Google Privacy: Something for Nothing?

David Crowe
Kentucky State University
400 East Main Street
Frankfort, KY 40601
+1 502-597-6661
David.Crowe@kysu.edu

Wasim A Al-Hamdani, Ph.D.
Kentucky State University
400 East Main Street
Frankfort, KY 40601
+1 502-597-6661
Wasim.Al-Hamdani@kysu.edu

ABSTRACT
With an ever-expanding portfolio of service offerings and the lion's share of the search market, Google stands to acquire, collate, and even infer a vast amount of information—individual, cohort, and aggregate—about each of us. The privacy policies of Google have an obvious impact on users of Google services. However, the policies that Google adopts also have an indirect impact on all Internet users: As the market-share leader, Google is the de facto trend setter for most, if not all, providers of Internet-based services. The policies of the market leader will surely filter down and be used as a template by other information vendors.

This work examines the changes to Google's privacy policy over time as Google seeks to conform to the Federal Trade Commission settlement of February, 2011. A contextual review of previous policies shows that many of the policy items are not "new" at all, and that several have a long-established lineage. At the very least, the change represents a clear line of demarcation between the "old" Internet and tomorrow's information economy. The arrival of this new economy has altered who is the customer and what (or rather, who) is the product, and has also changed the meaning of "free."

Categories and Subject Descriptors
• Proper nouns: People, technologies and companies ~ Google Inc.
• Social and professional topics ~ Privacy policies
• Security and privacy ~ Privacy protections
• *Security and privacy ~ Social aspects of security and privacy*
• *Security and privacy ~ Economics of security and privacy*
• Information systems ~ Internet communications tools
• Information systems ~ Social networks

General Terms
Management, Documentation, Economics, Security, Human Factors, Legal Aspects

Keywords
Google privacy policy

Information Security Curriculum Development Conference 2013
October 12, 2013, Kennesaw, GA, USA.

1. INTRODUCTION
A privacy policy provides insight about the views of a business or entity, and describes the procedures that govern the collection and use of information collected from website visitors. Though they are legal documents, privacy policies should be understandable, accurate, and should avoid "burying" (hiding) important information inside of "reams of text" [1]. Typical sections of privacy polices include:

- Introduction—informs visitors about the company or organization
- Information Collected—describes what information the entity is collecting, even if it may be obvious (e.g. asking visitors to complete a form)
- Method of Collection—details the method(s) used to collect information, i.e.: automation, visitor-completed forms, or indirect (visitors complete forms that contain information about others)
- Storage of Information—describes how the information is stored, including its location (some governments, such as the UK or the EU, may have additional regulatory constraints that apply to entities that store data inside their jurisdiction or that is about their citizens). This section should also acknowledge and address visitors' right to the safety and security of their stored information.
- Contact Details—provides visitors with the entity's contact information, including a "real world" address

- Adapted from PrivacyTrust [1]

Google's policies, like those of any other corporation, are subject to change over time. Once announced, the 2012 consolidation of Google's privacy policies and data sharing across all of its services garnered a good deal of attention. Often, the discussions missed that the then-future changes were rather minimal in and of themselves. Rather, most discussions focused on how Google would "begin" to integrate user data collection from all its collection points: even though this practice has clear origins in 2004. A more interesting avenue of discussion is why Google made such a change: namely, it's 2011 settlement with the Federal Trade Commission (FTC) regarding allegedly deceptive tactics in the implementation of Google Buzz, a social networking service.

By briefly analyzing the history of Google and its policies, Google's emphasis on and consideration of user privacy can be placed in context. This context can better illuminate the consolidated policy in light of the FTC settlement agreement.

This paper presents a brief history of Google (section 2) before chronicling its privacy policies (section 3). The examination is not meant to be exhaustive, but rather highlights general topics that show the lineage and trajectory of many elements found in the current, consolidated version. Section 4 briefly summarizes the events

leading up to the FTC complaint and the general terms of the settlement agreement that Google voluntarily agreed to. Section 5 describes three main elements of Google's consolidated policy: types of data collected, data usage, and user choices. Lastly, a discussion (section 6) and conclusion (section 7) examine the impact, assurances, and alternatives that accompany the changes, and how one's anonymity is becoming the currency of an information economy.

