

Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: October 13, 2015

T. Bray, Ed.
Textuality Services
April 11, 2015

Privacy Choices for Internet Data Services
draft-bray-privacy-choices-01

Abstract

This document argues in favor of Internet service providers deploying technologies which offer increased privacy to users of their services. The discussion is independent of any particular privacy technology. The approach is to consider common objections to the deployment of such technologies, and show that these objections are not well-founded.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 13, 2015.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in [Section 4.e](#) of

Internet-Draft Privacy Choices for Internet Data Services

April 2015

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Summary	2
3.	Terminology	3
4.	Background	3
4.1.	Asymmetric failure cost	3
4.2.	Privacy technology cost	3
5.	Common objections to privacy-technology deployment	4
5.1.	Free public data	4
5.2.	Privacy at user option	4
5.3.	Failures of privacy technology	4
5.4.	Affordability of privacy technology	5
	Author's Address	5

[1.](#) Introduction

Privacy issues are becoming increasingly important to users of Internet services, and the providers of those services must choose how much privacy it is appropriate to provide their users.

When discussing the deployment of privacy technology, certain objections are encountered repeatedly: That privacy protection is inappropriate for freely-public information and "brochure-ware", that it is too flawed to be worthwhile, that privacy choices are best left to end users, and that the cost of deploying privacy protection is too high.

This document considers these these arguments and shows that they are flawed; the conclusion is that in almost every case, the best choice for a service provider and its users is the one that maximizes privacy.

[2.](#) Summary

This document attempts to establish the following:

1. Whether or not information is considered "public" is not a good criterion for choosing whether or not to deploy privacy technologies for its users.

2. Privacy choices are difficult and context-dependent, so it's inappropriate to ask users to make them.

3. Privacy technologies offer benefits to users of data services even when those technologies are imperfect.
4. Cost should not be a significant factor while considering the deployment of privacy technologies.

[3. Terminology](#)

The term "data service" means any Internet-mediated offering that is accessible to the general public. Examples would include Web sites, HTTP APIs, streaming media, and various flavors of chat.

In this document, "privacy protection" means technology whose deployment increases the cost and difficulty, for anyone but the user and provider of a data service, of ascertaining who is accessing which services and what messages are being exchanged between the user and the service. Obvious examples are encryption and authentication technologies.

[4. Background](#)

This section establishes two background facts that will serve to support this document's central arguments.

[4.1. Asymmetric failure cost](#)

There are two classes of privacy-related failure in the operation of data services. A positive failure occurs when privacy was provided but was not necessary; a negative failure is when privacy was not provided, but was necessary for prudent use of the data service.

The cost of these failure classes is not symmetric; negative failures can endanger businesses, property, and lives, while positive failures usually incur at most a little extra expense.

[4.2. Privacy technology cost](#)

A wide variety of privacy technologies are available to Internet data service providers. They include public-key infrastructure, transport-level encryption, server-side encryption-at-rest, and token-based authentication/authorization technologies which reduce the use of passwords.

In every case, the monetary and engineering cost of acquiring the necessary resources and deploying the required software has been falling steadily in recent years, both absolutely and as a proportion of the total cost of service development and deployment.

[5.](#) Common objections to privacy-technology deployment

[5.1.](#) Free public data

It is reasonable to question whether, for freely-available public data, such as the contents of an online reference work or a promotional Web site, it makes sense to deploy privacy protection.

Unfortunately, it is very difficult to predict when a person accessing online information might suffer negative consequences. For example, some governments criminalize certain behaviors to the extent that accessing free public reference documents concerning that behavior could lead to arrest and prosecution.

Bearing this in mind, and given the asymmetric cost of privacy failure modes, the conclusion is that the "public" or "free" status of information is not a good argument against the deployment of privacy technology.

There is another, subtler point: If one groups available data services into those which are non-controversial and thus require no privacy protection, and those which are controversial and do, some will conclude that anything with privacy protection must be controversial and thus subject to suspicion. This effect is better avoided.

[5.2.](#) Privacy at user option

It is often argued that privacy choices are best left to the users of

data services; and thus, that opt-in privacy is an appropriate strategy.

However, the technical and social factors forming the context for such choices are complex; even experts often disagree on privacy requirements. Thus, the end-users of a data service are likely not well-equipped to make good choices.

Bearing this in mind, and given the asymmetric cost of privacy failure modes, it is usually best to remove the necessity for making these choices, by always providing the maximum practical amount of privacy protection.

[5.3.](#) Failures of privacy technology

Internet privacy technologies are known to be imperfect. Cryptography algorithms have been compromised and there is widespread dissatisfaction with the PKI infrastructure.

Furthermore, it is widely agreed that an attacker who wishes to attack a target's privacy has many means, ranging from social engineering to hardware hacking to zero-day exploits, to bypass privacy protection.

Therefore, it is reasonable to question the deployment of privacy protection, which may create an unrealistic expectation of safety when in fact that is not achievable.

However, this line of argument fails on economic grounds. Deployments of privacy technology, however imperfect, generally have the effect of increasing the cost to an attacker of invading end-users' privacy. Every time that cost goes up, certain surveillance activities, whether by government bodies or criminals, become uneconomic and will be abandoned, with the effect of globally increasing the security and privacy of Internet data services.

[5.4.](#) Affordability of privacy technology

Privacy technologies are not free; there are monetary costs for accessing PKI infrastructure, and bandwidth/computation costs related to encryption, authentication, and authorization.

Service providers may find it difficult to justify such expenses, particularly those who have severe budget constraints.

However, the monotonic decline in privacy technology costs decreases the force of this argument with every passing year. It is hard to imagine a situation where an organization can afford to acquire server resources, domain names, internet connectivity, and software deployment expertise, but still cannot afford to offer privacy protection.

There is a subtle related issue: Those who are operating on low budgets are often providing data services to disadvantaged groups, whose members may be in particular need of privacy protection.

Author's Address

Tim Bray (editor)
Textuality Services

Email: tbray@textuality.com
URI: <https://www.tbray.org/>