

Hough Graduate School of Business
Warrington College of Business Administration
Department of Management

direct line
shared fax

Dr. Gwendolyn K. Lee
Associate Professor
Chester C. Holloway Professor

Gainesville, FL 32611-7165
United States of America

Date: October 3, 2016

A request to present research at PRIVACYcon 2017.

Dear FTC staff reviewing research presentations on consumer privacy and security,

In this letter, we provide the information that you request and explain the motivation behind our request to present research. We have prepared a set of slides to show you the graphical illustration and data visualization of our empirical findings. A copy of the slides is uploaded with this letter for your review.

Motivation

The motivation behind our request to present research at PRIVACYcon 2017 is personal. We are **victims of identity theft** and have been burdened by **card-not-present fraud**. To help other consumers like ourselves reduce the suffering caused by informational privacy and data security issues, we embarked on a social mission by conducting research on Secure and Trustworthy CyberSpace. Our research aims to help companies make strategically valuable and *socially responsible decisions* about privacy practices. The research is funded by the **National Science Foundation**.¹

Our research develops a broadly applicable analytical framework on making decisions about information privacy under uncertainty by companies, organizations, governmental agencies, and individuals. In particular, the framework provides the first risk-based analysis on a company's decision-making about privacy practices. It is also among the first to analyze the strategic values of privacy practices and how such practices affect the relative performance of competing companies. The results of the research will lead to new conversations and provide a better understanding about the interplay among (1) companies' practices and attitudes toward privacy; (2) companies' competitive behavior and outcome; and (3) new technologies.

¹ Understanding the Strategic Values of Privacy Practices in Organizations
https://www.nsf.gov/awardsearch/showAward?AWD_ID=1537528&HistoricalAwards=false

The information that you request

Researchers making the request:

Gwendolyn Lee	gwenlee@ufl.edu	+1 352 846 2694
Ye Xia	yx1@cise.ufl.edu	+1 352 505 1571

Title of the research we propose to present:

The Harms Caused by Privacy Violations – [Attack Trends on Data Breaches](#), [Medical Identity Theft](#), [Card-Not-Present Fraud](#) and [Responses from FTC and CNIL](#)

Abstract summarizing our methodology, findings, and how our research differs from prior research in this area:

Methodology. The empirical results we request to present are based on our analysis of companies' privacy practices with three sources of data. The first data source is the U.S. Federal Trade Commission (FTC), which publishes its enforcement actions for protecting consumer privacy. The FTC has brought enforcement actions against both well-known companies, such as Google, Facebook, Twitter, and Microsoft, and lesser-known companies. We have compiled a database of FTC enforcement actions, covering a wide range of privacy practices, addressing spam, social networking, behavioral advertising, pretexting, spyware, peer-to-peer file sharing, and mobile. In addition, we have compiled a database of FTC enforcement actions against companies that have engaged in unfair or deceptive practices that exposed consumers' sensitive information—including personal, financial, health, and employment data—to unreasonable risk. The second data source, which also reports data security practices, is the Privacy Rights Clearinghouse (PRC). We have collected more than 5000 instances of security failure from the PRC's chronology of data breaches starting from the year 2005 through September 2016. For each type of security failure, we have analyzed the size distribution of the records breached. The third data source is the French National Data Processing and Liberties Commission (CNIL). We have examined each of the sanctions imposed by the CNIL during a ten-year period between 2006 and 2015. And we have compiled a database of CNIL sanctions for comparing between the U.S. and France the size distributions of penalty on privacy violations.

Findings. The harms caused by privacy violations increase with widespread data breaches and security failures. The harms are tangible and substantial: (1) The exposure of sensitive personal information leads to costly spam, phishing, and other unsolicited communications; (2) The risks range from identity theft to "phantom debt" collection, which involves predatory debt collectors who try to extract payments from consumers without the authority to collect the debts; and (3) Fraudulent purchases transacted with

stolen information cause substantial injury, including inconvenience, worry, and time loss dealing with the affected credit/debit cards.

