



Geo-Location: Risk, Strategies and Assurance Aspects

Urs Fischer, dipl. WP, CRISC, CISA
Fischer IT GRC Consulting & Training



1. Introduction: What is Geo-Location and How Does IT Work?
2. Business Benefits
3. Risk, Security and Privacy Concerns
4. Strategies for Addressing Risk
5. Assurance
6. Summary and Wrap-Up

- 1. Introduction: What is Geo-Location and How Does IT Work?**
- 2. Business Benefits**
- 3. Risk, Security and Privacy Concerns**
- 4. Strategies for Addressing Risk**
- 5. Assurance**
- 6. Summary and Wrap-Up**

What Geo-Location Is (simply stated)

Geo-location is a technology that uses data acquired from an individual's computer or mobile device (any type of radio or network-connection-enabled device) to identify or describe his/her actual physical location. It is one of the most popular manifestations of the current development of information technologies and is recently experiencing a significant rise in popularity.

Definition (More Systems-Oriented)

A geo-location system is an information technology solution that ascertains the location of an object in the physical (geo-spatial) or virtual (Internet) environment. Most often, the object is a person who wants to utilise a service-based on location, while maintaining his/her privacy.

Purpose

- Geo-Referencing or Positioning
- Geo-Coding
- Geo-Tagging

Collection of Geo-Location Data

- Web Browsing via IP-addresses
- Mobile Phones
- GPS Devices
- Radio Frequency Identification (RFID)
- Credit/Debit card transaction
- Tags in Photographs
- Postings on Social Networks as Facebook[®] und Twitter

Uses of Geo-Location Data

- Localisation and/or customisation of delivered content
- Enforcement of access and delivery restrictions
- Fraud prevention
- Network traffic analysis

Modes of Geo-Location Data Generation and Collection

Mode	Collection Method	Technologies Involved
Active: User— Device-based	<ul style="list-style-type: none"> • Uses firmware and software on user's computer or wireless device • Location determined via GPS chip and/or triangulation using cellular tower information • Request-response model 	<ul style="list-style-type: none"> • GPS • Assisted GPS (A-GPS) • Wi-Fi—Wireless positioning • 3G/4G • Mobile applications—iPhone, Android devices, BlackBerry®

Modes of Geo-Location Data Generation and Collection

Mode	Collection Method	Technologies Involved
Passive: Data-lookup— Sever-based	<ul style="list-style-type: none"> • Involves use of third-party geo-location service providers, e.g., Quova®, NetGeo, Bering Media • Based on non-location-specific IP address acquired from user device or service set identifiers (SSIDs) for wireless networks • Correlation with stored IP or SSID databases obtained from purchase records, user-provided information, network analysis of trace routes and domain name system (DNS) host names 	<ul style="list-style-type: none"> • IP location—Whois lookup, DNS LOC, geographic names in domain name user or application information, timing data using ping inference based on routing data, e.g., traceroute monitoring of Internet service provider (ISP) networks • 3G/4G • Wi-Fi—Wireless positioning

1. Introduction: What is Geo-Location and How Does IT Work?
- 2. Business Benefits**
3. Risk, Security and Privacy Concerns
4. Strategies for Addressing Risk
5. Assurance
6. Summary and Wrap-Up

Services and Applications

Geo-location technology has become a foundation for location positioning services and location-aware applications running on smartphones such as iPhone® and Android™ devices.

The Rise of Geo-Location

The capability to provide accurate and timely geo-reference data, tag items of interest with location metadata, and use location coordinates as a key to search databases has become the foundation for an expanding software market for applications that run on mobile platforms.

Business-Applications and -Benefits

- In advertising, use of designated market areas (DMA) and demographic data
- Know your customer (KYC)
- Delivery and asset management
- Content customization and delivery
- Augmented reality
- Fine-grained management of Internet commerce activities and interests
- E-discovery
- Highway toll devices, e.g., I-Pass, EZ-Pass® in the US
- Vehicle Ad Hoc Networks (VANS), as used in the EU
- Optimal request routing
- Fraud detection and prevention using IP location technology in conjunction with fraud profile data

The business benefits of geolocation are far-reaching and are being leveraged by all types of enterprises—manufacturing, retail sales, financial services, insurance, transportation, utilities and governments.

Benefits for Customers

- Discounts
- Promotions
- Customer preferences
- Access to information that can be instantly relevant to
 - a purchasing decision
 - Location-specific discounts
 - Location-specific services

Context Enriched Services

Geolocation in conjunction with cross-platform mobile applications will provide the basis for enhanced customer experiences and present opportunities for enterprises to merge location with social-media-based and other information into context enriched services.

