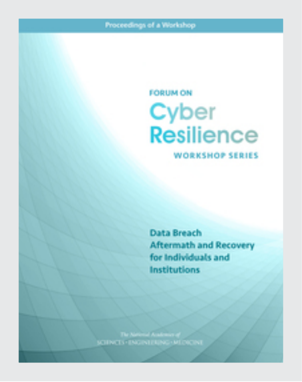
Proceedings of a Workshop
FORUM ON
Cyber Resilience
WORKSHOP SERIES
Data Breach Aftermath and Recovery for Individuals and Institutions
The National Academies of SCIENCES · ENGINEERING · MEDICINE

# Data Breach Aftermath and Recovery for Individuals and Institutions: Proceedings of a Workshop

DETAILS

66 pages | 8.5 x 11 | PAPERBACK
ISBN 978-0-309-44502-3 | DOI 10.17226/23559

CONTRIBUTORS

Anne Johnson and Lynette I. Millett, Rapporteurs; Forum on Cyber Resilience Workshop Series; National Academies of Sciences, Engineering, and Medicine

FORUM ON
Cyber
Resilience
WORKSHOP SERIES

# Data Breach Aftermath and Recovery for Individuals and Institutions

## Proceedings of a Workshop

Anne Johnson and Lynette I. Millett, *Rapporteurs*

*The National Academies of*
SCIENCES • ENGINEERING • MEDICINE

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
**www.nap.edu**

*The National Academies of*
SCIENCES • ENGINEERING • MEDICINE

The **National Academy of Sciences** was established in 1863 by an Act of Congress, signed by President Lincoln, as a private, nongovernmental institution to advise the nation on issues related to science and technology. Members are elected by their peers for outstanding contributions to research. Dr. Marcia McNutt is president.

The **National Academy of Engineering** was established in 1964 under the charter of the National Academy of Sciences to bring the practices of engineering to advising the nation. Members are elected by their peers for extraordinary contributions to engineering. Dr. C. D. Mote, Jr., is president.

The **National Academy of Medicine** (formerly the Institute of Medicine) was established in 1970 under the charter of the National Academy of Sciences to advise the nation on medical and health issues. Members are elected by their peers for distinguished contributions to medicine and health. Dr. Victor J. Dzau is president.

The three Academies work together as the **National Academies of Sciences, Engineering, and Medicine** to provide independent, objective analysis and advice to the nation and conduct other activities to solve complex problems and inform public policy decisions. The Academies also encourage education and research, recognize outstanding contributions to knowledge, and increase public understanding in matters of science, engineering, and medicine.

Learn more about the National Academies of Sciences, Engineering, and Medicine at **www.national-academies.org.**

## PLANNING COMMITTEE FOR THE WORKSHOP ON DATA BREACH AFTERMATH AND RECOVERY FOR INDIVIDUALS AND INSTITUTIONS

FRED B. SCHNEIDER, NAE,[1] Cornell University, *Chair*
FRED H. CATE, Indiana University
ERIC GROSSE, Google, Inc.
SUSAN LANDAU, Worcester Polytechnic Institute
DEIRDRE K. MULLIGAN, University of California, Berkeley
PETER SWIRE, Georgia Institute of Technology

***Staff***
LYNETTE I. MILLETT, Director, Forum on Cyber Resilience
EMILY GRUMBLING, Program Officer
SHENAE BRADLEY, Senior Program Assistant

## FORUM ON CYBER RESILIENCE

FRED B. SCHNEIDER, NAE,Cornell University, *Chair*
ANITA ALLEN, University of Pennsylvania
ROBERT BLAKLEY, CitiGroup, Inc.
FRED H. CATE, Indiana University
DAVID D. CLARK, NAE, Massachusetts Institute of Technology
RICHARD J. DANZIG, Center for a New American Security
ERIC GROSSE, Google, Inc.
DAVID A. HOFFMAN, Intel Corporation
PAUL C. KOCHER, NAE, Cryptography Research, Inc.
TADAYOSHI KOHNO, University of Washington
BUTLER W. LAMPSON, NAS,[2] NAE, Microsoft Corporation
SUSAN LANDAU, Worcester Polytechnic Institute
STEVEN B. LIPNER, Independent Consultant
DEIRDRE K. MULLIGAN, University of California, Berkeley
TONY W. SAGER, Center for Internet Security
WILLIAM H. SANDERS, University of Illinois, Urbana-Champaign
STEFAN SAVAGE, University of California, San Diego
PETER SWIRE, Georgia Institute of Technology
DAVID C. VLADECK, Georgetown University
MARY ELLEN ZURKO, Cisco Systems, Inc.

***Ex Officio***
DONNA F. DODSON, National Institute for Standards and Technology
WILLIAM B. MARTIN, National Security Agency
KEITH MARZULLO, Networking and Information Technology Research and Development Program

***Staff***
LYNETTE I. MILLETT, Director
EMILY GRUMBLING, Program Officer
KATIRIA ORTIZ, Research Associate
SHENAE BRADLEY, Administrative Assistant

For more information about the forum, see its website at http://www.cyber-forum.org, or e-mail the forum at cyberforum@nas.edu.

[1] NAE, National Academy of Engineering.
[2] NAS, National Academy of Sciences.

## COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

FARNAM JAHANIAN, Carnegie Mellon University, *Chair*
LUIZ ANDRE BARROSO, Google, Inc.
STEVEN M. BELLOVIN, NAE, Columbia University
ROBERT F. BRAMMER, Brammer Technology, LLC
EDWARD FRANK, Apple, Inc.
SEYMOUR E. GOODMAN, Georgia Institute of Technology
LAURA HAAS, NAE, IBM Corporation
MARK HOROWITZ, NAE, Stanford University
MICHAEL KEARNS, University of Pennsylvania
ROBERT KRAUT, Carnegie Mellon University
SUSAN LANDAU, Google, Inc.
PETER LEE, Microsoft Corporation
DAVID E. LIDDLE, US Venture Partners
FRED B. SCHNEIDER, NAE, Cornell University
ROBERT F. SPROULL, NAE, University of Massachusetts, Amherst
JOHN STANKOVIC, University of Virginia
JOHN A. SWAINSON, Dell, Inc.
ERNEST J. WILSON, University of Southern California
KATHERINE YELICK, University of California, Berkeley

***Staff***
JON EISENBERG, Director
LYNETTE I. MILLETT, Associate Director

VIRGINIA BACON TALATI, Program Officer
SHENAE BRADLEY, Administrative Assistant
JANEL DEAR, Senior Program Assistant
EMILY GRUMBLING, Program Officer
RENEE HAWKINS, Financial and Administrative Manager
CHRIS JONES, Program Officer
KATIRIA ORTIZ, Research Associate

For more information on CSTB, see its website at http://www.cstb.org, write to CSTB, National Academies of Sciences, Engineering, and Medicine, 500 Fifth Street, NW, Washington, DC 20001, call (202) 334-2605, or e-mail the CSTB at cstb@nas.edu.

# Preface

The Forum on Cyber Resilience—a roundtable of the National Academies of Sciences, Engineering, and Medicine established in 2015—facilitates and enhances the exchange of ideas among scientists, practitioners, and policy makers who are concerned with urgent and important issues related to the resilience of the nation's computing and communications systems, including the Internet, other critical infrastructures, and commercial systems. Forum activities help to inform and engage a broad range of stakeholders around issues involving technology and policy related to cyber resilience, cybersecurity, privacy, and related emerging issues. A key role for the forum is to surface and explore topics that can help advance the national conversation.

During its first year of activities, to begin exploring cyber resilience issues in the regulatory and civilian agency context, the forum welcomed Federal Trade Commission (FTC) Commissioner Julie Brill to its August 2015 meeting. Commissioner Brill spoke about FTC activities and perspectives on security, privacy, and the Internet of Things. That led to lively discussion that was part of the impetus for the development of a workshop on data breach aftermath and recovery.

A planning group was appointed to organize a workshop for exploring themes related to the extent of the harms from large-scale data breaches, the efficacy of different remediation actions, and ways to better help recover from breaches. The Workshop on Data Breach Aftermath and Recovery for Individuals and Institutions took place on January 12, 2016, in Washington, D.C., and featured invited speakers from government, the private sector, and academia. Participants examined existing technical and policy remediations, and they discussed possible new mechanisms for better protecting and helping consumers in the wake of a breach. Speakers were asked to focus on data breach aftermath and recovery and to discuss ways to remediate harms from breaches. But given the relationship between breach prevention and recovery from breaches, most speakers also addressed the whole gamut of challenges around data breach.

This workshop proceedings summarizes the presentations made by invited speakers and other remarks by workshop participants. In keeping with the workshop's exploratory purpose, this proceedings does not contain findings or recommendations, nor, in keeping with the Academies' guidelines for workshop proceedings, does it necessarily reflect consensus views of the workshop participants or planning committee. The planning group's role was limited to planning the workshop, and this proceedings has been prepared by the workshop rapporteurs and forum staff as a factual summary of what occurred at the workshop. The document draws on prepared remarks of workshop speakers, comments made by workshop participants, and the ensuing discussions.

The first chapter summarizes the introduction to the workshop and reproduces background material provided to all participants. The second chapter summarizes each of the speaker's presentations. The third chapter is organized into thematic areas, describes the content of the final discussion, and also integrates cross-cutting points made during presentations and earlier discussions, highlighting some of the broader themes that emerged throughout the workshop. The workshop agenda and participants list is provided in Appendix A. Short biosketches of the planning committee and speakers appear in Appendixes B and C, respectively.

We hope that the workshop and this proceedings will help to encourage the exchange of ideas and fresh thinking about the policy, legal, and technical ways in which our nation and its institutions respond to data breaches.

My sincere thanks go to the planning committee and staff who planned and organized the workshop as well as to the invited speakers for their thoughtful remarks and enthusiastic participation in the discussions that ensued. Writing support was provided by Anne Frances Johnson and Kathleen Pierce, Creative Science Writing. We also extend our appreciation to the National Science Foundation, the National Security Agency, and the Special Cyber Operations Research and Engineering Working Group for their support and encouragement of forum activities.

Fred B. Schneider, *Chair*
Forum on Cyber Resilience

# Contents

# ACKNOWLEDGMENT OF REVIEWERS

This workshop proceedings has been reviewed in draft form by individuals chosen for their diverse perspectives and technical expertise, in accordance with procedures approved by the Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will assist the institution in making its published proceedings as sound as possible and to ensure that it meets institutional standards for objectivity, evidence, and responsiveness to the project's charge. The review comments and draft manuscript remain confidential to protect the integrity of the deliberative process. We wish to thank the following individuals for their review of this proceedings:

Steven Bellovin, Columbia University,
Joel Reidenberg, Fordham University,
David Vladeck, Georgetown University, and
Mary Ellen Zurko, Cisco Systems.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the views presented at the workshop, nor did they see the final draft of the proceedings before its release. The review of this report was overseen by Samuel Fuller, Analog Devices, Inc., who was responsible for making certain that an independent examination of this proceedings was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this proceedings rests entirely with the authors and the institution.

