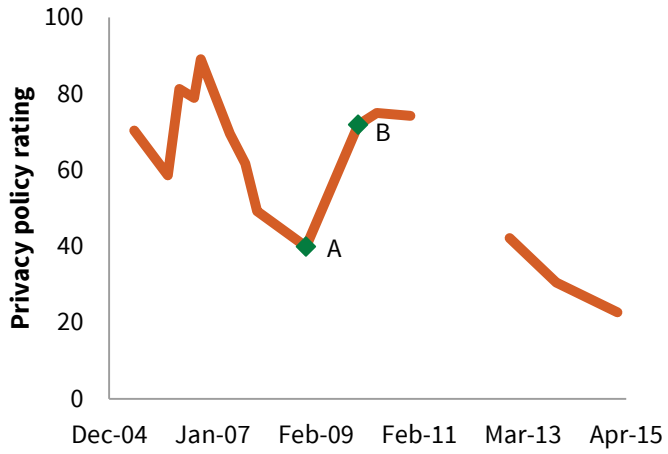
Shore J, Steinman J. Did You Really Agree to That? The Evolution of Facebook's Privacy Policy. *Technology Science*. 2015081102. August 11, 2015. http://techscience.org/a/2015081102

Did You Really Agree to That? The Evolution of Facebook's Privacy Policy

Jennifer Shore and Jill Steinman

Highlights

- We examined changes to Facebook's Privacy Policy from 2005 to 2015 using the relevant parts of the 2008 Patient Privacy Rights (PPR) framework.
- We found that Facebook's score declined by 2015 in 22 of 33 measures of privacy protection and transparency on a 5-point scale. The measures included the extent of internet monitoring, informing users about what is shared with third parties, clearly identifying data used for profiling, and giving users choices in privacy settings.



Facebook privacy policy rating over time as a percentage of the best possible score. Dots highlight dates of a policy heavily criticized by advocacy groups (A) and the next revision (B). Gap identifies missing archived policies.

Abstract

While the profusion of social media platforms creates positive opportunities for individuals to connect with others, the requisite openness of such online public spaces requires users to share more information in a context that is more open, recorded, and tracked than ever before. Users rely on stated privacy policies to understand their risks and to make decisions

about potential harms, especially when personal data are shared with third parties with whom the user has no direct knowledge. How good are privacy policies at helping users understand company practices? As personal data sharing seems to have increased over time, how have privacy policies changed? In 2008, Patient Privacy Rights (PPR) introduced a series of measures to assess a privacy policy's ability to inform users about company practices. In this paper, we assess Facebook's privacy policy over time using applicable PPR measures. Our findings suggest decreased accountability and transparency in Facebook's privacy policy over time, including the part of the policy referring to personal data that the company may share with third parties.

Results summary: We harvested old copies of Facebook's privacy policies from the Internet Archive's Wayback Machine from 2005 to 2015. We ranked each Facebook privacy policy based on its compliance with each of 33 relevant PPR Framework criteria, on a scale from 0 to 4 (with 0 indicating that the privacy policy did not meet a criterion at all, and 4 indicating that the criterion was fully met). We found a decline in 22 of the 33 standards we measured in Facebook's stated privacy policy. Here are some examples. The measure of whether Facebook's privacy policy fully describes use of Internet monitoring technologies, including but not limited to beacons, weblogs, and cookies, dropped from 4 to 0. The measure of whether the privacy policy fully describes under what circumstances data are externally disclosed started at 3, rose to 4 and then dropped to 0. The measure of whether the privacy policy describes a system that allows users to clearly identify data used for profiling and targeting started at 4 and dropped to 0. The measure of whether the privacy policy fully describes what ability the [user] has to change, segment, delete, or amend their information started at 4, bounced to 2 and back, and then dropped to 0. Drops in these measures suggest that privacy policies became less informative over time, even as word count soared.

Introduction

Founded in 2004, Facebook today is the most widely used social media platform in the United States [1], with 936 million daily active users (as of March 2015) who share information such as photos, locations, and networks of friends [2]. In 2008, Mark Zuckerberg, founder and CEO of Facebook, asserted that "privacy is the vector around which Facebook operates." [3] In 2010, he said that "people have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people...That social norm is just something that has evolved over time." [3] Did Facebook's privacy policy change to reflect this shift?

In addressing this question, we distinguished between two kinds of privacy that can exist on a social media platform. The first kind deals with user-to-user privacy, which reflects what an individual can explicitly choose to share with others on the platform. Facebook provides mechanisms that allow users to directly control, to some degree, what kinds of data are shared with Facebook friends, followers, users generally, and others. For example, Facebook users can delete previous comments and messages [4] and can set their profiles to have a

desired amount of public visibility based on the nature of the content they share [5]. Of course, these options, too, have changed over time [6]. The second kind of privacy deals with how an organization collects, handles, and further shares personal data from and about its users. For example, with whom does Facebook share or sell it? How could a user know? For answers, we turned to Facebook's privacy policy (or "data policy," as they often term it).

Background

The purpose of a privacy policy is to inform visitors of a website's data practices. In the United States, the Federal Trade Commission is the federal agency that chiefly enforces promises made in privacy policies [7]. Posting a statement of the policy on the website is a practice that was agreed upon by members of the World Wide Web Consortium to address growing privacy concerns [8]. Years later, posting a privacy policy on a website is not required by law but is considered a best practice. Stated privacy policies continue to dictate and describe what happens to personal information shared on a website [9].

Researchers previously reported on poor privacy practices gleaned from privacy notices [10], and some even recommended remedies, such as privacy-aware search engines that would rate privacy policies and sort search results based on those having better reported privacy practice [11].

Researchers also have reported on difficulties associated with reading and comprehending privacy policies [12]. A recent article recommended replacing privacy notices with a label to identify critical information similar to the way that nutrition facts appear on food labels [13].

In 2008, Microsoft, the Coalition for Patient Privacy, Patient Privacy Rights, and a consulting firm created the Patient Privacy Rights' Trust Framework ("the PPR Framework"), a set of 73 criteria to assess the quality of privacy policies and business practices [14]. The PPR Framework provides a method of evaluating business practices evidenced in the privacy policy as well as the policy's comprehensibility and clarity.

The criteria of the PPR Framework provide a comprehensive assessment not merely of a privacy policy but also of practices and operations within the business that must be expressed in the privacy policy. An example is a requirement that employees receive annual training on privacy and security. The company may actually satisfy the requirement, but if this is not expressed in the company's privacy policy, it does not meet the criterion.

Privacy policies have not adopted the guidelines established by the PPR Framework, presumably because privacy policies are optional, and there is no incentive for a company, even one that handles personal health information, to adopt a comprehensive and rigorous privacy policy when lesser options suffice. Therefore, it is likely that no existing privacy policy satisfies all the comprehensive criteria of the PPR Framework. However, for these same reasons, the PPR Framework can be considered a gold standard against which to measure privacy policies.

Although the PPR Framework was originally aimed at assessing privacy policies related to health data, we adapted it to be applicable generally to social media platforms' privacy policies based on iterations of the privacy policy overtime. See Table 1 through Table 15 for the PPR Framework criteria that we have used and excluded. We eliminated criteria that specifically involved medical practices and handling of medical data in ways not generally applicable to social media website practices and the handling of personal data generally. We changed "patient" to "user" within the criteria that we did retain.

Principle 1. User can easily find, review, and understand the privacy policy.

No.	Criteria
1.1	Privacy policy includes a short summary accurately describing the user's control of their data and all access to that data.
1.2	The policy must be easily accessible from the organization's home page. (Excluded because we were unable to test for this from historic policies alone.)
1.3	Privacy policy must not use passive structures ("we share" vs. "the sharing"), qualifying verbs and adverbs ("use" and "will" vs. "may," "occasionally," and "from time to time").
1.4	Privacy policy must have topic headings that link to plain language explanations of the type of data accessed and how the data are handled.
1.5	Privacy policy shall attain a Flesch Reading Ease score of 45 or higher. (Excluded because of its similarity and likely correlation to 1.6, which we included.)
1.6	Privacy policy shall attain a Flesch-Kincaid Grade level score (reading level) of 12 or lower.
1.7	Privacy policy shall use a minimum 9 pt. font.
1.8	Privacy policy is available in the native language of organization's significant customer populations.
1.9	Privacy policy provides easy access to definitions of technical terms.
1.10	Privacy policy includes explicit language on process and notification of "material changes" and allows customers a defined timeline to opt out before policy changes.

Table 1. The PPR Framework specifies 10 criteria for Principle 1, numbered as principles 1.1 through 1.10. We measured 8 and excluded 2 for the reasons noted.

Principle 2. Privacy policy fully discloses how personal information will and will not be used by the organization. Users' information is never shared or sold without the user's explicit permission.

No.	Criteria
2.1	Privacy policy states that personal information is collected only with informed consent, unless otherwise required by law.
2.2	Privacy policy must clearly state what the organization will and will not do with personal information.
2.3	Privacy policy fully describes use of internet monitoring technologies, including but not limited to beacons, weblogs, and cookies.
2.4	Privacy policy fully describes all data sharing circumstances that require a user to opt in.
2.5	Privacy policy fully describes what ability the user has to change, segment, delete, or amend their information.
2.6	Privacy policy fully describes who can access the information and when.
2.7	Privacy policy fully describes under what circumstances data is externally disclosed. (Excluded because of similarity and likely correlation to 2.6 and 2.8, which we included.)
2.8	Privacy policy fully describes with whom data are shared.
2.9	Privacy policy fully describes how information is not disclosed. (Excluded because it is specific to handling health data.)
2.10	Privacy policy describes how all access to data is recorded and how resultant audit trails are accessible to the patient. (Excluded because audit trails are specific to health data.)
2.11	Privacy policy describes procedures the organization will follow in the event of a security breach. (Excluded because breach laws and regulations may dictate procedures, in part.)
2.12	Privacy policy describes the organization's process for receiving and resolving complaints.
2.13	Privacy policy describes a mechanism for Third Party resolution of complaints.
2.14	Privacy policy confirms that all persons with access to the data must comply with privacy policies.

Table 2. The PPR Framework specifies 14 criteria for Principle 2, numbered as principles 2.1 through 2.14. We measured 10 of these and excluded 4 for the reasons noted.

Principle 3. Users decide if they want to participate.

No.	Criteria
3.1	System provides clear notification of informed consent during registration. All patients must opt-in. (Excluded because this is specific to health data.)
3.2	System allows user to opt out at any time, and the opt-out process must be simple and clearly states in the privacy policy.
3.3	System provides capability for all access to the user's data to be removed at any time. User has the ability to permanently delete all information upon closing an account.

Table 3. The PPR Framework specifies 3 criteria for Principle 3, numbered as principles 3.1 through 3.3. We measured 2 and excluded 1 for the reasons noted.

Principle 4. Patients are clearly warned before any outside organization(s) that does not fully comply with the organization's privacy policy can access their information.

No.	Criteria
4.1	Organization must contractually require all persons with access to data to clearly disclose whether they comply with its privacy policies. Audit trails are sufficient to verify data access compliance.
4.2	For internet applications, the organization must ensure patient can easily access any other website's privacy policy before linking to another site.
4.3	The organization shall prominently display the PPC™ seal of any organization that has obtained PPC™ certification prior to obtaining informed consent for information sharing.
4.4	Organization ensures visual indication distinguishing between outside organizations governed by HIPAA and outside organizations that are not governed by HIPAA with additional links to educational information explaining the difference.