1. Introduction: What is Geo-Location and How Does IT Work?
2. Business Benefits
- 3. Risk, Security and Privacy Concerns**
4. Strategies for Addressing Risk
5. Assurance
6. Summary and Wrap-Up

Companies should think carefully about their geo-marketing practices and examine whether their current privacy policies accurately reflect the collection and use of geolocation data.

Data Classification

There is a growing consensus that geolocation data should be classified as sensitive due to a number of concerns such as transparency about data collection practices, solicitations made based on geolocation data obtained without the user's consent and physical safety stemming from the misuse of information that can identify a user's current (or future) physical location.

Through data classification the enterprise should identify the data that are considered personal information and confirm that there are appropriate mechanisms such as encryption to mitigate the risk of disclosure.

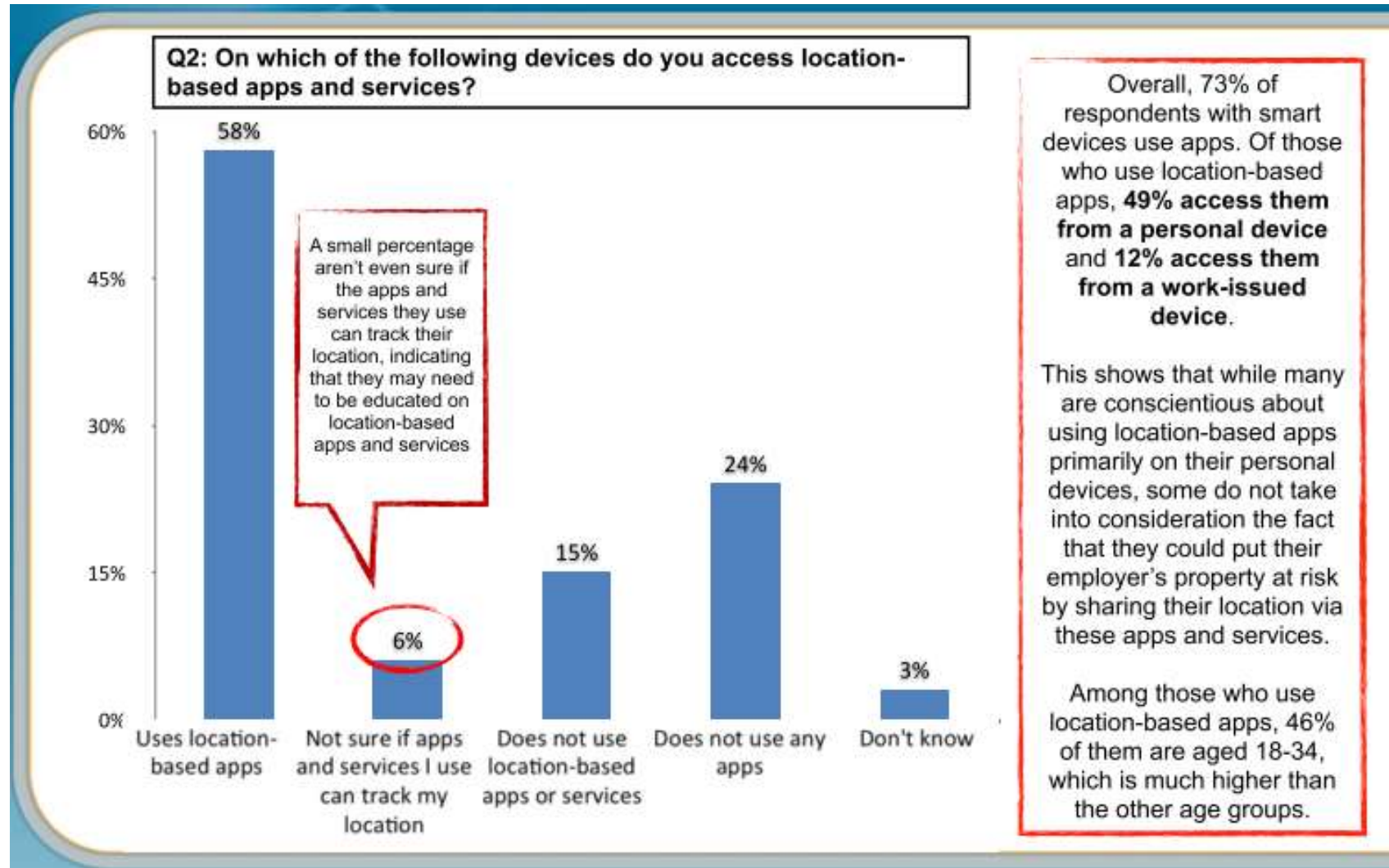
Potential Risks to Corporate IT

- **Privacy:** Geo-tagging is implemented by users, but there may be multiple entities that have access to the data, including the service provider and wireless access points/developers. Users can't always identify (or aren't aware of) the source or owner of their location data.
