Saving Private

The Perils of Google's Profit Model

Nick Heer
Media Arts & Digital Technologies
Alberta College of Art + Design
Calgary, Canada
desk@pxlnv.com

***Abstract*—The foundation of Google's business ventures is targeted advertising. Information usually considered private is used by Google for profits in a way that is detrimental to users.**

Keywords—advertising; Google; Internet; privacy

I. INTRODUCTION

…the existing law affords a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds [1].

Google's policy is to get right up to the creepy line and not cross it [2].

The first epigraph is taken from "The Right to Privacy", an editorial penned by Samuel Warren and Louis Brandeis, and published in the *Harvard Law Review*. It is the foundational text upon which our learned expectations of personal and informational privacy are based [3].This viewpoint is codified in our laws and engrained in our lives. Yet, with the advent of Internet advertising, we have allowed our privacy to be encroached upon if it provides us with desirable services for free. The biggest and, arguably, most influential provider of free services is Google, whose ex-CEO Eric Schmidt provided the second epigraph above. Google is not a technology services company; in 2012, 95% of their revenue was generated through advertising [4]. The ads that the company provides are tailored to individual users by learning their interests and habits across Google's many popular services. While this advertising was relatively innocuous when they were simply a search engine, the company now provides a myriad of products and services: email, calendars, address books, mobile and desktop operating systems, streaming video, online retail, and hardware products designed to accompany users everywhere. In spite of Google's liberal privacy policy [5][6], these products and services are extraordinarily popular, arguably due in large part to their price: free. This paper examines the problematic rise in popularity of Google's products into what most people would consider their private lives, making more public what was once personal, all for profit.

II. BIRTH

Google is the archetypical college dorm success story. Founded at Stanford in 1998 by Larry Page and Sergey Brin [7], the company has since grown to become one of the largest in the world by market capitalization and quarterly revenue [8]. Driving this growth is the transition from a single-product company to one with hundreds; while Google officially acknowledges twelve primary categories [9], third-party lists [10][11] are more comprehensive in their cataloguing of the company's offerings. Google is able to offer the vast majority of these products for free to users [10] owing to their extensive use of advertising: in the 2012 fiscal year, 95% of Google's revenue was from advertisements [4]. Advertising, in general, is not the privacy concern. Rather, it is Google's specific type of advertising, and how they target it.

III. COOKIES

To understand Google's revenue model, it helps to understand how ads have traditionally been targeted in other mediums, such as television, radio, or print. As a rule, advertisers wish to have a high amount of engagement with a specific target audience. In the halcyon days of static advertising, the media company – the radio station, newspaper, or television channel, or the owners thereof – would provide advertisers with a profile of their audience, culled from surveys, local demographics, and other information. This allowed advertisers to gain a better understanding of the audience they were selling to. This is why it's less likely to hear ads for bridal stores on a classic rock station, or see an ad for a monster truck show in a student-run campus newspaper.

The Internet – and, specifically, HTTP cookies – changed all of that. Cookies are small text files stored on a user's computer, each of which can be set and modified by a website when the user visits it [12]. Cookies can come in many forms; a session cookie, for example, remembers user-specific information – such as items in the user's shopping cart – relevant to their current browsing session. Cookies which are set for longer durations are known as persistent cookies. These are used to identify a specific user across multiple sessions of browsing, and are therefore of greater concern with regards to their security and privacy [12].

Since cookies have the possibility to store enough content to specifically identify a user, there are a number of technical guidelines which establish how cookies are set and read [12]. To prevent nefarious websites from reading this information, a cookie may only be read and modified by the domain that set it. There is also a delineation between first- and third-party cookies; the latter refers to a cookie which was set by one domain within the context of another (for example, an analytics cookie set by exampleanalytics.com on a webpage located at mygreatblog.com), though each domain can still only read and write a cookie by the same domain [12].

IV. The Creep

In 2000 [13], Google introduced their AdWords targeted advertisements product. AdWords sets a unique identifying cookie on users' computers which allows for substantially greater accuracy in demographics for the purposes of targeting advertisements. This product was initially limited to the text-only ads shown on search results pages, back when Google was just a search engine. But this advertising strategy grew with their product range, giving Google access to staggering amounts of personal data from each of their users.

