Journal of Applied Logic 20 (2017) 32–48

Contents lists available at ScienceDirect

Journal of Applied Logic

www.elsevier.com/locate/jal

Price of privacy

Pavel Naumov [a,*], Jia Tao [b]

[a] *Vassar College, Poughkeepsie, New York, USA*
[b] *The College of New Jersey, Ewing, New Jersey, USA*

ARTICLE INFO

Article history:
Received 21 April 2015
Accepted 7 November 2016
Available online 24 November 2016

Keywords:
Completeness
Axiomatization
Privacy
Epistemic logic
Knowledge
Cost analysis

ABSTRACT

The article proposes a logical framework for reasoning about agents' ability to protect their privacy by hiding certain information from a privacy intruder. It is assumed that the knowledge of the intruder is derived from the observation of pieces of evidence and that there is a cost associated with the elimination of the evidence. The logical framework contains a modal operator labeled by a group of agents and a total budget available to this group. The key contribution of this work is the proposed incorporation of the cost factor into privacy protection reasoning within the standard modal logic framework. The main technical result are the soundness and completeness theorems for the introduced logical system with respect to a formally defined semantics.

1. Introduction

Privacy and costs The cost associated with maintaining privacy is a topic of public [10,5] and scholarly [11, 17,13,18] discussions. There are at least two aspects in our daily life where costs are explicitly or implicitly associated with people's privacy.

On one hand, catering to the increasing desire to protect afore-disclosed personal information, several companies[1] offer services of removing references to such information from public sites, search engines, and commercial databases for a fee. Some of them[2] offer an additional service of disseminating positive information about a person on the Internet so that the negative information is harder to find. Similarly, before mobile phones became popular, close to one third of American households paid monthly fee to have their number unlisted [1]. Nowadays, the unlisted phone service is still being offered by the phone companies and for significantly higher monthly fees than before [6].

* Corresponding author.
E-mail addresses: pnaumov@vassar.edu (P. Naumov), taoj@tcnj.edu (J. Tao).

[1] reputation.com, abinedeleteme.com.
[2] reputation.com/reputationdefender.

http://dx.doi.org/10.1016/j.jal.2016.11.035
1570-8683/

On the other hand, consumers often reveal their private information unintentionally to companies in exchange for a small discount by using mail-in rebates, coupons, or store discount cards. Such information may later be analyzed for marketing purposes. For example, the second-largest US discount retailer Target developed an approach to identify pregnant women by tracking their shopping patterns of seemingly not-baby-related items such as scent-free soap and extra-big bags of cotton balls [2]. In these cases, consumers usually have an option not to use the promotional discount, and thus to pay a bit more, but to avoid the disclosure of their private information. In practice, this option of preserving privacy for an additional cost is rarely used by consumers, possibly due to the lack of awareness.

The price that people have to pay for protecting their privacy may differ from one individual to another. For example, European "right to be forgotten" law [14] makes it essentially free for individuals to remove certain information from online search engines. At the same time, the removal of similar information in the United States might be impossible or achievable only by paying significant legal fees.

Modal language In this article we introduce a logical system for reasoning about costs of protecting privacy by hiding some knowledge from a given privacy intruder. We assume that the information is being hidden from a single fixed privacy intruder that often will be referred to as just "the intruder". In the conclusion we talk about possible extensions of our logical systems to handle multiple privacy intruders.

To specify such a logical system, one could consider modality $\mathbf{H}_a^c\varphi$ with meaning "at cost c agent a can *hide* φ from the intruder". Such a modality, however, does not satisfy the standard Necessitation rule from modal logic:

$$\frac{\varphi}{\mathbf{H}_a^c\varphi}$$

for any value of c. To observe this, assume that formula φ is a propositional tautology. For example, let φ be of the form $\psi \vee \neg\psi$. Being a propositional tautology formula $\psi \vee \neg\psi$ is universally true. At the same time, for each non-negative value c, formula $\mathbf{H}_a^c(\psi \vee \neg\psi)$ is not true because no matter what actions with total cost c are taken by agent a to hide $\psi \vee \neg\psi$ from the privacy intruder, it is still known to the intruder by the virtue of being a propositional tautology.

To solve this issue, in this article we use modality $\Box_a^c\varphi$ that stands for "at cost c agent a *cannot* hide φ from the intruder", which is the negation of the "hiding" modality: $\Box_a^c\varphi \equiv \neg\mathbf{H}_a^c\varphi$. This modality does satisfy the Necessitation axiom

$$\frac{\varphi}{\Box_a^c\varphi}$$

because if φ is universally true, then, as we have just discussed above, its knowledge cannot be hidden by the agent a from anyone at any cost.

As usual in modal logic, one can also define dual modality $\Diamond_a^c\varphi$ as $\neg\Box_a^c\neg\varphi$. Under our semantics statement $\Diamond_a^c\varphi$ is interpreted as "at cost c agent a can leave the intruder under an impression that φ could be true". Note that

$$\mathbf{H}_a^c\varphi \equiv \neg\Box_a^c\varphi \equiv \Diamond_a^c\neg\varphi. \tag{1}$$

In other words, hiding φ means creating an impression that $\neg\varphi$ could be true. The formal semantics of these modalities will be given in Definition 6.

Second order privacy Statement $\mathbf{H}_a^c\varphi$ says that agent a can hide information φ from the intruder at cost c. Some agents, especially corporate entities, treat their business costs as a tightly guarded secret. Such agents might be interested not only in hiding φ, but also in hiding how much it costs to them to hide φ. The "second