2. COMPANY HISTORY

Originally a research project in 1996 at Stanford University, Larry Page and Sergey Brin collaborated on the search engine that eventually became known as Google [2] and that served 1.2 *trillion* searches in 2012 [3]. As his dissertation theme, Page chose to focus on "backlinks"—counting the number of web pages that link to a given page. Page considered the "number and nature of such backlinks to be valuable information about that page" [4].

Google has steadily added to its portfolio of service offerings, which now includes everything from image manipulation (Picasa), to productivity software (Google Apps), to its own operating system (Chrome OS). As would any company, Google has had its share of growing pains over time. One of the more publicized events concerns the policies regarding the privacy of user's information with Google's social networking site, Google Buzz. This event became the catalyst that led to the involvement of the Federal Trade Commission and the subsequent settlement agreement that is examined in Section 4 below.

3. POLICY HISTORY

By examining the history of the policies of Google's services, the gradual shifts in user control (or loss of) can be traced. The policies are presented in chronological order, and provide a background for the sections that follow. It is not meant to be exhaustive, but attempts to call attention to points of interest or significance.

3.1 August, 2000

The August, 2000 policy [5] is the first listed on the Archive page [6], which contains past iterations of Google's privacy policies. It defines a cookie as "a piece of data that identifies […] unique user[s]" that is used to improve Google's services by storing a user's preferences. The policy declares that no unique information (e.g.: name, e-mail address, etc.) about a user is gathered without the user knowingly and specifically providing it, but includes the specific examples of IP address and browser language as items that are collected by default.

Google disclaims any connection to or control over sites listed in any given search result, and states that these third-parties may have privacy policies of their own. However, Google may collect out-click data (information about which site(s) a user selects from a web search) to improve service quality. Google states that they will only share aggregated information with outside parties, and may share personally identifiable information (PII) only when the user has expressly consented. The exception to the express consent clause is if Google is releasing information in response to a valid legal action. The policy ends with informing users that their use of Google services signifies acceptance of the privacy policy and terms of service.

3.2 2004

The next policy provided is from 2004 [7], and lists Google search, Toolbar, News, and "some other services" as not requiring any PII from users. It states there are some services that require registration, and that PII collection will be accompanied by notice of the types and uses of the required information. The circumstances surrounding the release of PII are expanded to include: user consent; trusted business partners acting on behalf of Google (subject to their agreement to comply with Google's policy and to maintain user privacy); response to legal action; or if Google has a "good faith belief" that such release is "reasonably necessary to protect the rights, property or safety of Google, its users or the public."

The concept of data sharing across Google services is introduced, however, account information will only be disclosed as listed above. Further, PII may be stored and processed at any Google facility in any country of operation. Aggregated information is still subject to release, use of Google services still constitutes acceptance of their policies, and the disclaimer regarding sites linked-to in search results in repeated.

3.3 2005

The 2005 iteration [8] appears to clarify that a single policy will apply to "all of the products, services, and websites offered by Google, Inc. or its subsidiaries or affiliated companies." However, separate PII-specific policies may be posted for "particular services." The specific services are not named in the archived version, but rather are "accessible from the navigation bar to the left of this notice" (the archive page does not include the referenced links). The U.S. Department of Commerce safe harbor program is given its first mention.

Again, data sharing across services is explicitly stated, as are the use of cookies, out-click tracking, and the third-party sites disclaimer. Two new items are the inclusion of provisions that allow Google to retain communications sent to Google from users and language stating that affiliated sites may collect PII in order to provide services on behalf of Google. These affiliated sites may have policies of their own, but Google's use of PII gained in this way will comply with Google's policy.

The purposes to collect and process PII are more explicitly defined as providing, maintaining, protecting, and improving services as well as developing new services. Provisions will be made to allow users to opt out of PII uses not agreed to in advance, and "sensitive information" (described in the Frequently Asked Questions as information "relating to confidential medical facts, racial or ethnic origins, political or religious beliefs or sexuality") is only collected according to policy, or with prior consent. Information sharing with outside parties is essentially unchanged from the 2004 policy, with the addition of an opt-in requirement for sharing of sensitive PII.

