# On the impact of the digital age on the conflict between privacy and transparency

Steve Roach and Christian Servin

University of Texas at El Paso
Computer Science Department
500 W. University, EL Paso TX 79968
sroach@utep.edu

**Abstract.**

## 1 Introduction

Any privacy-related problem consists in protecting non-public information. We can refer as the Non-public information (NPI) to all the information required in a financial service (e.g., credit card, bank account). NPI can include: names, addresses, account numbers, salaries, social security numbers, passwords, medical information, and account balances. Treating information separately, i.e., having information in different databases, may not cause any privacy problem. However, a compilation of different information can potentially disclose someone's privacy. A clear example is obtaining your social security number (which is considered as a sensitive information) and your name. With this information someone can access the Internal Revenue Service department (IRS) records, and then have an idea of how much money you earn. Using this information with malicious intentions can lead to a fraud or an abuse of personal information.

Medical Doctors and patients conversations/files is an example of a private manner. Patients medical examinations should not be disclosed to anyone but the patient. If that information becomes public, that sensitive information (about diseases, DOB, or special medication) can be used against the patient or limit opportunities, e.g., discrimination, denial of insurance, others The voting is treated as a private matter, nobody should know (at least if you want to) for whom you vote or which party you support. However, counting votes is a transparent matter, as well as we count with our checks in our banks every month. (Idea of depositing checks at the bank branch and the teller knows how much money is in our banks accounts).

Claim: in order to maintain a stable society we have to rude root out the evil elements in out society Google servers contains an enormous amount of information about millions of users. Emails, instant messages, search queries, calendars Google uses Googles adds to announce products that might be of your special interest (according to your preferences). The Googles administrators cannot give this collection of information to the sellers because they will be violating users privacy. If we could use Googles information to find terrorism, sexual-abuse, environmental degradation, or any other compiled interest, maybe they can prevent serious problems. Where can we define the real boundary? Radio Frequency Identification (RFI) or the Global Positioning Systems (GPS): These days mobile phone users can add a GPS feature to their mobile for only $2.99 a month, and be informed where their buddies are located. Very handy to trace lost or kidnapped children. At the same time, everyone in the authorized network (or perhaps unauthorized) can monitor you every second, every place you have been for the past 24 hours, and the time spent in that place.

Transparency example: the media  newspaper or TV channel news. Religious vestments. In the book Right to Privacy, mention several cases, that the media broadcast events (e.g., a dead body, a house in a certain neighborhood) and people believed was an offense to their private rights. In some cases courts decided that was no such offense.

Individuals, groups, and institutions all have some expectations of privacy, yet in many cases we willingly sacrifice privacy for a greater good. This paper explores the inherent conflict between privacy and transparency and the impacts of modern and future technology on this conflict. Specifically, the paper attempts to answer the following set of questions: What is a privacy concern? What is a transparency concern? When does a privacy concern outweigh a transparency concern? When does a transparency concern outweigh a privacy concern? What are the fundamental principles or issues that must be considered when trying to decide whether transparency outweighs privacy? How do we decide, as a society or as ethicists, which of these is most important? What options do we have, as technologists, to change our own behaviors? What obligations do we have for our behaviors? If an individual isnt doing anything wrong, why not expose the activities. What difference does it make? If an individual isnt doing anything wrong, why expose the activities? What difference does it make?