



Surveying Online Privacy in a Digital World

M. Barba, N. Tsalis

January 2016



Surveying Online Privacy in a Digital World

Melina Barba

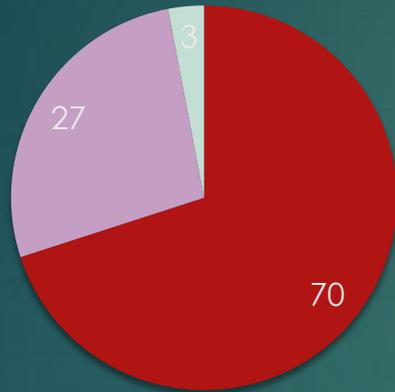
Supervisors: **Prof. Dimitris Gritzalis**
Nikolaos Tsalis

Dept. of Informatics
Athens University of Economics and Business Greece

Introduction

- In the last 20 years, the Internet has become drastically essential in everyday tasks associated with stationary and mobile computer devices. People have easy access to the Internet and this digit world has provided them with a lot of benefits. In this survey, it will be discussed how comfortable people feel as the Internet has entered their daily lives.
- Firstly, people felt that they totally have lost control about the amount of the information collected by :
 - companies for their purposes
 - social networking sites
 - government.
- Moreover, it will be analyzed the fact that people started to worry about their smartphones and they think if they would be safer with other cell phones.
- People would not have revealed personal information if they had read the privacy policies for each website.
- Last but not least will be analyzed the option to browse the Internet while keeping their user information private which is private browsing.

Consumer's concerns about online privacy



■ Total "Concerned" ■ Total "Not Concerned" ■ Don't Know

Figure1-How concerned were people about companies data gathering.

- 50% of the people felt familiar with data gathering techniques and devices.
- 30% of the people deleted cookies in order to avoid targeted advertising
- 73% of them said that “Privacy is a right so it is wrong to be asked to pay to keep companies from invading my privacy”.
- 74% of the people mentioned that their specific approval should be required in all cases before any kind of personal information was collected.
- However 51% of the people would sacrifice their privacy in order to achieve lower prices and better services.
- Last but not least 71% of them only some of the time could trust companies, especially advertising companies.

Social media and online privacy

- 90% of the people revealed a lot of their personal information to social networking sites.
- 61% of them disclosed personal information in order to have access to the service.
- 80% of them changed privacy settings only when they experienced a personal invasion.
- 50% of the parents pointed that they used parental controls such as blocking, filtering or monitoring their child's online behavior with the purpose of protecting them.
- 60% of the teenagers users have set their Facebook account to private
- 81% of the people felt not at all secure using social media sites.

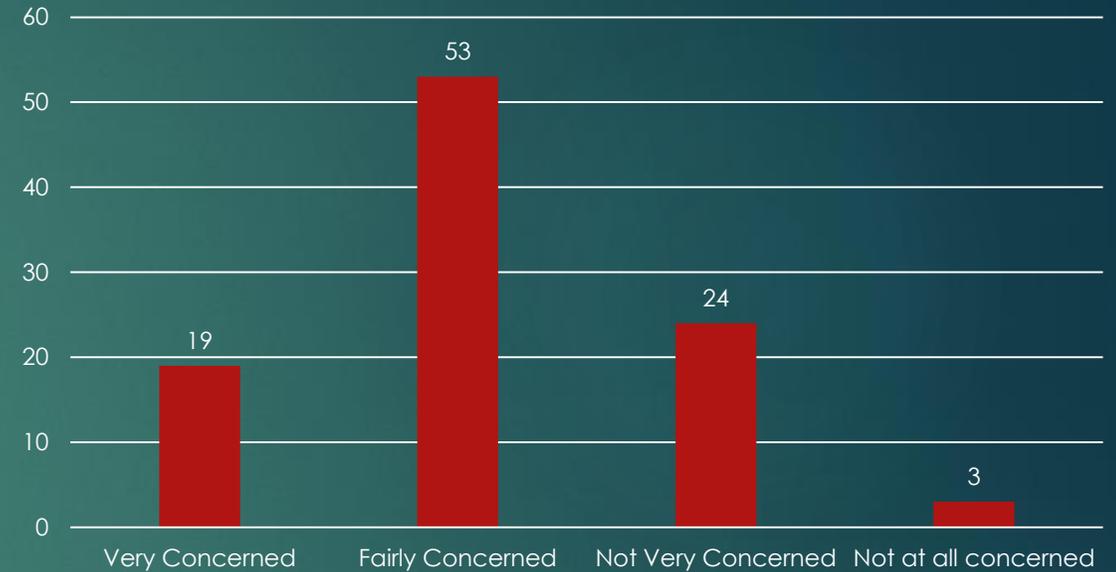


Figure2- How concerned were people about the disclosure of information in social media.