**THE NATIONAL ACADEMIES PRESS 500 Fifth Street, NW Washington, DC 20001**

This project was supported by the National Science Foundation under award number CNS-14194917. Any opinions, findings, conclusions, or recommendations expressed in this publication do not necessarily reflect the views of any organization or agency that provided support for this project.

Digital Object Identifier: 10.17226/23559

Copies of this report are available from:

The National Academies Press
500 Fifth Street, NW, Keck 360
Washington, DC 20001
(800) 624-6242
(202) 334-3313
http://www.nap.edu

Printed in the United States of America

Suggested citation: National Academies of Sciences, Engineering, and Medicine. 2016. *Data Breach Aftermath and Recovery for Individuals and Institutions: Proceedings of a Workshop.* Washington, DC: The National Academies Press. doi: 10.17226/23559.

*The National Academies of*
SCIENCES · ENGINEERING · MEDICINE

**Reports** document the evidence-based consensus of an authoring committee of experts. Reports typically include findings, conclusions, and recommendations based on information gathered by the committee and committee deliberations. Reports are peer reviewed and are approved by the National Academies of Sciences, Engineering, and Medicine.

**Proceedings** chronicle the presentations and discussions at a workshop, symposium, or other convening event. The statements and opinions contained in proceedings are those of the participants and are not necessarily endorsed by other participants, the planning committee, or the National Academies of Sciences, Engineering, and Medicine.

For information about other products and activities of the Academies, please visit nationalacademies.org/whatwedo.

# Workshop Introduction

The Forum on Cyber Resilience of the National Academies of Sciences, Engineering, and Medicine hosted a Workshop on Data Breach Aftermath and Recovery for Individuals and Institutions. The meeting was held on January 12, 2016, in Washington, D.C.

The workshop featured nine speakers addressing a broad range of perspectives on data breaches: empirical, consumer, and data holders' perspectives and legal and policy perspectives. Distinguished scholars, lawyers, consumer advocates, and industry executives contributed their varied expertise to help draw out key themes and examples and to offer their views on response mechanisms for mitigating harm when data breaches occur.

Cross-cutting themes that emerged throughout the day and were discussed in the concluding plenary session include the following: defining harm, data breach and analysis and the need for a feedback loop to learn from aftermath and remediation to help prevent future breaches, data breach remediation itself, and possible mechanisms for future change.

The meeting was open to the public. This proceedings was created from the presenters' slides, notes, and a full transcript of the workshop. The proceedings thus serves as a public record of the workshop presentations and discussions. Individuals' affiliations are provided for identification purposes only.

# OPENING REMARKS

Fred B. Schneider, Ph.D., the Samuel B. Eckert Professor of Computer Science at Cornell University and Chair of the Forum on Cyber Resilience, opened the workshop. He began with an emphasis on the word "resilience," which was deliberately chosen to reflect the broad goals of the Forum on Cyber Resilience. In addition to typical aspects of information technology, such as security, reliability, and usability, resilience also encompasses social aspects, such as policy, regulation, and economics. By framing the workshop in this context, Schneider underscored the workshop's broad aim to understand the wide range of potential harms from data breaches and its intention to take a holistic look at how we can build resilience in the face of increasingly large, frequent breaches.

Schneider noted that historically, data breaches have been mostly seen as a threat that leaves people open to personal identity theft; as such, remedies focus on addressing that specific risk. But data breach harms can be more nebulous, and sometimes far more dangerous, than that. He observed that recent breaches on the dating site Ashley Madison, or the U.S. government's Office of Personnel Management, or the toy company VTech, prove that more than just financial loss is at stake: the harms from data breaches extend into the realms of personal reputations, national security, and even the safety of children.

It is clear that credit monitoring, currently the main remediation for data breaches, has become an inadequate remedy, Schneider said. The question now is, What *would* be appropriate? Schneider said that proper remediation cannot be determined until the wide range of possible harms, which can range from financial, to national security, to psychological, are understood. Once we identify the harms, he noted, the next step would be to incentivize data holders to anticipate, and mitigate, the risk of harm from future data breaches. He referred attendees to a short document that provided some context-setting material and discussion questions for the workshop (reproduced in the box on the following page).

Having this discussion in Washington, D.C., Schneider noted, is a useful reminder of who has the power to facilitate the types of changes workshop participants are discussing, researching, and advocating. Schneider expressed his hope that the workshop and discussions can have an impact on policy makers and power brokers beyond its participants.

# Workshop Context and Charge

**The following materials were provided to workshop speakers and attendees to offer context on the subject of data breaches and frame the workshop's intended purposes.**

## Background

This workshop is an activity of the National Academies' Forum on Cyber Resilience. The Forum on Cyber Resilience facilitates and enhances the exchange of ideas among scientists, practitioners, and policy makers concerned with urgent and important issues related to the resilience of the nation's computing and communications systems, including the Internet, other critical infrastructures, and commercial systems. Forum activities help to inform and engage a broad range of stakeholders around issues related to technology and policy in the context of cyber resilience, cybersecurity, privacy, and related emerging issues. A key role for the forum is to surface and explore topics that can help advance the national conversation around these issues.

This workshop focuses on the topic of response mechanisms to remediate harm when massive data breaches occur. Additional context and questions to consider for discussion are below.

## Context

This workshop will focus primarily on response mechanisms to remediate harm when massive data breaches occur. Today, large-scale data breaches are becoming increasingly common and have the potential to cause significant harm to individuals as well as to institutions. Incidents such as the Target and Office of Personnel Management hacks and the Ashley Madison breach have compromised, and in some cases exposed, sensitive information about millions of people. Although breaches of major retailer databases typically raise concerns about exposure of financial information and credit card numbers, other major breaches raise different concerns for individuals whose data have been stolen or exposed. The hack of the Office of Personnel Management database was a significant national security breach and also gained access to a trove of personal information on millions of individuals who had applied for positions of trust with the U.S. government. The Ashley Madison hackers deliberately released the names of millions of people using a dating service that those individuals most likely would have preferred not be linked to them.

Organizations that have been breached may offer affected constituencies free credit monitoring for a limited period or other forms of remediation or restitution, but it is unclear whether that actually helps affected individuals understand, minimize, and/or manage the implications of exposure. Moreover, the relevance of such monitoring is not clear in cases where financial data were not the sole type of data exposed, for instance, a breach of a defense contractor, a financial firm whose customers are themselves other financial firms, theft of intellectual property, or exposure of data that underpins critical infrastructure.

Complicating matters, exposure and theft of data are not the only risks; data (and its backups) could be destroyed or altered. What are the types of harms that flow from breaches today and what are potential remedies? Some harms, such as reputational embarrassment, that can result from breaches may not trigger typical security breach notification laws. For individuals, state laws confer rights to certain notices and protections. The Federal Trade Commission has published suggested self-help measures as well as guidelines for businesses to respond to a breach, in order to protect consumer data. Developing effective responses to breaches will surely involve planning for breaches and an understanding of the risks that relates to the mission and goals of the organization. Improper assessment of what privacy losses can occur if there is a breach can lead to situations where there is little room for resilience. Is there more that could be done?

Can we create a useful framework or taxonomy that includes types of breaches (and data) and types of harms (including harms and harmed parties)? Is there data available about the frequency and magnitude of harm? How is it measured and assessed? Is there data available about the effectiveness of available or proposed remediations? Some axes to consider:

- Types of breaches—breadth of exposure, mechanism, motivation;
- Types of harm—physical, reputational, financial, national security, short-term, long-term, reversible, autonomy/well-being, emotional distress, time/effort, diminished trust in services, reduced standing in the community, stalking, reduced economic opportunity, interference with family;
- Who can be harmed—users of a service, data subjects, institutions/data holders, third-party institutions, third-party individuals, society;
- Types of data breached—financial, communications, trade secrets, classified information, PII, health/medical, transactional, metadata, location; and
- Types of remediation—credit monitoring, reduction in liability, roll-back of transactions, reimbursements.

## Questions for Discussion

For these discussions, the term *data breach* can refer to

- Data that is stolen or exfiltrated;
- Data that is inappropriately exposed, published, or distributed;
- Data that is destroyed (perhaps along with its backups); or
- Data that is altered or modified (either overtly or surreptitiously).

What are the types of harm to individuals and to institutions that can occur from data breaches?

What remediations are common today? How is their effectiveness assessed?

What technical protections are common and what are their strengths and limitations once a breach has occurred?

Suppose a breach occurs at multiple providers for a certain swath of customers (e.g., executives at power companies, and mail accounts have been hacked at multiple providers). What should be done if multiple providers of the same type of service have been simultaneously hacked?

Once a breach has been detected, how is harm to data subjects assessed? Who is responsible and what are the processes to determine how those who have been harmed will be notified and, eventually helped? How does recovery or remediation activity begin?

What should take place under what timeframe? What should be done in first two hours after a breach is discovered? First twenty-four and forty-eight hours? Within a month?

For those companies that service both consumer and enterprise, how do responses differ between consumer and enterprise customers?

In the case of data modification, how is that detected and what mechanisms are or could be in place to recover and/or reconstitute original data?

What are other policies, processes, or mechanisms that might achieve better results?

What are high-leverage academic research opportunities in this space?

# Remarks of Speakers

The following sections summarize remarks by speakers at the workshop, along with discussion among attendees at the conclusion of each set of remarks. Speakers were clustered into two groups. The first group, consisting of Joel Reidenberg, Sasha Romanosky, Beth Givens, Tom Murphy, and Heather Adkins, offered empirical, consumer, and data holder perspectives. The second group, consisting of Bob Belair, James Harvey, David Vladeck, and Aaron Burstein, offered legal and policy perspectives.

## RESILIENCE AND REMEDIATION

**Joel Reidenberg, Fordham University**

Joel Reidenberg, J.D., Ph.D., the Stanley D. and Nikki Waxberg Chair at Fordham University School of Law and a visiting research affiliate of the Center for Information Technology Policy at Princeton University, conducts research and teaches courses in information technology law, privacy, cybersecurity, and intellectual property. He introduced the types and impacts of data breaches and offered perspectives on their remediation.

The types of data breaches that are most salient for consumers are unlawful exfiltration of personal data and wrongful dissemination, destruction, or corruption of that data, Reidenberg said. These breaches are common—Reidenberg suggested that every adult person in the United States has likely had personal information breached in some way—and in some cases these breaches can have significant consequences. For consumers, data breaches cause many types of harms, including loss of privacy, economic loss, safety hazards, fear of future damages, and inconvenience. Reidenberg mentioned a striking case from 1999 in which a woman's personal information was acquired by a stalker and resulted in her murder. For companies, he said, loss of trust, economic loss, and business disruption are the most salient harms.