- **Enterprise reputation:** When breaches occur or policies have not been communicated clearly to customers, organisations risk negative perceptions of their brand.
- **Compromise of sensitive information:** The physical location of an enterprise and its remote facilities/equipment can be identified, increasing potential loss of sensitive information through a variety of attacks.

From ISACA's Survey

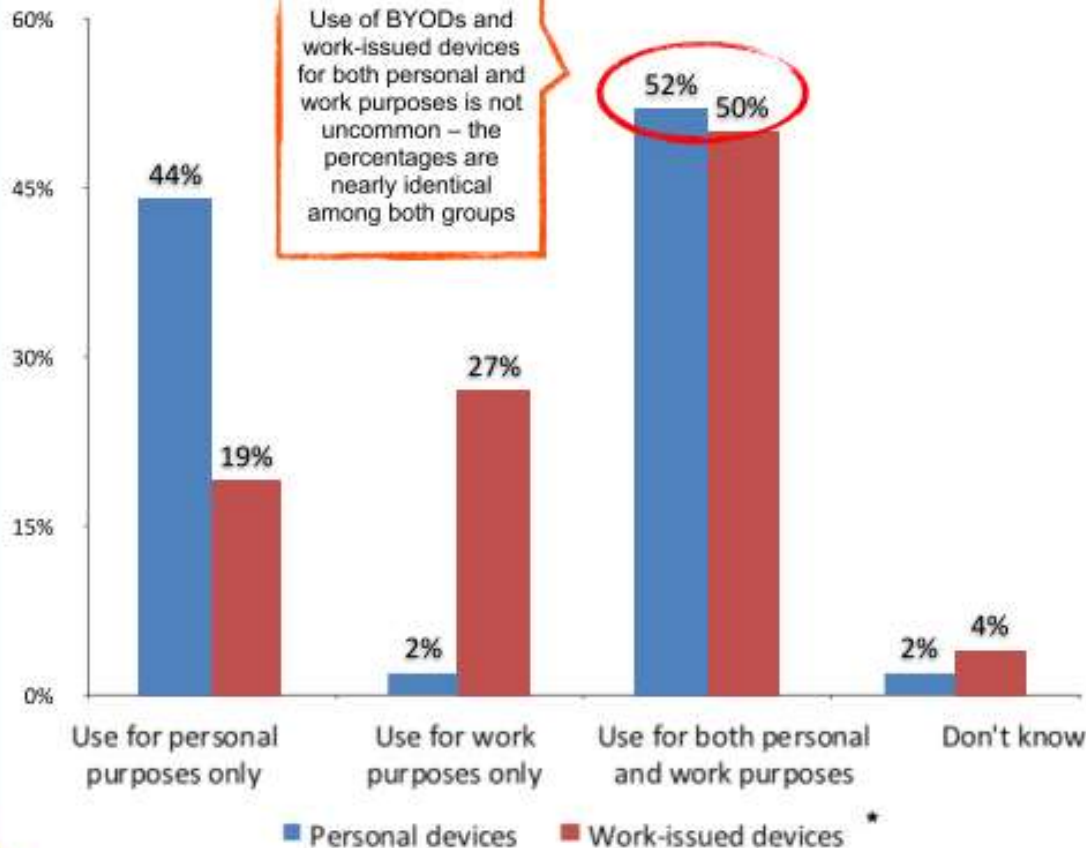
- There is an overall lack of knowledge regarding the risk involved with location-based apps given that the majority of those downloading them either don't read or don't understand terms/agreements.
- Considering the digital age in which we live, where what we ate for breakfast is shared on Twitter and Facebook, it is interesting that the top two concerns are about sharing too much information about themselves, followed closely by concern about personal safety.
- The people who are using company-issued devices for both location-based apps and personal reasons could be putting those organisations at risk.

Use of Location-based Apps



BYOD vs. Work-issued Devices

Q1: How do you use each of the following types of smart devices?



