Perspectives on Academic Impact from Inside the Federal Trade Commission

Michael Brennan

Drexel University, Computer Science Department,
3141 Chestnut Street, Philadelphia, Pennsylvania

Abstract

The privacy field of academic computer science produces a large body of work with potential for impact on the lives of end users. An important avenue for this impact, and one of the most overlooked, is the Federal Trade Commission (FTC). This paper summarizes the impact that academic research has had in recent years on the policies, actions and opinions of the FTC and proposes approaches for increasing the impact of academic work. It also analyzes contributions of the non-academic research communities, argues for greater acceptance of action by the FTC and similar agencies as an impact measurement in academia, and details roadblocks that limit bridge-building between government and academia. The author has been is a staff technologist for the FTC's Division of Privacy and Identity Protection.

1 Disclaimer

The author has worked for the Federal Trade Commission since August of 2010. This paper reflects the personal opinions of the author and not the official opinions or positions of the Commission or the United States.

2 Introduction

How does academic privacy research result in real-world privacy protection or enhancement? This question of impact is not just an issue of broader research impact but a fundamental scientific research question in the field of privacy. A major means to accomplish impact is through existing regulation and oversight institutions. The call for papers for the Workshop on Privacy in Electronic Society points this out explicitly: "The need for privacy-aware policies, regulations, and techniques has been widely recognized" [7].

One approach towards achieving privacy is through action at the Federal Trade Commission (FTC or the Commission). The FTC is the only federal regulatory agency in the United States with jurisdiction over general privacy concerns. It has the authority to take action against companies with unfair or deceptive privacy practices through a variety of means including investigations resulting in orders that seek to correct the issue and set precedent for best practices. The FTC also has impact beyond the United States through action concerning multinational companies and cooperation with international data protection agencies[1].

The FTC has taken a number of influential actions in recent years to address allegedly deceptive and unfair privacy practices. These include consent orders against search and advertising giant Google [20], social media service Twitter [1], and the ad network Chitika [5]. Results of these orders include mandating independent privacy audits over the course of 20 years for Google and 10 years for Twitter, and requiring

[1] FTC Office of International Affairs `www.ftc.gov/oia/`

a link to opt out of targeted advertising in ads served by Chitika. The Commission has also issued an influential staff report proposing a new framework for protecting consumer privacy [9], representatives of the Commission have spoken on privacy issues in a number of major forums [23, 24] including the US Congress, and the Commission has regularly issued consumer education reports concerning technical privacy and security threats [10].

Identifying violations, anticipating harmful business practices, and protecting consumer privacy in technical domains takes a large amount of resources. The FTC does not have a dedicated technical research arm for privacy matters. A number of the actions and investigations carried out by the FTC are initiated by work in the academic and independent privacy and security research communities. Unfortunately I do not believe these communities realize the extent to which the FTC listens and relies upon their work. I base this assertion on my personal experience as a technologist at the Division of Privacy and Identity Protection. I have interacted with many researchers on current technical privacy issues and more often than not I am met with surprise that the FTC is knowledgeable and interested in these issues.

The primary impediment to research communities understanding and recognizing the impact of their work at the FTC is the fact that all ongoing investigations are nonpublic. The only point at which an investigation becomes public is in the case where a matter is settled or publicly closed. Many more issues never see the light of public scrutiny because they are closed or resolved privately. While unfortunate, this is a necessary aspect of the work of the FTC. An investigation into privacy-related events or actions of a company is not an implicit assertion of that company's guilt. It is my opinion, based on my experience, that the FTC recognizes the market impact of an investigation and does not wish to unjustly punish business based on an accusation.

Another issue is the lack of a consistent bridge between technical academia, independent researchers and the FTC. The FTC is a legal organization and, as such, builds most of its bridges with legal academia. The FTC has not maintained a significant presence at technical academic conferences. It makes sense that there is a lack of recognition among academics that their work can – and does – significantly affect the policy of the FTC. Only recently with the introduction of Ed Felten as Chief Technologist has the Commission began to build a bigger bridge to the technical sectors of academia.

