



# Outline

1. Introduction: Privacy and Context-Aware Applications
2. Pseudonym Mechanism
3. In Use
4. Conclusions and The Future

# 1. Introduction: Privacy and Context-Aware Applications







# Principle

Limit data understanding, as opposed to using access control,  
and associate information with pseudonyms.

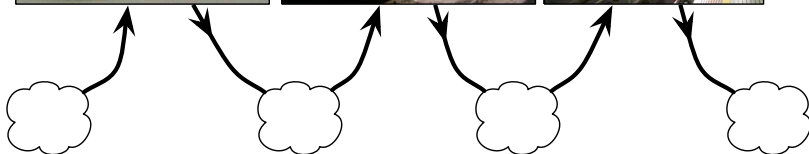
# Anonymising Personal Information

## Static pseudonym



# Anonymising Personal Information

## Dynamic pseudonym



## 2. Pseudonym Mechanism

# Idea

Bind ID, key, and context into a pseudonym







# Pseudonym Properties

1. Given access to  $P$ , an attacker without the correct key cannot infer the ID or the context of the corresponding person.
2. Given access to  $P$  and the correct key, a user may be able to infer the context.
3. Given  $P_{i,j}^{(n)}$  and  $P_{i,j}^{(m)}$ , individual  $j$  can link the movement of user  $i$  from context  $C_n$  to  $C_m$ .
4. Given access to  $P = P_{i,j}^{(n)}$ ,  $P' = P_{i,j}^{(m)}$ , but not  $K_{i,j}$ , an attacker cannot determine that  $P$  and  $P'$  represent the same person.
5. Unrestricted distribution of the pseudonym does not compromise real-world identity.

# Pseudonym Properties

1. Given access to  $P$ , an attacker without the correct key cannot infer the ID or the context of the corresponding person.
2. Given access to  $P$  and the correct key, a user may be able to infer the context.
3. Given  $P_{i,j}^{(n)}$  and  $P_{i,j}^{(m)}$ , individual  $j$  can link the movement of user  $i$  from context  $C_n$  to  $C_m$ .
4. Given access to  $P = P_{i,j}^{(n)}$ ,  $P' = P_{i,j}^{(m)}$ , but not  $K_{i,j}$ , an attacker cannot determine that  $P$  and  $P'$  represent the same person.
5. Unrestricted distribution of the pseudonym does not compromise real-world identity.

# Pseudonym Properties

1. Given access to  $P$ , an attacker without the correct key cannot infer the ID or the context of the corresponding person.
2. Given access to  $P$  and the correct key, a user may be able to infer the context.
3. Given  $P_{i,j}^{(n)}$  and  $P_{i,j}^{(m)}$ , individual  $j$  can link the movement of user  $i$  from context  $C_n$  to  $C_m$ .
4. Given access to  $P = P_{i,j}^{(n)}$ ,  $P' = P_{i,j}^{(m)}$ , but not  $K_{i,j}$ , an attacker cannot determine that  $P$  and  $P'$  represent the same person.
5. Unrestricted distribution of the pseudonym does not compromise real-world identity.

# Pseudonym Properties

1. Given access to  $P$ , an attacker without the correct key cannot infer the ID or the context of the corresponding person.
2. Given access to  $P$  and the correct key, a user may be able to infer the context.
3. Given  $P_{i,j}^{(n)}$  and  $P_{i,j}^{(m)}$ , individual  $j$  can link the movement of user  $i$  from context  $C_n$  to  $C_m$ .
4. Given access to  $P = P_{i,j}^{(n)}$ ,  $P' = P_{i,j}^{(m)}$ , but not  $K_{i,j}$ , an attacker cannot determine that  $P$  and  $P'$  represent the same person.
5. Unrestricted distribution of the pseudonym does not compromise real-world identity.

# Pseudonym Properties

1. Given access to  $P$ , an attacker without the correct key cannot infer the ID or the context of the corresponding person.
2. Given access to  $P$  and the correct key, a user may be able to infer the context.
3. Given  $P_{i,j}^{(n)}$  and  $P_{i,j}^{(m)}$ , individual  $j$  can link the movement of user  $i$  from context  $C_n$  to  $C_m$ .
4. Given access to  $P = P_{i,j}^{(n)}$ ,  $P' = P_{i,j}^{(m)}$ , but not  $K_{i,j}$ , an attacker cannot determine that  $P$  and  $P'$  represent the same person.
5. Unrestricted distribution of the pseudonym does not compromise real-world identity.

# Pseudonym Database