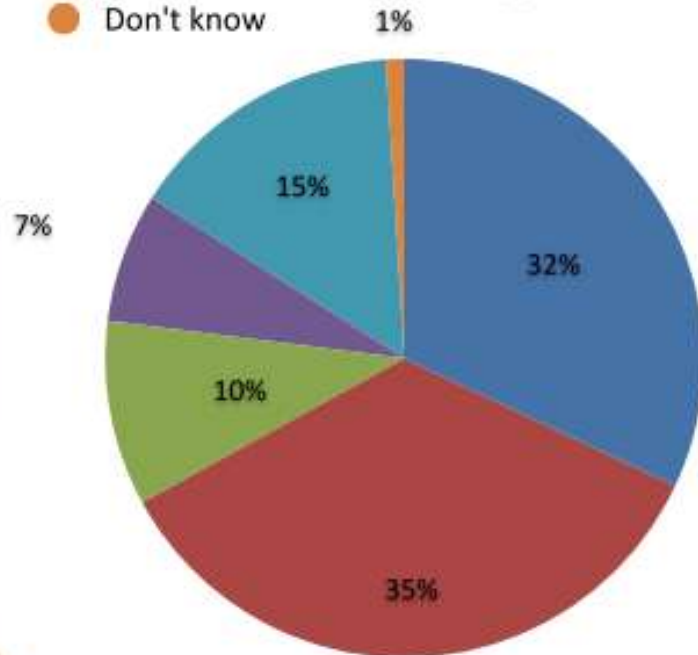
Use of BYODs and work-issued devices for both personal and work purposes is not uncommon – the percentages are nearly identical among both groups

Those with smart devices (whether personal or work-issued) tend to use their device for both personal and work purposes. More than half (52%) use their personal device for both personal and work purposes—a growing trend known as bring your own device (BYOD).

More than half (62%) of those aged 18-34 use their personal device for both personal and work purposes, vs. 40% of those aged 55-64. The younger crowd blurs the line between personal and professional much more than the older set does.

Q3: Do you use location-based apps and services more or less than you did 12 months ago?

- I use them more
- I use them the same amount
- I use them less
- I'm not sure if the apps/ services can track my location
- I never use location-based apps/ services
- Don't know



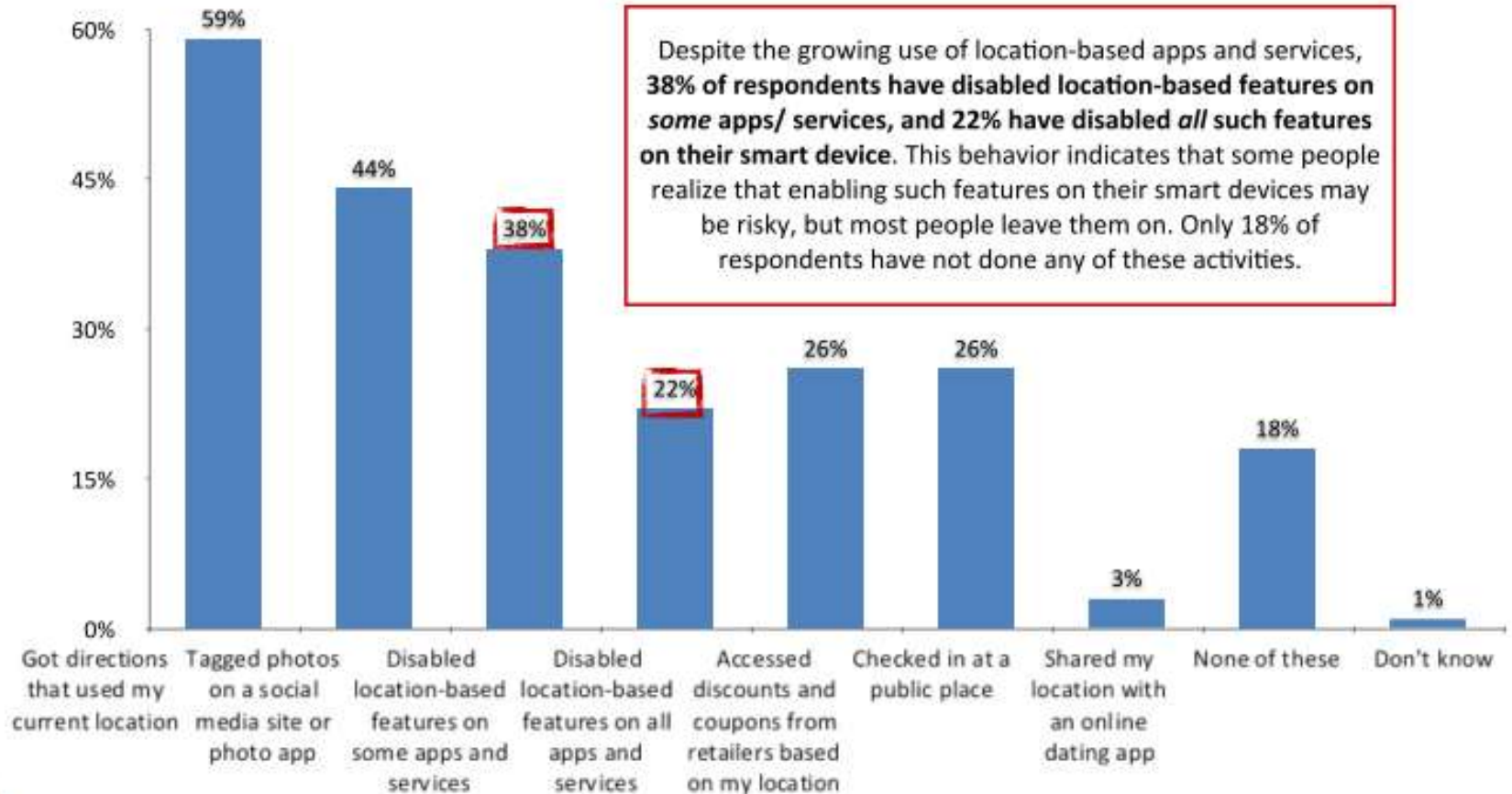
Two-thirds (67%) use location-based apps and services **the same amount or more** than they did 12 months ago.

