NRC · CNRC

Feature Interactions in Policy-Driven Privacy Management

George Yee **Larry Korba**

Network Computing Group
Institute for Information Technology
National Research Council Canada

{George.Yee, Larry.Korba}@nrc-cnrc.gc.ca

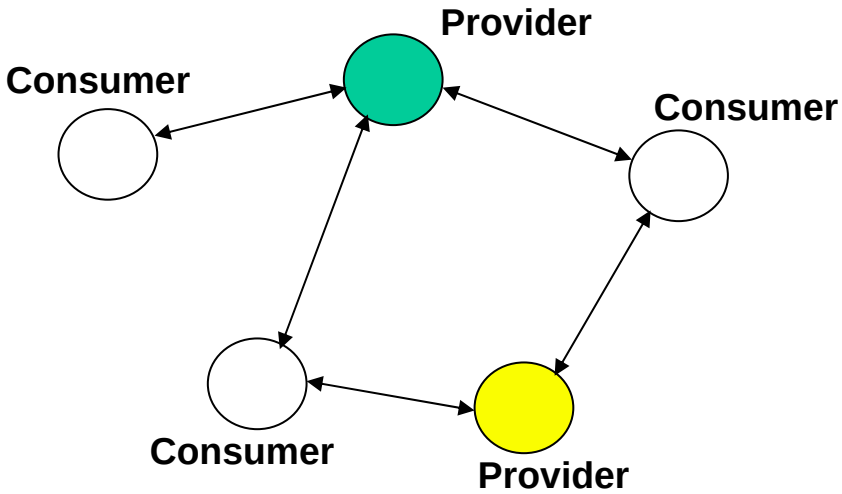
www.nrc-cnrc.gc.ca/iit

Contents

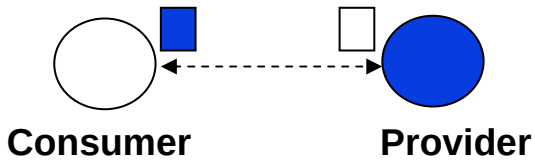
- **Introduction**
- **Privacy Policies**
- **Privacy Policy Interactions**
- **Preventing Unexpected Bad Outcomes**
- **Conclusions and Future Research**

Introduction

– **Proliferation of e-services**



– **Exchange of privacy policies**



Policy Exchanges → ? Interactions, ? Outcomes

How can the bad outcomes be avoided?

– **Started with negotiation of privacy policies for e-learning**

Privacy Policies

- **Privacy Principles → *who, what, purpose, time***

Privacy Policy: E-learning *Owner: E-learning Unlimited*	*Privacy Policy: Book Seller* *Owner: All Books Online*	*Privacy Policy: Medical Help* *Owner: Nursing Online*
Who: **Any** ***What:*** **name, address, tel** ***Purpose:*** **identification** ***Time:*** **As long as needed** ***Who:*** **Any** ***What:*** **Course Marks** ***Purpose:*** **Records** ***Time:*** **1 year**	***Who:*** **Any** ***What:*** **name, address, tel** ***Purpose:*** **identification** ***Time:*** **As long as needed** ***Who:*** **Any** ***What:*** **credit card** ***Purpose:*** **payment** ***Time:*** **until payment complete**	***Who:*** **Any** ***What:*** **name, address, tel** ***Purpose:*** **contact** ***Time:*** **As long as needed** ***Who:*** **Any** ***What:*** **medical condition** ***Purpose:*** **treatment** ***Time:*** **1 year**

Privacy Policy: E-learning *Owner: Alice Consumer*	*Privacy Policy: Book Seller* *Owner: Alice Consumer*	*Privacy Policy: Medical Help* *Owner: Alice Consumer*
Who: **Any** ***What:*** **name, address, tel** ***Purpose:*** **identification** ***Time:*** **As long as needed** ***Who:*** **Any** ***What:*** **Course Marks** ***Purpose:*** **Records** ***Time:*** **2 years**	***Who:*** **Any** ***What:*** **name, address, tel** ***Purpose:*** **identification** ***Time:*** **As long as needed**	***Who:*** **Any** ***What:*** **name, address, tel** ***Purpose:*** **contact** ***Time:*** **As long as needed** ***Who:*** **Dr. Alexander Smith** ***What:*** **medical condition** ***Purpose:*** **treatment** ***Time:*** **As long as needed**

Privacy Policy Interactions

- **Rules of Policy Exchange**

  - **Provider wants more private info; consumer wants to give up less private info**
  - **Match: privacy(consumer) ≤ privacy(provider), otherwise mismatch**
    - **privacy (long time) < privacy (short time)**
    - **policy upgrade → more privacy**
    - **policy downgrade → less privacy**