When a data breach occurs, the usual procedure is for the breached entity to notify those whose data has been compromised. Although warning victims is important and meant to be helpful, this notification can, unfortunately, work to decrease trust in systems, Reidenberg observed. The consumer, he said, is now concerned about financial or medical privacy, distrustful of the breached entity, and fearful for any potential short-term or long-term harm. In Reidenberg's view, notifications of compromised data are not a systemic solution for resilience or remediation; while these notifications may treat a symptom, they do not provide a cure.

Reidenberg highlighted two critical questions: Who is responsible for losses that result from a data breach, and what is the best remediation for consumers?

After notifying consumers of a data breach, most companies then offer free credit monitoring as remediation. That may reassure some consumers, or help consumers forestall any costs of identity theft, but Reidenberg observed that it fails to address safety issues, future breaches, the psychological impact on consumers, or the actual financial loss. If money has been stolen in some way, the attribution of economic loss often remains unaddressed: Who should be responsible for the loss? If someone adopts a false identity and receives medical care under the assumed name, how can the real and false medical records be identified and corrected to avoid potential safety problems in the context of future medical treatment for the identity theft victim? In Reidenberg's view, there is currently no effective mechanism to deal with remediation of such potential downstream consequences of data breaches. "At the moment, we don't have anything that can really effectively focus on all of these kinds of harms," said Reidenberg. "This is a systemic need that will not be solved by one-off fixes; a solution is not going to be something as simple as a data breach notification."

A further complication, he observed, is that it is nearly impossible to measure the psychological harms or the full extent of the damage from a data breach. In the breach of the dating website Ashley Madison, for example, personal information was publicized and harmed individuals' privacy and reputations, but that harm is not easily quantified. In the case of Sony Pictures, the data breach likely had adverse economic impact on actors' salaries as a result of the disclosures and also caused the cancellation of a movie production. These economic harms are easier to quantify, but the costs of a myriad of indirect consequences are difficult to estimate, he said. The impact of compromised personal safety is similarly difficult to measure.

Industries are working to combat the problem of data breaches, of course. Information sharing and analysis centers (ISACs) are common in many industries and serve as central resources to help reduce the threat of cyberattacks, Reidenberg noted. Sharing information through ISACs can, for example, help mitigate a cyberattack on healthcare systems or a financial services malware attack. However, he said, the practice of sharing threat and attack information can also potentially increase the risk of exposing private data. "The more that personal data circulates across different organizations, the greater the vulnerability is," said Reidenberg. There is little in the ISAC framework, he argued, that articulates consumer rights or the need for consumer protections.

Reidenberg highlighted two critical questions: Who is responsible for losses that result from a data breach, and what is the best remediation for consumers? In the context of credit cards, a 1978 statute provides some answers—the consumer may be liable for the first $50 and the rest is on the card issuer—but disputes between card issuers and merchants have generated a great deal of litigation in subsequent years, he noted, with no clear resolution. Without relevant statutes for other contexts, such as brokerage services and utilities, there is an even greater lack of clarity, he said. Who would be responsible, for example, if a power plant were breached, resulting in widespread blackouts? Would the utility company help bear the costs? Individuals and small businesses often wind up assuming the costs of data breaches, yet they have the fewest assets to absorb them.

Sometimes it is the consumer who, knowingly or not, undertakes risky behavior that leads to privacy breaches, Reidenberg noted, pointing to consumer education about risk and liability as one area in need of work. Another area that needs to be examined, he suggested, is the definition and management of "critical infrastructure." Although an individual's personal computer or smartphone may not itself control communications infrastructure or sensitive data, consumer devices, especially if used to access sensitive systems, can become an entry point for a massive breach and thus become a vector for harm.

Reidenberg also pointed to a need for clarity, oversight, and regulations to guide cybersecurity countermeasures. As an example, he pointed to the 2013 takedown of more than 1,000 networks that were part of the Citadel botnet using malware to control and access private financial information on millions of personal computers. Reidenberg observed that Microsoft, in collaboration with the Federal Bureau of Investigation (FBI), obtained a court order to proceed with a counterattack, but the process did not pay attention to how this takedown could adversely affect the unwitting owners of the malware-infected computers and did not have a plan to address any collateral damage, passing the resulting costs on to the owners.

Concluding, Reidenberg stressed the need for academic research: "We have a huge need today for good, carefully thought-out empirical work to provide a sound basis for any kind of policy decision making," he said. Four main areas he sees as particularly ripe for investigation include mapping the harms of data breaches to the breach type and characteristics of affected stakeholders; developing a comprehensive understanding of the full costs of remediation and the benefits of prevention; creating policies or procedures to standardize the reporting of security breaches; and developing a framework for accountability when implementing countermeasures.

## COSTS AND CAUSES OF CYBER INCIDENTS

**Sasha Romanosky, RAND Corporation**

How much does a data breach cost a business? Which industries are at the most risk for losses? When does a data breach lead to litigation? The answers to these questions are crucial because they influence whether and to what extent businesses invest in preventing data breaches and other cyber incidents. The incentives (or disincentives) for strong data protections on the part of industry can shed light on business practices and help to inform policy decisions.

Sasha Romanosky, Ph.D., is a policy researcher at the RAND Corporation with expertise in the economics of security and privacy, cybercrime, national security, applied microeconomics, and law and economics. He summarized his research findings on the empirical costs of cyber incidents and discussed how those costs might (or might not) incentivize companies to implement better data protections.

Romanosky's research is based on a data set of 12,000 cyber events collected by the insurance analytics company Advisen through news reports, Freedom of Information Act requests, academic databases, and other sources. This data set is more than twice as large as other publicly available data sources used for previous analyses. Even with so much data, Romanosky noted some limitations: Many events are not even publicly known; they may not have been detected by the company; they may have been detected but not disclosed; or they may have been disclosed but not entered into any industry or legal database. It is also challenging to put a dollar amount on the myriad impacts of cyber incidents. Despite these limitations, Romanosky's analysis offers a rough estimate of the empirical costs of these events. With this knowledge, he noted, firms could choose to invest heavily in data security to prevent a breach, or take the opposite path and assume that breaches will happen and accept the financial burden of mitigating their effects.

Either way, he argued, better data can lead to more informed decisions, not only for businesses themselves, but also for insurers, consumers, and policy makers.

Based on the available data, Romanosky identified four main types of cyber incidents that put consumers or businesses at risk of financial loss: data breaches, defined as the unauthorized disclosure of personal information; security incidents, in which computers are used to attack a company; privacy violations, in which companies intentionally collect or use personal information; and phishing or skimming, which include various types of financial crimes against targeted individuals and companies. His analysis revealed that data breaches outnumber all other incident types by at least four to one, although security incidents appear to be rapidly becoming more frequent.

Quantifying the costs and risks of cyber events is challenging. Romanosky used three main measures to identify general trends: (1) incidents, as measured by the total number of incidents, and incident rate, or the proportion of companies that experience these events within an industry; (2) litigation, as measured by the total number of lawsuits, and litigation rate, or the proportion of companies that are sued for cyber event-related harms within an industry; and (3) costs, as measured by the total costs and losses per event. With this data, he claimed, companies can assess where their industry falls on the spectrum of severity of cyber events and better understand and prepare for the specific risks their company faces.

Romanosky's analysis suggests data breaches outnumber all other incident types.

Romanosky's results show that breaches, small and large, affect a wide range of industries and that different industries suffer different consequences and costs from these events. While his analysis suggests that the highest numbers of incidents occur in the finance, insurance, and healthcare industries, government and education suffer the highest incident rates. His research also suggests that while the information, finance, and insurance industries receive the highest total number of lawsuits, the mining, oil, and gas industry and the companies providing administrative and support services have the highest litigation rates. Romanosky's analysis suggests that the transportation industry has the highest cost per event, and the highest overall risks (combining cost, incident rate, and litigation rate) are borne by the manufacturing, retail, finance, and insurance industries.

Drilling deeper into the financial costs to firms from data breaches, Romanosky described two kinds of costs: "first-party costs" and "third-party costs." First-party costs are those a company bears after a data breach, such as the costs to notify consumers, cover remediation, and implement increased security measures as necessary. Third-party costs come from litigation and settlements. As other workshop attendees pointed out, there are multiple ways to measure costs incurred by a company—for example, it can be debated whether staff time should be counted if it is incurred by salaried staff who are not paid overtime. However, Romanosky said the analysis is likely not granular enough for such distinctions to affect the overall findings of this study.

Analyzing the 12,000 cyber incidents in the database, Romanosky found that despite there being some very large, expensive data breaches—such as those at Target, Sony, Anthem, and Home Depot—that drive the mean cost of a breach toward the $5 million range, which has been frequently cited, the *typical* cost to an entity is less than $200,000.

He said that although this may seem surprisingly low, an important additional finding is that nearly 40 percent of all companies affected have suffered multiple incidents—a group Romanosky calls "repeat players"—and these companies suffer higher costs for some types of events. "These repeat players don't seem to be litigated more than the non-repeat players," he said. "But the cost to these repeat players, at least in terms of data breaches, is significantly different—almost twice as much with repeat players." So, even if the per-incident cost is low, he said, an entity hit again and again would have more cause for concern. In addition, trends within industries can be telling. For example, in the finance and insurance sectors, he found that 50 percent of incidents involve repeat players, a phenomenon that is ripe for further research.

Romanosky said a "back-of-the-envelope" calculation based on the 12,000-incident data set puts the total annual cost of cyber events at about $10 billion. While granting that this figure is probably not completely correct and that a lot depends on how many breaches go undetected or unreported, he argued that the estimate is useful in a broad sense. "It gives us a general sense based on the information that we have of what we think the annual cost of these events would be," he said.

Based on a rough comparison to other sources of industry losses, such as retail theft, healthcare fraud, or loss of intellectual property, the aggregate loss from cyber events is relatively small, Romanosky argued. Although the costs of these events may total approximately $10 billion, these costs only represent about 0.4 percent of annual revenue, he said, making cyber events a far less significant risk to businesses than other losses, such as shrinkage and fraud.

Data breaches and other cyber events are certainly increasing, but Romanosky's research suggests that the *typical* costs to companies are relatively small, both in absolute terms and as a proportion of revenue. Thus, although there have been a number of rare, astoundingly costly events, he argued that companies overall may not have a strong financial incentive to invest in the infrastructure and systems required to rigorously protect data.