3 The Federal Trade Commission

The Commission was established by the Federal Trade Commission Act of 1914. While the original goal was to regulate unfair competition, Congress has expanded the Commission 's powers to include a number of consumer protection issues. The FTC is divided into the Bureaus of Competition, Economics and Consumer Protection. The FTC is presently the only federal agency general jurisdiction over unfair and deceptive privacy practices in the United States. Much of this is done through the Bureau of Consumer Protection and its Division of Privacy and Identity Protection.

3.1 Division of Privacy & Identity Protection

The Division of Privacy and Identity Protection (DPIP) is the most recent division to be added to the Bureau of Consumer Protection. In addition to Section 5 of the FTC Act, DPIP also enforces the Fair Credit Report Act (FCRA) and the Gramm-Leach-Bliley Act. The FCRA gives consumers the right to know what information credit bureaus and consumer reporting agencies have on them. The Gramm-Leach-Bliley Act requires financial institutions to maintain the security and confidentiality of customer information.

Action at DPIP does not only take the form of investigations into illegal business practices. Consumer and business education, legislative analysis, white papers, policy outreach, and public speeches are just some examples of the tools at the disposal of DPIP and the FTC in general.

3.2 Mandate and Authority

A significant number of DPIP investigative actions regarding privacy are based on section 5 of the FTC Act. Specifically the statute that states "unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful" [12].

Deception can take many forms but it is generally considered to be a misleading representation or an omission that is counter to a reasonable consumer's expectations. In the privacy or data security context, this might be an undisclosed practice that is counter to the representations made to consumers. One example is the case of Chitika where a mechanism was presented to consumers for opting out of behaviorally targeted advertising but the opt-out cookie expired 10 days after receipt [5]. Poor data security practices despite a representation that the privacy and security of a consumer will be protected may also be deceptive, as in the case of Twitter's failure to protect the personal information of consumers despite stating that they took a number of measures to protect this it from unauthorized access [4].

Unfairness generally means a demonstration of actual harm to consumers, not speculative harm. This may come in the form of financial harm, such as tricking consumers into purchasing fraudulent or unwanted goods or services, or, in some cases, emotional harm such as that which might occur due to exposure of sensitive health information.

4 Academic Impact at the FTC

The work performed by the FTC is greatly facilitated by input from academic research communities, journalists, and independent researchers. The role of academia is particularly important. Computer science publications lend facts and credibility to FTC action. This is often overlooked in academic circles despite the significant real world impact that takes place as a result of some publications. This section highlights some of the important work by academics and independent researchers that have informed FTC actions.

4.1 Demonstrated Impact in Investigations

Investigations within the FTC can become public in a few ways but the most common are through complaints that lead to settlement or litigation and through closing letters. In March of 2010 the FTC made public its investigation into Netflix by way of a closing letter [15]. The letter states the concerns of the FTC about the risk of re-identifying anonymized data in the second Netflix Prize data set. In addition to a citation of Narayanan and Schmatikov's work on the subject, the first such citation of an academic computer science paper in any closing letter by the commission, the FTC also cited work by Paul Ohm titled "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" [19]. While Ohm's work was published in a legal venue, the UCLA Law Review, it is reliant on a bed of research by computer scientists that demonstrates the widespread use of ineffective anonymization techniques.

Direct references to academic research in documentation from the Commission is not the only way to identify impact. Oftentimes investigations are spurred by well documented complaints by organizations such as the Electronic Fronteir Foundation (EFF) and Electronic Privacy Information Center (EPIC). The recent investigation and subsequent settlement between the FTC and Facebook [6] followed a complaint by a coalition of consumer groups led by EPIC [2, 21]. The complaint cites a number of academic work, such as Arvind Narayan and Vitaly Schmatikov's work, "De-anonymizing Social Networks" [17] and writing by Ed Felten of Princeton University [11].