Security assurance is given mention, as is the disclaimer that Google relies on users to update and maintain the accuracy of collected data. A new addition is provision for users to access, update, and request deletion of PII. There are a number of reasons Google may decline such requests that mostly center around the amount of operational effort required to comply with the request.

3.4 2008 & 2009

Two services, Double-Click and Postini, were explicitly excluded from the general privacy policy in both the August, 2008 and March, 2009 versions, and were governed by separate policies until October, 2010 when DoubleClick was no longer listed as an excluded service [9].

The 2008 policy [10] and January, 2009 policy [11] are nearly identical to the 2005 version, with the main difference being the ability to opt out of Google's Ad Serving by following the DoubleClick cookie opt-out process (no link is available for inclusion in this paper, as the link from the Policy page is user-specific). March, 2009 [12] changes very little, except to add language regarding information collection by Google Gadgets (to be

controlled by the provider's policy) and location data (such as actual location based on GPS data, or approximate location based on cell phone cell ID).

3.5 October, 2010

The October, 2010 version [9] represents a significant revision. Of particular note is the introduction of the Google Dashboard as the primary means for users to review and control the information associated with their Google Account. Additionally, Google now states that services utilizing SMS messaging may give Google the opportunity to collect and store information relating to those messages, including phone numbers and the contents of the messages.

Another significant change is how Google may now use collected information. This policy iteration limits data use to service provision and improvement and to protect the rights or property of Google or its users. This is significant in that the language allowing data use to develop new services has been eliminated. Also, the language regarding additional use of collected data now appears to require prior consent, rather than requiring users to review separate policies. This seems to be an opt-in provision instead of the more loosely defined opt-out language of previous policies.

3.6 October, 2011

The October, 2011 version [13] is the policy in effect immediately before the consolidation of 2012. The only change from the previous version outlines Google's compliance with the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks, and the inclusion of a link to Google's certification of adherence to the Safe Harbor Privacy Principles.

4. FTC SETTLEMENT

On 9-February-2010, Google launched a new social networking site: Google Buzz [14]. Shortly after Buzz was launched, the Federal Trade Commission (FTC) investigated Google's behavior based on complaints received by the from the Electronic Privacy Information Center (a "public interest research center" [15]. This investigation eventually led to Google voluntarily agreeing to a proposed settlement. This settlement was the first occurrence of two significant events: it was the first settlement requiring that a company implement a comprehensive privacy program to safeguard the privacy of customers' information, and was the first allegation by the FTC that "substantive privacy requirements" of the U.S.-EU Safe Harbor Framework had been violated [16].

4.1 The Complaint

The complaint alleged that Google had violated its own then-current privacy policy in its implementation of Buzz. The allegation was that Google had used information provided by users when they had signed up for Google's Gmail service (including the user's name and e-mail contacts) to enroll users into Buzz. The violation allegedly occurred because of language in the then-current policy stated that Google would inform users if any PII collected would be used for purposes other than those disclosed at the time of collection—and would seek consent to use the information for any new purpose(s). Further, the complaint alleged that Google misled users about their ability to opt out, as they were enrolled in certain features of Buzz even after turning Buzz "off" or having declined to join the service altogether. Additionally, it was alleged that Google failed to adequately inform users that their contacts list would become public. In some cases, this led to public disclosure of confidential information such as the names of a user's patients, students, or employer, or relational information such as a user's contact with ex-spouses or business competitors. Lastly, the FTC alleged that Google misrepresented its self-certification of compliance to the U.S.-EU Safe Harbor privacy framework by failing to give users "notice and choice before using their information for a purpose different from that for which it was collected" [16].

4.2 The Settlement Agreement

The agreement, which was unanimously accepted by the FTC [17] and voluntarily agreed to by Google, is multifaceted and imposes several restrictions. Chiefly, Google:

- Is barred from future privacy or confidentiality misrepresentations,
- Is required to implement a comprehensive privacy program,
- Must submit to independent privacy and data protection audits every two (2) years for the next twenty (20) years,
- Is barred from misrepresenting compliance with the U.S.-EU Safe Harbor privacy framework, or other privacy, security, or compliance programs, and
- Must obtain users' consent before sharing information with third-parties if Google changes its product or service, and such change results in sharing contrary to the policy in existence at the time of collection.