Privacy Policy Interactions

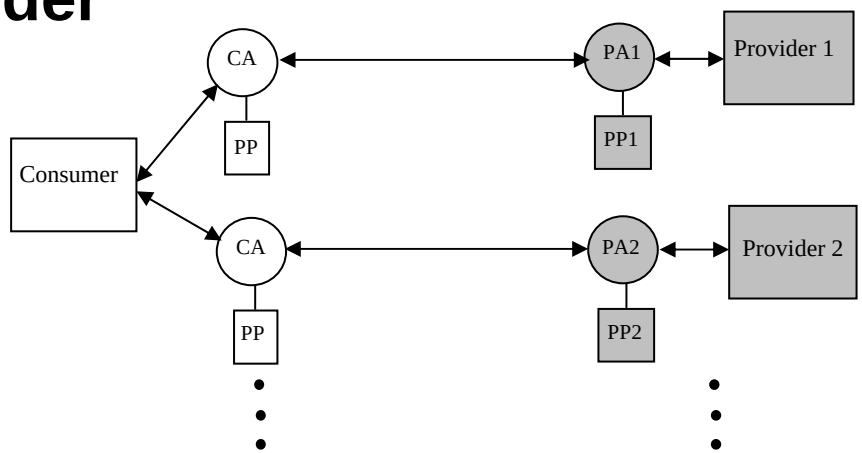
- **Privacy policy vs. telecom feature**
  - **Similarities**
    - **Privacy policy: handling of private data, Telecom feature: handling of traffic**
    - **Executions**
    - **Individual correctness, unexpected outcomes in combination**
  - **Differences**
    - **Telecom FI: side-effects; Policy FI: normal working**
    - **Certainty of unexpected outcomes**

Privacy Policy Interactions

- **1 consumer to 1 provider**
  - **Policies match; have service**
    - **If match is last of many failed attempts, provider may be less attractive in other criteria**
    - **If match after downgrade, may be hidden costs of less privacy**
    - **Hidden costs of safeguards**
    - **Unexpected outcomes, e.g. Nursing Online**
  - **Policies mismatch; no service**
    - **Consumer, provider may downgrade their policies**
    - **Possible denial of service with very serious consequences, e.g. Nursing Online**

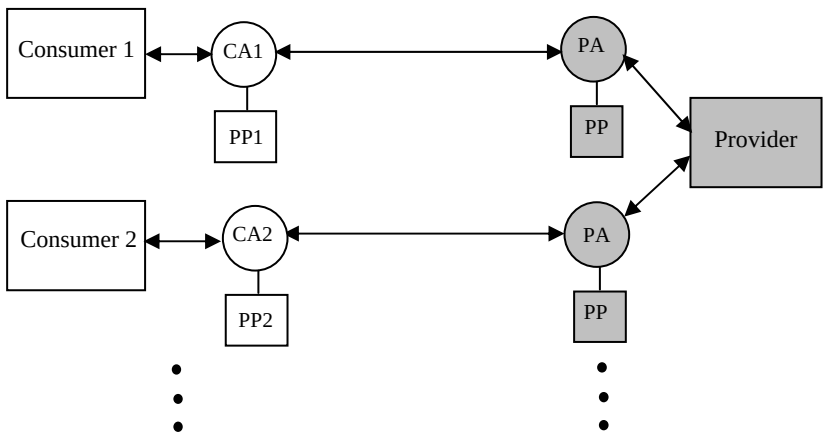
Privacy Policy Interactions

- **1 consumer to *n*>1 providers**
  - **Policies match for at least 1 provider, have service**
    - **Above 1-1 outcomes for match**
    - **Consumer may be able to select best provider**
  - **Policies mismatch, no service**
    - **Above 1-1 outcomes for mismatch**
    - **Consumer may downgrade policy to match best provider**



Privacy Policy Interactions

- ***n*>1 consumers to 1 provider**
  - **Policies match for at least 1 consumer, have service**
    - **Above 1-1 outcomes for match**
    - **Provider may be able to select best consumer**
  - **Policies mismatch, no service**
    - **Above 1-1 outcomes for mismatch**
    - **Provider may be able to downgrade policy to match best consumer**



Preventing Unexpected Bad Outcomes

- **Consumer and provider agents negotiate privacy policies to mitigate or eliminate bad outcomes**
  - **Reduce number of mismatches**
  - **Force consideration of policy implications**

Nursing Online (Provider)	***Alice (Consumer)***
OK if a nurse on our staff sees your medical condition?	*No, only Dr. Alexander Smith can see my medical condition.*
We cannot provide you with any nursing service unless we know your medical condition.	*OK, I'll see Dr. Smith instead.*
You are putting yourself at risk. What if you need emergency medical help for your condition and Dr. Smith is not available?	*You are right. Do you have any doctors on staff?*
Yes, we always have doctors on call. OK to allow them to know your medical condition?	*That is acceptable.*

Conclusions and Future Research

- **Privacy policies may be expressed in terms of *who, what, purpose,* and *time***
- **Agent proxies for consumers and providers exchange and compare privacy policies prior to service initiation**
- **Such exchanges can lead to unexpected interaction outcomes with negative consequences**
- **Rather than simple matching, privacy policies need to be negotiated, reducing or eliminating harmful interaction outcomes**
- **Future research:**
  - **Policies can change over time → revisit agreed policies?**
  - **Other methods in conjunction with negotiation?**
  - **Experiment with privacy negotiation prototype**