4.2 Impact in the 2010 Privacy Report

In December of 2010, the FTC issued a report entitled, "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policy Makers" [9]. It proposes a framework for balancing privacy with innovation based on consumer information. It reflects the FTC staff's position regarding current consumer privacy concerns.

The privacy report has had substantial impact in the area of consumer privacy. Over 450 public comments were submitted by multinational corporations, special interest groups and individual consumers. Comments by Microsoft, Google, AT&T, and Facebook illustrate the influence of the report and the FTC in general. Many of these comments note the impact that the FTC has had in recent years, including Google statement that "The Commission has been instrumental in discouraging practices that are harmful or deceptive and undermine user trust... Google supports the Commission's promotion of a framework to guide the privacy efforts of all commercial entities, coupled with continued consumer education and enforcement against bad practices." [3].

Every citation and footnote in the report indicates serious discussion over a specific issue and, in the case of research papers, reflects substantial impact on the policy being outlined in the report. A citation in the report indicates strong influence within the Commission. This is unlike many academic papers where a citation may simply be a passing acknowledgement of previous work. The end goal of research, especially with the field of privacy, is to effect change in the world. In those terms a citation in an FTC order or major report is near the highest form of real world impact and should thus be considered a high form of academic impact.

The report also received widespread media coverage including a space at the top of the front page of the New York Times [18]. It is not often that academic computer science research directly supports high profile media coverage.

The Commission's report cites several specific academic works. McDonald and Cranor's 2008 work, "The Cost of Reading Privacy Policies" [14], is used to support the Commission staff's opinion that lengthy privacy policies do not enable a consumer's ability to make informed privacy decisions. Egelman et. al. demonstrated that consumers were willing to pay more in exchange for better privacy protections in their 2009 CHI paper, "Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators" [8]. This work is used to support the FTC staff's argument that customers are uncomfortable being tracked and that they are willing to sacrifice potential benefits in order to maintain a greater level of privacy. Narayanan and Schmatikov's 2008 paper at the IEEE Symposium on Security and Privacy, "Robust De-anonymization of Large Sparse Datasets" was the foundation of DPIP's technical understanding of the privacy implications of a large data set released by Netflix [16].

The privacy report uses academic papers in exactly the way they are supposed to be used: as scientific evidence to inform and support a factually sound understanding of technical policy issues. These papers do not present an agenda, they present facts. And, ideally, these facts will serve as a foundation for effective policymaking.

4.3 Other Demonstrations of Impact

David Vladeck, the director of the Bureau of Consumer Protection, has spoken multiples times on the surreptitious collection of private information through a method known as "CSS history sniffing" [23, 24]. In speeches to both the International Association of Privacy Professionals and the Consumer Watchdog Conference, Vladeck revealed the influence of Jang et. al.'s "An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications" published at CCS 2010 [13].

The FTC played a major role in closing down the ability for malicious websites to exploit CSS in order to mine the history of unsuspecting visitors. Browser vendors were urged to tackle the exploit which had

been known for nearly a decade but not seen in widespread use until recently. Jang's paper illustrated the popular use of this tactic and that persuaded the FTC to take action.

The FTC also regularly brings in speakers from the academic research community. The Commission's technologists are responsible for arranging technical speakers on issues relating to both specific investigations and generally relevant privacy and security issues. While these talks are not officially nonpublic, they are not formally announced to avoid indicating potential investigative agendas. The privacy roundtables of 2009 and 2010 indicate the level of interest the Commission has in bringing in knowledgeable academics with speakers such as Alessandro Acquisti, Fred Cate, Lorrie Cranor, Peter Eckersley, Arvind Narayanan, and many others[2]. Academic researchers have also testified in front of members of the Commission, such as Aleecia McDonald [22].