As they launched, each product was governed by its own privacy policy. That is to say that information gleaned from a user's interaction with YouTube videos could not inform the ads that appeared alongside their Gmail messages, for example. This is a privacy-conscious and responsible way of ensuring that targeted advertising is sufficiently controlled. In March of 2012, however, Google decided that the multitude of privacy policies across their products was unwieldy and inefficient, and began a process to consolidate the privacy policies and end-user agreements into one unified policy [14] [15]. Rather than treating each product as an individual unit, products were now treated as services under a common "Google" product. Therefore, the company argued, advertisement targeting data could be bundled together. Ads on Gmail could now be informed by what a user clicked through to on Google, what blogs the user read on Blogger, and — yes — what YouTube videos they watched. There are exceptions to this revised privacy policy. Business customers, for example, are not affected [16], and the policy does not pertain to Wallet, Google Chrome, or Books [17]. But to the millions of ordinary users of Google's products, this represented a radical shift in users' expectations of the gathering and use of their information. It was such a significant change that the European Union believed that it did not comply with European law [18].

V. A History of Gaffes

This policy shift would be somewhat concerning even if Google were a company with an exemplary track record; as it is, the company has engaged in egregious violations with regard to their users' expectations of privacy.

In 2010, Google launched Buzz, a Twitter-esque microblogging product. Upon signing up with a Gmail account, a user's entire contact list was automatically built and made public based on their Gmail contacts [19]. For journalists, this would mean exposing their sources; for others, it could mean exposing frequent contact with a competitor's recruiter to their boss [20].

In 2012, Stanford student Jonathan Mayer found that Google used a subtle technique to circumvent the default cookie settings of Apple's Safari browser, which are set to block third-party cookies [21]. While Safari represents just 5.31% of the desktop browser market, the same cookie settings are the default on iPhones and iPads, with 61.79% of mobile browser usage [22]. *The Wall Street Journal* published a report which corroborated this finding, after which Google turned off the script [23]. A resulting investigation by the FTC resulted in a $22.5 million fine for the company [24].

Perhaps the most blatant disregard for user privacy began in 2006, when a Google engineer added some code to their Street View photo cars which collected data from non-password-protected WiFi networks [25]. In 2010, Google disclosed that they had been collecting this data after German authorities asked them to audit their code [25][26]. As of April 22, 2013, Google was being investigated in over a dozen countries worldwide for this breach of privacy. In the United States, Google settled for $7 million [27]; in Germany, they were fined nearly $200,000 [28], though the Hamburg Commissioner for Data Protection lamented his inability to fine them a greater amount:

In my estimation this is one of the most serious cases of violation of data protection regulations that have come to light

so far. Google did cooperate in the clarification thereof and publicly admitted having behaved incorrectly. It had never been the intention to store personal data, Google said. But the fact that this nevertheless happened over such a long period of time and to the wide extent established by us allows only one conclusion: that the company internal control mechanisms failed seriously. [29]

With this grievous and blatant flouting of their power in the market and their vast amount of user data, it is difficult to become comfortable with Google's revised privacy policy. I posit that this amount of information in the hands of a government agency, for example, would be met with widespread disagreement, though it is seen as reasonable in the more private hands and servers of Google. Whether this is because governments direct make policy decisions in a way that private corporations do not, or due to our perception of capitalism, or for whatever reason is up for debate, and is worthy of its own paper. However, it is a position worth pondering.

VI. Distinct Advantages

Make no mistake – this attitude of fewer barriers between user information allows Google to create products which innovative in a way that their more privacy-conscious competitors never could. In 2012, Google launched Google Now, a new layer of their Android mobile operating system. The application combs through the user's email, calendar, and web browsing history, and it even tracks routine locations – for example, the user's daily commute. It then tries to predict what the user will be interested in based on location, time, and other factors, and displays relevant information on "cards". For example, if an airline ticket is found in the user's email and the user is at or near the airport, invoking Google Now will display a card with the gate number and departure time, without any additional user interaction. As another example, when the user wakes up in the morning, Google Now can display areas of bad traffic along their commute, and suggest alternate routes. This product is only possible through Google's revised policy which allows them to consolidate and share information across multiple Google services.

