Preserving Privacy in Caller ID Applications

Stefanović Tamara   Ghilezan Silvia

University of Novi Sad, Serbia

LAP, September 2020

Outline

Table of Contents

What is Caller ID?

Caller identification (or Caller ID) is a telephone service.

- It transmits a caller's phone number to a receiving party's telephony equipment when the call is being set up.
- It may transmit a name associated with the calling telephone number.

📄 Papakipos, M.N., Walkin, B.M.: Caller identification using social network information (Aug 2012)

Caller ID App Features

The main Caller ID app features:

- identification of incoming calls from the unknown numbers

Caller ID App Features

The main Caller ID app features:

- identification of incoming calls from the unknown numbers
- blocking calls and messages

Caller ID App Features

The main Caller ID app features:

- identification of incoming calls from the unknown numbers
- blocking calls and messages
- call recording

Caller ID App Features

The main Caller ID app features:

- identification of incoming calls from the unknown numbers
- blocking calls and messages
- call recording
- search function

Violating Individual's Privacy

Once you install a Caller ID application, it will have access to your:

- address book,
- call list,
- messages

During the installation, you confirm that all the persons from your address book have given their **consent** to share their phone number and the name under which their number is stored in your address book.

Violating Individual's Privacy

Once you install a Caller ID application, it will have access to your:

- address book,
- call list,
- messages

During the installation, you confirm that all the persons from your address book have given their **consent** to share their phone number and the name under which their number is stored in your address book.

Example

Alice, the journalist, working on sensitive stories.

Compliance with the Data Drivacy Laws

Caller ID App Privacy Policies:

- Truecaller
- Everybody

Data Privacy Laws:

- GDPR
- ePRivacy Directive
- ePrivacy Regulation

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓
- The information reffered above shall be provided at the latest when the personal data are first disclosed.

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓
- The information reffered above shall be provided at the latest when the personal data are first disclosed. ✓

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓
- The information reffered above shall be provided at the latest when the personal data are first disclosed. ✓
- Right of deletion of your personal data.

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓
- The information reffered above shall be provided at the latest when the personal data are first disclosed. ✓
- Right of deletion of your personal data. ✓

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓
- The information reffered above shall be provided at the latest when the personal data are first disclosed. ✓
- Right of deletion of your personal data. ✓
- Sharing of your personal data based on the consent.

Compliance with the Data Privacy Laws: Conclusion

- Right to be provided with informations about collecting and processing of your data ✓
- The information reffered above shall be provided at the latest when the personal data are first disclosed. ✓
- Right of deletion of your personal data. ✓
- Sharing of your personal data based on the consent. **??**

Table of Contents

Inverse Privacy

Inverse Privacy

An item of your personal information is **inversely private** if

- some party has access to it,
- but you do not have.

The inaccessibility to you of your personal data is the inverse privacy problem.

📄 Gurevich, Y., Hudis, E., Wing, J.M.: Inverse privacy. CoRR abs/1510.03311 (2015), http://arxiv.org/abs/1510.03311

Solution for the Inverse privacy problem and Privacy of a phone number

- The Biggish platform

Solution for the Inverse privacy problem and Privacy of a phone number

- The Biggish platform
- Private, non-private and partially private phone number

Non-user's Privacy and Inverse Privacy
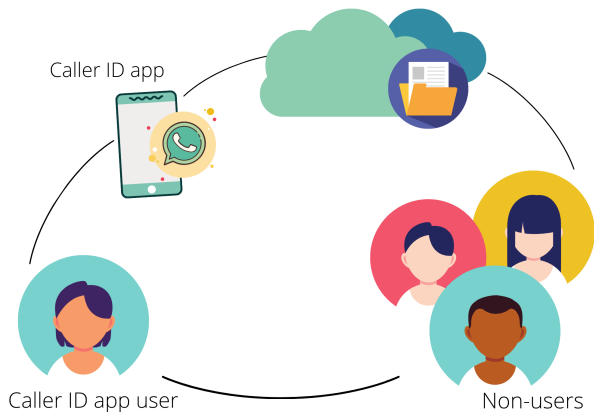
The connection between users, non-users and the Biggish platform.