Table 4. The PPR Framework specifies 4 criteria for Principle 4, all of which we excluded because the principle is specific to health data.

Principle 5. User can easily find, review, and understand the privacy policy.

No.	Criteria
5.1	Any profiling must be optional (opt in) with the ability to opt out.
5.2	The system must allow users to clearly identify data used for profiling and targeting.
5.3	Users must be able to opt out of any profiling at any time. The opt-out process must be simple and clearly stated in the privacy policy.
5.4	The user may choose which specific data elements may be used for profiling and targeting.
5.5	Opting out of profiling and targeting has no secondary effects on the patient. This is clearly stated in the privacy policy. (Excluded because this is specific to the medical community.)
5.6	The system never shares profiling data without patients' prior informed consent. (Excluded because this is specific to the medical community.)

Table 5. The PPR Framework specifies 6 criteria for Principle 5, numbered as principles 5.1 through 5.6. We measured 4 and excluded 2 for the reasons noted.

Principle 6. Users decide how and if their sensitive information is shared.

No.	Criteria
6.1	System allows user to selectively release each element of their personal information.

Table 6. The PPR Framework specifies 1 criterion for Principle 6, numbered as principle 6.1, which we measured.

Principle 7. Users are able to change any information that they input themselves.

No.	Criteria
7.1	System allows user to delete, change, or annotate each element of their personal information.
7.2	The user may permanently delete their personal information from the system upon user request.

Table 7. The PPR Framework specifies 2 criteria for Principle 7, numbered as principles 7.1 and 7.2, which we measured.

Principle 8. Users decide who can access their information.

No.	Criteria
8.1	Access to personal health information and system functions is limited by role based and individual access. (Excluded because "role-based access systems" are specific to health data.)
8.2	System provides the functionality to control access to the data.
8.3	System provides functionality for access to specific system functions (e.g., viewing audit records). (Excluded because the described functions are specific to health data.)
8.4	The ability to control the type of access that is provided to the system (e.g. read, write, delete) is controlled by the user.
8.5	The system specifies how long access to data is available (e.g., indefinitely or one week).
8.6	Organization must document processes in place for emergency access to data and demonstrate that the procedures are operating effectively either through testing or analysis of actual events. (Excluded because emergency access is specific to health data.)
8.7	All aggregation processes must be documented and assure that the organization uses state of the art methods to prevent the disclosure of identifiable information. (Excluded because data are often expected to be identifiable on these social media websites.)

Table 8. The PPR Framework specifies 7 criteria for Principle 8, numbered as principles 8.1 through 8.7. We measured 3 and excluded 4 for the reasons noted.

Principle 9. Patients with disabilities are able to manage their information while maintaining privacy.

No.	Criteria
9.1	Corporate commitment to Section 508 of the Rehabilitation Act in 1998 and specific Voluntary Product Accessibility Template (VPAT) for product.
9.2	Full compliance to 508 and VPAT

Table 9. The PPR Framework specifies two criteria for Principle 9, both of which we excluded because measuring disability access was beyond the scope of this project.

Principle 10. Patients can easily find out who has accessed or used their information.

No.	Criteria
10.1	Organization maintains audit trails of every event. Retention cycles for maintaining audit trails are based on the minimum HIPAA-entity requirements (e.g., six years)
10.2	Audit trail includes who performed the action.
10.3	Audit trail includes what action was performed.
10.4	Audit trail includes what data object was involved.
10.5	Audit trail includes when the action occurred.
10.6	The system does not allow the audit trail function to be ""turned off." The audit record cannot be altered, and records do not expire.
10.7	Audit trails must be readily available to the patient.
10.8	Audit logs can be searched or filtered by who performed the action.
10.9	Audit logs can be searched or filtered by what action was performed.
10.10	Audit logs can be searched or filtered by what data object was involved.
10.11	Audit logs can be searched or filtered by when the action occurred.

Table 10. The PPR Framework specifies 11 criteria for Principle 10, all of which were excluded because audit trails are specific to health data.

Principle 11. Users are notified promptly if their information is lost, stolen, or improperly accessed.

No.	Criteria
11.1	Following discovery of a breach of personal information, organizations must notify each individual whose information has been accessed because of such breach.

Table 11. The PPR Framework specifies 1 criterion for Principle 11, numbered as principle 11.1, which we measured.

Principle 12. Users can easily report concerns and get answers.

No.	Criteria
12.1	The organization must have a process [reported on the privacy policy] that enables users, advocates, employees and government regulators to report potential or actual privacy violations.
12.2	The organization must acknowledge a patient's concerns, investigate, and inform the patient of the outcome of the investigation and any take corrective action within fifteen business days. (Excluded because the measure is specific to health data.)
12.3	The organization provides a link to the PPC™ website allowing the patient to file a complaint with PPC™ if the matter is not resolved by the organization to the patient's satisfaction. (Excluded because a requirement to reference the framework itself is beyond the scope of this study.)
12.4	The organizational will provide a quarterly report to PPC™ that describes the privacy complaint, resolution and actions to ensure the problem does not recur. (Excluded because a requirement to reference the framework itself is beyond the scope of this study.)

Table 12. The PPR Framework specifies 4 criteria for Principle 12, numbered as principles 12.1 through 12.4. We measured 1 and excluded the other 3 for the reasons noted.

Principle 13. Patients can expect the organization to punish any employee or contractor that misuses patient information.

No.	Criteria
13.1	The misuse or improper access of confidential personal health information must include penalties up to and including termination of employment and referral to public prosecutors.
13.2	All key personnel with system access must have at least one day of privacy training on an annual basis.
13.3	All personnel with system access must sign appropriate annual agreements to illustrate their understanding of the organization's privacy policies.

Table 13. The PPR Framework specifies 3 criteria for Principle 13, which we excluded because the requirements seem specific to health data.

Principle 14. Patients can expect their data to be secure.

No.	Criteria
14.1	The system has undergone a security assessment by an independent third party, and there is a viable plan in place to mitigate any identified issues.
14.2	The organization has designated a person with responsibility for and authority over privacy matters.
14.3	Organization only stores patients' information in the United States, its territories, or in countries that meet the requirements of the EU Data Protection Directive.
14.4	Organizations have processes and tools in place to identify and track where patients' information is allowed to be stored by the organization or its business partners acting on its behalf.

Table 14. The PPR Framework specifies 4 criteria for Principle 14, which we excluded because the requirements seem specific to health data.

Principle 15. Users can expect to receive a copy of all disclosures of their information.

No.	Criteria
15.1	Users can expect to receive a copy of all disclosures of their information.

Table 15. The PPR Framework specifies 1 criterion for Principle 15, numbered as principle 15.1, which we measured.

Despite the thoroughness of the PPR Framework, it does not capture all aspects of data handling and sharing that could inflict privacy harm on an individual. For example, most measures are binary and do not capture degrees of data sharing or the number or nature of third parties.

Methods

We assessed the evolution of Facebook's privacy policy by locating old copies of the privacy policy and applying adapted measures from the PPR Framework to those policies. In order to employ the PPR Trust Framework to assess the evolution of Facebook's privacy policy, we adapted it by eliminating the 40 criteria that were specifically related to medical and health-specific issues and not pertinent in this context (see Tables 1 through Table 15). We chose the remaining 33 standards because we believe they provide an impartial and applicable set of metrics around which to measure Facebook's evolving privacy policy. These measures also allowed us to identify areas in which the policy was improving, deteriorating, or remaining consistent over time.

Facebook Privacy Policies

In order to determine the ways in which Facebook's privacy policy has changed, we explored the changes in Facebook's privacy policy between June 28, 2005 and May 8, 2015. The Internet Archive's Wayback Machine lists 17 versions of Facebook's privacy policy [15]. These are dated June 28, 2005; February 27, 2006; May 22, 2006; September 5, 2006; October 23,

2006; May 24, 2007; September 12, 2007; December 6, 2007; November 26, 2008; December 9, 2009; April 22, 2010; December 22, 2010; September 23, 2011; June 8, 2012; December 11, 2012; November 15, 2013; and January 30, 2015. We retrieved these copies, with the exception of the versions of the privacy policy from September 23, 2011 and June 8, 2012, which we were unable to access on the Wayback Machine's website. We also copied the May 8, 2015 version of the policy directly from Facebook's website. We then used measures identified in Tables 1 through 15 from the PPR Framework to assess the changes in Facebook's privacy policy.

Criteria Ratings

We ranked each privacy policy based on the extent to which it complied with each of our 33 identified criteria in the PPR Framework. We introduced a scale from 0 to 4 (with 0 indicating that the privacy policy did not meet a criterion at all, and 4 indicating that the criterion was fully met). Ranking the privacy policy's compliance with some criteria involved identification of a specific characteristic, sentence, or even word (e.g. "privacy policy shall use a minimum 9 pt. font," Principle 1.7), whereas other criteria required a comprehensive assessment of the privacy policy (e.g., "the system must allow users to clearly identify data used for profiling and targeting," Principle 5.2). Tables 16 through 23 describe our 0 to 4 scales for the 33 criteria we measured.

We then looked at patterns of change in individual criteria over time and changes that occurred across criteria at a given point of time. We hoped to determine both the ways in which the privacy policy has gotten better or worse at protecting user's data and to see if there were particular moments of sudden change.

Principle 1.1 Privacy policy includes a short summary accurately describing the user's control of their data and all access to that data.
0 Privacy policy lacks summary altogether
1 Privacy policy provides a short summary that contains little information about the privacy policy
2 Privacy policy provides a short summary that accurately describes around half of the information contained in the policy
3 Privacy policy provides short statement that accurately describes most, but not all, of users' control of their data
4 Privacy policy has a summary that contains all pertinent information
Principle 1.3 Privacy policy must not use passive structures ("we share" vs. "the sharing"), qualifying verbs and adverbs ("use" and "will" vs. "may," "occasionally," and "from time to time").
0 Privacy policy only uses passive structures
1 Privacy policy uses mostly passive structures
2 Privacy policy uses some passive structures
3 Privacy policy uses mostly active structures
4 Privacy policy only uses active structures
Principle 1.4 Privacy policy must have topic headings that link to plain language explanations of the type of data accessed and how the data are handled.
0 Privacy policy lacks topic headings and access to plain language explanations
1 Privacy policy lacks either topic headings or plain language explanations