5. CONSOLIDATION OF POLICIES

Because Google was required to implement a "comprehensive" privacy program, its privacy policy was revised—almost in toto. It is written in plain language that "lays out our policies regarding your information in a simple and straightforward way" [18] to support the claim that Google "tried to keep it as simple as possible" [19], and includes a link to "Key Terms" [20] that provides plain-language definitions of various terms. The following are three areas of particular note to the present discussion.

5.1 Types of Data Collected

By entering PII to create a Google Account, users help Google deliver more personalized services, ads, and content. Users may also create a Google Profile, which becomes publicly searchable. Beyond explicitly supplied information, Google may also collect information about: the services used and the way they are used; clickstream behavior; device-specific information such as hardware signature, operating system, mobile phone information, etc.—and may associate this information with the user's account; search queries; telephony log information (phone numbers, time/date/duration of calls, etc.); IP address; cookies or anonymous identifiers; location information; and unique application numbers (associated with installed Google applications or services). Also, Google may collect and store information locally on a user's device.

5.2 Data Usage

The policy states that Google uses "information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer [users] tailored content – like giving [them] more relevant search results and ads." The name provided for a Google Account may be used across all services, and a user's Profile will be available to other users that already have some "information that identifies [them]."

As with past policies, Google may keep communications sent to it by users, and will continue to use cookies to store user preferences. However, for the purposes of user-tailored ads, cookies will not be associated with sensitive information (recall that sensitive information includes information about race, religion, sexual orientation, health, etc.). Google reiterates the practice of data sharing across services and explicitly includes PII, with the exception that DoubleClick cookie information sharing involving PII is now

opt-in. Lastly, Google restates the prior-consent requirement to use information for purposes other than those permitted during collection, and that PII may be processed in countries other than the user's country of residence.

5.3 User Choices

Users are now directed to various applets to control their information exposure to Google. Google Dashboard, Ads Preferences Manager, Google+ Circles, and the Data Liberation Front are all available from the policy page [19] and allow users to interact with where-, if-, and how their information is stored. Users are also advised that they can disable cookies altogether in their browser, although there may be functionality issues that result from doing so. Further, there is a series of pages collectively called "Good to Know" that provides "quick tips and how-to's that explain what you can do to stay safe and secure on the web" [21] and also provides links to the privacy-controlling applets listed above.

Carried over from the 2005 policy is a mechanism to correct PII, or request its removal. Details of this process are now more readily available on the Frequently Asked Questions page [22]. Many of the provisions for third-party sharing found from 2000 and 2004 are still present, including aggregated non-PII, with the explicit addition of opt-in for sharing of sensitive PII. Information security features are listed including SSL, two-step verification for Google Accounts, and Safe Browsing for Google Chrome. The policy concludes with: the disclaimer of responsibility for third-party search results or non-affiliates; language stating that future changes that reduce users' privacy rights will require explicit consent; and links to the specific privacy policies of Chrome and Chrome OS, Google Books, and Google Wallet (and Google Fiber, as of July, 2012).

6. DISCUSSION

Although the new policy represents a complete revision, many of its elements can easily be traced back to prior versions—even as far back as the beginning of the archive. The use of cookies, the distribution of non-PII aggregate information, and collection of clickstream behaviors have been addressed in every policy researched. It may even surprise the reader to see that data sharing amongst Google services was introduced in 2004. In other instances, technologies such as telephony and GPS/location services did not exist (or were not wide-spread) during Google's infancy and so it makes sense that these new capabilities were addressed only in later policies.

The obvious pivot point is the FTC complaint-based settlement agreement. As the motivator for the adoption of a comprehensive privacy program, it stands as a clear waypoint on Google's journey from past to present. The conditions of the agreement seemed harsh—even to then-FTC Commissioner J. Thomas Rosch [23], leading one to wonder why Google voluntarily agreed to their imposition.

6.1 Impact

Google's comprehensive policy will have an impact on its users directly and all users of Internet-based services indirectly, as more information vendors adopt similar policies. The consolidated policies and explicit data sharing across services can be viewed as either positive or negative, depending on one's viewpoint. Regardless, there is a clear need for Google to have extraordinary security measures in place to safeguard its vast collection of user information.

