Privicons:*
An Approach to Communicating Privacy Preferences Between Users

E. Forrest[†] **Jan Schallaböck**[‡]

Stanford/Berlin, November 2010

1 Introduction

Alongside privacy challenges posed by technical problems like faulty architecture or insecure protocols are everyday privacy harms caused by basic failures of communication. For example, when a user unthinkingly forwards an e-mail chain that includes crass private remarks, or casually passes along information from an e-mail that was meant to have been kept secret, that user violates privacy by ignoring or misunderstanding norms, not code. Privicons uses a strategy of code-based norms[1] or a "neighborliness" approach[2] to address communications privacy problems like e-mail carelessness that occur within the bounds of code but nevertheless are ultimately problems of privacy norms and social signals: problems not readily solvable by code alone.

Purely code-backed strategies, like e-mail clients that refuse to allow certain messages to be forwarded or printed, tend to restrict speech indiscriminately. Such approaches can be overbroad and paternalistic toward users. Moreover, such strategies are usually limited to certain platforms, such as Microsoft Outlook or iPhone apps like TigerText. Privicons, however, uses an adaptable, open source strategy to place easily understandable privacy communications tools in users' hands, on any platform, without restricting what the user can do or say.

The code in Privicons thus serves mainly to help users clarify and understand social norms, signals, and expectations about privacy. If users can easily convey their privacy expectations, and recipients can understand and process those expectations in terms of widely understood social norms about privacy, then courtesy and care will help to prevent privacy harms caused by carelessness or misunderstanding about privacy expectations.

*This paper is the outcome of joint work from everyone involved in the Privicons project. It is inspired by and based on numerous recent approaches for simplifying privacy policies via the use of icons. As the Creative Commons project simplified copyright licenses using icons and attendant legal explanations, privacy policies might be enhanced by being expressed on several layers, including one with simple-to-understand icons and brief instructions for senders and recipients. After a presentation given by Mary Rundle at the United Nations Internet Governance Forum (IGF) in Athens in October 2006, this idea for refining privacy policies was further discussed and promoted within the IGF's Dynamic Coalition on Rights and Principles. At the same time, researchers with the European Projects PRIME and its follow-up PrimeLife have been looking into ways to simplify privacy policies. They found that the plethora of ways to process privacy makes it difficult to define what actually needs to be represented. Nevertheless, fascinated by this approach, they teamed up with United States privacy experts at Stanford to drive the experiment further. The idea of developing "Privicons" for e-mail was born. Specic thanks is owed to each member of the Privicons team: Ryan Calo (Stanford), Max Senges (Berlin), Andreas Braendhaugen (San Francisco), and Uli König (Kiel).

[†]Stanford Law School. email: ethanf@stanford.edu

[‡]University of Kassel and Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Germany. email: ULD62@datenschutzzentrum.de

[1]The Power of Code-Backed Norms by Jonathan Zittrain, http://yupnet.org/zittrain/archives/20#70.

[2]Gelman, Lauren Amy, Privacy, Free Speech, and 'Blurry-Edged' Social Networks (November 1, 2009). Boston College Law Review, Vol. 50, No. 5, 2009.

It is important to note that Privicons merely asks an e-mail's recipient to respect the sender's preference. Unlike, for example, DRM-oriented approches, our approach relies on social norms meant to be followed by the recipient, rather than technical enforcement mechanisms. However, developers who choose to create other applications to interact with Privicons – such as e-mail clients coded to recognize Privicons – might create new solutions that allow users to decide whether to opt-in to technical enforcement of users' preferences. Allowing Privicons' instructions to be overridden enables users to take control of their speech, placing communication before code. Code here functions mainly to distribute Privicons' conceptual core.

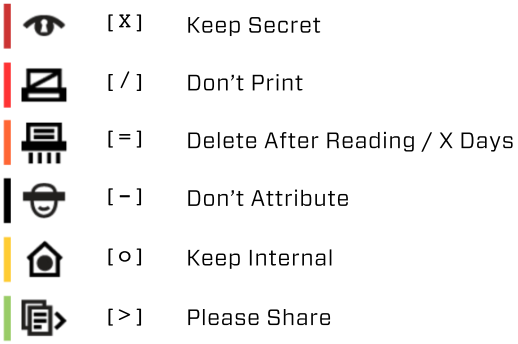

Figure: Draft Privicons including their respective ASCII-representation and a graphical symbol

2 Vocabulary

The conceptual core is a vocabulary of icons – Privicons themselves – that communicate a user's privacy expectations, like "Don't Attribute," "Keep Internal," and "Keep Private." These icons are meant to be implemented through lightweight, open source applications that affix the icons and their explanations to e-mails, per the user's preferences – like laundry instructions for your e-mail, or a Creative Commons for privacy preferences. Based on intuitive ASCII symbol combinations, like [X] for "Keep Private" and [o] for "Keep Internal," Privicons are easily visualized through either text or an image-based Privicons application. This visual flexibility gives Privicons wide adaptability across platforms and devices, ensuring easy applicability to all current and developing forms of visual electronic communication. The options currently represented in the vocabulary are as follows:

Keep Private: Sometimes we want to share information with one specific person, and also to ensure that no one else knows of it. The "Keep Private" Privicon asks the recipient to keep private all aspects of the e-mail: the sender here requests that the recipient reveal neither the fact that she has sent an e-mail, nor any information about it, including the sender's name or the e-mail's content. To strengthen this request, the sender might also attach another Privicon like "[/] - Don't Print" or a "[=] - Delete after Reading/Within X days."