The data breaches and security failures that we analysed show the following [attack trends](#): (1) Hacking or Malware is the leading type of data breach; (2) A small number of breaches accounts for a large proportion of the records lost; (3) Healthcare, education & businesses are the leading entities suffering the most data breach; (4) Electronic devices (portable and stationary) represent the leading source of data breach in healthcare, *not hacking or malware, which is the leading type of data breach when all industries are combined in the analysis*; and (5) Illegally obtained account information across many states heightens the risk for unauthorized use and card-not-present fraud.

The [responses](#) from government agencies such as FTC and CNIL provide legal enforcement actions and sanctions. The empirical finding we report on FTC enforcements shows that privacy violations are caused by failures of companies across different industries involving a wide range of privacy practices. This finding is critical to our analytical framework on making decisions about information privacy. Our preliminary findings derived from the analytical framework, as described in the publication details below, suggest that, without penalty, there will be always one and one company only choosing to take risks that carry the possibility of inflicting extreme privacy harm. This choice is general across a broad family of shapes of risk distribution (e.g., changing from Gaussian to Pareto distributions where the tails of the distribution become longer or heavier). Penalty is necessary in helping companies make strategically valuable and socially responsible decisions about privacy practices.

We also find that, compared to CNIL, FTC actions cover more companies across different industries involving a wider range of privacy practices. This empirical finding further motivates our research in investigating the role of penalty, compared to consumer education, in affecting companies' decision-making about privacy practices. The current phase of our research analyzes the frequency and size of penalty for deterring privacy violations and reducing future harms. The analytical framework we develop shows how penalty affects a company's decision-making about privacy practices along stages of the value chain and across industries.

How our research differs from prior research in this area. Our research differs from what has been reported by the FTC, CNIL, and PRC. The annual reports published by the FTC on Privacy & Data Security Update provide overviews of the FTC's enforcement, policy initiatives, and consumer outreach and business guidance in the areas of privacy and data security. The findings we request to present supplement the FTC overviews by focusing on three types of privacy violations: (1) Unauthorized access; (2) Identity theft; and (3) Card-not-present fraud. What the FTC overviews haven't emphasized is that privacy violations are caused by failures of companies across different

industries involving various privacy practices, as opposed to failures of companies in a particular stage of the value chain (e.g., software development vs. retail) or a particular industry (e.g., social network vs. healthcare) engaging in a particular type of privacy practice.

CNIL publishes annual reports on the activities undertaken by the CNIL that protect personal data, support innovation, and preserve individual liberties. While the CNIL oversees the level of security applied by organizations in systems and networks, the advocated security compliance is based on an assessment of the risks on privacy (who, what?), and not on the mere comparison with best practices or on the mere application of the policy principle (which principle?). A comparison between FTC and CNIL suggests that FTC actions cover more companies across different industries involving a wider range of privacy practices. Our empirical finding complements the CNIL advocacy by featuring three types of privacy violations: (1) Cyber surveillance security flaw and failures; (2) Video surveillance failing to ensure data security; and (3) Data breach and security failure.

Privacy Rights Clearinghouse (PRC) is a nonprofit consumer education and advocacy organization, with a mission to engage, educate, and empower consumers to protect their privacy. While the PRC publishes a Chronology of Data Breaches, the empirical findings that we show using the breach data reveal differences between types of breaches across industries. Among the patterns of attack trends that we show, the most surprising finding is the following: *Electronic devices (portable and stationary) represent the leading source of data breach in healthcare, not hacking or malware, which is the leading type of data breach when all industries are combined in the analysis.* This finding reveals that addressing the challenges to privacy and security requires our understanding of industry-specific root causes.

Publication details for any research that has been previously published or accepted for publication:

Lee GK, Xia Y. 2016. "**Risk Strategy for Managing Information Privacy**"
The annual meeting of The Institute for Operations Research and the
Management Sciences (INFORMS), Nashville, TN USA.