2 Privacy policy contains a few topic headings and plain language explanations, but does not clearly demarcate all sections
3 Privacy policy clearly marks most sections and provides plain language explanations
4 Privacy policy provides topic headings and plain language explanations
Principle 1.6 Privacy policy shall attain a Flesch-Kincaid Grade level score (reading level) of 12 or lower.
0 Privacy policy has a grade reading level that far exceeds a 12th grade reading level
1 Privacy policy very complicated to understand, though not impossible
2 Privacy policy uses language that is clear to a person who reads the document closely, though not clearly understandable at a glance
3 Privacy policy contains language that is generally understandable to a person who reads at the 12th grade reading level
4 Privacy policy understandable to people who read at the 12th grade reading level or lower
Principle 1.7 Privacy policy shall use a minimum 9 pt. font.
0 Privacy policy contains less than 9 pt. font
1 Privacy policy font around 9 pts. and very small to read
2 Privacy policy font around 10 pts. and challenging to read
3 Privacy policy font around 11 pts. and generally an easy size to read
4 Privacy policy font 12 pts. or larger
Principle 1.8 Privacy policy is available in the native language of organization's significant customer populations.
0 Privacy policy in a language that most users do not speak
1 Privacy policy available in a language that few users speak
2 Privacy policy in a language that half of its users use
3 Privacy policy available in a language that most of its users use
4 Privacy policy available in native language of users
Principle 1.9 Privacy policy provides easy access to definitions of technical terms.
0 Privacy policy does not provide any access to technical terms
1 Privacy policy uses technical terms but does not provide access to a majority of them
2 Privacy policy provides access to around half of the technical terms used
3 Privacy policy provides access to a majority of technical terms used
4 Privacy policy provides access to all technical terms used
Principle 1.10 Privacy policy includes explicit language on process and notification of "material changes" and allows customers a defined timeline to opt out before policy changes.
0 Privacy policy excludes all language regarding to changes to the privacy policy
1 Privacy policy includes language about "material changes" but fails to offer timeline to notify users and provide them an opportunity to opt out
2 Privacy policy includes explicit language about "material changes" and notifies users of the changes, but fails to provide an opportunity to opt out
3 Privacy policy contains explicit language about "material changes" and properly notifies user, but does not offer an explicit timeline to opt out
4 Privacy policy includes explicit language on how to opt out after being notified of "material changes"

Table 16. Measurement scales for the 8 criteria of principle 1 that we assessed. Principle 1 is "User can easily find, review, and understand the privacy policy."

Principle 2.1 Privacy policy states that personal information is collected only with informed consent, unless otherwise required by law.
0 Privacy policy does not state what information is collected and how it is done

1	Privacy policy states that personal information is collected, but fails to mention what information is collected
2	Privacy policy states that personal information is collected, but only mentions the types of data in general terms
3	Privacy policy states that personal information is collected, though it only specifies that some information is collected through informed consent
4	Privacy policy states that personal information is collected only with informed consent
Principle 2.2 Privacy policy must clearly state what the organization will and will not do with personal information.	
0	Privacy policy does not state what the organization will and will not do with personal information
1	Privacy policy only most generally tells user what it will do with personal information and uses vague language
2	Privacy policy explicitly tells users what it will and will not do with certain segments of personal information
3	Privacy policy states what the organization will and will not do with the personal data it collects for the majority of the data it collects about the user
4	Privacy policy clearly states what the organization will and will not do with personal information
Principle 2.3 Privacy policy fully describes use of internet monitoring technologies, including but not limited to beacons, weblogs, and cookies.	
0	Privacy policy does not name or describe any of the technologies
1	Privacy policy mentions that technologies are used but does not specify which ones are used
2	Privacy policy names specific technologies used but fails to describe them
3	Privacy policy names specific technologies and then describes most of them
4	Privacy policy fully describes use of internet monitoring technologies
Principle 2.4 Privacy policy fully describes all data sharing circumstances that require a user to opt in.	
0	Privacy policy does not describe any data sharing circumstances that require a user to opt in
1	Privacy policy mentions data sharing circumstances but does not mention opt-in requirement
2	Privacy policy describes a few data sharing circumstances that require opt-in but does not allow opt-in for all data sharing
3	Privacy policy describes most of the data sharing circumstances that require a user to opt in
4	Privacy policy fully describes all data sharing circumstances that require a user to opt in
Principle 2.5 Privacy policy fully describes what ability the user has to change, segment, delete, or amend their information.	
0	Privacy policy does not describe what ability the user has to change, segment, delete or amend their information
1	Privacy policy describes a few instances where the user has the ability to edit their information
2	Privacy policy describes the ability for the user to edit around half of the personal data the organization collects
3	Privacy policy describes the ability for the user to edit most of the personal data the organization collects

4	Privacy policy fully describes what ability the user has to edit their information
Principle 2.6 Privacy policy fully describes who can access the information and when.	
0	Privacy policy does not describe who can access the information and when
1	Privacy policy describes data access for less than half of the data collected
2	Privacy policy describes data access for about half of the data collected
3	Privacy policy describes data access for the majority of the data collected
4	Privacy policy fully describes who can access the information and when
Principle 2.8 Privacy policy fully describes with whom data are shared	
0	Privacy policy does not mention with whom data are shared
1	Privacy policy mentions a few instances where data is shared and with whom
2	Privacy policy describes most generally with whom data are shared
3	Privacy policy specifies more explicitly with whom data are shared
4	Privacy policy fully describes with whom data are shared
Principle 2.12 Privacy policy describes the organization's process for receiving and resolving complaints.	
0	Privacy policy does not describe the process for receiving and resolving complaints
1	Privacy policy alludes to a process to receive and resolving complaints but does not describe the process
2	Privacy policy mentions process, but does not provide specific ways to resolve complaints
3	Privacy policy describes the organization's process for receiving complaints, but not necessarily for resolving them
4	Privacy policy describes process for receiving and resolving complaints
Principle 2.13 Privacy policy describes a mechanism for Third Party resolution of complaints.	
0	Privacy policy describes no mechanism for Third Party resolution of complaints
1	Privacy policy mentions mechanism for Third Party resolution, but does not explain process
2	Privacy policy describes mechanism for Third Party resolution and explains a portion of the mechanism
3	Privacy policy is more explicit in describing a mechanism for Third Party resolution of complaints
4	Privacy policy fully describes a mechanism for Third Party resolution of complaints
Principle 2.14 Privacy policy confirms that all persons with access to the data must comply with privacy policies.	
0	Privacy policy makes no mention that all persons with access to data must comply with privacy policies
1	Privacy policy states that a small group of select people must comply with privacy policy
2	Privacy policy states that around half of the people with access to the data must comply with privacy policies
3	Privacy policy states that most people with access to data must comply with privacy policies
4	Privacy policy states that all people will access to the data must comply with privacy policies

Table 17. Measurement scales for the 10 criteria of principle 2 that we assessed. Principle 2 is "Privacy policy fully discloses how personal information will and will not be used by the organization. Users' information is never shared or sold without the user's explicit permission."

Principle 3.2 System allows user to opt out at any time, and the opt-out process must be simple and clearly states in the privacy policy.
0 System does not allow users to opt out at any time and does not state process in policy
1 System may allow user to opt out at specific times but does not state the opt out process
2 System allows user to opt out at most times from data collection but does not state the process
3 System allows user to opt at most times and clearly states the process
4 System allows user to opt out at any time and clearly states the process in the privacy policy
Principle 3.3 System provides capability for all access to the user's data to be removed at any time. User has the ability to permanently delete all information upon closing an account.
0 System does not allow user to permanently delete data at any time
1 System allows for specific portions of data to be deleted, but all data will not be deleted upon closing an account
2 System allows for access to user data to be removed at specific times. User's information may be deleted upon closing an account
3 Access to user data can be removed at any time, though data not permanently deleted upon closing an account
4 System provides capability for all access to the user's data to be removed at any time. User has the ability to permanently delete all information upon closing an account

Table 18. Measurement scales for the 2 criteria of principle 3 that we assessed. Principle 3 is "users decide if they want to participate."

Principle 5.1 Any profiling must be optional (opt in) with the ability to opt out.
0 All profiling occurs, no option to opt in or out
1 Some profiling is involuntary, while other profiling is opt-out only
2 Some profiling is involuntary, while other profiling is opt-out only, and other profiling is opt-in
3 All profiling is either opt-in or involuntary with the ability to opt out
4 All profiling must be optional (opt-in) with the ability to opt out
Principle 5.2 The system must allow users to clearly identify data used for profiling and targeting.
0 The system does not allow user to chose what data is used for profiling and targeting
1 The system allows user to chose a few data used for profiling and targeting
2 The system allows user to identify some data used for profiling and targeting
3 The system allows user to identify most of the data used for profiling and targeting
4 The system allows user to identify all data used for profiling and targeting
Principle 5.3 Users must be able to opt out of any profiling at any time. The opt-out process must be simple and clearly stated in the privacy policy.
0 User not able to opt out of profiling at any time
1 User able to opt out of certain data collection under specific circumstances
2 User able to opt out of around half of any profiling
3 User able to opt out of most profiling
4 User able to opt out of any profiling at any time

Principle 5.4 The user may choose which specific data elements may be used for profiling and targeting.
0 User does not control data elements used for profiling
1 User has ability to control a certain elements used for profiling
2 User has ability to control around half of the elements used for profiling
3 User has the ability to control most of the elements used for profiling
4 User has the ability to control all elements used for profiling

Table 19. Measurement scales for the 4 criteria of principle 5 that we assessed. Principle 5 is "User can easily find, review, and understand the privacy policy."

Principle 6.1 System allows user to selectively release each element of their personal information.
0 System does not allow user to selectively release each element of their personal information
1 System allows user to selectively release a few elements of their personal information
2 System allows user to selectively release around half of their personal information
3 System allows user to selectively release most of their personal information
4 System allows user to selectively release each element of their personal information

Table 20. Measurement scales for principle 6, "Users decide how and if their sensitive information is shared."

Principle 7.1 Systems allows user to delete, change, or annotate each element of their personal information.
0 System does not allow user to edit each element of their personal information
1 System allows user to edit a few elements of their personal information
2 System allows user to edit around half of the elements of their personal information
3 System allows user to edit most of the elements of their personal information
4 System allows user to edit each element of their personal information
Principle 7.2 The user may permanently delete their personal information from the system upon user request.
0 User cannot delete their information from system upon request
1 User can permanently delete some personal information from the system upon request
2 User can permanently delete around half of their information from the system upon request
3 User can permanently delete most of their personal information from the system
4 User can permanently delete their personal information from the system upon request

Table 21. Measurement scales for the 2 criteria of principle 7 that we assessed. Principle 7 is "Users are able to change any information that they input themselves."

Principle 8.2 System provides the functionality to control access to the data.
0 System does not provide the functionality to control access to the data
1 System provides functionality to control access to a few parts of the data
2 System provides functionality to control access to some of the data
3 System provides functionality to control access to most of the data
4 System provides functionality to control access to all of the data

Principle 8.4 The ability to control the type of access that is provided to the system (e.g., read, write, delete) is controlled by the user.
0 The user does not control the type of access that is provided to the system
1 The user controls a few types of access that is provided to the system
2 The user controls some of the types of access that is provided to the system
3 The user controls most of the types of access that is provided to the system
4 The user controls all types of access that is provided to the system
Principle 8.5 The system specifies how long access to data is available (e.g., indefinitely or one week).
0 The system does not specify how long access to the data is available
1 The system provides a very general timeframe for how long the data is available
2 The system provides a general, but not concrete, timeframe for how long the data are available
3 The system provides a series of timeframes that specify how long access to the data is available
4 The system specifies how long access to data is available

Table 22. Measurement scales for the 3 criteria of principle 8 that we assessed. Principle 8 is "Users decide who can access their information."