Don't Print: The "Don't Print" Privicon asks the recipient not to print the received e-mail. In some situations, this might be used to request that the recipient save paper, but in a privacy setting, this Privicon means that the e-mail's sender does not want to risk his e-mail being left at a public printer or otherwise floating around the physical world.

Delete after Reading = Within X Days: The "Delete after Reading" Privicon requests that the e-mail's recipient delete the sender's e-mail either immediately or within a specified number of days. The Privicon may be represented in three different ways: 1) [=] Delete after reading; 2) [=0] Delete after reading (this is simply an alternate way of representing situation 1); 3) [=X] Delete after X days.

Don't Attribute (Keep Author Anonymous): The "Don't Attribute" Privicon asks the recipient not to attribute, name or even mention the original sender of the e-mail in any way associated with the e-mail's content or status. However, unlike a situation in which the sender has used the "Keep Private" Privicon, the recipient may quote, follow-up, or paraphrase the content, facts and opinions expressed in the original e-mail. In other words, the recipient may freely use information re-

ceived from the e-mail, but may not reveal the identity or affiliation of the speaker(s). (This is similar to the Chatham House Rule for meetings.)

Keep Internal: The "Keep Internal" Privicon asks the recipient to share the sender's e-mail – either its content or the e-mail itself, by forwarding it – only to those people who are common friends with the sender and the recipient, or who are otherwise part of a group of people with whom the sender might conceivably wish to share the e-mail's contents. Note that the judgment of whether a person is within this group belongs solely to the recipient, unless otherwise indicated by the sender. Essentially, the "Keep Internal" Privicons indicates recipients should think carefully about to whom to forward an e-mail, and that the sender does not want the message to be forwarded arbitrarily.

Please Share: The "Please Share" Privicon asks the recipient to share this e-mail with anyone of her choosing – essentially, it is an open invitation or license for the recipient to redistribute the e-mail. This Privicon may be supplemented by further instructions that clarify the e-mail's copyright status: for example, the sender might also attach a Creative Commons license to her e-mail that allows copying and redistribution with attribution.

3 Specification

To allow for protocol- or standards-based privacy strategies to support Privicons in the future, we have disseminated a first-draft experimental RFC (Internet Draft). This Internet Draft provides a detailed outline on how developers should use Privicons in the e-mail environment.[3] Based on the Internet Draft's specifications, e-mail headers might eventually incorporate Privicons preferences, creating the possibility of different levels of code-backed responses for supporting clients that interpret these headers. Other options are possible: the Internet Draft means only to standardize the basic functionality of Privicons.

Specifically, the Internet Draft proposes a syntax and semantics for an extension of the Internet Message Format[4] (e-mail message), which would allow a Sending User of an e-mail to express his or her preferences on how the message content should be handled by the Receiving Users. For this purpose, the Internet Draft describes semantic sets of different character combinations – the Privicons in ASCII form – as outlined above, and describes how they may be used in a protocol- or standards-based setting.

These semantic sets can syntactically be integrated in the first line of the e-mail's body, in the e-mail's subject line, and/or in a dedicated header of any e-mail message. The specification also provides rules for handling conflicts amongst Privicons, effectively allowing for a smooth transaction and migration for clients and users intending to make use of Privicons in a code-oriented context. The applied specification would allow a user to type a Privicon in an e-mail's body or subject line – conforming clients would then interpret this information and, for example, include the relevant Privicons and attendant privacy information in the e-mail's header, or automatically insert additional information on the specific meaning of a Privicon in the e-mail's footer. A possibility for expressing this vocabulary in HTML-based e-mails using the Privicons' graphical symbols is also envisioned in the next draft: the Internet Draft is meant to be a uniform set of guidelines for any developer who wishes to incorporate Privicons into her project, thereby ensuring that Privicons remains coherent even as the project is widely and collaboratively distributed.

4 Implementation

The first such Privicons application, currently in development, is a Google Chrome extension that incorporates Privicons seamlessly into the Gmail user interface. We hope to expand this implementation to other e-mail and browser platforms, and perhaps to social networks like

[3] http://www.ietf.org/id/draft-koenig-privicons-00.txt.

[4] RFC 5322, http://tools.ietf.org/html/rfc5322.

Facebook. As the first Privicons application reaches completion, the team hopes to proceed with tentative commitments from e-mail service providers to test Privicons more widely. We also plan to provide the code through open source channels in order to encourage adaptation and development on a horizontal model. Since norms and social signals are at the core of what Privicons means to do, keeping the community of users and developers at the center of the project ensures that the Privicons language will grow and change with evolving privacy expectations and modes of communication.

5 Related Work

- International Data Protection and Digital Identity Management Tools by Mary Rundle • Iconset Data-Privacy Icons v0.1“ by Matthias Mehldau wetter@berlin.ccc.de

- PRIME and its follow-up PrimeLife EU public private partnership research project.

- (Modularized) Human Readable Privacy Policies by Max Senges, Internet Rights and Principles Coalition

- Privacy Icons by Mozilla

- Know Privacy by UC Berkeley School of Information

- Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. 2009. A "nutrition label" for privacy. In Proceedings of the 5th Symposium on Usable Privacy and Security (Mountain View, California, July 15 - 17, 2009). SOUPS '09. ACM, New York, NY, 1-12. DOI = http://doi.acm.org/10.1145/1572532.1572538