Overall, only 10% of respondents reported that they use apps *less* today than they did 12 months ago, indicating that these types of apps are showing strong growth among those with smart devices.

Among those aged 18-34, 81% are using location-based apps the same amount or more than they were 12 months ago.

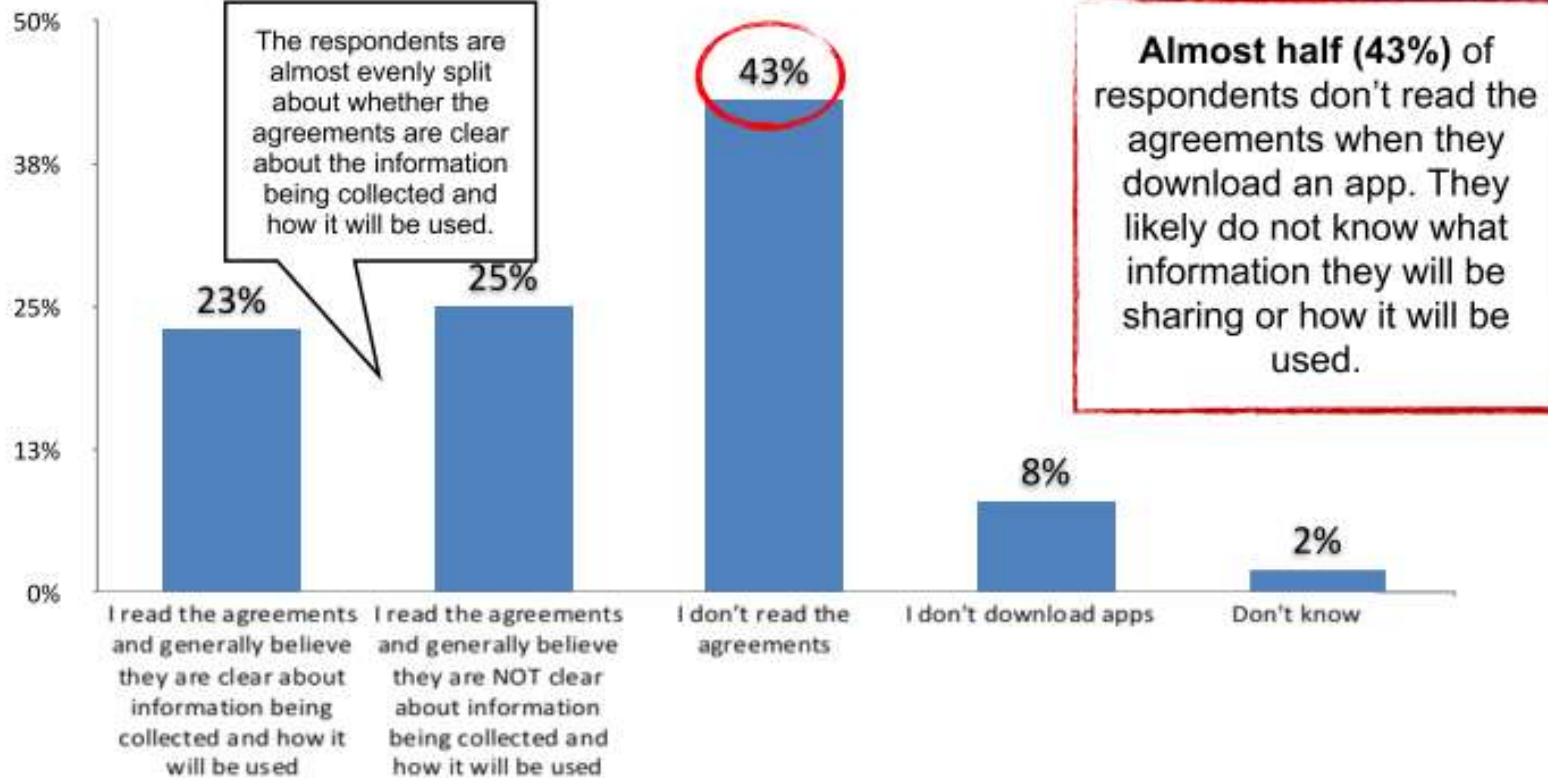
Activities on Mobile Devices

Q4: Which of the following have you done on your smartphone, tablet or laptop?



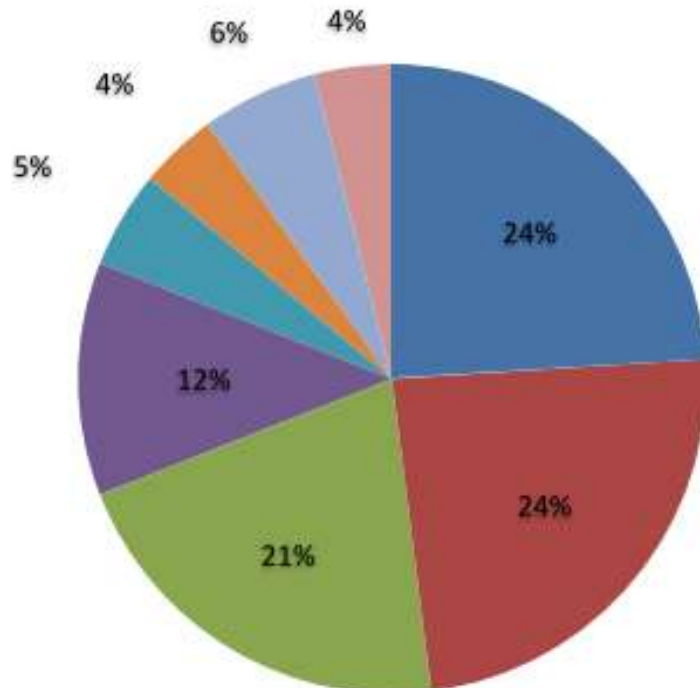
Agreements

Q5: When downloading apps, would you say...



Q7: Which of the following are you MOST concerned about in relation to location-based apps and services?

- Strangers knowing too much about my activities
- My information being shared and used for marketing purposes
- Personal safety
- Government knowing too much about my activities
- Family and friends knowing too much about my activities
- Employer knowing too much about my activities
- I am not concerned about location-based apps and services
- Don't know



Overall, **89%** of respondents have some type of concern about location-based apps and services and could benefit from education on how to safely and securely use these services.

The top concerns for men and women differ slightly:
For women, the top concern is strangers knowing too much about their activities (29%), followed by concerns about their personal safety (27%).

The top concern for men is their information being shared and used for marketing purposes (29%), followed by strangers knowing too much about their activities (19%).

Addressing the concerns that people have will differ slightly between genders – women may respond better to learning about protecting themselves, while men may respond better to learning about the marketing activities that may occur using their information.

User Awareness

Geo-location risk extends farther than to a sole individual. The location data risk also pertains to enterprises, employees and families. The areas of concern regarding privacy and safety on geo-location are:

- What data are collected?
- Who is collecting location data? How are the data used? With whom can the data be shared? How long can the data be stored?
- Spamming by advertisements or offers based on physical location
- Accidental or unintentional sharing of location data resulting in annoyance, embarrassment or danger to an individual

1. Introduction: What is Geo-Location and How Does IT Work?
2. Business Benefits
3. Risk, Security and Privacy Concerns
4. **Strategies for Addressing Risk**
5. Assurance
6. Summary and Wrap-Up

Risk Mitigation?