Principle 11.1 Following discovery of a breach of personal information, organizations must notify each individual whose information has been accessed because of such breach.
0 Organizations do not notify each individual following a discovery of a breach
1 Organizations notify individuals in a few circumstances, following the discovery of a breach
2 Organizations notify individuals in some circumstances, following the discovery of a breach
3 Organizations notify individuals in most circumstances, following the discovery of a breach
4 Organizations notify individuals after the discovery of a breach
Principle 12.1 The organization must have a process [reported in the privacy policy] that enables users, advocates, employees, and government regulators to report potential or actual privacy violations.
0 The organization does not provide a way to report potential or actual privacy violations
1 The organization provides a nominal process that provides a way to report privacy violations
2 The organization has a process to report some privacy violations
3 The organization has a process to report most privacy violations
4 The organization has a process that enables people to report potential or actual privacy violations
Principle 15.1 Users can expect to receive a copy of all disclosures of their information.
0 Users cannot expect to receive a copy of any disclosures of their information
1 Users may be able to receive a copy of a few disclosures of their information
2 Users may be able to receive a copy of around half of the disclosures of their information
3 Users may be able to receive a copy of the majority of the disclosures of their information
4 Users may receive a copy of all disclosures of their information

Table 23. Measurement scales for criterions we measured for principle 11, principle 12, and principle 15. Principle 11 is "Users are notified promptly if their information is lost, stolen, or improperly accessed." Principle 12 is "Users can easily report concerns and get answers." Principle 15 is "Users can expect to receive a copy of all disclosures of their information."

Results

Figures 1 through 33 report our findings when we applied our measurement scales (Tables 16 through 23) to historical copies of Facebook privacy policies. (For an explanation of the A and B dots, see Discussion.) Below is a summary by principle.

Principle 1: "User can easily find, review, and understand the privacy policy." Examining the 8 measurements for Principle 1 from the oldest policy statement to the most recent policy statement, we found that one measurement improved (went up); it was Principle 1.3 (Figure 2). Facebook's privacy policies eventually removed passive voice. Two measurements remained the same. Facebook's privacy policies had top-level headings (Principle 1.3, Figure 3) and were available in multiple languages (Principle 1.8, Figure 6) throughout the study period. However, 5 of the 8 measures, or 63 percent of the measures for Principle 1, worsened (went down).

Principle 2: "Privacy policy fully discloses how personal information will and will not be used by the organization. Users' information is never shared or sold without the user's explicit permission." Examining the 10 measurements for Principle 2 from the oldest policy statement to the most recent policy statement, we found that 2 of the measurements improved slightly from beginning to end of the study period. These concerned information about employee access to information (Principle 2.14, Figure 18) and resolution and handling of complaints (Principle 2.13, Figure 17). One measurement remained the same, starting and ending at the lowest possible level. This was the measurement for Principle 2.4 (Figure 12) that describes the completeness of the description of circumstances for data sharing. Overall, however, 7 of the 10 measures (or 70 percent) worsened.

Principle 3: "Users decide if they want to participate." Examining the 2 measurements for Principle 3 from the oldest policy statement to the most recent policy statement, we found both measurements oscillated between the lowest (worst) and highest (best) values, ending lower at the end of the study than at the beginning.

Principle 5: "User can easily find, review, and understand the privacy policy." Examining the 4 measurements for Principle 5 from the oldest policy statement to the most recent policy statement, we found that all 4 measures started the study period at the highest (best) possible rating, oscillated within the study period, and ended at the lowest (worst) possible rating.

Principle 6: "Users decide how and if their sensitive information is shared." Examining our sole measure for Principle 6 (Figure 25), we found it started the study period at the highest (best) possible rating, oscillated within the study period, and ended at the lowest (worst) possible rating at the end of the study period: System does not allow users to selectively release each element of their personal information for sharing.

Principle 7: "Users are able to change any information that they input themselves." Examining the 2 measurements for Principle 7 from the oldest policy statement to the most recent policy statement, we found that both measurements ended at the lowest (worst)

possible rating, even though one (Principle 7.1, Figure 26) started at the highest (best) possible rating.

Principle 8: "Users decide who can access their information." Examining the 3 measurements for Principle 8 from the oldest policy statement to the most recent policy statement, we found that all 3 measurements ended at the lowest (worst) possible rating even though one measurement (Principle 8.2, Figure 28) started at the highest (best) possible rating. Another of the measurements (Principle 8.5, Figure 30) started and ended at the lowest possible rating, but during the study period, achieved the highest (best) possible rating.

Principle 11: "Users are notified promptly if their information is lost, stolen, or improperly accessed." Examining our sole measure for Principle 11 (Figure 31), we found the measure unchanged at the lowest (worst) possible rating throughout the study period.

Principle 12: "Users can easily report concerns and get answers". Examining our sole measure for Principle 12 (Figure 32), we found it started and ended the study period at the lowest (worst) possible rating, even though it jumped to the highest (best) possible rating during the study period.

Principle 15: "Users can expect to receive a copy of all disclosures of their information." Examining our sole measure for Principle 15 (Figure 33), we found the measure unchanged at the lowest (worst) possible rating throughout the study period.

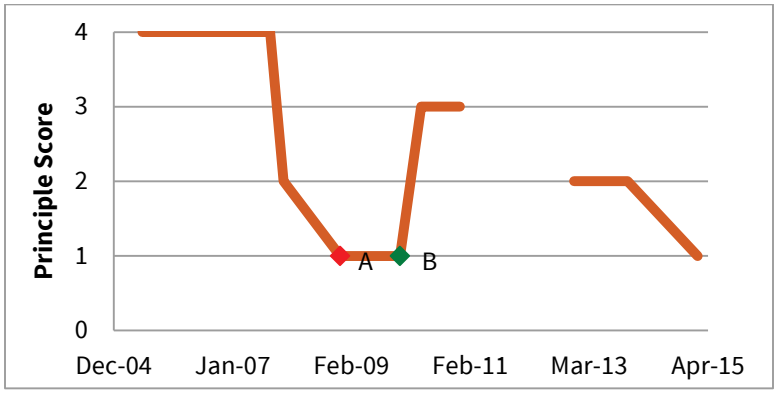


Figure 1. Principle 1.1: Privacy policy includes a short summary accurately describing users' control of their data and all access to that data. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

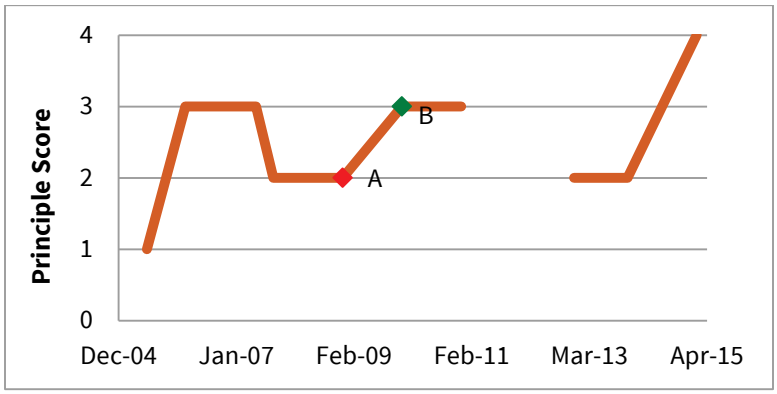


Figure 2. Principle 1.3: Privacy policy must not use passive structures ("we share" vs. "the sharing"), qualifying verbs and adverbs ("use" and "will" vs. "may," "occasionally," and "from time to time"). Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

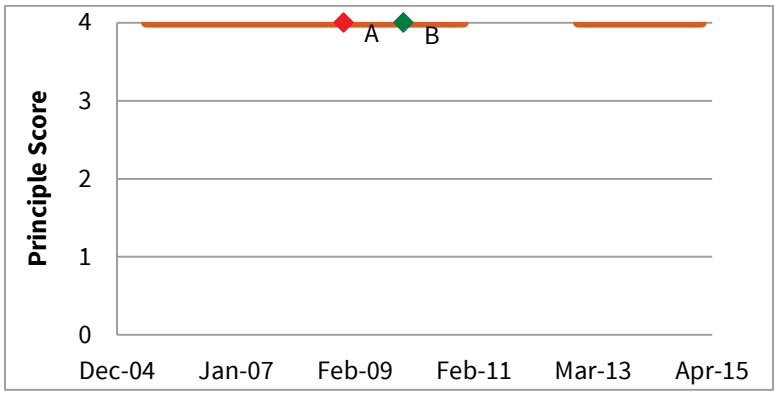


Figure 3. Principle 1.4: Privacy policy must have topic headings that link to plain language explanations of the type of data accessed and how the data are handled. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

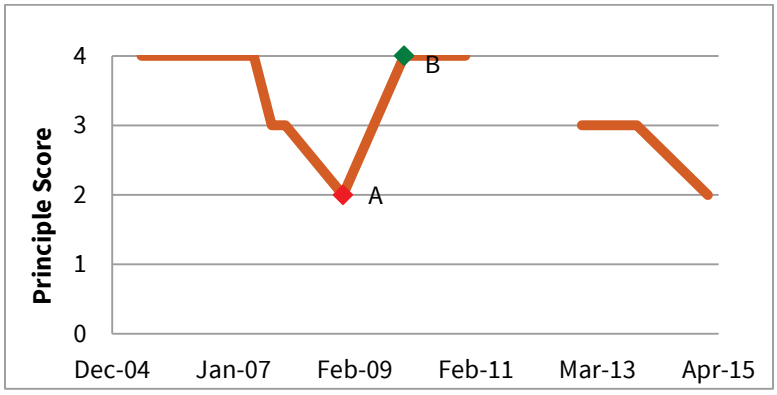


Figure 4. Principle 1.6: Privacy policy shall attain a Flesch-Kincaid Grade level score (reading level) of 12 or lower. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

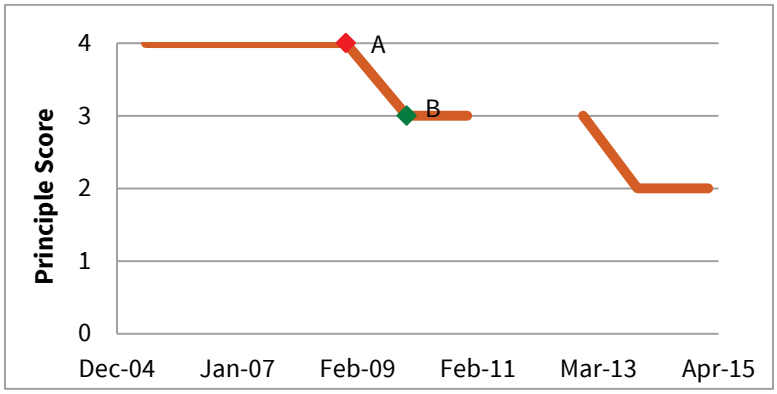


Figure 5. Principle 1.7: Privacy policy shall use a minimum 9 pt. font. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