Government Surveillance

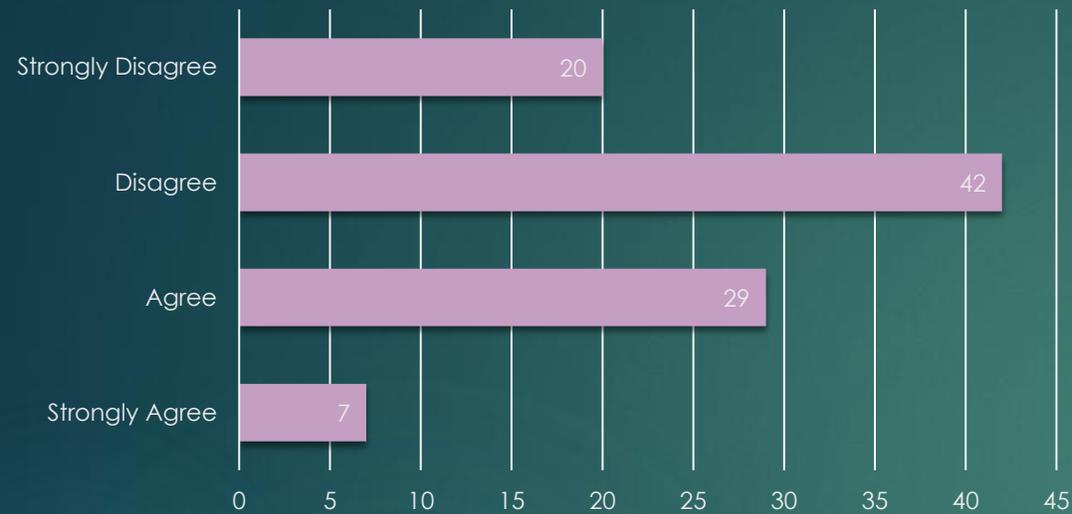


Figure3-How many people agreed with the statement that it is a good thing for society if they were being watched online by government surveillance programs.

- 43% of the people had heard a lot about government surveillance programs.
- 71% of them have searched about their name in order to see what kind of information was online about them
- 95% of them felt not secure sending private information via email.
- 76% of them believed that government should monitor suspected terrorists.

Mobile Devices

- 30% of the smartphone users had turned off location tracking vs. 7% of the other cell phone users.
- 54% of smartphone users decided not to install an application in order to avoid collection of personal data.
- **66%** of the people felt secure sharing personal information using **landline phones**.
- 50% of the people felt secure sharing private information using smartphones.

Ways to achieve privacy

- 71% of the people use private browsing.