Caller ID app graph

Definition (Caller ID App Social Graph)

The Caller ID application data is modeled by a **graph** $G = (V; E; A; P)$, where

- V-set of nodes representing users and non-users,
- $E \subseteq V \times V$-set of edges,
- A-set of attributes associated with every node,
- P-set of privacy variables.

Privacy Variables

A **privacy variable** is a variable associated with the name attribute:

- name,
- surname,
- hometown,
- school,
- profession ...

Privacy variables have only two values:

- 0, for non-private information
- 1, for private information

Privacy Variables

A **privacy variable** is a variable associated with the name attribute:

- name,
- surname,
- hometown,
- school,
- profession ...

Privacy variables have only two values:

- 0, for non-private information
- 1, for private information

Motivation: The greater sensitivity of certain names compared to other names.

Name Sensitivity

Definition (Name Sensitivity Function)

Let X be a name attribute and x any value of the name attribute, sensitivity of x denoted by $S(x)$ is defined by:

$$S(x) = \left\{ \begin{array}{ll} 0, & \text{if } 1^\circ \text{or } 2^\circ \\ \frac{n}{m}, & \text{if } 3^\circ \\ 1, & \text{if } 4^\circ \text{or } 5^\circ \end{array} \right.$$

where

- n - a number of variables that are marked as private, and the value x matches them,
- m - a total number of variables that are marked as private.

Name Sensitivity

Definition 2(Name Sensitivity)

$1°$ The phone number associated with the name x is non-private.

$2°$ The phone number associated with the name x is partially private, but x does not match any variable that is marked as private.

$3°$ **The phone number associated with the name x is partially private and x matches some of the variables that are marked as private.**

$4°$ The phone number associated with the name x is private.

$5°$ The phone number associated with the name x is partially private and x matches all the variables that are marked as private.

Name Sensitivity

Example

Journalist example. Given the set of privacy variables $P = \{P_1, P_2, P_3\}$ where P_1 defines name, P_2 defines profession, P_3 defines affiliation, and setting P_2 and P_3 to be private, the sensitivity of the following names associated with her phone number is:
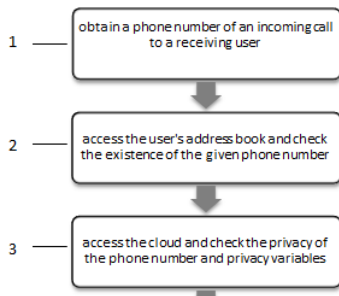
- if $x_1 =$ "Alice", $S(x_1) = \frac{0}{2} = 0$;
- if $x_2 =$ "Bob", $S(x_2) = \frac{0}{2} = 0$;
- if $x_3 =$ "Alice the journalist", $S(x_3) = \frac{1}{2}$;
- if $x_4 =$ "Bob the journalist New York Times", $S(x_4) = \frac{2}{2} = 1$.

Algorithm for Name Sensitivity Check

Step 1. Obtain a phone number of an incoming call.
Step 2. Check whether the phone number is stored in the user's address book.
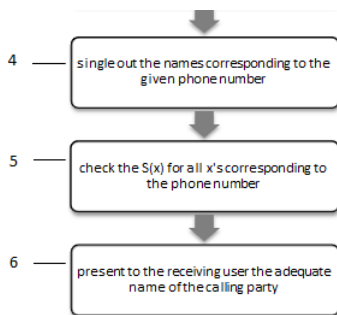**Step 3.** Check the privacy of the phone number.

The first part of the algorithm

Algorithm for Name Sensitivity Check

Step 4. Single out the names associated with the given phone number from the database.
Step 5. Check the sensitivity of every name that has been singled out. Select one of the names with zero sensitivity.
Step 6. Present the adequate name of the calling party, or inform the user that it was not possible to find an adequate name.

4 — single out the names corresponding to the given phone number

5 — check the S(x) for all x's corresponding to the phone number

6 — present to the receiving user the adequate name of the calling party

The second part of the algorithm

Concluding Remarks

- The problem of privacy preservation in Caller ID apps
- The connection between this problem and the inverse privacy problem.
- The notion of privacy variables and name sensitivity.
- An algorithm for name sensitivity check.

Further Work:

- matching the names with a certain privacy variable
- privacy from the server side, learning personal information from the social graph

"Data is the pollution problem of the information age, and protecting privacy is the environmental challenge."

Bruce Schneier