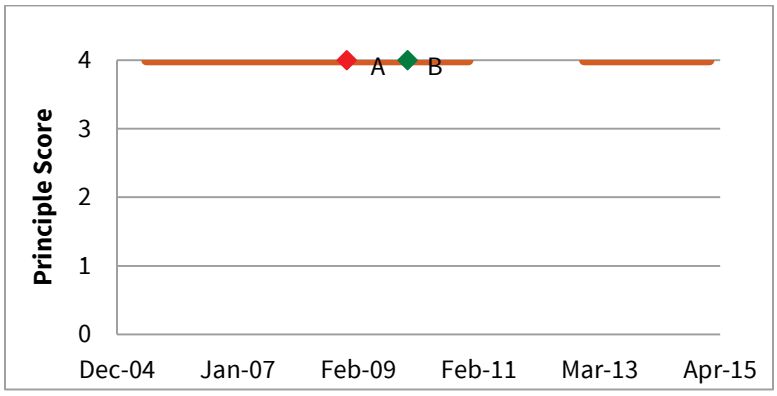


Figure 6. Principle 1.8: Privacy policy is available in the native language of the organization's significant customer populations. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

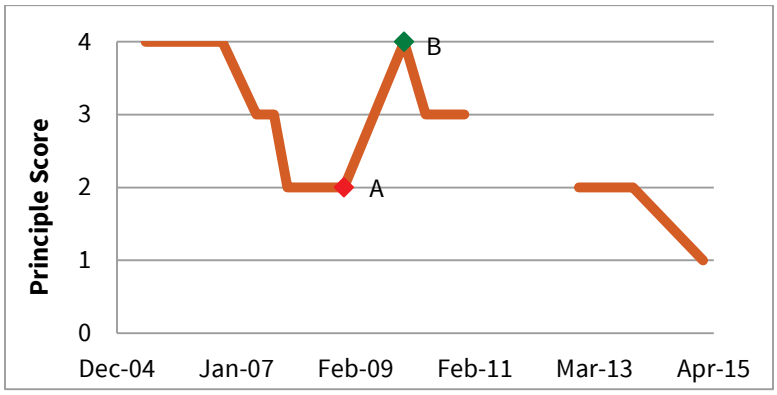


Figure 7. Principle 1.9: Privacy policy provides easy access to definitions of technical terms. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

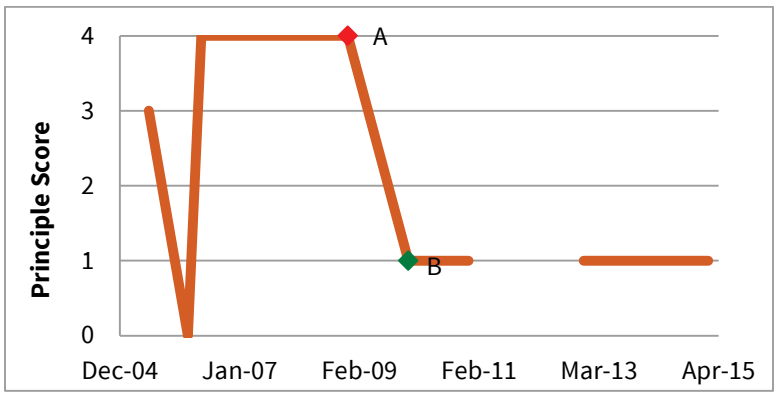


Figure 8. Principle 1.10: Privacy policy includes explicit language on process and notification of "material changes" and allows customers a defined timeline to opt out before policy changes. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

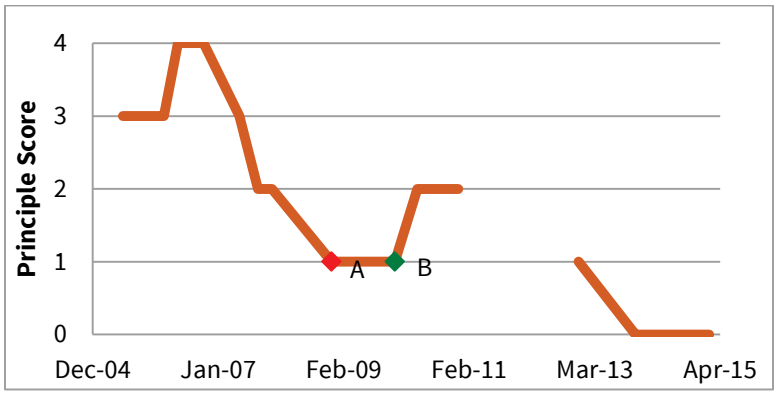


Figure 9. Principle 2.1: Privacy policy states that personal information is collected only with informed consent, unless otherwise required by law. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

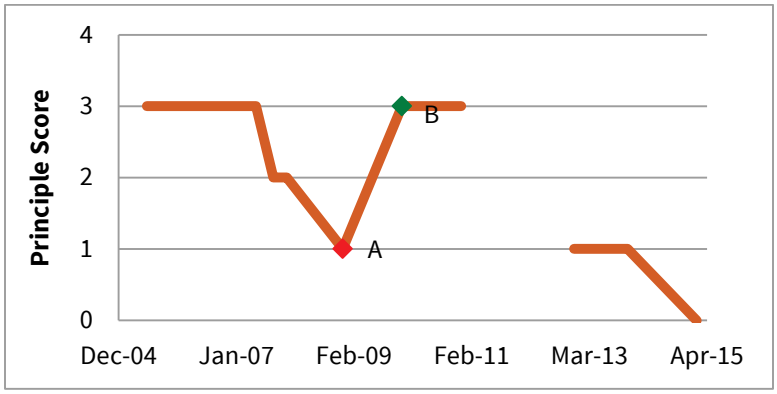


Figure 10. Principle 2.2: Privacy policy must clearly state what the organization will and will not do with personal information. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

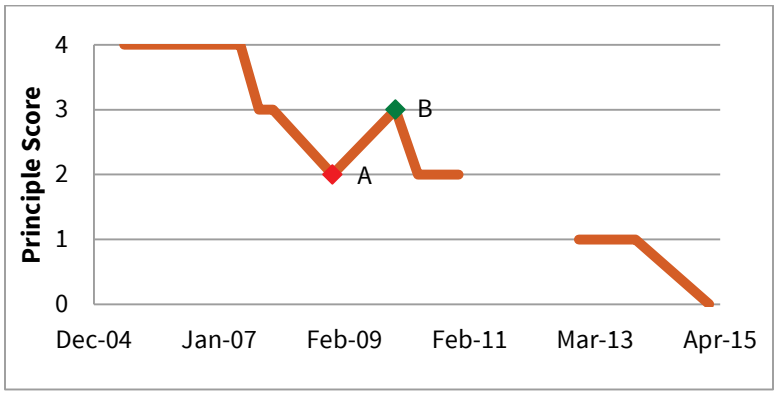


Figure 11. Principle 2.3: Privacy policy fully describes use of Internet monitoring technologies, including but not limited to beacons, weblogs, and cookies. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

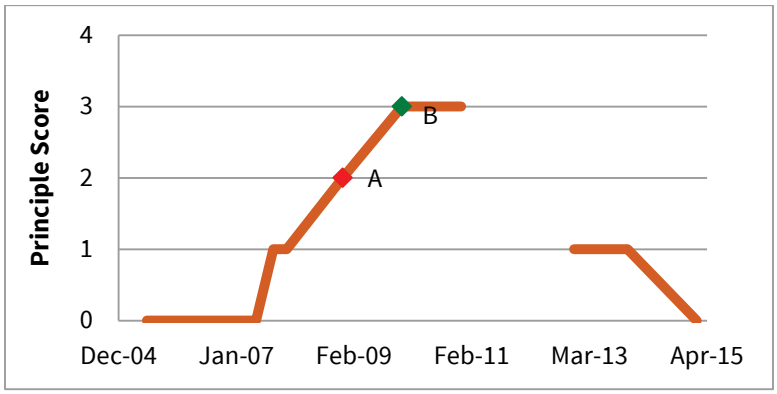


Figure 12. Principle 2.4: Privacy policy fully describes all data sharing circumstances that require a user to opt-in. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

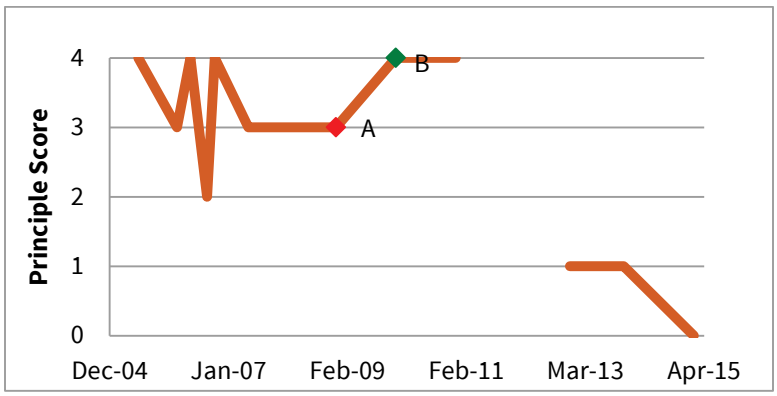


Figure 13. Principle 2.5: Privacy policy describes ability the user has to change, segment, delete, or amend their information. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

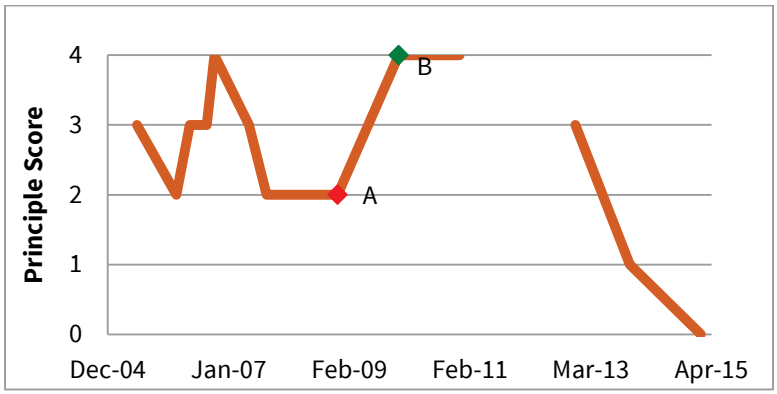


Figure 14. Principle 2.6: Privacy policy fully describes who can access the information and when. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

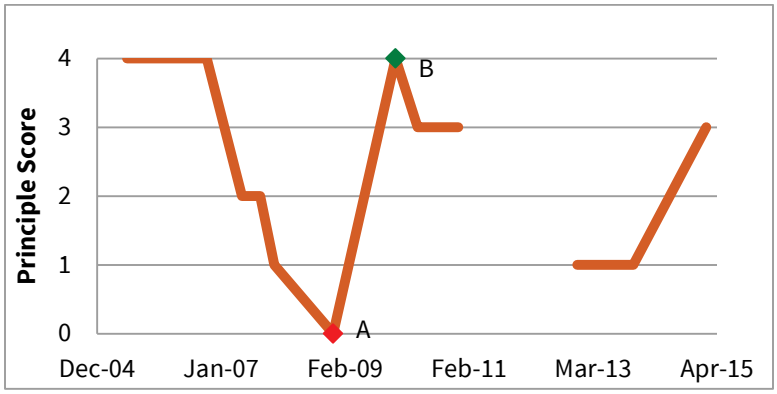


Figure 15. Principle 2.8: Privacy policy fully describes with whom data are shared. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

