Our private data and the market for third-party providers of functionality to websites

Your personal information is out there. You did not give it out, so how did it get there? Internet websites provide visitors with different levels of interaction, ranging from delivering basic information to providing sophisticated features and tools such as profile management, interactive visual communication, and of course, advertising. Like many traditional businesses, websites turn to **third-party outsourcing** to offer these features and tools. Such services include functionality (password and account control, social media integration, video hosting, chat and forum services, payment services, etc.), performance (backup service, security and firewalls, responsiveness tools, etc.) and targeting/advertising (advertising, lead generation, analytics, etc.).

Use of third parties is ubiquitous among top websites. A website visitor is also making contact with all third parties enabled on the site. Much of this contact is hidden from view. A U.S. Senate report found that visits to online news sites may involve connecting with hundreds of other parties, and "[t]he sheer volume of such activity makes it difficult for even the most vigilant consumer to control the data being collected or protect against its malicious use."

While many third parties provide utility or functionality for visitors, they also pose a potential privacy risk. A simple example is the integration of the Google Maps API within a website, where Google obtains valuable location data. Third parties often obtain visitor information in return for services they provide to the website. This is often done without explicit visitor consent and/or disclosure. Policies regarding how visitor information is shared with third parties are often hidden in obscure and lengthy privacy statements and/or terms of use, and are often ignored or blindly accepted by visitors. Simply landing on a website can cause substantial and instantaneous sharing with third parties.

The convenience of easy sign-ins with Facebook, Google, or Twitter accounts results in immediate identification with these third parties. Third parties also use cookies and other emerging tracking technologies such as flash cookies and device IDs to track individuals across much of their online activity. The reduced cost of data storage and processing technologies has allowed third parties to stockpile large amounts of visitor data and run analytics on this data. Due to the sheer number of third parties that perform analytics and targeting, and the advanced technologies they use, it is now very hard to know who is tracking us online.

Through rapid advancement in analytical techniques, third parties are able to create fairly comprehensive pictures of not only individual behaviour, but also of individual psychological traits. An individual's online activity is being tracked across the web, and through re-identification, this activity can be merged with other aspects of our lives. For many, this sounds like an Orwellian prophecy coming true.

This begs the question, "What's going to limit this privacy intrusion?" Privacy issues related to online websites, third-party use, and tracking an individual's activity is a public concern. Regulatory organisations such as the Federal Trade Commission and the European Union are looking into policy enforcement strategies. The other method of limiting this privacy intrusion is through the invisible hand of the market itself. Our work focuses on the possibility that websites dealing with visitors who are more concerned about their privacy will be faced with a market that curbs their behaviour.

We conceptualise websites as having two sources of income, through subscriptions and through selling visitor data to third parties. A website using the subscription model needs a large base of visitors, but it can also sell visitor information in secondary markets through advertising or other third parties. Therefore, the website must strike a balance between subscription and third-party monetisation in this two-sided market.

Our analysis indicates that when visitor privacy concerns for a website are high relative to the competition, the website will have a smaller niche market of customers willing to pay high subscription prices in exchange for privacy protection. At the other extreme, a website facing low visitor privacy concerns can tap into a larger market of customers willing to exchange their personal information to access the website. We find that the website's profits are highest when visitors have moderate privacy concerns – not too low and not too high – especially when the competition faces very high privacy concerns.

We also analyse how the third-party industry structure is impacted by visitor privacy concerns. We find that higher visitor privacy concerns will result in the website using fewer third parties, and the result is a higher concentration in the third-party market for that industry. Higher industry security requirements result in higher barriers to entry, which also increase the industry concentration of third parties.

Our empirical findings of the third-party market corroborate the finding that third-party concentration is higher in markets with high privacy concerns. Ironically, in a concentrated market, the fewer, but more powerful third parties collect data from many websites. These third parties gain a more comprehensive visitor profile, which has greater value, but also greater privacy risk to visitors.

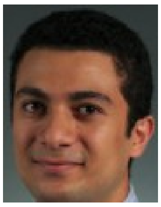
We recommend that policy makers and regulatory organisations monitor the third-party market for potential privacy violations in markets with high privacy concerns such as healthcare. Additionally, requiring transparency with respect to the exact third parties and the types of data they are receiving would allow consumers to make better decisions regarding their privacy. Adding tracking features for consumers to see where their data goes beyond these third parties would create additional and potentially important transparency. Currently, there is effectively no tracking of where your data goes and no ability for a consumer to know what is done with their data.

♣♣♣

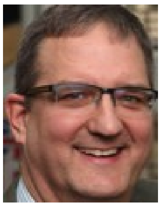
Notes:

- *This blog post is based on the authors' paper* How Much to Share with Third Parties? Users' Privacy Concerns and Website's Dilemma, MIS Quarterly, forthcoming
- *The post gives the views of the authors, not the position of LSE Business Review or the London School of Economics.*
- *Featured image credit: Electronic Frontier Foundation (eff.org) graphic created by EFF senior designer Hugh D'Andrade, under a CC-BY-3.0 US licence, via Wikimedia Commons.*
- *When you leave a comment, you're agreeing to our Comment Policy.*

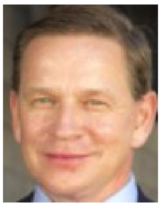
Ram D. Gopal is GE Capital Endowed Professor of Business and Head of the Department of Operations and Information Management in the School of Business, University of Connecticut. His current research interests are in the areas of big data analytics, information security, privacy and valuation, intellectual property rights, online market design and business impacts of technology. His research has appeared in *top academic* journals and conference proceedings. He can be reached at *ram.gopal@uconn.edu.*



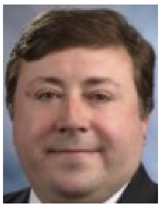
Hooman Hidaji is an Assistant Professor of Business Technology Management at the Haskayne School of Business, University of Calgary. His current research interests include information systems security, online privacy, and third party sharing of visitor information. Hooman's publications appear or are forthcoming in top academic journals. He can be reached at *hooman.hidaji1@ucalgary.ca.*



Raymond A. Patterson is Area Chair and Professor of Business Technology Management at the University of Calgary, and a Visiting Professor at the University of Alberta. He conducts research in the fields of analytics, health-care, information systems, operations management and service science. Ray has published extensively in premier journals. He can be reached at *raymond.patterson@ucalgary.ca.*



Erik Rolland is Dean and Professor with the College of Business Administration at California State Polytechnic University, Pomona. He conducts research in the fields of analytics, health-care, information systems, operations management, and service science. His research has appeared in a number of leading academic journals. He can be reached at *erolland@cpp.edu*.



Dmitry Zhdanov is an Assistant Professor of Computer Information Systems with J. Mack Robinson College of Business at Georgia State University. His research interests include information security and privacy, large-scale data analysis, design of intelligent agents, green IT, and social impacts of information technology. His research has appeared in leading journals. He can be reached at *dzhdanov@gsu.edu.*

Date originally posted: 2017-10-16

Permalink: http://blogs.lse.ac.uk/businessreview/2017/10/16/our-private-data-and-the-market-for-third-party-providers-of-functionality-to-websites/

Blog homepage: http://blogs.lse.ac.uk/businessreview/