4.4 Influence by Non-Academic Research

While the focus of this paper is on academic publications that directly impact policy, research that falls outside of the published academic record is also vital. Security researchers, hackers, and independent journalists have a long history of ties with the academic privacy and security community as can be seen through a number of conferences such as Chaos Communication Congress, Hacking at Random, DEFCON and organizations like the Electronic Frontier Foundation, Chaos Computer Club and the Tor Project.

The FTC staff privacy report cites Samy Kamkar's *evercookie*[3] to demonstrate the potential for pervasive online tracking beyond the commonly recognized method of utilizing third party cookies [9]. In fact, this citation is directly followed by the most publicized aspect of the report, a call for a single comprehensive mechanism to opt out of online behavioral advertising commonly known as "Do Not Track."

The FTC's Division of Consumer and Business Education regularly issues reports on current threats and countermeasures through OnGuard Online, a repository for consumer education[4]. "Wise Up about Wi-Fi: Tips for Using Public Wireless Networks" warned consumers about the dangers of unencrypted connections over public wireless networks [10]. The report specifically cited the EFF's HTTPS-Everywhere and Sid Stamm's Force-TLS add-ons for Firefox as mechanisms that can be used to help mitigate this threat.

5 Increasing Influence and Impact

The Commission does not have a technical research arm for privacy matters. In fact, as of this writing there are only two staff technologists for the entire commission, excluding IT staff. There are varying numbers of technically savvy staff or interns at different times but in general it is up to non-technical staff to read and understand much of the technical literature that exists relating to privacy and data security.

Academic influence at the Commission, and policy and enforcement agencies in general, would be improved by being aware of the a non-technical audience of your paper and accompanying technical literature with memos that explain the research and implications to that audience.

An accompanying memo should contain three elements. The first is an understanding of current trends within the target agency and how the work fits in or, if it doesn't fit, why it is important and how it relates to the mandate of the agency. In the case of the FTC, browsing the recent list of actions[5] and closing letters[6] can be a good indicator, as can recent speeches delivered by Commissioners and FTC staff[7].

[2] www.ftc.gov/bcp/workshops/privacyroundtables
[3] http://samy.pl/evercookie
[4] www.onguardonline.gov
[5] www.ftc.gov/opa/index.shtml
[6] www.ftc.gov/os/closings/
[7] www.ftc.gov/speeches/speech1.shtm

The second element is an understanding of the basic legal theories that influence the target organization and how that may fit with your work. It can be difficult for staff to understand how a technical issue translates to an actionable item. For the FTC, understanding the concepts of deception and unfairness, legal jurisdictions, and history of action in the area, if any, will increase the likelihood for impact.

The third is a general focus on the scope and impact of your work in the context of the target audience. How does it fit into the big picture? With the FTC, answer questions like "How does this directly affect consumer privacy choices?" And "why does this matter to my parents?" not "why does this matter to a computer scientist?"

Overall, the most important action to take is to talk to people at the FTC and other relevant agencies. Start with the staff technologists to explain your work to initially. Contact staff members who have worked on previous cases you are interested in or that might be relevant. And finally, remember that this memo is also helpful in widely disseminating your work to journalists and non-technical audiences in general.

6 Conclusions

As researchers we can easily forget that the ultimate audience for our work is not the program committee of the next conference or the members of a tenure committee. This is especially true in the field of privacy where research is often intended to directly inform technically sound policy decisions for everyone from national government to an end user.

The question of broad impact is a fundamental research question in privacy and security. How to get users to make good privacy and security decisions, encourage governments to adopt effective policies, and the pursuit of meaningful regulation are important scientific questions. As such, work in the privacy and security fields being adopted or cited by the Commission and other governmental bodies that have a direct role in these questions should be considered the same, depending on the specific instance, as invited talks, conference publications and journal publications.