6.1.1 Perceived Positives

There are many aspects which could be considered positive about Google's explicit cross-service data sharing. Google stands to benefit from being able to better allocate resources. With the centrally availability of user data across the enterprise, fewer servers need be dedicated to database storage. This can both free up resources for other uses and speed up access to stored data. Google can construct a more detailed "picture" of each user, which will ostensibly lead to better focused search results, ads, and service delivery.

Also, users have a clearer, more explicit set of expectations that are centrally located, rather than a disparate collection of individual policies. Most importantly, users have clear, direct tools to use to affect their data. Links to Dashboard, Ads Preferences Manager, Google+ Circles, and the Data Liberation Front are easily found on the new policy page and offer a range of options and controls that, if they were present before, may have been difficult to find.

6.1.2 Perceived Negatives

Of course, not everyone will view the data sharing favorably. With so many data points describing each individual, the same "complete picture" that stands to aid in service delivery can be disconcerting for some users. Such a massive amount of data about so many individuals may appear as a step toward Orwellian-style monitoring—even if only on a macro level. Such grand-scale data collection can fuel an inherent distrust of any one entity having so much knowledge (as it is said, "knowledge is power").

Also, the potential for misuse grows with every bit and byte collected. Few other targets must be so attractive to malicious actors as "complete pictures" of millions of Internet users. Such abuse could come from several vectors: a disgruntled Google employee, an untrustworthy third-party affiliate, an amoral competitor, a low-level "hacker" seeking fame and notoriety, organized criminal elements attempting to gain financial information or control, even state-sponsored agents or terrorists working to disrupt an enemy nation's cyber structure or perception of security.

6.1.3 Security and Countermeasures

All of these negatives certainly existed before the current policy. However, the overt consolidation of user information can only amplify the meaning and implication of any malicious act. Also, the consequences of public disclosure—intentional or otherwise—are equally amplified. Take for instance the disclosure of Gmail users' contact lists with the initial launch of Buzz. Likewise, many Google search users would prefer that no one knows *exactly* what they have been searching for recently: for any number of reason, they would rather people "just didn't know."

With such a massive accumulation of data and pointers to individual users what security measures does Google have in place? The new policy lists several safeguards in particular. SSL encryption and two-step verification form a baseline of security. Security policies and procedures minimize vulnerabilities, including both cyber- and physical access to systems and other assets. Presumably, the policies proscribe state-of-the-art intrusion detection and very tight user permission controls. Internal reviews and biannual independent audits can (a) identify deficiencies in the policies, (b) confirm and verify compliance, and (c) detect intrusion attempts, security lapses, or even actual breaches. Access to PII is "need to know", and confidentiality agreements cover employees, contractors, and agents. Almost certainly, Google does not list every countermeasure it employs. Doing so would only provide a roadmap for potential attackers.

6.2 Compliance Assurance

Google states that privacy and security are the "two the most common topics of questions" and that they "take both topics very seriously" [24]. Yet, having a policy in place can only safeguard assets if it is correct and followed. How can users be sure Google complies with its own polices? Internally, Google self-audits and

reviews compliance, and the independent audits stipulated in the agreement must occur every two years at a minimum. Additionally, Google claims compliance with: the US-EU Safe Harbor Framework, the US-Swiss Safe Harbor Framework, the UK Internet Advertising Bureau Good Practice Principles for Online Behavioural Advertising, the Australian Best Practice Guideline for Online Behavioural Advertising, and IAB Europe's European Framework for Online Behavioural Advertising. Additionally, Google is a member of the Network Advertising Initiative. Is this enough? Time will tell, but this certainly seems to be quite a few sets of "eyes" watching on our behalf—even though many of the frameworks are "self-regulatory." And, of course, the FTC will continue to keep Google "on the radar" for at least the next twenty years.

6.2.1 Future Policy Changes

Beginning with the first policy researched, Google has maintained the right to change its policy from time to time. Since 2005, the policies have consistently included the phrase, "We will not reduce your rights under this Privacy Policy without your explicit consent." Note that every change to the policy has been unilateral. That is: users cannot affect Google's policy or only portions of it to their liking.

