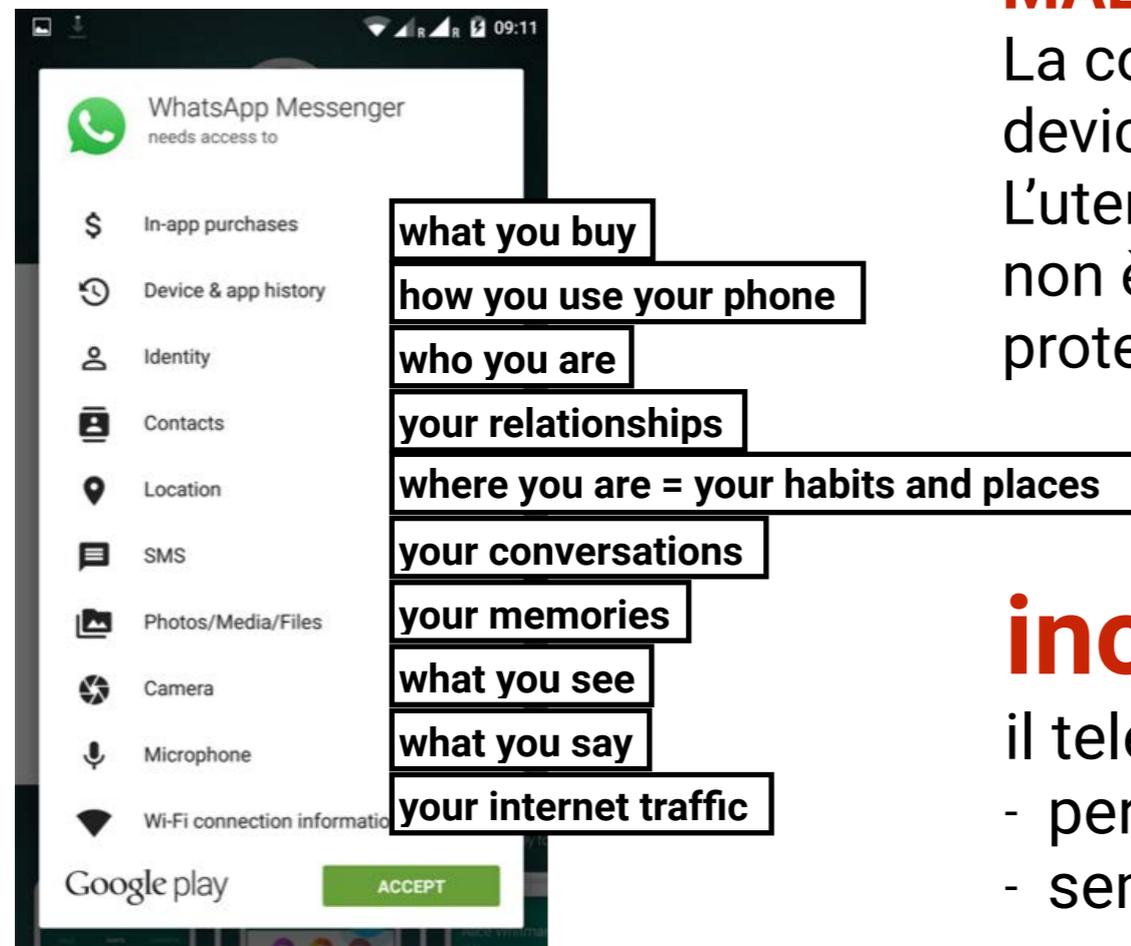
19/06/17

- **CONFIDENZIALITÀ** - la privacy e la riservatezza del dato sanitario.
- **INTEGRITÀ** - l'integrità del valore del dato e le sue policy di modifica, aggiornamento, sincronizzazione (data stores e data source)
- **AUTORIZZAZIONE** - la possibilità di accedere a diversi livelli a diverse informazioni dei dati sanitari in base alla qualifica ed alla tipologia di operatore del dato (ssn, medico, ricerca, fondazioni)

PER PROPENSIONE D'USO

**come i nostri utenti usano il telefono?
MALE.**

La consapevolezza dell'utente medio del device portatile è infinitamente bassa. L'utente medio è un utilizzatore passivo e non è in grado di provvedere alla minima protezione del dispositivo.



inoltre...

il telefono è:

- personale
- sempre acceso
- sempre connesso
- sincronizzato con i sistemi server
- **una sorgente di dati**
- **un repository remoto di dati**

PER MODELLO ARCHITETTURALE

Web app classica

client



2 endpoint

tutto avviene nel network



server - data



Mobile application





PROTEZIONE E SECURITY





Il dato sanitario deve essere protetto sia nell'**accesso**, che nell'**autorizzazione** che nel **trattamento** in diversi momenti e quindi al giorno d'oggi in diversi luoghi (fisici o virtuali che siano).

Il dato deve essere protetto quando viene **creato**, quando viene **salvato**, quando viene **usato e/o modificato**.

Purtroppo queste fasi, che un giorno erano relegate a specifici momenti della catena di trattamento del dato ed a specifici luoghi/usi/operatori, ora sono **ricorrenti** in **qualsiasi momento** e **qualsiasi posizione** del processo.

TUTTO

In ciascun luogo ed in ciascuna fase della sua vita il dato può essere acceduto, modificato, verificato, aggiornato.
Un dato può essere creato fisicamente in un sistema centrale, in una struttura sanitaria, in un dispositivo wearable.

OGNI ENDPOINT DELLA FILIERA MOBILE DEL DATO SANITARIO DIVENTA **DATASOURCE, DATASTORAGE, DATAUSER** IN UNO SPECIFICO MOMENTO DELLA FILIERA.

SIAMO DI FRONTE AD UNA MODIFICA SOSTANZIALE DELL'**ARCHITETTURA DELL'INFORMAZIONE**.
COME RIVEDERE IL MODELLO DI SECURITY E PROTECTION?



FILLING THE GAP



Tutti i player coinvolti nella filiera del dato sanitario devono essere sensibili alla loro pertinenza di protezione.

L'UTENTE

Deve maturare una maggior consapevolezza del mezzo e deve considerare il device mobile come uno strumento.

Il passaggio di sensibilizzazione sarà reso più fluido dalla diffusione dei device medicali portatili.

LA PUBBLICA AMMINISTRAZIONE

Deve garantire la modalità di formulazione della normativa (raccomandazioni e obblighi), promulgata da un organo di governo, regolatorio ed in quanto tale interessato all'indicazione di principio e di tutela.

IL MERCATO, I SOLUTION PROVIDER

Devono aumentare la cultura e la specificità del mondo mobile per adeguare metodologie e prassi di security e protection ad oggi non ancora compartimentate sul nuovo modello di information architecture.



contacts: benetton@mobisec.com