Google is, of course, not the only technology company with severe privacy concerns. Like Google, Yahoo sells inline ads against the contents of email messages. The case of Facebook is interesting, too. The social network has come under fire since it was launched for its unique combination of encouraging users to share as much information as possible, its byzantine privacy controls, and its selling of information to advertisers [30][31][32].

Furthermore, there are some privacy-infringing services that are less visible to users. Scripts by analytics firms such as ComScore, Quantcast, Scorecard Research, and Chartbeat are used on many popular websites to acquire demographics information [33][34]. Because these scripts are used across so many websites, the aggregate amount of information they collect is hard to measure, but is likely significant. Quantcast, for example, brags that their tracking script is in use on TMZ, Gawker, the Economist, Tumblr, and a plethora of other high-traffic websites [33].

In addition, there are offline privacy concerns along similar terms. In February of 2012, the New York Times published an article explaining how US retailer Target sends coupons based on expected shopping patterns on a per-visitor basis:

One Target employee I spoke to provided a hypothetical example. Take a fictional Target shopper named Jenny Ward, who is 23, lives in Atlanta and in March bought cocoa-butter lotion, a purse large enough to double as a diaper bag, zinc and magnesium supplements and a bright blue rug. There's, say, an 87 percent chance that she's pregnant and that her delivery date is sometime in late August. [35]

As the technology becomes available to quantify our practices, routines, and purchases, it's unlikely that this level of data collection will recede.

But while Google is by no means the only company with a concerning attitude towards individual user privacy, it is one of the most engrained in consumers' Internet usage. The search engine itself represents 67.5% marketshare according to ComScore [36], while YouTube receives nearly three times the viewers as its nearest competitor [37]. The ostensibly simple response to these privacy concerns is to stop using Google services, but that's extremely difficult. Given that the products are reliable and are offered at the unbeatable price point of "free", it becomes both expensive and risky to migrate to other services. The alternatives to Google's services [38][39] tend to be of either dubious reliability or poorer quality, and most are not free. This places Google in a special position of power, and therefore, responsibility.

VII. Saving Private

Owing to Google's demonstrable dominance in the markets in which they compete, it should be of paramount concern for users that they accept the responsibilities that are part of that package. They are a company with an unimaginable amount of private data sitting in server farms

worldwide. Users need finer-grained controls over the use and release of this private data within Google's applications and products, but this presents the challenge of designing a user interface that is straightforward enough for users – a challenge with which Facebook, for example, is struggling [40]. While Google does provide a mechanism for entirely opting out of targeted advertising [41], it is difficult to find; perhaps this is intentional, given the business model the company has chosen.

These problems, however, are not unsurmountable. Google is a notoriously difficult company at which to gain employment. They attract some of the cleverest and most learned engineers in the world, and should therefore have the skills to design a better end-user-privacy situation. But, as their revenue model almost entirely relies upon users' willingness to cede their right [42] to privacy online, they are unlikely to change without significant pressure from the outside, whether it is from regulatory agencies, or from users' demands.

As noted prior in this paper, Google has already been subject to fines from the FTC and other regulatory agencies – their $7 million settlement for Street View's WiFi data sniffing being the latest. But to a company that has a net income of $10.7 billion on revenues of $50.1 billion [4], a $7 million fine is somewhat inconsequential. That fine is proportionally akin to $7 on a moderate annual household income of $50,000 – hardly a significant motivator of change.

However, regulatory bodies should not have to resort to fining companies which break ever-ageing privacy laws. All websites which use private data need to be forthcoming. Users should be able to understand and consent to the use of tracking or other cookies prior to the website setting them, and be provided the option to opt-out if they disagree. The United Kingdom attempted to do this by requiring websites which set cookies to disclose their use upon arriving at the website [43]. However, hours before the law was to take effect, it was amended to add "implied consent" to the allowable consent types, effectively rendering the law meaningless [44]. Further neutering laws to this effect is the inability for the Internet to be regulated – consider any law that has ever passed regarding online piracy, for example.

What this means, in effect, is that an entire viewpoint shift needs to occur for users if they value their private information. All Internet users need to be aware of the use of cookies, tracking scripts, and demographic analytics firms, and they must demand better management of this from the websites they frequent. Only then is there a hope that a response can be elicited, and websites can take their users' privacy with appropriate gravity. As a temporary measure, users should ensure that their web browser is set to block cookies from third-party sources.