# AN ON-THE-GROUND LOOK AT CONSUMER IMPACTS OF DATA BREACHES

**Beth Givens, Privacy Rights Clearinghouse**

Beth Givens directs the Privacy Rights Clearinghouse, an organization based in San Diego, California, whose mission is to educate and empower consumers to protect their data and their privacy. Her work focuses on the fallout for consumers when their data is breached, and she offered an on-the-ground perspective on the history of breach notification laws in California, research about the experiences of breach victims, and possible future trends in data breaches.

California was the first state to implement a data breach notice law. The catalyst for the law was a 2002 large-scale data breach of the state's payroll database, which affected 265,000 employees, including the governor and the state legislature. The resulting law, implemented in 2003, mandated that firms must notify those individuals whose personal information (specifically, name plus driver's license or identification numbers, or social security number, or financial account numbers) had been compromised.

Since the passage of California's initial data breach notice law, the legal framework around data breaches has been continually updated in response to emerging threats and consumer harms. For example, the laws were updated in 2008 and 2009 to include medical and insurance data and harsher penalties after Los Angeles-area hospital staff were caught selling celebrities' medical data. In 2012, the laws were updated to clarify the often opaque legal language used in data breach notifications. These updates also required additional information to be included in a data breach notification, such as the type of information that was breached, when the breach happened, and contact information for credit reporting agencies, and required breach notices to be posted on the website of the state attorney general.

A 2014 California law required local governments to send data breach notices and expanded the definition of personal information to include online login credentials, such as usernames, passwords, or a mother's maiden name. In 2015, breached entities were required to provide free "identity theft prevention and mitigation," which goes beyond credit monitoring, for 1 year if the data breached included a social security number or driver's license number. In 2016, the law was again revised to better define "encryption" and outline required headings for data breach notices. Those headings are "What Happened," "What Information was Involved," "What We Are Doing," "What You Can Do," and "For More Information" and are intended to clarify the situation for consumers and empower them to take any needed action. Givens said it is unclear whether these improved notice formats would cause any change in consumer behavior after a breach. She suggested that this would be a fruitful topic for research.

A theme throughout Givens' talk was that breaches are constantly changing, and so too must our responses to them. She noted that the rapid evolution of California's legal framework around this issue demonstrates how state legislatures are generally able to be more active and nimble than the federal government on this issue. Givens said that the California experience has also shown that requiring public reporting of data breaches can increase transparency of and research access to these events. She noted, as an example, that in California the attorney general has published helpful breach reports and analyses based on the information collected over the years.

Givens also offered insights on the experiences of the consumer victims of data breaches. A key finding from her organization's close work with affected individuals is that victims most often report confusion after a notification. She suggested that this confusion might stem from the lack of clarity in data breach notices—a factor that recent revisions to California's data breach notification laws might help address.

Givens observed that the purpose of the notice, however, is not just to inform the victim of the situation, but also to prevent a data breach victim from becoming a fraud victim. To prevent identity fraud, companies typically offer free credit monitoring for 1 year. Givens said that credit monitoring is appropriate if certain information, such as a social security number, is compromised. However, she said it is not helpful if the data breached included credit card information or health information, for example. Credit monitoring in that case only offers a false sense of security to the victim, Givens argued.

Another change Givens observed is that it can no longer be assumed that data breaches are always financially motivated.

One company Givens spoke with offers "identity theft service" that includes monitoring the black market for a customer's information and making sure that individual is not defrauded. Givens said that this service is actually much less expensive than credit monitoring and can be used for a wider range of compromised information. Givens observed that a conundrum of data breach response is that credit monitoring is considered a "best practice" after a data breach, despite the fact that it is inappropriate and inadequate in many situations, is more expensive than identity theft service, and is widely ignored by consumers. Givens posited that companies are perhaps afraid not to offer it because it has become so widely expected by consumers and regulators.

Another crucial aspect of data breach remediation is what affected consumers choose to do with the information and resources offered to them, Givens said. In her organization's analysis, Givens was surprised to discover that a mere 5 percent of breach victims took advantage of the free credit monitoring offered to them after their data had been compromised. She cites two reasons for this low rate. One is that in order to enroll in a credit-monitoring service, users must enter their social security number and/or date of birth. She said that many victims may be understandably risk-averse after being told they were a victim of a breach and, as a result, are reluctant to share such personally identifiable information. The second reason is that, in her view, credit monitoring simply is not perceived as valuable by many consumers. What most want instead is a quick repair if there is identity fraud that results from the breach.

Credit monitoring and identity theft services are efforts to prevent a victim of identity theft from becoming a victim of identity fraud. Givens offered some statistics about fraud: In 2011, one in five breach victims became a fraud victim. In 2012, this proportion rose to one in four, and in 2013, it was one in three. In 2014, this proportion decreased to one in seven, mostly thanks to the remediation efforts stemming from the large point-of-sale data breaches at Target and Home Depot (figures from research provided by Javelin Strategy and Research), Givens said. To rectify those breaches, credit card companies issued cardholders new cards, which was expensive but effective at reducing fraud, as the numbers show.

Givens noted that the nature of data breaches is constantly evolving. Today, almost any nugget of data can be valuable to thieves, not just social security numbers or financial account information. Those involved in perpetrating fraud are casting a much wider net, including information such as school or medical records, online login credentials, and more. Givens said that according to Javelin's 2015 Fraud Impact Report, "Nearly any piece of information that fraudsters can get their hands on can be used to initiate or strengthen an attack."

Another change Givens observed is that it can no longer be assumed that data breaches are always financially motivated. Although they are not within her purview, Givens mentioned the recent breaches by suspected Chinese hackers, breaches of medical records, and breaches of personnel files at the Office of Personnel Management. This highly sensitive data may have been compromised for a variety of nonfinancial motivations.

As always, companies are trying their best to stop data breaches from happening in the first place. Chip cards have made credit and debit accounts more secure, but Givens likens this development to "squeezing the balloon—it's just going to push fraud in other directions." For example, she said fraudsters may switch to a focus on new-account fraud, in which a person's social security number or other information is used to open a new credit account, which is quickly spent down before the fraud is detected. Or they may focus more on transactions in which the card is not present—for example, in online transactions.

In Givens' view, the areas that are perhaps most vulnerable to future fraud include online commerce, healthcare institutions, government agencies, and schools, largely because those institutions all use social security numbers, which can be used to open fraudulent new accounts. Healthcare records in particular contain so much information about a person (and sometimes about the person's family members) that they are worth far more than a credit or debit card number on the black market, she said. Healthcare institutions, should, Givens urged, take every precaution to encrypt patient data and also segregate information based on whether it is medically pertinent. She also suspects that after bigger companies become smarter about data protection, fraudsters will target mid-size and smaller places of business, which may not invest heavily in data protection or have time available to train staff in proper handling of sensitive records.

Transparency of data breaches could help consumers when deciding which financial or medical institutions to trust, Givens said. Deirdre Mulligan, University of California, Berkeley, likened breach notifications that are required to be made public (e.g., through publication on the attorney general's website in the state of California) to the publication of pollution records by the U.S. Environmental Protection Agency. After a breach, she said, consumers might opt to take their business elsewhere, which could be a powerful motivator for companies to better protect their customers' data. Givens agreed that this was an important point but noted that the research on this matter is somewhat mixed. She noted a study by Javelin found that 70 percent of consumers said they would take their business elsewhere following a breach when, in reality, only 19 percent actually did. However, a change in behavior even by just one in five could still have a significant impact, she said.

In conclusion, Givens said breaches will continue to happen and will likely expand into different spheres, depending on which data are the most valuable and the most vulnerable. The challenge for lawmakers, consumer advocates, and companies, she said, is to keep one step ahead of the attackers.

## INFORMATION SECURITY IN THE UNIVERSITY ENVIRONMENT

**Tom Murphy, University of Pennsylvania**

Tom Murphy, who became the university chief information officer (CIO) for the University of Pennsylvania after decades of experience leading information technology strategy in private and public companies, began his talk with a stark summation of the challenges in information technology (IT) security. "I've worked in both public and private companies, and I can tell you from our perspective, information security is the boxing match that never ends," he said. "And we just keep taking beating after beating."

As a university CIO, he is responsible for providing appropriate and effective information security within a highly decentralized, diverse university ecosystem. In his talk, he outlined the challenges of working in a university environment and detailed the plan his team developed to balance information access with information security.

Higher education faces the same security challenges as large companies, he said, including the explosion of mobile and cloud computing, the need to handle large amounts of sensitive data, and the responsibility to uphold customers' expectations of data privacy. However, he noted that higher education has some additional challenges that complicate its security landscape. Most universities, for example, have a tradition of embracing collaboration, freedom of expression, and decentralization of authority and are unlikely to take well to tight management or uniform regulation. In addition, he continued, universities today provide services that extend far beyond their primary educational missions, with many playing host to healthcare facilities, large housing complexes, major sporting events, and independent police departments. As Murphy described them, today's universities are "more akin to a small city than a single, monolithic company."

Because of these extra-educational services, most universities must already comply with laws such as the Health Insurance Portability and Accountability Act, the Family Educational Rights and Privacy Act, and numerous other state and federal regulations that protect personal and financial information. However, Murphy argued that universities must go even further in protecting their varied, highly sensitive, and extremely valuable data.

Murphy described his university: The University of Pennsylvania is an enormous, complex place, with an overall operating budget in fiscal year 2016 of $7.74 billion and a research budget of $940 million. It is a research university with 141 research centers and institutes, which means it has a high volume of proprietary and sensitive data. It houses sensitive personal data from about 25,000 students and more than 40,000 faculty and staff members distributed among a wide network of schools, centers, and institutes.

Murphy noted that the overall computing structure of a premier educational and research institution like the University of Pennsylvania must be quick and reliable, but different departments and schools have different information needs, different financial and human resources, and competing priorities within their vast, decentralized governance. Murphy and his team have no direct authority over students or staff, yet they are accountable for the security of all that information. They cannot impose mandates on technology use, yet their users—the students, faculty, staff, and alumni—expect universal, instantaneous access to information. Facilitating effective, appropriate IT security within this complex environment is challenging, but has also generated "a number of information security success stories," Murphy said, with innovative and effective solutions arising across the university system's diverse schools and centers.

In 2015, Murphy was tasked by the university's Institutional Risk Committee and trustees to answer the question of how best to do information security in such a highly decentralized and complex environment. First, he and his colleagues took stock of the people, processes, and technology involved in IT security at the university, and then they added resources to better align with customer demand, including the first campus firewall, as well as analytics and central logging. With a team in the process of doubling from 5 to 10 full-time staff members, Murphy and his colleagues are working to establish a security baseline, create a set of universal recommendations, and increase campus-wide efficiency, training, and education.