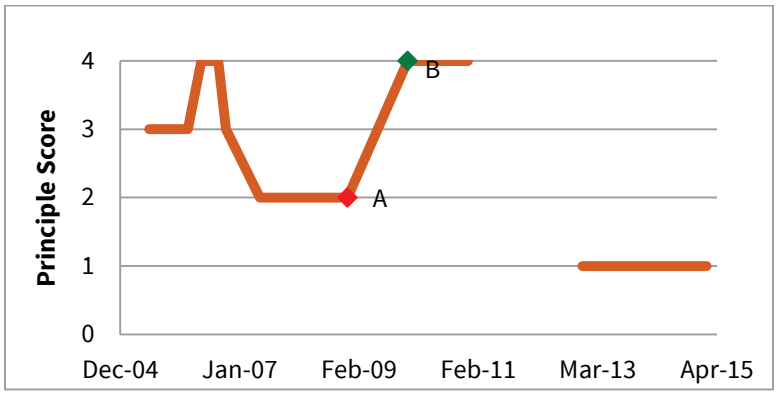


Figure 16. Principle 2.12: Privacy policy describes the organization's process for receiving and resolving complaints. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

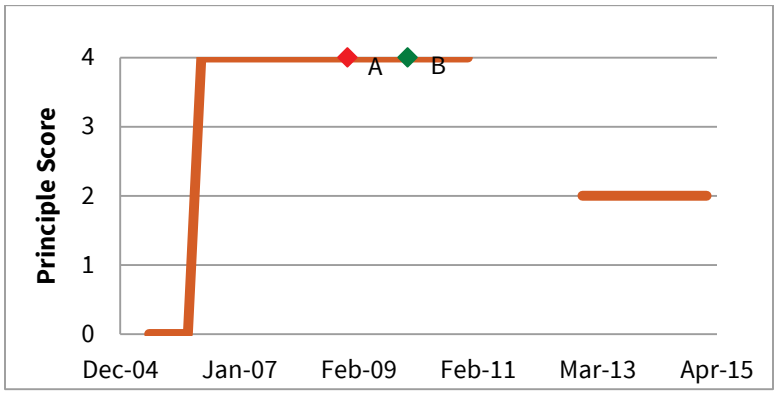


Figure 17. Principle 2.13: Privacy policy describes a mechanism for Third Party resolution of complaints. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

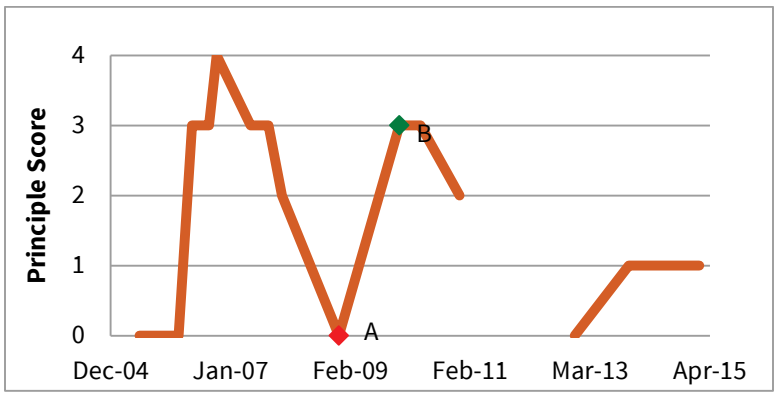


Figure 18. Principle 2.14: Privacy policy confirms that persons with access to data comply with privacy policies. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

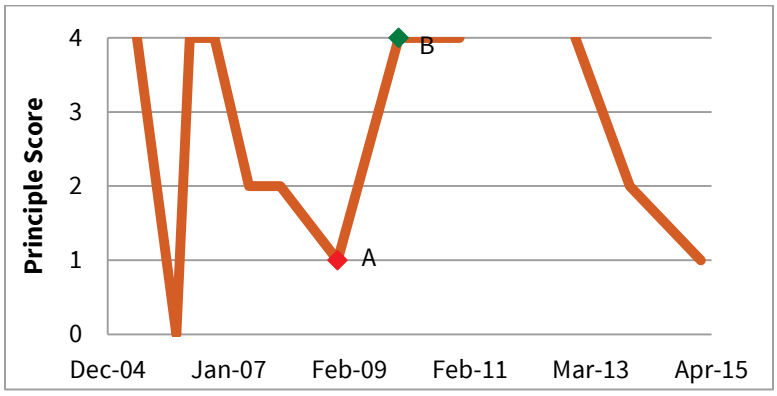


Figure 19. Principle 3.2: System allows user to opt out at any time, and the opt out process must be simple and clearly stated in the privacy policy. Scale is from 0

(minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

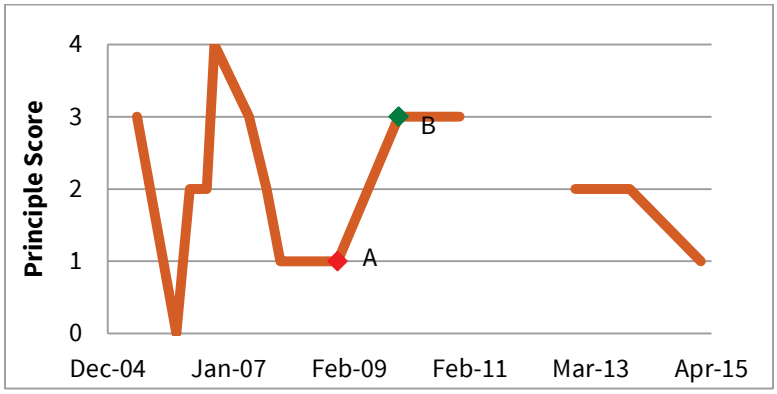


Figure 20. Principle 3.3: System provides capability for all access to the user's data to be removed at any time. User has the ability to permanently delete all information upon closing an account. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

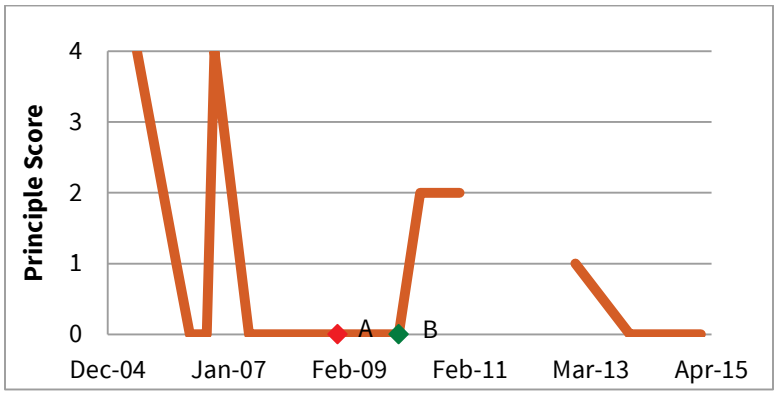


Figure 21. Principle 5.1: Any profiling must be optional (opt in) with the ability to opt out. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

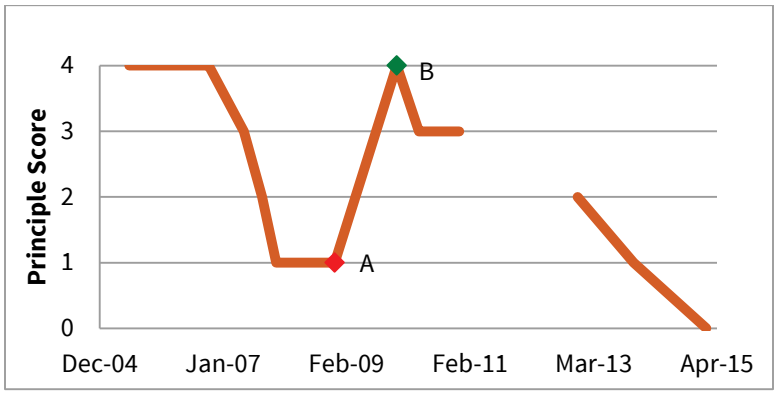


Figure 22. Principle 5.2: The system must allow users to clearly identify data used for profiling and targeting. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

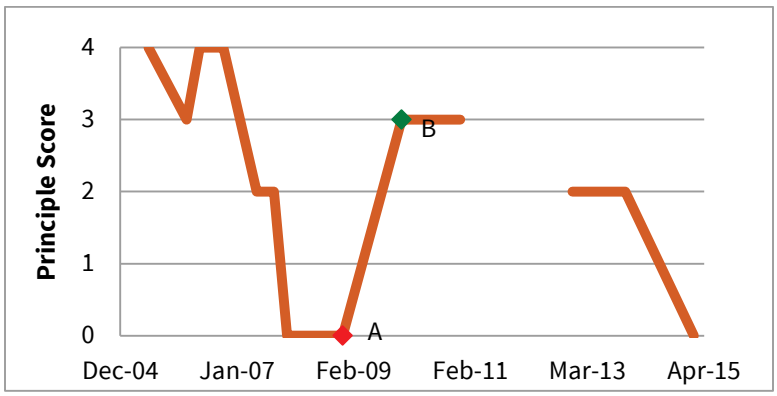


Figure 23. Principle 5.3: Users must be able to opt out of any profiling at any time. The opt out process must be simple and clearly stated in the privacy policy. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

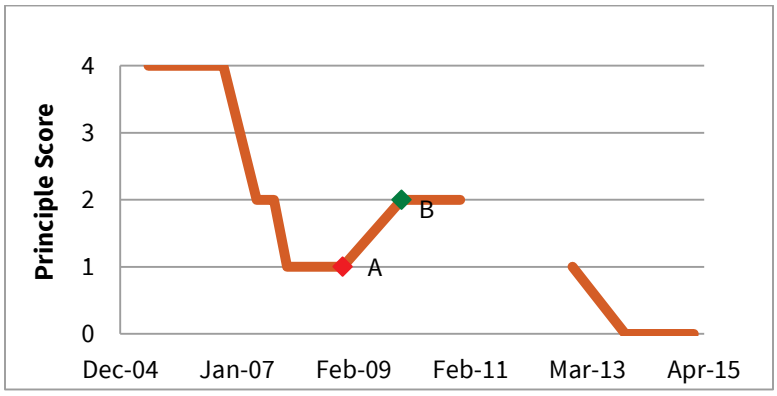


Figure 24. Principle 5.4: The user may choose which specific data elements may be used for profiling and targeting. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

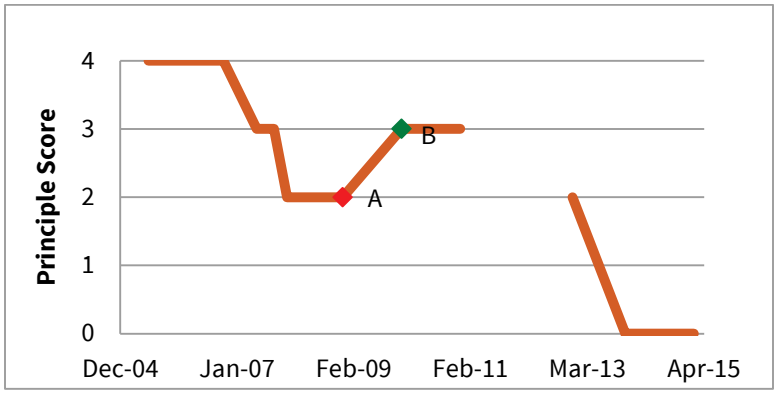


Figure 25. Principle 6.1: System allows user to selectively release each element of their personal information. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