Two paths that can mitigate the risk of geo-location:

- through technology safeguards and
- through the user.

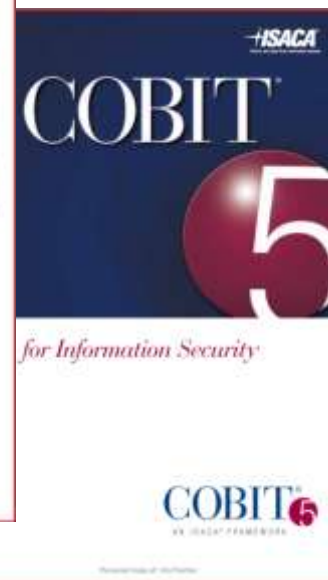
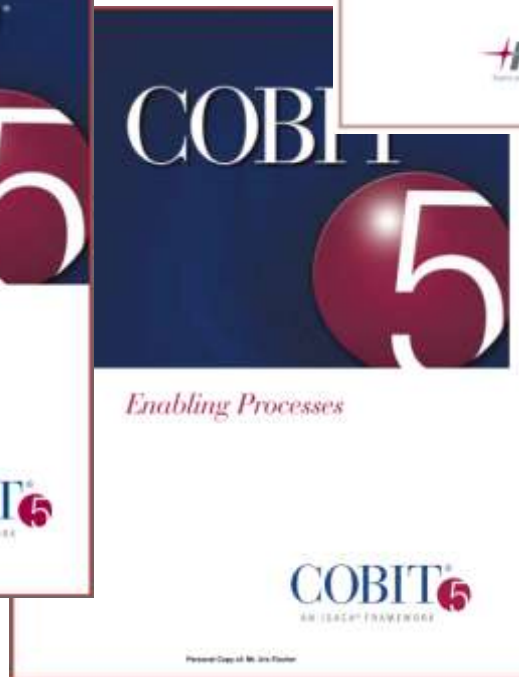
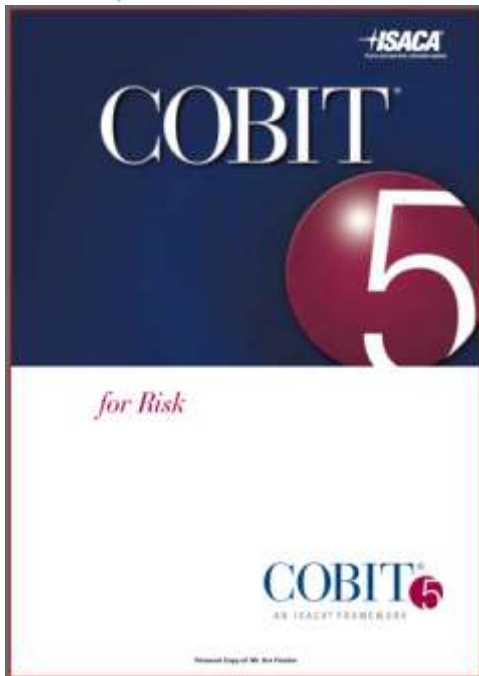
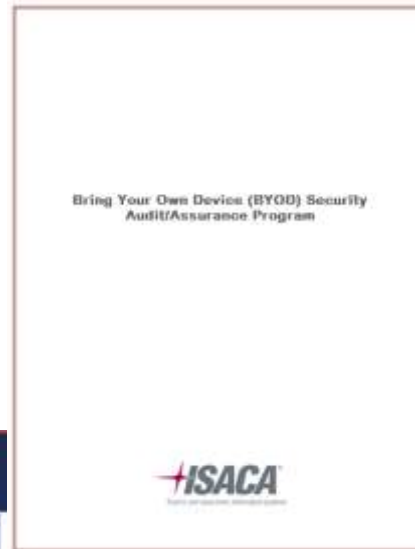
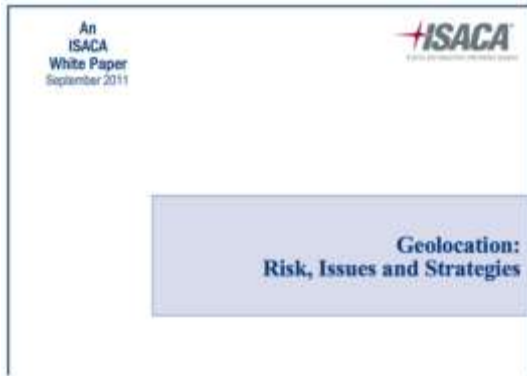
There is an implied urgency in addressing such risk as the geo-location genie is out of the bottle, so to speak.