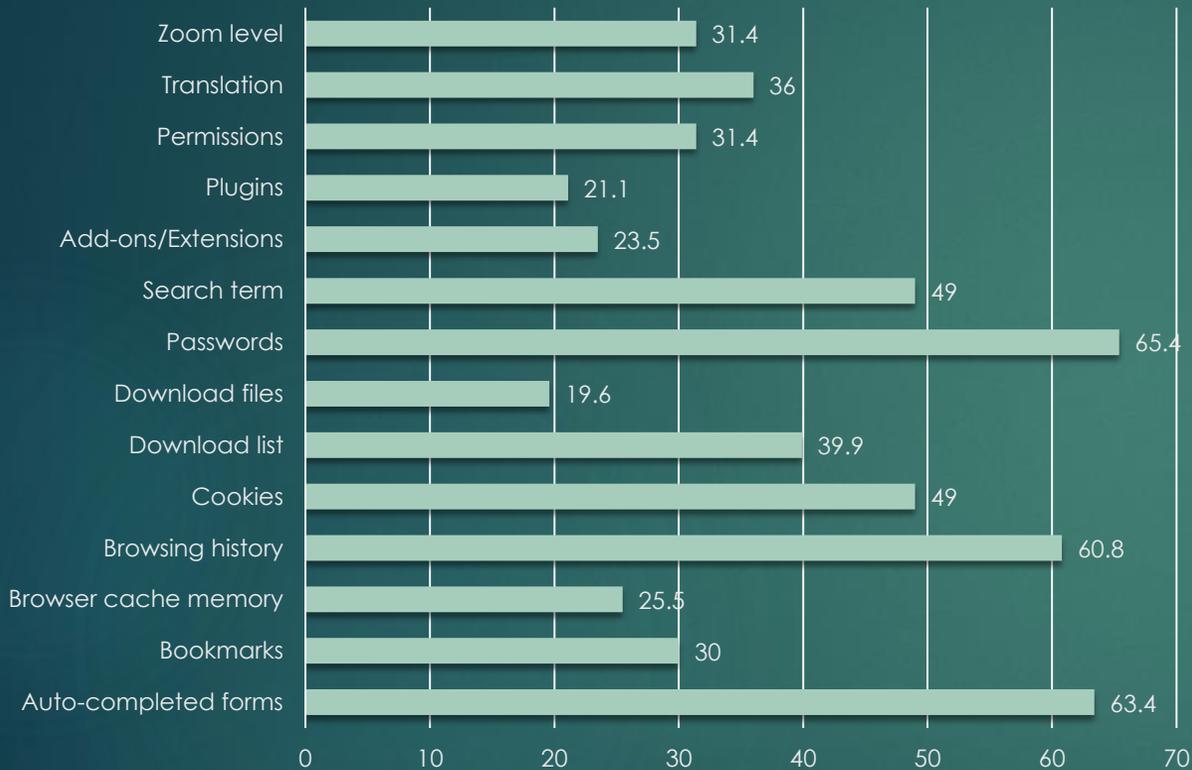


Figure4-How many people believed that these artefacts did not remain after private browsing.

- 82% of the people were aware about privacy laws.
- 68% of them mentioned that current laws could not protect people's privacy online.
- 51% of the people did not read privacy policies on the websites.
- 52% of the respondents believed that privacy policy was too long
- 68% of them mentioned that they had chosen not to use a website due to the content of the privacy policies.
- 65% of the people found privacy policies for the websites at least vague.

Conclusions

- Consumers felt that they had lost control of the personal information that companies had gathered.
- People disclosed a lot of personal information in social networking accounts.
- People changed default privacy setting to private in social networking accounts.
- People felt uncomfortable in communicating through emails and send private information because they believed that their information was monitored by government
- Smartphone users turned off location tracking.
- People didn't read privacy policies while parents always did at the websites that their child visited.
- People used private mode in order to protect their personal information.

References

1. Theoharidou M., Tsalis N., Gritzalis D., “In Cloud we trust: Risk-assessment-as-a-service”, in Proc. of the 7th IFIP International Conference on Trust Management, pp. 100-110, Springer (AICT 401), Spain, 2013.
2. Tsalis N., Mylonas A., Gritzalis D., “An intensive analysis of the availability of security and privacy browser add-ons”, in Proc. of the 10th International Conference on Risks and Security of Internet & Systems, Springer, Greece, 2015.
3. Tsalis N., Virvilis N., Mylonas A., Apostolopoulos A., Gritzalis D., “Browser blacklists: A utopia of phishing protection”, in Security & Cryptography, Springer (CCIS), 2015.
4. Tsalis N., Theoharidou M., Gritzalis D., “Return on security investment for Cloud platforms”, in Proc. of the Economics of Security in the Cloud Workshop, pp. 132-137, IEEE Press, 2013.
5. Virvilis N., Mylonas A., Tsalis N., Gritzalis D., "Security busters: Web browser security vs. rogue sites", Computers & Security, Vol. 52. pp. 90-105, July 2015.
6. Virvilis N., Tsalis N., Mylonas A., Gritzalis D., "Mobile devices: A phisher's paradise", in Proc. of the 11th International Conference on Security & Cryptography, pp. 79-87, ScitePress, Austria, 2014.
7. Virvilis N., Gritzalis D., “The Big Four - What we did wrong in Advanced Persistent Threat detection?”, in Proc. of the 8th International Conference on Availability, Reliability & Security, pp. 248-254, IEEE Press, Germany, 2013.
8. Virvilis N., Gritzalis D., “Trusted Computing vs. Advanced Persistent Threats: Can a defender win this game?”, in Proc. of 10th IEEE International Conference on Autonomic & Trusted Computing, pp. 396-403, IEEE Press, Italy, 2013.
9. Acquisti A., Brandimarte L., Loewenstein G., “Privacy and human behavior in the age of information”, *Science*, 347(6221), 509-514, 2015.