Firms' risk strategy involves choosing a probability of success/failure in realizing a certain size of impact on the firm's competitive strength. We observe a disturbing pattern general across a broad family of shapes of risk distribution (e.g., changing from Gaussian to Pareto distributions where the tails of the distribution become longer or heavier). One and one firm only always chooses to take risks that carry

the possibility of inflicting extreme privacy harm. The risk strategy does not shift as the risk-return distribution changes its shape. The risk strategy for managing information privacy is studied in the context of firms pursuing data-intensive innovation such as personalized medicine.

Lee GK, Xia Y. 2016. "**Information Privacy: A Risk Management Perspective on Innovation, Entrepreneurship and Coopetition**" The Strategic Management Society Special Conference on the Strategy Challenges in the 21st Century: Innovation, Entrepreneurship and Coopetition. Rome, Italy.

We detect the relationship between innovation, entrepreneurship, and coopetition with the context of information privacy. Considering both the positive and the negative small-probability large-impact extremes, we develop a risk management perspective on firms' decision-making about how to balance between information privacy and data-intensive innovation. Firms compete on collecting personal data in increasingly larger quantity and mining the data more deeply. Yet, as the competition on data collection and data mining intensifies, the risks of a privacy catastrophe increase. To manage such risks, firms cooperate to reduce the privacy harms they may inflict on data subjects and invest in privacy-enhancing innovation. We examine the conditions under which privacy-enhancing innovation affects cooperation. Based on our preliminary results, we suggest that the distribution of privacy risks may affect a firm's choice to invest in developing privacy-enhancing innovation. Yet, one firm may choose to take risks that carry the possibility of inflicting extreme privacy harm, when all the other firms choose to invest in developing privacy-enhancing innovation. The incentives to take risks on inflicting privacy harm diminish as the degree of competitive rivalry increases.

Our completed or draft research paper or extended abstract:

Please review our extended abstract (as shown below) jointly with a set of slides that we have prepared for **graphical illustration and data visualization**.

Extended abstract

The harms caused by privacy violations increase with widespread data breaches and security failures. Using multiple sources of information on data breaches and security failures, we report the following attack trends: (1) Hacking or Malware is the leading type of data breach; (2) A small number of breaches accounts for a large proportion of the records lost; (3) Healthcare, education &

businesses are the leading entities suffering the most data breach; (4) Electronic devices (portable and stationary) represent the leading source of data breach in healthcare, *not hacking or malware, which is the leading type of data breach when all industries are combined in the analysis*; and (5) Illegally obtained account information across many states heightens the risk for unauthorized use and card-not-present fraud.

Crucial responses to the widespread data breaches and security failures are legal enforcements actions and sanctions. We compare the responses made by the U.S. Federal Trade Commission (FTC), which publishes its enforcement actions for protecting consumer privacy, to those by the French National Data Processing and Liberties Commission (CNIL), whose mission is to protect personal data, support innovation, and preserve individual liberties. Compared to CNIL sanctions, FTC actions cover more companies across different industries involving a wider range of privacy practices.²

Our empirical findings suggest that privacy violations are caused by failures of companies across different industries involving various privacy practices, as opposed to failures of companies in a particular stage of the value chain (e.g., software development vs. retail) or a particular industry (e.g., social network vs. healthcare) engaging in a certain type of privacy practice.

With our warm regards from [Florida, a state with alarming privacy violations](#),

Gwendolyn Lee

Chester C. Holloway Professor, University of Florida

Massachusetts Institute of Technology BS '95 MS '96

University of California-Berkeley MS '00 PhD '03

² Our presentation is on empirical research about the harms caused by privacy violations, not opinion pieces about law or policy. We use the cases and sanctions reported by the FTC and CNIL as sources of data for analyzing the harms caused by privacy violations.