General Controls

- Operating system and software should be updated periodically with antivirus software
- Patches should be implemented and backups should be performed regularly
- There should be logical and physical access controls that restrict access to a “need to know basis” and are monitored for unauthorized access
- Subscribing to the principle of “keep the least for the shortest period”
- Using anonymisation techniques

1. Introduction: What is Geo-Location and How Does IT Work?
2. Business Benefits
3. Risk, Security and Privacy Concerns
4. Strategies for Addressing Risk
- 5. Assurance**
6. Summary and Wrap-Up

Where you can find help?



4 Aspects

- ISACA's COBIT 5 product family can be used by service providers and requestors to provide the basis for risk management, compliance and proper use of geo-location information.
- Auditing, vetting and certifying geo-location service providers and third-party users.
- Providing security and safety assessment of mobile applications employing geo-location capabilities.
- Ensuring compliance with privacy and usage laws and regulations by service providers and technology developers across diverse international jurisdictional boundaries. Compliance in this context would also include consideration of the full spectrum of ethics of use issues.

Assurance Strategy

- Proper Guidelines, Processes and Procedures
- Integrity of the technologies used
- Security of Devices
- Analysis of user-behaviour in view of compliance

1. Geolocation: Was ist es und wie funktioniert das?
2. Geschäftsvorteile
3. Risiko-, Sicherheits- und Datenschutz-Überlegungen
4. Strategien für den Umgang mit Risiken
5. Überlegungen zur Prüfung (Audit)
6. **Zusammenfassung / Wrap-Up**

1. Introduction: What is Geo-Location and How Does IT Work?
2. Business Benefits
3. Risk, Security and Privacy Concerns
4. Strategies for Addressing Risk
5. Assurance
6. **Summary and Wrap-Up**

The right questions

- How have mobile devices, networks and location-based services changed our values regarding privacy, data collection and data use?
- What rights do people and organizations have regarding the data collected? What rights do people and organizations expect and are these expectations changing as services become more popular?
- What rights are granted and recognized internationally, and how can compliance with local and international standards be assured? What rights should corporations ethically grant their users?
- What standards should apply to government access to, and collection of, location data? What limits should there be on law enforcement access to these data?
- What are the most significant international differences in the standards for government access to location data?

Conclusion

The increasingly global nature of content and the migration of multimedia content distribution from typical broadcast channels to the Internet make geo-location a requirement for enforcing access restrictions, supporting fraud prevention, and providing the basis for traditional performance-enhancing and disaster recovery solutions.

Take The ROUTE Approach



Questions / Discussion



Urs Fischer, CPA (Swiss), CRISC, CISA
Fischer IT GRC Consulting & Training

Mail: info@fischer-it-grc.ch

Xing: https://www.xing.com/profile/Urs_Fischer12?sc_o=mx_b_p

Linkedin: http://www.linkedin.com/profile/edit?trk=hb_tab_pro_top



- CPA (Swiss) by origin, CRISC, CISA & CIA
- 5 year external auditor
- Switch to IT Audit – In IT Audit for 13 years incl. Head of IT Audit
- 2004-2010 Head IT Governance & Risk Mgmt
- Since 2011 independent IT GRC Consultant and Trainer

- Co-Author of CobiT4 and now participant of the development of COBIT5
- Co-Developer of CobiT Control Practices
- Co-Developer of ISACA's "IT Control Objectives for Cloud Computing"

- Board member of ISACA CH Chapter for about 8 years
- Member of the CobiT Steering Committee for 3 years
- Member and Chair of ISACA's EuroCACS Conference Programme Committee for 6 years
- 2008 – 2009 Chair of ITGI's 'Risk IT' Task Force
- 2009 – 2010 Chair of ISACA's CRISC Task Force
- 2006 – 2011 Member of ISACA Audit Committee (since 2008 – 2011 Chairman)
- 2010 – 2011 Member of ISACA's Guidance and Practice Committee
- 2009 – 2012 Member of ISACA's Credentialing Board
- 2010 – 2012 Chair of ISACA's CRISC Committee
- 2012 Member of ISACA/ITGI's Nomination Committee

- 2010 Receiver of the 'John W. Lainhart IV – Common Body of Knowledge Award'