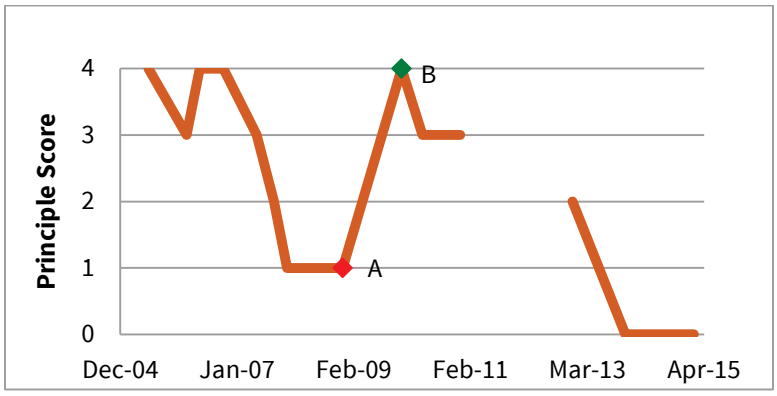


Figure 26. Principle 7.1: System allows user to delete, change, or annotate each element of their personal information. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

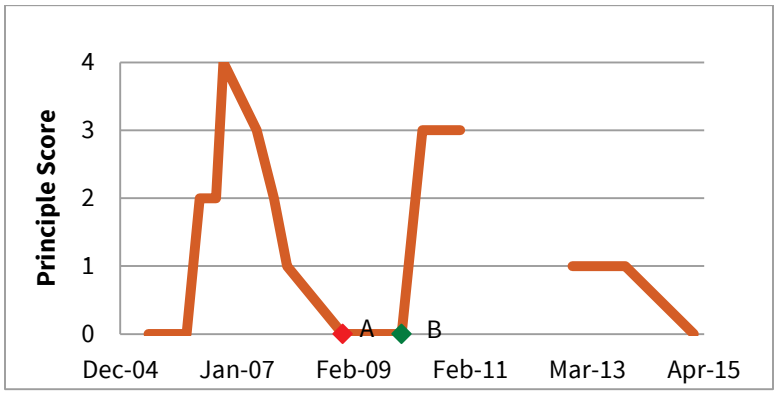


Figure 27. Principle 7.2: The user may permanently delete their personal information from the system upon user request. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

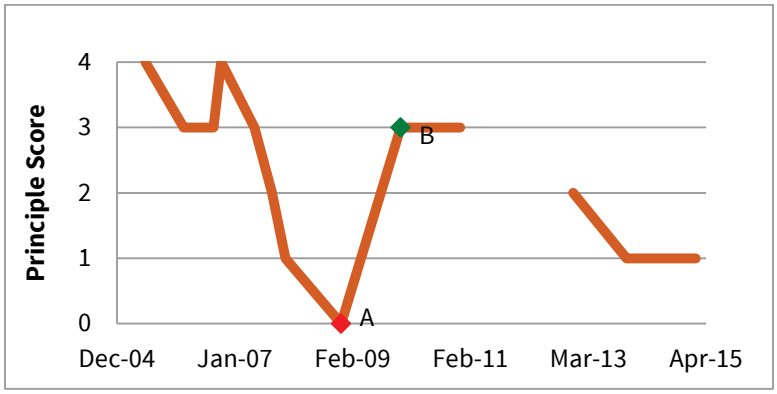


Figure 28. Principle 8.2: System provides the functionality to control access to the data. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

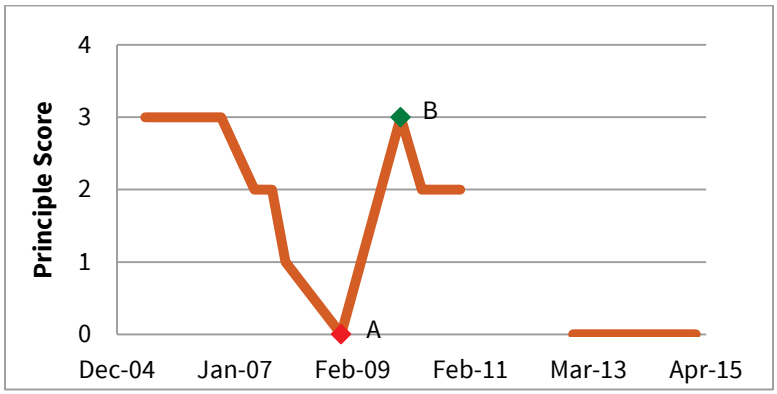


Figure 29. Principle 8.4: The user has the ability to control the type of access that is provided to the system (e.g. read, write, delete). Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

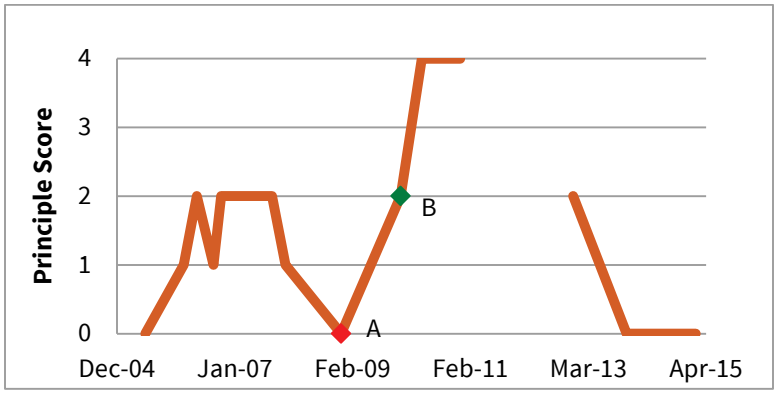


Figure 30. Principle 8.5: The system specifies how long access to data is available (e.g. indefinitely or one week). Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

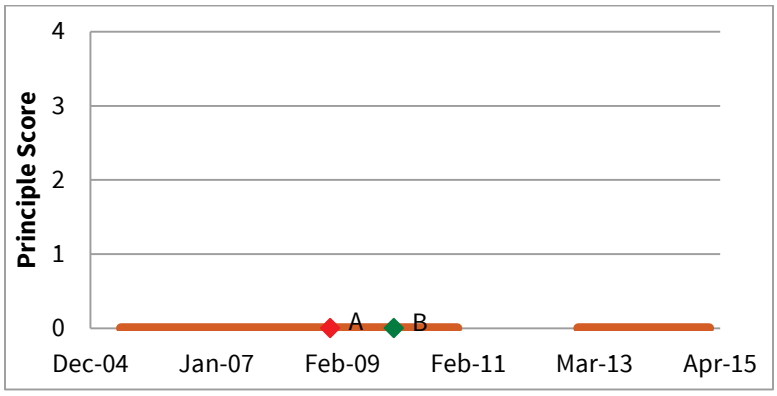


Figure 31. Principle 11.1: If a breach occurs, organization notifies relevavnt users about breach or potential breach. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

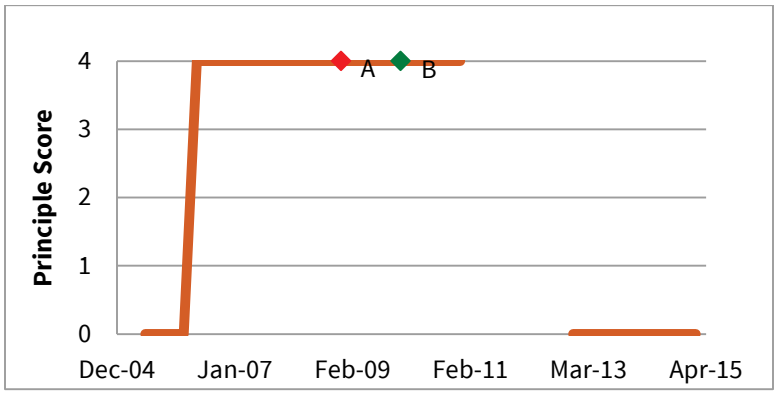


Figure 32. Principle 12.1: The organization must have a process that enables users, advocates, employees, and government regulators to report potential or actual privacy violations. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

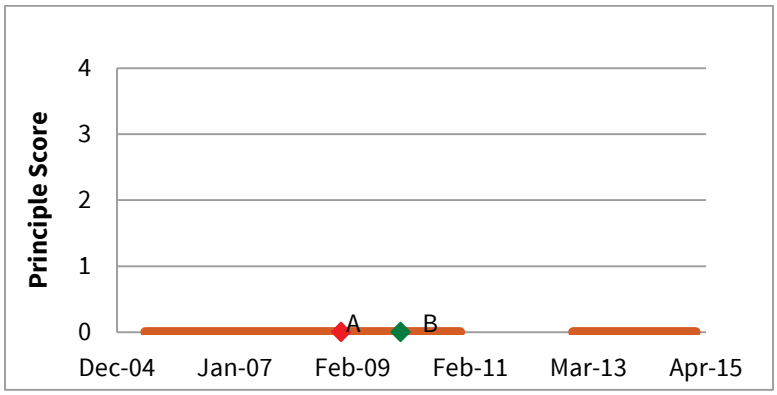


Figure 33. Principle 15.1: Users can expect to receive a copy of all disclosures of their information. Scale is from 0 (minimum or worst) to 4 (maximum or best). Gap results from missing archived policies.

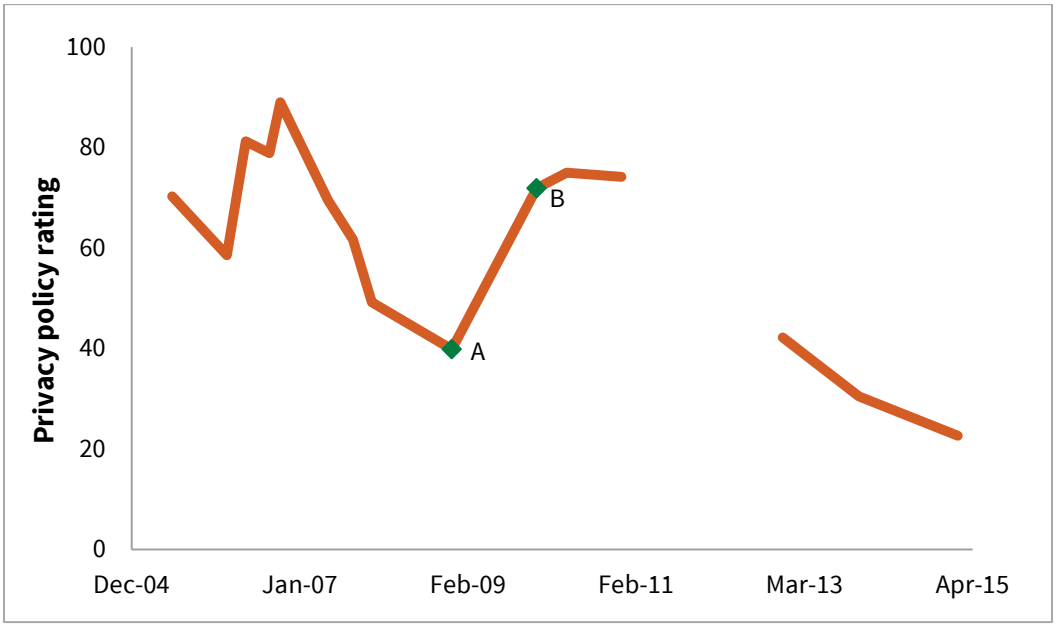


Figure 34. Percentage of total possible score across all measured criteria, as reported in Figures 1 through 33.