Without these measures, the control of web users' personal information is at the behest and whim of companies which will only get more powerful as the Internet permiates deeper into our routines and our lives. The relinquishing of our control of what can be used to individually identify us is not an inevitable tradeoff. These issues can be mitigated with the appropriate attention and action they deserve.

References

[1] S. D. Warren and L. D. Brandeis, "The right to privacy," *Harvard Law Review*, vol. 4, no. 5, pp. 193-220, 1890.

[2] D. Thompson. (2010, October 1) *Google's CEO: 'the laws are written by lobbyists'*. [Online]. Available: http://www.theatlantic.com/technology/archive/2010/10/googles-ceo-the-laws-are-written-by-lobbyists/63908/

[3] D. V. S. Kasper, "The evolution (or devolution) of privacy," *Sociological Forum*, vol. 20, no. 1, pp. 69-92, 2005.

[4] (2012) *Google Inc. Form 10-K*. [Online]. Available: http://www.sec.gov/Archives/edgar/data/1288776/000119312513028362/d452134d10k.htm

[5] R. Reitman. (2012, February 1) *What actually changed in Google's privacy policy*. [Online]. Available: https://www.eff.org/deeplinks/2012/02/what-actually-changed-google's-privacy-policy

[6] (2012, July 27) *Privacy policy - policies & principles* - Google. [Online]. Available: http://www.google.com/intl/en/policies/privacy/

[7] (2013) *Company - Google*. [Online]. Available: http://www.google.com/about/company/

[8] (2013) *Google on the Forbes Global 2000 list*. [Online]. Available: http://www.forbes.com/companies/google/

[9] (2013) *Google - products*. [Online]. Available: http://www.google.com/intl/en/about/products/

[10] (2013) *Exhaustive Google product list*. [Online]. Available: https://spreadsheets.google.com/pub?key=ty_BGDs9hnuBMRvj3AFeB2g&output=html

[11] M. Mohan. (2012, October 1) *Over 101 Google products and services you probably don't know*. [Online]. Available: http://www.minterest.com/60-google-products-services-you-probably-dont-know/

[12] A. Barth. (2011, April) *HTTP state management mechanism*. [Online]. Available: http://tools.ietf.org/html/rfc6265

[13] (2000, October 23) *Google launches self-service advertising program*. [Online]. Available: http://googlepress.blogspot.ca/2000/10/google-launches-self-service.html

[14] (2012) *Archive: privacy policy*. [Online]. Available: http://www.google.com/intl/en/policies/privacy/archive/

[15] A. Whitten. (2012, January 24) *Updating our privacy policy and terms of service*. [Online]. Available: http://googleblog.blogspot.ca/2012/01/updating-our-privacy-policies-and-terms.html

[16] J. Brodkin. (2012, March 1) *Google's new privacy policy: what has changed and what you can do about it*. [Online]. Available: http://arstechnica.com/tech-policy/2012/03/googles-new-privacy-policy-what-has-changed-and-what-you-can-do-about-it/

[17] S. Vankin. (2012, March 1) *Five ways Google's unified privacy policy affects you*. [Online]. Available: http://howto.cnet.com/8301-11310_39-57388626-285/five-ways-googles-unified-privacy-policy-affects-you/

[18] (2012, March 1) *Google privacy changes 'in breach of EU law'*. [Online]. Available: http://www.bbc.co.uk/news/technology-17205754

[19] R. Mansfield. (2010, February 12) *Google's Buzz has 'serious privacy flaws'*. [Online]. Available: http://news.sky.com/story/758801/googles-buzz-has-serious-privacy-flaws

[20] N. Carlson. (2010, February 10) *Warning: Google Buzz has a huge privacy flaw*. [Online]. Available: http://www.businessinsider.com/warning-google-buzz-has-a-huge-privacy-flaw-2010-2

[21] J. Mayer. (2012, February 17) *Safari trackers*. [Online]. Available: http://webpolicy.org/2012/02/17/safari-trackers/

[22] L. Whitney. (2013, April 1) *Safari jumps to 61 percent of mobile browser share*. [Online]. Available: http://news.cnet.com/8301-1035_3-57577246-94/safari-jumps-to-61-percent-of-mobile-browser-share/?part=rss&tag=feed&subj=