Murphy described how each step of this process required a tremendous amount of fact-gathering and diplomacy to provide compelling cases to justify the group's recommendations and expenditures. It also required relationship-building on Murphy's part, to win over influential campus groups, such as the faculty senate, and to convince researchers that their life's work is safer in a secured environment than on an unsecured personal laptop.

Murphy observed that relationships outside the university proved important as well: Peers at other universities, in particular the other Ivy League schools, were valuable resources for information and approaches to emulate, Murphy said. He also cited the value of close relationships with other university CIOs, as well as with Philadelphia's FBI branch and police department. Despite all the research, diplomacy, and significant investment, however, Murphy emphasized the hard truth that no amount of spending could guarantee complete protection from a data breach.

After establishing a security baseline, Murphy's team developed the Simplification, Automation, Visibility, and Engagement (SAVE) program. The primary goals of SAVE are to prevent privacy breaches; avoid loss of intellectual property, resources, or reputation; and reduce noncompliance. He noted that the program offers strong recommendations, but no mandates, to improve data security, access, awareness, and training for safe data handling.

While SAVE is meant to help prevent privacy intrusions and other harms from cyber incidents, Murphy's team fully recognized that some breaches would be unavoidable. As a result, the program also includes a breach-response plan that empowers an incident response team to make decisions on behalf of the university. Within hours of a data breach, the team (following the Planning, Identification, Containment, Eradication, Recovery, Lessons learned model) begins determining a communications plan, identifying the cause, and putting containment measures in place.

Murphy noted that the team also has an annual SPIA (Security and Privacy Impact Assessment) program that assesses internal compliance with the recommendations that keep student, operational, financial, medical, or other data secure. While no penalties exist, finding security lapses motivates Murphy's team to work closely with a department to eliminate such gaps and better protect data. Every school or center is also required to have a security liaison, a staff member who received security training and becomes the "eyes and ears" for data security on their site.

University research is particularly vulnerable to intellectual property or data theft, and such an enormous, decentralized environment cannot fully control all its data access points. Murphy addresses these concerns through yearly assessments, and through the office of security liaisons. Extra staffing and security are also needed for applications that require special handling, such as data encryption or protection from physical theft. Yet, he said, his greatest fear remains the "unknown unknown"—an act that is completely unpredictable.

Murphy suggested that information security could benefit from a "public health" campaign.

Murphy observed that there are also "known knowns" that even the most robust security system cannot protect against. One of the biggest, he said, is human error. "No matter how good the tools are that I put into place, we're dependent on our constituents to help secure our data and our systems," he said, emphasizing that for a system to truly be secure, it must be easy for nonexperts to use. While analogies to crime or war are common in discussions of cybersecurity, Murphy pointed to healthcare as perhaps a better analogy for cybersecurity today. In healthcare, most people are not doctors, but patients. The same is true in cybersecurity: most people are not security experts, but everyday users. Continuing the analogy, he noted that while everyone gets sick at some point, vaccines, immunizations, and basic hygiene can keep most people healthy most of the time. Similarly, in cybersecurity, he said, there might be inevitable security breaches, but basic security measures can keep most intruders at bay. In addition, no two diseases or breaches are exactly alike, and a given diagnosis may have multiple treatments, which may work in some situations but not in others.

Taking the discussion further, he noted that evidence-based medicine optimizes decision making by relying on well-designed research, which has led to effective solutions such as the use of checklists in improving hospital sanitation. Murphy argued that the information security community should use similar practices. A succinct checklist of responsible computer or smartphone ownership, repeated often, he suggested, could significantly reduce breaches. Users need frequent reminders, but it's worth it. After all, even doctors need to be reminded to wash their hands. "The [IT] community must agree on the four or five most critical basics of what people need to know to safely own a computer and create a universal and oft-repeated campaign to make sure they are not forgotten," Murphy said.

Despite an emphasis on public education and awareness around data breaches, the truth is that people make mistakes or bad security decisions all the time, Murphy said. Information security could benefit from a "public health" campaign encouraging everyone to better protect their data, which would make for a more secure environment overall, Murphy argued. While his office is now launching a campus campaign to deeply engage the entire community, Murphy recognized that his efforts have their limits. "I can't stop all of that behavior. All I can do is educate," he said.

## AN INDUSTRY PERSPECTIVE ON BREACH DISCLOSURES

**Heather Adkins, Google, Inc.**

As manager of information security at Google Inc., Heather Adkins offered the perspective of someone who spends each day assessing and responding to information security threats in the private sector. She is responsible for Google's global data security—no small task at a company with more than 60,000 employees in more than 40 countries. Adkins' talk focused on the benefits, and some downsides, of data breach disclosure in four main areas: assistance to customers, identification of attackers, deterring future attacks, and aid in data-security education for everyone.

Adkins noted that a primary reason companies disclose data breaches is that they are required to by law. At Google, Adkins said there are several additional factors at play. An important reason Google supports disclosure, for example, is because it is ethically the right thing to do, Adkins said, noting that disclosure aligns with one of Google's mottos, which is to "put the user first, and all else will follow." Disclosing a breach is the right thing to do because it empowers the user to take action to defend themselves against fraud, and because it empowers users to make informed choices as consumers.

Some consumers might elect to leave a company that has compromised their data; however, Adkins offered a few examples suggesting that this is uncommon, and perhaps impractical. She noted that the highly publicized breach at Target, for example, wound up costing the company an estimated 0.1 percent of its 2014 sales (after subtracting insurance payouts and tax deductions), and the company's profits and stock have risen 21 percent since then, suggesting that few consumers actually made the decision to "vote with their feet" by taking their business away from Target. Another example she observed is that after the 2014 Sony breach, the company is estimated to have lost 0.9 to 2 percent of its sales for the year, yet the event gave the company free publicity for a movie, *The Interview*, that might otherwise have been more of a financial loss.

Because breaches have become so frequent and widespread, Adkins said consumers' apparent reluctance to leave companies that disclose data breaches may also be attributable to the fact that a consumer would be hard pressed to find a company that has *not* been compromised. The truth, she said, is that no company's data is completely secure. "Every organization is compromised, and they're compromised repeatedly whether they know it or not," Adkins said.

Citing personal experience of data breaches and fraud, Adkins argued that credit monitoring should become a consumer's default status, not a temporary, 1-year service used only after a known breach has occurred. Adkins described how she became a fraud victim in 2007 as a result of a data breach that had occurred in 2003. In such a case, she said, a 1-year period of credit monitoring after the 2003 breach would not have been sufficient to prevent or alert her to the subsequent fraud 4 years later. "We should just be offering [credit monitoring] by default all the time—it should be something you always have," she said. However, she acknowledged that this is not a foolproof fix; despite near-constant credit monitoring and multiple credit card re-issues, she noted that her personal data is likely still vulnerable to breach and fraud.

Another reason to disclose data breaches is to aid in the deterrence of future attacks, Adkins argued. For example, disclosure and attribution of state-sponsored breaches could start a more official conversation between nations. Or, financially motivated attackers might reconsider targets that are publicizing their stringent security measures. However, she also observed that in some situations it is possible for disclosures to backfire by feeding valuable information to attackers, raising difficult questions around when and how to disclose a breach and its suspected causes or responsible parties.

Adkins said that it is useful to consider an attacker's motivations when deciding how to respond; for example, a hack could be motivated by espionage, financial gain, or simply fun and fame. Companies such as Google sometimes use warnings or alerts as a remediation when a breach or attack is detected, but that can pose its own challenges. She noted that disclosing information about a breach can be dangerous if the breach is misattributed, misdiagnosed, or otherwise misunderstood. For example, Adkins posed a hypothetical situation in which two attackers hack into a company's system but only one is caught: "Then the other one gets to watch us play incident response against the other, and they can do their jobs much better. In fact, disclosure gives the attacker situational awareness, and we must take that into account," she said.

Often breaches become a game of cat-and-mouse, with each party trying to guess what the other knows. Adkins said that Google might choose to alert users who may be targeted by hackers by posting a pink status bar at the top of the person's Gmail account. The attacker can also see the pink bar, and so they know that Google knows there has been a breach, but they might not know exactly *what* Google knows. In another example, she described when a security software company was breached in 2013; the company posted on its website some of the evidence for the breach, such as where the malware was found. For the attacker, that disclosure may have offered valuable clues about what was discovered, and, more importantly, perhaps what was *not* discovered, such as a second "back door" that the attacker could continue to exploit. Acknowledging that this is a difficult tension, Adkins said that although it is not advisable to publicly lie, deceiving your attackers can be an important tactic. "I think we can make smart choices about what we disclose and in what detail . . . We need the laws to not be so prescriptive that we have no agility in those situations," she said.

Another reason for breach disclosure is to improve the security awareness and habits of consumers and employees. Adkins told a story of a breach in 2010 that affected data from Google and at least 20 other companies. Employees were required to change their passwords, lost their access to virtual private networks, and were directed to take other precautions without knowing why, causing understandable frustration on the part of many affected workers. Once the breach was disclosed, she observed that the experience presented a useful starting point for a deeper conversation with employees about information security and vulnerabilities.

Adkins posited that information sharing works best among small communities in which players have established deep relationships.

One of Adkins' roles at Google is to engage employees on the day-to-day security issues that they encounter. Through education campaigns, she noted that Google employees have learned to identify phishing attacks, detect penetration tests, and identify software vulnerabilities. Disclosing known attacks to employees offers valuable fodder for engaging in collaborative conversations about improving data security.

Adkins closed with a few comments about formal groups for information sharing (ISACs), which have recently sprung up in many industries as a means to facilitate company-to-company exchange related to preventing breaches. One reason for skepticism about their benefits and effectiveness, she said, is that there are a large number of small startup companies that are left out of the conversation, largely because they are not well equipped to detect breaches affecting them and thus have little to share. "If you have nothing to share, nobody will share with you," she said. But when large companies suffer and disclose breaches, "it's a magnet for information sharing when you are able to disclose and to talk very openly about what happened about your organization."

Adkins posited that information sharing works best among small communities in which players have established deep relationships. When asked by Bob Blakley, Citi-Group, Inc., about that viewpoint, Adkins noted that Google has indeed benefitted from Structured Threat Information eXpression (STIX$^{\text{TM}}$) and Trusted Automated eXchange of Indicator Information (TAXII), which seek to standardize and automate the exchange of information about cyber threats. However, to truly have an impact, information sharing must go beyond indicators: "It has to be a rich conversation about attackers, who they are, their modus operandi, their speed of attack through victim A, through victim B. There's a lot to a forensic analysis that is helpful outside of IP addresses," Adkins said.