Overall: Figure 34 totals the results from all criteria and principles we measured to show the percentage of total possible ratings of the privacy policies. Over time, Facebook's privacy policy generally ranked lower on the PPR Framework criteria. These standards included whether the user has the ability to opt out (Principle 3.2), and the accessibility of the policy in terms of format and style (Principles 1.6 and 1.7).

Since 2005, Facebook has revealed consistently less information about the technology that it uses to collect data such as cookies, beacons, and weblogs (Principle 2.3, Figure 11). Additionally, since 2009, Facebook's new privacy policies do not have provisions that explain exactly which outside sources receive user information (Principle 2.6, Figure 14).

While Facebook's privacy policy generally ranked lower on PPR Framework criteria between 2005 and 2008, the exception to this otherwise steady trend occurs in December 2009, labeled B in the figures, when the privacy policy disclosed information about data sharing practices and gave the user agency in managing disclosure of some information. However, despite the disruption in December 2009, the trend has been for the privacy policy to provide less transparency and less user agency in terms of options to opt out (Principle 5.2, Figure 22).

Starting in 2009, Facebook fully described the ability a person would have to amend and delete his or her information. Prior to 2009, the different versions of the privacy policy fluctuated in their provisions to allow people to amend or delete their personal information. However, since 2009, this provision has also seen a steady decline as Facebook has been less

clear in their privacy policy about users' ability to delete their information (Principle 2.5, Figure 13 and Principle 3.3, Figure 20).

Furthermore, users' ability to opt out of data collection has experienced two major fluctuations. It reached a low in 2008 and a peak in 2009 (Principle 3.2, Figure 19).

Finally, Facebook's privacy policy has become more inaccessible in readability terms. The PPR Framework provides several criteria to assess this including the ease of reading, the size of the font, and the length of the policies. The privacy policies have become more difficult for the average user to understand (Principle 1.6, Figure 4), the size of the font has gotten smaller (Principle 1.7, Figure 5), and the word length has increased from approximately 1,000 words to over 12,000 words (see Figure 35).

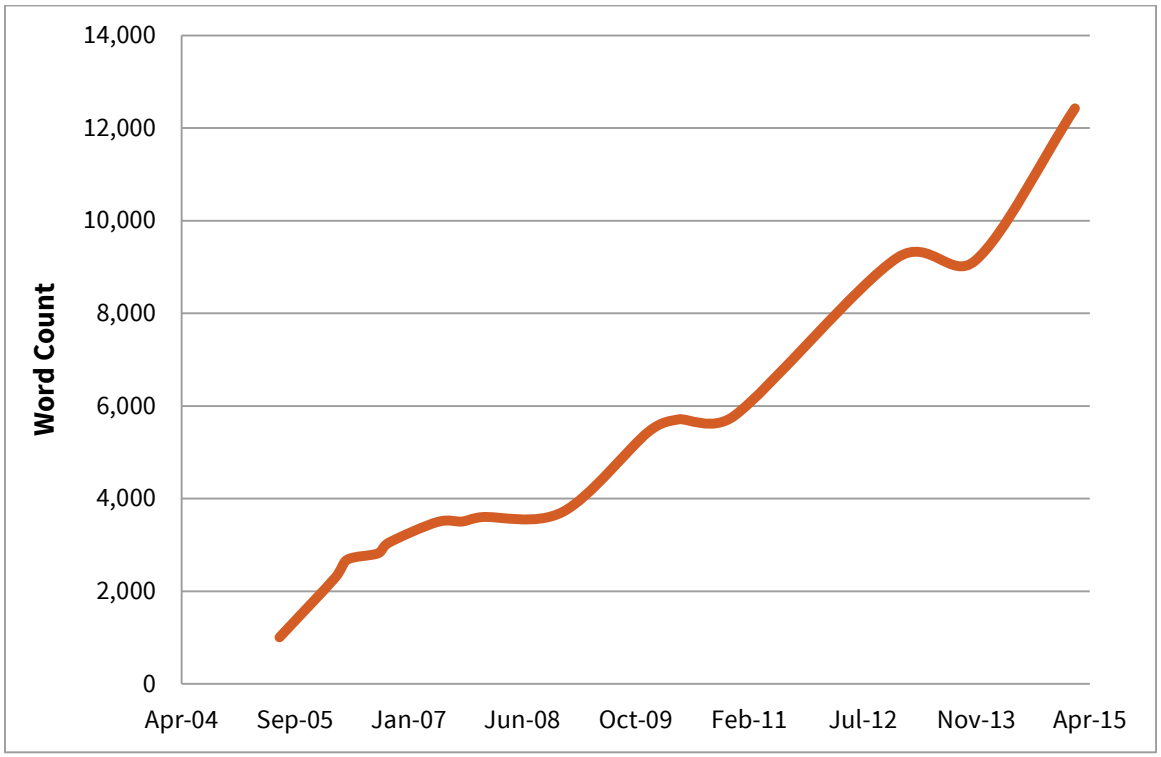


Figure 35. Word count of Facebook's privacy policy over time.

Discussion

Our findings suggest that Facebook's privacy policy has become less transparent, is harder for users to understand, and contains fewer options for user control over personal data in connection with third party access.

We found that there was an improvement in privacy standards across a range of criteria in December 2009. The dots labeled "A" and "B" in Figures 1 through 34 indicate an

improvement in the transparency and accessibility of standards. This improvement coincides with concerns expressed by external advocacy groups such as the American Civil Liberties Union, the Electronic Frontier Foundation, the media, and users [17]. While the views of those groups suggest that the November 2008 version of the privacy policy was less successful at protecting user data, than previous iterations, the transparency and accessibility improvements—the PPR Framework metrics—made it possible for external policy actors to have greater influence the following year. While there was an improvement for a short time following the November 2008 dip (marked by the "A" dot in Figures 1-8), it was not sustained over the long term, as evidenced by the subsequent steady decline in Facebook's privacy policy quality indicated by the downward trajectory following the second dot "B" (see Figures 1 through 34). Furthermore, other periods of external pressure from civil liberties groups [18] on Facebook regarding their privacy policy as well as actions taken in this regard by the Federal Trade Commission [19] do not coincide with any improvements in the policy in terms of fulfilling the PPR Framework criteria.

These findings point to a few ways to improve privacy policies for users through increased transparency and accessibility. First, it might be beneficial to provide greater transparency regarding third-party data sharing by explicitly stating with whom data are shared or providing a mechanism for users to track that information. Furthermore, it may prove fruitful to provide users with information in a more accessible format, including using bigger fonts and fewer words, improving Flesch-Kincaid reading scores, and providing clearer instructions for opt-in and opt-out data collection.

References

1. Duggan, M, Ellison N, Lampe C, Lenhart A, and Madden M. Social Media Update 2014. Pew Research Center, Jan 9, 2015. http://www.pewinternet.org/2015/01/09/social-media-update-2014/

2. Facebook. Our Mission. Accessed July 20, 2015. http://newsroom.fb.com/company-info/

3. Kirkpatrick M. Facebook's Zuckerberg Says the Age of Privacy is Over. ReadWrite, Jan 9, 2010. http://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov

4. boyd d. It's Complicated: The Social Lives of Networked Teens. New Haven: Yale University Press, 2014: 64. Accessed May 12, 2015. http://www.danah.org/books/ItsComplicated.pdf

5. Tufekci Z. Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society 28.1 (2008): 20-36. Accessed May 12, 2015.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.304.6929&rep=rep1&type=pdf

6. McKeon M. The Evolution of Privacy on Facebook. May 19, 2010. http://mattmckeon.com/facebook-privacy/

7. Federal Trade Comission. Protecting Consumer Privacy. Accessed July 20, 2015. https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy

8. Platform for Privacy Preferences Initiative. Platform for Privacy Preferences (P3P) Project: Enabling Smarter Privacy Tools for the Web. November 20, 2007. http://www.w3.org/P3P/

9. Federal Trade Commission. Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers. December 2010. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf

10. Ibid.

11. Zerr S, Siersdorfer S, Hare J, and Demidova E. I Know What You Did Last Summer!: Privacy-Aware Image Classification and Search. August 16, 2012. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.473.4609&rep=rep1&type=pdf

12. Federal Trade Commission. pp. 26-27.

13. Kelly P, Bresee J, Cranor L, and Reeder R. A Nutrition Label for Privacy. Proceedings of the 5th Symposium on Usable Privacy and Security. No. 4. July 15, 2009. https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf

14. Patient Privacy Rights. Patient Privacy Rights Trust Framework. 2013. https://patientprivacyrights.org/trust-framework/

15. Web Archive: The Wayback Machine. The Facebook Privacy Policy. Accessed April 28, 2015. http://web.archive.org/web/20050809235134/www.facebook.com/policy.php

16. Stone B. Facebook's Privacy Changes Draw More Scrutiny. New York Times. December 10, 2009. http://bits.blogs.nytimes.com/2009/12/10/facebooks-privacy-changes-draw-more-scrutiny

17. Johnson, Bobbie. "Facebook Privacy Change Angers Campaigners." The Guardian, 10 Dec. 2009. Web. Accessed 12 May 2015. http://www.theguardian.com/technology/2009/dec/10/facebook-privacy

18. See for example Kerr D. Facebook Faces Criticism over Its Privacy Policy. CNET. September 4, 2014. http://www.cnet.com/news/facebook-faces-criticism-over-its-privacy-policy/

19. Goel V and Wyatt E. Facebook Privacy Change Is Subject of F.T.C. Inquiry. New York Times. September 12, 2013. http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html

Authors

Jenny Shore is a junior at Harvard College concentrating in Social Studies with an expected secondary in Modern Middle Eastern Studies. At Harvard, she is founder and co-chair of the Tech & Innovation Policy group at Harvard's Institute of Politics. This past summer she interned at the Berkman Center for Internet and Society. Previously, she was a civic tech fellow at Microsoft and an intern for CBS's 60 Minutes and Al Jazeera Arabic TV.

Jill Steinman is a junior at Harvard College studying government and economics. During her free time, she is a staff writer for the Harvard Crimson and currently covers the Graduate School of Arts and Sciences.

Editor: Latanya Sweeney

Citation

Shore J, Steinman J. Did You Really Agree to That? The Evolution of Facebook's Privacy Policy. *Technology Science*. 2015081102. August 11, 2015. http://techscience.org/a/2015081102

Data

Shore J, Steiman J. Replication Data for: Did You Really Agree to That? The Evolution of Facebook's Privacy Policy. Harvard Dataverse. August 6, 2011. http://dx.doi.org/10.7910/DVN/JROUKG