[23] J. Angwin and J. Valentino-Devries. (2012, February 17) *Google's iPhone tracking*. [Online]. Available: http://online.wsj.com/article/SB10001424052970204880404577225380456599176.html?mod=WSJ_hp_LEFTTopStories

[24] J. Angwin. (2012, July 10) *Google, FTC near settlement on privacy*. [Online]. Available: http://online.wsj.com/article/SB10001424052702303567704577517081178553046.html

[25] A. Eustace. (2010, May 14) *WiFi data collection: an update*. [Online]. Available: http://googleblog.blogspot.ca/2010/05/wifi-data-collection-update.html

[26] A. Efrati and D. Clark. (2012, April 29) *Google engineer told others of data scoop*. [Online]. Available: http://online.wsj.com/article/SB10001424052702304868004577374272894249402.html

[27] (2013, March 12) *Attorney General announces $7 million multistate settlement with Google over Street View collection of WiFi data*. [Online]. Available: http://www.ct.gov/ag/cwp/view.asp?Q=520518&A=2341

[28] C. Farivar. (2013, April 22) *Germany fines Google a paltry $189,000 over Street View WiFi scanning*. [Online]. Available: http://arstechnica.com/tech-policy/2013/04/germany-fines-google-a-paltry-189000-over-street-view-wi-fi-scanning/

[29] (2013, April 22) *Fine imposed upon Google*. [Online]. Available: http://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/PressRelease_2013-04-22_Google-Wifi-Scanning.pdf

[30] A. J. Tabak. (2004, February 9) *Hundreds register for new Facebook website*. [Online]. Available: http://www.thecrimson.com/article/2004/2/9/hundreds-register-for-new-facebook-website/

[31] L. Story. (2007, November 30) *Coke is holding off on sipping Facebook's Beacon*. [Online]. Available: http://bits.blogs.nytimes.com/2007/11/30/coke-is-holding-off-on-sipping-facebooks-beacon/

[32] R. Esguerra. (2010, April 28) *A handy Facebook-to-English translator*. [Online]. Available: https://www.eff.org/deeplinks/2010/04/handy-facebook-english-translator

[33] (2013) *Quantcast measure participants*. [Online]. Available: http://www.quantcast.com/measurement/quantified-publishers/

[34] (2013) *Chartbeat*. [Online]. Available: http://chartbeat.com

[35] C. Duhigg. (2012, February 16) *How companies learn your secrets*. [Online]. Available: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?&pagewanted=all

[36] M. McGee. (2013, March 13) *Google, Bing both gain market share in February [ComScore]*. [Online]. Available: http://searchengineland.com/google-bing-both-gain-market-share-in-february-comscore-151523

[37] (2013, April 25) *ComScore releases March 2013 U.S. online video rankings*. [Online]. Avalable: http://www.comscore.com/Insights/Press_Releases/2013/4/comScore_Releases_March_2013_U.S._Online_Video_Rankings

[38] T. Henderson. (2013, April 1) *My divorce from Google – one year later*. [Online]. Available: http://www.itworld.com/software/350485/my-divorce-google-one-year-later

[39] B. Brooks. (2013, March 25) *You can't quit, I dare you*. [Online]. Available: http://brooksreview.net/2013/03/quit-i-dare-you/

[40] D. Gross. (2012, December 12) *Facebook to overhaul its privacy controls*. [Online]. Available: http://www.cnn.com/2012/12/12/tech/social-media/facebook-privacy-changes

[41] (2013) *Ads preference manager*. [Online]. Available: http://www.google.com/ads/preferences

[42] (2013) *Do you have a legally protected right to online privacy?* [Online]. Available: http://www.abine.com/yourrights.php

[43] Z. Whittaker. (2012, May 26) *UK 'cookie law' takes effect: what you need to know*. [Online]. Available: http://www.zdnet.com/blog/london/uk-cookie-law-takes-effect-what-you-need-to-know/4910

[44] C. Arthur. (2012, May 26) *Cookies law changed at 11th hour to introduce 'implied consent'*. [Online]. Available: http://www.guardian.co.uk/technology/2012/may/26/cookies-law-changed-implied-consent