Companies are required to disclose information about data breaches to the government, and many also disclose this information to users and employees for a variety of other reasons. In addition, William Sanders, University of Illinois, Urbana-Champaign, pointed out that detailed information about these breaches could have a lot of value for academic research; measuring the user's response, and any attacker's counterresponse, to a warning on an Internet browser, could be a rich place for Google and academia to partner, for example. Adkins concurred, saying that conducting studies on users and employees would likely be more feasible than studies on adversaries. Sharing Google's breach data would require removing any personally identifiable information, and so it might be easier, safer, and more useful for Google to share data around an attack: how it started, what techniques were used, and so forth. She further observed that additional complications include the fact that huge attacks, like those at Target and Home Depot, are not characteristic of most data breaches, and also, many breaches simply go undetected. Some academic researchers have tried creating sham companies and databases to lure attackers for research purposes, but Adkins noted that it is extremely difficult to pull off this approach.

For both academic research and companies' breach prevention purposes, Adkins said that the information that is likely most useful is that concerning how the attack occurred. Although many companies are capable of identifying that an attack has occurred, she noted that fewer are equipped to "build out the full kill chain" and trace the root causes of the breach. Finding—and sharing—such information would be a valuable weapon against future breaches.

## DATA BREACH AFTERMATH AND RECOVERY

**Bob Belair, Arnall Golden Gregory, LLP**

Bob Belair is a partner at the law firm Arnall Golden Gregory, LLP, where he serves as practice leader of the Privacy Practice Group and co-chair of the Government Relations Practice. He has been active in data privacy issues since 1971, when he was a law student assistant to Alan Westin, a celebrated legal scholar whose work was instrumental in defining information privacy in the modern era. Belair began by recounting how he had assisted Westin on his second book, *Data Banks in a Free Society*, which grew out of a National Academy of Sciences study that articulated a comprehensive approach to information privacy, later popularized by the Privacy Protection Study Commission and what was then the Department of Health Education and Welfare.

Belair's presentation focused on the thorny legal issues companies face in the aftermath of a data breach, and it stressed the need for standards across all aspects of breach prevention and remediation. In his view, the current lack of good remedies for data breaches underscores the need for further scrutiny and the type of "thoughtful and creative" solutions for which the Academies are known.

Belair began with a discussion of common ramifications after a breach and the harms and remedies that may be involved. He contended that class-action lawsuits do not represent an effective remedy for most data breaches. The research, document discovery, and attempts to prove concrete harm for these suits add up to a great deal of expense, and worse, in his view, class-action suits are not generally beneficial to consumers because they tend to award little money to the actual victims—those consumers whose information has been breached.

He noted that other types of lawsuits can be brought after a breach and spoke specifically about shareholder derivative or employee lawsuits. He observed that although data breaches have not proven to cause significant financial losses for their companies in the long run, in the short run, they can be very damaging for stock prices, and thus for their shareholders, who might try to bring suit. In addition, he noted that employees could also sue the company if it is their data being compromised, regardless of whether it was an employee responsible for the breach in the first place.

Belair described how there can be numerous longer-term costs for companies after a data breach, apart from those related to litigation or settlements. Employees and senior executives can lose their jobs; for example, Target's CEO resigned after the company's 2013 breach. In addition, he noted that there is the clear potential for harm to the company's reputation and its future costs of auditing and security can skyrocket. Reiterating the impact of even short-term stock plunges, Belair emphasized that these events can be a significant blow to a company's bottom line as well as the stock market more broadly.

Belair described how companies also face regulatory actions after a data breach. He noted that the Office for Civil Rights, the U.S. Department of Health and Human Services, the Federal Trade Commission (FTC), and other government agencies may get involved, depending on the nature of the data that was breached. Despite often being their opponent in lawsuits, Belair praised these agencies for being reliable, vigilant, and fair. He singled out the FTC in particular for focusing on breaches that showed gross negligence or malicious intent (such as a shocking eight separate breaches at one state university system) instead of breaches with little evidence of wrongdoing. As an example, he characterized a data breach lawsuit from 2008, in which Belair argued against the FTC, as a fair investigation, and one that resonated throughout the industry. "The point is, we need the FTC on the beat here," he said.

In fact, Belair posited that the FTC's power is currently too limited. Enabling the FTC to prescribe what constitutes adequate information security could lead to a more effective security standard that would help to prevent breaches. Other regulatory bodies, such as the Federal Communications Commission, the Securities and Exchange Commission, the Consumer Financial Protection Bureau, and state attorneys general, might also provide valuable input, he said.

Despite what he views as a true need for a national standard for data security and breach recovery, Belair said he is not optimistic that one will emerge. Pointing out that there have been a number of failed bills introduced in Congress, he contended that no privacy bill would be balanced in a way that would satisfy both consumer advocates and businesses. Privacy is a complex issue, and he observed that lawmakers can be reluctant to pass a bill that can have unforeseen consequences.

Despite what he views as a true need for a national standard for data security and breach recovery, Belair said he is not optimistic that one will emerge.

Belair offered an outline of some of the many questions to answer before a standard can be developed: for example, What is the right standard for liability—strict liability, negligence, reasonability, or some combination of these? How much should be offered in damages? What types of information are protected, and should there be state, federal, or court-imposed requirements for data security?

Belair brought up the breaches at Ashley Madison and VTech as situations without obvious financial harm, but with potentially deep psychological harms. In response to a question from Yoshi Kohno, Belair considered whether it might become more common to see breaches in which personal or reputational damage is the main target, rather than financial or fraud-related ends. For example, he said, in this presidential election year, it would not be surprising to see a major breach that is intended to undermine the campaign of a presidential candidate. The data breach laws, in his view, are not nuanced enough to cover these situations, despite the information leaks being serious, potentially devastating events in people's lives.

Belair closed by highlighting three constructive changes he has observed over the past 20 years. First, he emphasized that real progress has been made around data security. For example, most states have some kind of data privacy laws in place, and the Gramm-Leach-Bliley Act requires financial institutions to safeguard consumer data. Second, he expressed optimism that technology will continue to offer fixes, such as encryption, that make data security easier and better, although of course, companies will have to decide to invest in these fixes. And finally, Belair said he believes the culture around data security is changing. More and more, consumers have higher expectations for data security, and he noted that companies are now making clear investments in meeting these expectations by creating positions such as chief security officer, chief privacy officer, and chief compliance officer.

Prompted by Eric Grosse, Google, Inc., Belair addressed the tensions between information sharing and legally privileged company information. He offered the caveat that, as a lawyer who represents breached companies, his perspective is likely different from many others in the room. Belair noted that it is natural for companies and their legal teams to take advantage of whatever opportunities and resources are available. He said that companies can often satisfy the needs of the FTC or other regulators without divulging privileged information, yet in the context of litigation, privilege must be used in a much more limited way.

In a theme that ran throughout his presentation and the discussion that followed, Belair expressed concern over the state and influence of cybersecurity insurance. With dozens of such insurance carriers today—up from just six carriers in 2008—the vast majority of companies have cybersecurity insurance. Belair described how when issuing policies, insurers collect enormous amounts of data on the companies they cover, requiring comprehensive questionnaires and documentation covering all aspects of the company's security measures, company processes, and employee policies. Because of the lack of federal policies for security standards, Belair said these insurance companies are essentially creating security policy. Describing a specialist insurer client of his as an example, Belair said that the company has such a large percentage of the market share for cybersecurity that it "probably makes more pervasive and important decisions about cybersecurity inside America's corporations than any other entity."

Policy created by insurers may or may not be the optimal way to create national standards, Belair said: "The question for you guys is, does that make sense? Is that what we want?" The answer may be yes—Bob Blakley pointed to the success of fire and building codes, which were largely driven by the insurance industry, as an example of the potential benefits of this approach—but Belair emphasized that it is still a question worth asking.

## BREACH RESPONSE—VIEW FROM THE TRENCHES

**James Harvey, Alston & Bird**

James Harvey, a partner in the Technology and Privacy Group at the multinational law firm of Alston & Bird, was among the first attorneys in his firm to establish a special practice in data privacy and cybersecurity. As co-chair of Alston & Bird's Privacy and

Security Task Force and the firm's Cybersecurity Preparedness and Response Team, he has been focusing on data breaches and breach responses nearly exclusively for the past several years.

In his talk, Harvey attempted to demystify the actions lawyers often recommend to a company after it discovers a data breach. From a legal perspective, everything changes once a company discovers or is notified of a breach, he said, describing the complexities of a breach response as "a pressure-cooker of an experience" and "truly a corporate root canal." However, this process can begin slowly, he said; rather than a bright line being crossed, it is often more like an evolving realization as evidence accrues, until the point at which the company truly understands what has happened and what its liability is.

Harvey noted that it often takes a third party to discover that a company has been hacked. Sometimes companies are contacted, formally or informally, by a government agency, such as the FBI. Reporters also break these stories through connections within the hacker community or other companies. Harvey mentioned Brian Krebs, a former *Washington Post* journalist who now writes the blog *Krebs on Security*, who is a well-known and widely respected source of information on security breaches. Harvey said Krebs is often remarkably accurate; he constantly monitors Krebs' Twitter feed for stories about his clients. Harvey said that when Krebs notifies a company about a potential breach, that company goes on high alert.

Harvey described how the data breach at the payment processing company Global Payments in 2012 illustrates the power Krebs and other security journalists wield when they disclose a possible breach. He said that the breach was reported on between 9:00 and 9:15 a.m. on a Friday, and within 2 hours, the company's share price had dropped 24 percent, and trading in the stock was halted altogether. Because Global Payments is a publicly traded company, the breach had enormous implications not only for the company itself, but also for its investors and the wider financial services industry. Harvey pointed out that companies suffer these implications regardless of whether a reported breach turns out to be true or not, and he cautioned that journalists should be cognizant of the disastrous consequences data breach stories can have.

Harvey discussed how once they suspect a breach, executives have many decisions to make: Should the company put out a press release? When? What if the first release is wrong, and they have to retract the initial report? What effect will disclosure or nondisclosure have on the company's stock price, customers, or reputation? It is the legal team's job to be aware of the potential liabilities when advising clients. Harvey said that companies must also be aware that suspected or potential data breaches are tantalizing stories for the media, prosecutors, regulators, and other stakeholders. Disclosures and their timing can have immediate and lasting effects on stock prices, customers' trust, and other downstream effects. In some cases, he said, even Congress will probe exactly what the company did from the first red-flag event until the breach was investigated and disclosed.

Harvey discussed a major breach at Target, noting that the company stated in an initial press release after the company's 2013 breach that they had "identified and resolved the issue." Two weeks later, another press release admitted that the breach was more extensive than the company had realized, and that it was not in fact resolved. While companies may want to rush to disclose, Harvey said that he advises them to choose their language carefully in order to avoid issuing retractions or incurring lawsuits or regulatory fines. He encourages clients to view breaches as a brand-building experience; customers might remember the breach if the company handled it well, but they will certainly remember it if the company botched it.