Given the number of past changes, future changes are all but certain. What will become of user data as the policy changes is not clearly explained. For that matter, there does not appear to be any mention of how long Google will retain user data—whether PII or pedestrian. Another unanswered question is what choices users will have regarding the data already collected if the policy changes and becomes less inclusive. Suppose that a user permits Google to collect their name, DOB, and city of birth. Then, at some future point, Google decides it no longer needs user's city of birth. What will become of the data already on record: will it be deleted or kept in an archive? Or conversely, what if Google does not now ask for city of birth, but decides to do so later: will existing users be able to continue using the affected service without supplying the new data, or will they need to opt out? And then, what becomes of their data? Likewise, consider the data Google shares with external parties: what control will users have over archived data or data given for a service they later opt out of?

6.3 User Alternatives

Serving over a 1.2 trillion web searches a year [3] certainly makes it appear that most Internet users interact with Google on a near-daily basis in some form or another. What are the choices, then, regarding the combined policy?

6.3.1 To Stay or Go

Historically, the changes to Google's privacy policy have been unilateral: take it, or leave it. Users can continue using Google's services just as they have in the past, or they can abandon Google and all of its services completely. There is a middle alternative to this "Hobson's choice": users can only use a portion of the services offered by Google, and select alternative sources for their remaining needs. Even so, Google will still collect some amount of information, and therefore this hybrid method does not entirely allow a wary user to avoid becoming another entry in Google's data banks.

6.3.2 Identity Obfuscation

There are alternatives that can, to some degree, separate a user from Google. Although it requires effort to maintain and may be less than practical, obscuring one's true identity can allow a user to retain some anonymity.

6.3.2.1 Change Identity

By creating an on-line alias, Google may collect PII, but it will not actually be personal. That is: it will not really be "me." A user could create an entire alias—an alter ego of sorts—and use the alias' credentials to access Google services. However, this becomes problematic: What would the alias use as a shipping address? What credit card (or PayPal account) would it use? A user could also create multiple Google Accounts, and register each account with a different service. This would require the user to track which account is associated with which service, and could quickly become burdensome. Neither alias method overcomes the fact that much of Google's tracking is based on IP address and hardware signatures, and so Google would still be able to make connections on some level between the activity and the actor.

6.3.2.2 Anonymizers/Proxies

Users could also use CGI proxies or web anonymizers to interact with Google services. The shortcomings here are that the proxies may not handle cookies adequately to allow full functionality of a given service, and many employers and organizations block access to such sites as a matter of policy.

7. CONCLUSION

Whether or not we agree with or even like Google's new policy seems largely irrelevant, given the history of being unilateral and Google's level of ubiquity. Google is not likely to "go away" anytime soon. What is relevant, however, is the policy's effect on the privacy of Google users and the likelihood that these policies will not only continue along the same trajectory but will also ripple across to other service providers. Users are never under any obligation to use any of Google's services. For every service provided by Google, alternatives can be readily found (and ironically, using Google to find them!). Some users will use the new policy as a reason to seek services from another provider. Even then, the new provider may very well have policies fashioned after Google's, or possibly provide even fewer protections for users' anonymity.

The poster "blue_beetle" is credited with quipping on the community blog site Metafilter that, "If you're not paying for something, you're not the customer; you're the product being sold" [25]. Is it true that users of Google's services are not paying for the services, or are they in fact paying with a new form of currency: their anonymity? Is it even possible to be truly anonymous in the ever-connected world of the Internet? And lastly, if we are using our identities as payment for services rendered, how can we determine if we are getting what we pay for: How can we accurately calculate the value or exchange rate of this new currency?

The authors submit that we should collectively acknowledge that the new Google privacy policy is, at the very least, a clear line of demarcation between the "old" Internet and tomorrow's information economy. As the new paradigm of always-on/always-connected becomes increasingly pervasive, the argument could be made that it is also becoming increasingly invasive. For good or for ill, the Internet, like Google and other service providers that solicit and barter information, is here to stay.