The broader impact of important privacy and security research is served by greater communication and cooperation between the academic community and the FTC. Technologists at the FTC are seeking to build upon this bridge by bringing in more academic research and speakers into the decision making processes of the Commission. Building this bridge can also come through the invitation of government participation in conferences by way of speakers and presence on program committees. There are legal conflicts of interest to be aware of but these can be navigated by organizers communicating with government representatives and allowing them extra time to obtain approval for participation.

7 Acknowledgments

Many thanks for the valuable input and insight from Rachel Greenstadt of Drexel University, Ed Felten and Peder Magee of the FTC, Thomas Lowenthal of Princeton, and former FTC technologists Chris Soghoian and Ashkan Soltani.

References

[1] L. D. Berger and C. T. Han. Twitter, inc., file no. 092 3093. Consent Agreement, June 24, 2010.

[2] E. P. I. Center. In the matter of facebook, inc.: Complaint, request for investigation, injunction, and other relief. Complaint, January 14, 2010.

[3] P. L. Chavez. Comments of Google, Inc. The New York Times, February 18, 2011.

[4] D. S. Clark. Twitter, inc., file no. 092 3093. Complaint, March 11, 2010.

[5] D. S. Clark. Chitika, inc., file no. 102 3087. Complaint, June 17, 2011.

[6] D. S. Clark. Facebook, inc., file no. 092 3184. Complaint, November 29, 2011.

[7] Workshop on Privacy in the Electronic Society Call for Papers, 2011. `http://wpes11.rutgers.edu/#cfp`.

[8] S. Egelman, J. Tsai, L. F. Cranor, and A. Acquisti. Timing is everything?: the effects of timing and placement of online privacy indicators. In *Proceedings of the 27th international conference on Human factors in computing systems*, CHI '09, pages 319–328, New York, NY, USA, 2009. ACM.

[9] Federal Trade Commission. Protecting consumer privacy in an era of rapid change: A proposed framework for businesses and policymakers. Staff Report, December 2010.

[10] Federal Trade Commission. Wise up about wi-fi: Tips for using public wireless networks. OnGuard Online, February 2011.

[11] E. Felten. Another privacy misstep from facebook, December 14 2009.

[12] Federal Trade Commission Act, September 8, 1914.

[13] D. Jang, R. Jhala, S. Lerner, and H. Shacham. An empirical study of privacy-violating information flows in javascript web applications. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 270–283, New York, NY, USA, 2010. ACM.

[14] A. M. Mcdonald and L. F. Cranor. The cost of reading privacy policies. *I/S: A Journal of Law and Policy for the Information Society*, 4:1–22, 2008.

[15] M. Mithal. Netflix, inc., file no. 102 3027. Staff Closing Letter, March 12, 2010.

[16] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *IEEE Symposium on Security and Privacy*, pages 111–125, 2008.

[17] A. Narayanan and V. Shmatikov. De-anonymizing social networks. In *IEEE Symposium on Security and Privacy*, pages 173–187, Washington, DC, USA, 2009. IEEE Computer Society.

[18] Front page. The New York Times, December 2, 2010. www.nytimes.com/indexes/2010/12/02/pageone/scan.

[19] P. Ohm. Broken promises of privacy: Responding to the surprising failure of anonymization. In *UCLA Law Review*, volume 57, page 1701, 2009.

[20] K. D. Ratté and K. R. Brin. Google, inc., file no. 102 3136. Consent Agreement, March 30, 2011.

[21] S. Sengupta. F.t.c. settles privacy issue at facebook. The New York Times, November 29, 2011.

[22] Stanford Law School. Aleecia mcdonald. http://cyberlaw.stanford.edu/profile/aleecia-mcdonald.

[23] D. Vladeck. Remarks of David C. Vladeck. Consumer Watchdog Conference, December 1, 2010.

[24] D. Vladeck. Remarks of David C. Vladeck. IAPP Practical Privacy Series, December 7, 2010.