Harvey noted that the United States has a patchwork of state laws for handling data breaches, as opposed to one clear and straightforward system.

Cyber incidents are expensive, and Harvey said that one of the highest costs is the investigation. Within hours of learning about a potential breach, he said, incident response forensic investigators, who operate under legal privilege on the company's behalf, are called in. In the case of a large breach, Harvey said that the cost of this response team can be five times higher than the legal costs.

Harvey highlighted how far-reaching and expensive data breaches are, as well as how complicated the web of liability can be. In the 2015 breach of Anthem, Inc., for example, although the data was breached on Anthem's servers, it was their customers—the administrators of benefit plans and insurance companies, for example—who had to notify affected consumers, he said. In the Target hack the same year, Target was liable, to the tune of tens of millions of dollars, to the credit card companies whose card numbers were stolen. In fact, Harvey observed that credit card companies have a great deal of power when it comes to data breaches involving credit card information; Harvey categorized the companies as "judge, jury, and executioner" in these situations. "It's a very difficult circumstance," he said. "From a monetary exposure perspective, particularly for retailers and those involved in the payment card business, this is where the real money is at issue."

Right now, Harvey said that the United States has a patchwork of state laws for handling data breaches, as opposed to one clear and straightforward system, yet plaintiffs often rush to bring data breach suits that can threaten confidential company information. When a company shares breach information, officially or unofficially, with a third party—such as law enforcement, regulators, or an ISAC—that information may become public during a lawsuit, potentially exposing the data and the company to additional risk, he noted. Harvey expanded on this point in response to a question raised by Richard Danzig, Center for a New American Security, specifying that malware signatures and IP addresses will likely be shared, but companies have a legitimate interest in keeping personally identifiable data, as well as information about the ongoing investigation, under privilege, in the context of breach investigations or lawsuits. Although forensics investigators may uncover a trove of information, this information should be generally considered under legal direction in anticipation of a lawsuit. Harvey recognized that this delicate balance of sharing or not sharing information can raise tensions, but he pointed out that companies have a right to a certain level of privacy while they are trying to investigate and respond to a breach.

Harvey switched gears and asked a question that provoked a wide discussion among attendees: Is there true consumer harm when a credit card number is stolen? If no identity fraud is committed, he posited that a consumer has not suffered a tangible loss. "A lot of times there is no consumer harm, in terms of those pure dollars out of pocket," he said. "The other types of harm are intangible, if you will, and much more difficult to quantify."

Fred Schneider pointed out that time spent resolving the issue is indeed a cost and, therefore, represents a harm to a consumer. Fred Cate, Indiana University, suggested that credit card companies could reduce this burden by making the process of changing one's credit card numbers after a breach more automated, for example, not just by sending a new card in the mail but by making it easy for consumers to automatically update the card numbers on all of their regular charges. Expanding on this idea, Bob Blakley noted that payment systems such as Apple Pay and Samsung Pay use one-time numbers that are distinct from the primary account number for each transaction, suggesting that such technological solutions could help further reduce the burden of replacing credit cards after a breach.

Tying into this discussion, Harvey raised the issue of "breach fatigue," suggesting that after so many breaches, consumers no longer judge breached companies as harshly and no longer take breach notifications as seriously as perhaps they once did. But while the harms from disclosure of credit card numbers alone may represent limited harm in his view, combining credit card data with additional personal details such as social security numbers, fingerprints, or federal background checks amounts to a potentially much bigger problem. The threat is particularly acute, he noted, if such information falls into the hands of a foreign adversary as part of a nation-state backed hack.

Paul Kocher, Cryptography Research, Inc., expanded on the different types of harms that can result from breaches, citing suicides that allegedly resulted from the Ashley Madison breach. In addition, he noted that a reporter told him that she fears cybercrime reporting because of the risk that hackers will make public her personal information, a practice known as doxxing. He pointed out that these are real harms that remuneration or credit monitoring cannot resolve.

Turning from consumer harms to the harms suffered by a breached company, Yoshi Kohno raised the question of whether there is any indication that breaches might—in the future, or even today—result not only in the exfiltration of data but in the modification of a company's records. Harvey said this is a real danger that can call a company's publicly reported numbers into question, but it depends on what data has been accessed. It can be extremely difficult to determine exactly what data has been accessed, acquired, or even modified, and all of these unknowns can have ramifications for the company and its liability, he said. As a result, data breaches can create a legal quagmire for consumers and for companies, with far more questions than answers.

## THE CHALLENGES OF REMEDIATION

**David Vladeck, Georgetown University**

David Vladeck, currently a professor at Georgetown University Law Center, formerly served as director of the Bureau of Consumer Protection at the FTC, where he oversaw numerous data breach and privacy-related investigations. He shared his perspective on the inadequacy of current data breach remediation measures, addressed the motivations for breaches and the types of harms they cause, and raised pointed questions about ways to not only mitigate the effects of breaches, but actually prevent them from occurring in the first place.

Data breaches are all too common and affect a huge swath of the population, essentially making normal what should, in Vladeck's view, be considered unacceptable. In 2014 alone, 110 million Americans—more than one-third of the population—had their data breached, he noted. Vladeck began by emphasizing how important it is to find better solutions for data breaches, which in his view have not been properly addressed in the policy sphere. "I'm really delighted that this group is taking a hard look at this problem, because this problem has plagued us for a long time and it has not received the attention I think it deserves from policy makers," he said.

Expressing little confidence in current remediation efforts, Vladeck characterized typical breach remedies as "crude," "a poor substitute for avoidance," "the least robust remedy available," "the last step in a cascade of bad options," and "simply an effort to staunch a wound, when the wound has already been inflicted." Financial remediation, he said, cannot return the user to the pre-breach status quo, because the information is still vulnerable. It also cannot begin to address the $25 billion aggregate annual losses to businesses from identity theft in the United States, a figure Vladeck noted is $11 billion larger than the aggregate loss from all property crime. In response to a question raised by Bob Blakley, Vladeck noted that although consumers likely do not end up footing the bill for that full figure in dollars, "they pay with their time, with their mental health" as they go through the difficult processes required to correct credit card fraud or claim identity theft.

In the case of a breach involving nonfinancial information, such as children's data, medical data, or private photographs, Vladeck said, "remediation is essentially a mirage." No amount of credit monitoring, credit freezes, or other currently available remediation tools can offer comfort to victims, for example, who had their medication use, their children's information, or their personal photos exposed in situations in which they had an expectation of privacy. "There's no remediation for this kind of outrageous assault on privacy," Vladeck said.

Because remediation does not currently address the harms done by data breaches, Vladeck urged attendees to devise strategies "to reverse the tide of data breaches in the first place." Two changes are needed if that is to happen, he said: companies and the government must secure data in a way that is appropriate to its level of sensitivity and volume, and lax security practices must be penalized to a far greater degree than they are currently.

In order to assess whether companies are securing data appropriately, what constitutes appropriate data security must first be defined. To do this, Vladeck suggested that researchers should conduct retrospective analyses of data breaches (once the details have been publicized and anonymized). Vladeck said that when the FTC brings data breach cases to court, it does make those elements public, but for every breach case, there are many more investigations where potentially valuable information—rich data from which researchers could glean insight into how breaches happen—is not publicized, due to existing FTC statutes. Although researchers, as a result, only have access to what Vladeck said is "the tip of the iceberg" in terms of total data breaches, that information can be a useful starting point for greater insights into what works and what does not in terms of data security protections.

Vladeck noted that the most common type of data breached, and the majority of the cases the FTC has brought so far, is personally identifiable information. He contended that these breaches can often be attributed to "inexcusably poor security measures by the company." As an example, he cited the 2008-2009 breaches at Wyndham Worldwide Corp., in which the company was breached three times in 18 months, which resulted in the credit card information of more than 600,000 people winding up in the hands of the Russian mafia.

Vladeck noted that the release of personally identifiable information has concrete harms because it allows criminals to commit identity fraud, a crime that has skyrocketed in recent years. He said that in 2014, the FTC fielded 332,000 identity fraud complaints, a number that only includes those who completed the FTC's exhaustive online form. The agency estimates that for every completed form, there are 10 to 20 other victims who either never completed the form or never even knew to file one in the first place—amounting to an estimated 1,000 identity theft victims each day.

The enormous growth in identity fraud coincides with the enormous growth of the Internet economy, said Vladeck; he cited several examples of vulnerabilities in home Internet use. TRENDnet recently settled a case in which its baby monitors were using an unsecured wireless video feed that allowed hackers to easily gain access to videos of children and individuals inside their homes. FrostWire, a peer-to-peer file-sharing application, settled with the FTC because its default setting made it too easy for customers to unwittingly expose their personal files. The so-called "Internet of Things," a trend in which our daily lives and homes are becoming ever more tied to the Internet, further increases our vulnerability. Vladeck imagined a "smart" refrigerator alerting its owner that he has run out of beer through an insecure connection with no data encryption. While this may not be personally identifiable information, that doesn't mean that it shouldn't stay private.

In addition to intentional hacks, Vladeck observed that the accidental release of information presents a serious concern for data security and privacy. As an example, Vladeck pointed to an accidental release of data about Prozac users by the drug company Eli Lilly in 2002. Pharmacies use unsecured trash receptacles to dispose of sensitive medical information. Stiff penalties might be the only way to stop companies from being so egregiously careless with private, potentially valuable information, Vladeck said.

Like the other speakers at the workshop, Vladeck recognized the difficulty of quantifying harm to a consumer after a breach. To address this, he suggested drawing ideas from fields that quantify harm probabilistically. For example, in medicine, it is impossible to say that being exposed to a toxic substance means a person is 100 percent likely to develop cancer, but the exposure is considered harmful if it raises the person's cancer risk past a certain threshold. Similarly, Vladeck noted, when a person's data is breached, it is not guaranteed that identity fraud will occur today, but, as the criminal's intention is likely to use or sell that data, there is undoubtedly an increased risk of identity fraud in the future. In that sense, the harm is virtually certain, although it is impossible to predict when the fraud will occur. "We need to recognize that the risk of identity theft itself is a real harm, just the way the risk of cancer and the risk of other things that are bad are real harms," Vladeck said.

As for tangible financial harm after a breach, Vladeck rebutted the suggestion that current measures to protect consumers against fraudulent credit card charges makes a credit card breach essentially harmless: "It is simply not true that the people whose financial information was taken as the result of the big breaches suffered no loss." While they are protected from unauthorized credit card charges, that right is time limited, he noted. In a case like Wyndham, in which the fraud unfolded over the course of 18 months and some victims were not notified until years later, that time window might have closed. In addition, to benefit from these protections, consumers must notice a fraudulent charge in the first place, which Vladeck suggested is often not the case. Thieves are creating sophisticated, believable charges that don't raise red flags. They "are not stupid enough to put 'Russian mafia' on your credit card statement," said Vladeck. Rather, they create a small charge, such as $7.99 or $9.99, with a generic name. He cited a scam based in Eastern Europe that used the names of U.S. presidents as part of the names of phony companies, in the hopes that consumers wouldn't notice anything amiss. In that case, he said, they judged consumers correctly, and were able to skim hundreds of millions of dollars.