The explosive growth and capabilities of the Internet disguise the fact that for all the advances made, it is only just now coming to the end of its first "generation." TCP/IP was only born in 1978. The first commercial ISP (PSINet) was founded in 1989. This was followed shortly after by the first website coming online in 1991 (http://info.cern.ch/hypertext/WWW/TheProject.html). All of these have happened during the lifetime of the authors (indeed, since the primary author was in the 5th grade). It seems perfectly reasonable that any company—along with the rest of us—born into an age of such expansion and growth would have growing pains as we all try to figure out what this "Internet" thing is, how to use it, and how to

limit how it uses us. Google is not the only vendor in the information market place, and is certainly not the only vendor suffering privacy-related growing pains: it just happens to be the most visible vendor that has caught the public's notice. Incidentally, all these Internet facts came from Google searches. Try them for yourself if you like—it's "free."

8. REFERENCES

[1] PrivacyTrust, "Importance of a Privacy Policy." [Online]. Available: http://www.privacytrust.org/guidance/privacy_policy.html. [Accessed: 20-Apr-2013].

[2] Google, "Our history in depth." [Online]. Available: http://www.google.com/intl/en/about/company/history/. [Accessed: 20-Apr-2013].

[3] Google, "Zeitgeist 2012," 2012. [Online]. Available: http://www.google.com/zeitgeist/2012/#the-world. [Accessed: 22-Apr-2013].

[4] "History of Google," Wikipedia. 2013.

[5] Google, "Privacy Policy," 2000. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20000814/. [Accessed: 20-Apr-2013].

[6] Google, "Archive: Privacy Policy." [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/. [Accessed: 20-Apr-2013].

[7] Google, "Privacy Policy – Policies & Principles," 2004. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20040701/. [Accessed: 20-Apr-2013].

[8] Google, "Privacy Policy," 2005. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20051014/. [Accessed: 20-Apr-2013].

[9] Google, "Privacy Policy," 2010. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20101003/. [Accessed: 20-Apr-2013].

[10] Google, "Privacy Policy," 2008. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20080807/. [Accessed: 20-Apr-2013].

[11] Google, "Privacy Policy," 2009. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20090127/. [Accessed: 20-Apr-2013].

[12] Google, "Privacy Policy," 2009. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20090311/. [Accessed: 20-Apr-2013].

[13] Google, "Privacy Policy," 2011. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20111020/. [Accessed: 20-Apr-2013].

[14] Federal Trade Commission, "Analysis of Proposed Consent Order To Aid Public Comment," no. 1023136, pp. 1–3, 2010.

[15] Electronic Information Privacy Center, "Electronic Privacy Information Center." [Online]. Available: http://epic.org/epic/about.html. [Accessed: 22-Apr-2013].

[16] Federal Trade Commission, "FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network," 2011. [Online]. Available: http://www.ftc.gov/opa/2011/03/google.shtm. [Accessed: 20-Apr-2013].

[17] Federal Trade Commission, "FTC Gives Final Approval to Settlement with Google over Buzz Rollout," 2011. [Online]. Available: http://www.ftc.gov/opa/2011/10/buzz.shtm. [Accessed: 20-Apr-2013].

[18] Google, "Policies & Principles." [Online]. Available: http://www.google.com/intl/en/policies/. [Accessed: 20-Apr-2013].

[19] Google, "Privacy Policy," 2012. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/20120301/. [Accessed: 20-Apr-2013].

[20] Google, "Key terms." [Online]. Available: http://www.google.com/intl/en/policies/privacy/key-terms/. [Accessed: 20-Apr-2013].

[21] Google, "Good to Know – A guide to staying safe and secure online." [Online]. Available: http://www.google.com/intl/en/goodtoknow/. [Accessed: 22-Apr-2013].

[22] Google, "FAQ – Policies & Principles." [Online]. Available: http://www.google.com/intl/en/policies/faq/. [Accessed: 20-Apr-2013].

[23] J. T. Rosch, "Concurring Statement of Commissioner J. Thomas Rosch," 2011.

[24] Google, "Security and privacy overview - Google Apps Help," 2013. [Online]. Available: http://support.google.com/a/bin/answer.py?hl=en&answer=60762. [Accessed: 20-Apr-2013].

[25] Metafilter, "User-driven discontent | MetaFilter," 2010. [Online]. Available: http://www.metafilter.com/95152/Userdriven-discontent#3256046. [Accessed: 20-Apr-2013].