> Vladeck emphasized that we need to recognize that the risk of identity theft itself is a real harm.

While one could argue that consumers must be responsible for their own protection, Vladeck contended that practically speaking, that is incredibly difficult. A consumer must not just own a computer, but be a skilled user. After a breach affecting financial data or personally identifying information, phone calls to the organizations theoretically capable of addressing identity theft or fraud typically offer little assistance: Calling a credit monitoring service, or even the Internal Revenue Service, often gets a victim nowhere, he said. For these reasons, Vladeck is emphatic that consumer harm is real. There is virtually no pathway to follow after a breach of nonfinancial information, such as medical data, private photographs, or the like. In those situations, the onus of reclaiming identity falls to consumers. When a child's data is breached, the fraud often isn't discovered until a child reaches adulthood and needs to rely on his or her identity to open a credit account, buy medical insurance, or sign up for a loan. In these instances, again, current remediation efforts provide little value.

Vladeck concluded by enumerating another harm from today's constant stream of data breaches: a growing mistrust of the Internet economy. Computer hacking was the crime most worrisome to Americans in 2014, and more than 60 percent of Americans are concerned about the security of their credit card information, phones, or computers.[1]

In a question, Deirdre Mulligan raised the point that remediation is necessary because no matter how solid data protections become, breaches will remain, at least to some degree, inevitable. Vladeck agreed, but restated his position that companies must try as hard as they can to prevent breaches, but he acknowledged that some data

[1] R. Riffkin, 2014, "Hacking Tops List of Crimes Americans Worry About Most," October 27, http://www.gallup.com/poll/178856/hacking-tops-list-crimes-americans-worry.aspx.

breaches take place even when strong security measures are in place. He observed that although it may be good news for the company that breaches ultimately are not very expensive with today's remediation measures, that is bad news for the consumer. He contended that holding companies who fail to take adequate precautions to a strict liability regime, covering all types of data, would offer a stronger motivation to protect consumers' data. "Sometimes a stick is as good as a carrot," he said.

Noting that data is often sold or passed to multiple third parties, Yoshi Kohno asked which parties should be legally responsible for securing that data and responding to any breaches. Vladeck answered that whoever had the data breach is the one responsible, not necessarily the first company who collected or generated the data. Expanding on this point, he noted that even data that is properly secured, encrypted, or quarantined can be breached. While conceding that breaches will continue to happen, Vladeck emphasized that they are less significant when a company has done a thorough job securing data and that, in many cases, companies likely have the capability to better secure consumer data. After all, he observed, companies often aggressively guard their own trade secrets even while they take far less rigorous measures to protect payment information or other personally identifiable data.

Fred Cate pointed out that the government never intended for social security numbers to be secret; they only became so when banks started using them for account passwords. Perhaps instead of protecting certain numbers, there is a way to make the infrastructure more flexible when proving an identity, he suggested. Vladeck concurred that this is a promising idea that warrants further research. Picking up on Cate's point, Schneider parsed the problem as one between personal identifiers (such as labels, phone numbers, or names) and personal authenticators (such as a PIN, token, or biometric), and instead of protecting identifiers, we should be requiring authenticators. Vladeck cautioned that authentication is difficult for the user to navigate, although he agreed that it is more secure.

Returning to an idea explored in several other presentations, Steve Lipner brought up the role insurers play in this sphere. Vladeck suggested that their presence improves data security discipline among companies, for example, by refusing coverage to companies who do a poor job of data security. However, on balance, he said he agreed with Belair that interests of insurance companies are not always aligned with the consumer's or the public's, and thus these companies might not be the appropriate parties to, essentially, create security policy. Although security standards are needed, Vladeck said, insurers—and even government bodies—are not necessarily the only or best ones to create them. For example, private standard-setting organizations, such as the International Organization for Standardization, could collaborate to develop enforceable, effective security standards for companies.

# DATA BREACHES AND THE FEDERAL TRADE COMMISSION

**Aaron Burstein, Federal Trade Commission**

Aaron Burstein is a senior legal advisor to Commissioner Julie Brill at the FTC, where he advises on enforcement and policy matters concerning privacy, data security, financial practices, and a range of other consumer protection issues. He has also focused on consumer protection issues in past roles at the White House and the U.S. Department of Commerce. He specified that he was speaking at the workshop for himself and not on behalf of the FTC.

Noting that his experience overlaps that of David Vladeck, Burstein expanded on and clarified some of the themes brought up in Vladeck's presentation and subsequent discussion. He sought to widen the lens from a focus on data breach incidents themselves to the broader context of data security practices and the FTC's role in policing those practices.

Burstein began by delineating the boundaries of the FTC's authority. As a consumer protection agency, the FTC does not pursue criminal activity and does not try to chase down hackers. Rather, its charge is to protect consumers from unfair or deceptive practices, which is generally how a data breach against a company is characterized. Burstein noted that not every breach FTC investigates leads to an enforcement action, nor does every action include a data breach. Of the hundreds of FTC investigations that have been conducted following reported breaches, he said that only about 60 cases have been brought. (In response to a question from Sasha Romanosky, Burstein said it is likely that there are more cases worth bringing than the FTC currently has the capacity to handle, but he did not specify how many more would potentially be brought if more attorneys were available.)

Through these cases, the FTC has developed a broad notion of both qualitative and quantitative harm; Burstein reiterated how difficult it is to measure qualitative harm and noted that the FTC proceeds cautiously in addressing it. One reason for this is that the FTC is governed by a legal standard of "unfairness," which, in order to win a case, requires "proof of substantial injury to consumers, costs that don't outweigh the benefits, and something that wasn't reasonably avoidable by consumers." However, the variety of potential consumer harms is increasing as data breaches evolve into new areas. Burstein observed that qualitative harm can now be caused by breaches of sensitive information such as private photos, children's information, geolocation information, or medical data, for example. Burstein described a case in which a medical transcription company inadvertently made transcriptions of doctors' patient notes available to public search engines. The case resulted in FTC enforcement action.

It is also possible for the FTC to bring cases before a data breach has occurred.

Burstein described instances in which the FTC took action after discovering apparently inadequate data security measures. In response to a question from Paul Kocher, Burstein noted that disclaimers by a company may do little to protect them from FTC action, because the FTC is empowered to look more broadly at the underlying practices of a company. If the agency discovers statements that appear to be deceptive or practices that may be unreasonable, the FTC may still build a case, despite any stated disclaimers.

In the vast majority of cases in which it takes action against a company, Burstein said that the FTC enforces nonmonetary "conduct" remedies. Depending on the facts of a particular case, the agency can require a company to implement a comprehensive security program or require that the company obtain and submit to the FTC biennial security assessments for a period of 20 years, for example. These conduct remedies are meant to fix errant behavior and send a strong message to other companies about security expectations. Burstein observed that conduct remedies do not offer immediate relief for the consumers whose data has been breached, and only in rare cases does the FTC recover money from a data security defendant. In response to a question raised by Paul Kocher about cases involving organizations with no revenue stream, such as open-source software, Burstein said that a monetary judgment can still be entered, although it is typically suspended for amounts that are beyond a defendant's ability to pay. By entering it into the record, Burstein said, the judgment can help to inform future cases even if the company does not actually pay the full amount of the judgment.

Burstein observed that these conduct remedies are meant to fix errant behavior and send a strong message to other companies about security expectations.

Turning to the question of what more could be done to prevent or reduce the impact of breaches, Burstein reiterated the idea, discussed earlier in the workshop, that technical measures may be employed to make information less useful after a breach. He noted, however, that especially with the trend toward the Internet of Things, the economics of convincing companies to invest properly in information security becomes more challenging when devices are low-cost, abundant, and designed to be used for only a relatively short period of time. In his view, the FTC can help address this by identifying appropriate information security practices, or, at the very least, identifying what constitutes an unreasonable vulnerability. Burstein observed that the FTC has learned a great deal about best security practices that can be useful to help companies identify and address weak security measures. He noted that through publications, workshops, and direct interaction with industry, the FTC aims to help software developers understand the lessons that have been learned—sometimes the hard way—by other companies.

Yoshi Kohno asked whether the FTC had insights into the security practices of U.S. companies as they compare to companies in other countries, a question Burstein said he was unable to address because he had not been closely involved in examining companies outside of the United States.

In response to questions raised by Mulligan and Sanders regarding standard setting, Burstein said it would be a "tough balance" for the FTC to participate in setting technical standards because of its primary role as an enforcer, but that security guidance could be a better role for the FTC. For example, the FTC could theoretically recommend that consumer products be set to the highest privacy settings by default, or issue reminders for users to tighten their own security measures, such as by varying their passwords or using conservative privacy settings. He also noted that the FTC does not have authority to issue regulations in the way that is typical of other agencies, and that the breadth of companies the FTC focuses on makes it challenging to create a rule that could be binding and required of companies that are subject to it.

# Concluding Plenary Discussion

The workshop concluded with a period of open, moderated discussion, giving participants a chance to raise additional issues and circle back to matters raised during the preceding presentations and discussions. This chapter, organized into thematic areas, describes the content of the final discussion and also integrates cross-cutting points made during presentations and earlier discussions, highlighting some of the broader themes that emerged throughout the workshop.

## DEFINING HARM

Many participants touched on the complexities of defining harm in the context of data breaches. Data breaches can cause harm at many levels, including harm to individuals, groups, companies, governments, and nations. Participants described examples of harms to individuals that include, among other possibilities, identity theft, the exposure of financial and medical information, damage to personal reputation, endangerment of personal safety, and psychological harms related to fear, loss of trust, and inconvenience. Several noted that data breaches have repercussions not just for individuals, but also for business practices and trade secrets, the economy, and national security.

David Clark, Massachusetts Institute of Technology, reiterated the need for a taxonomy of harms. A breach raises many unanswered questions; when one occurs, it is generally difficult to determine with certainty the motives of the attacker or the consequential harms that might occur months or years later, he said. When determining how to quantify, insure against, and recover from breaches, Clark pointed out that various types of harms—financial, medical, reputational—are all different in important ways.

At several points throughout the workshop, debate emerged about the degree to which disclosures of certain types of information, or the burden of dealing with the repercussions of a data breach—for example, the time and inconvenience of replacing a credit card—constitutes harm to a breach victim. Noting that it is easy to acquire, for a small fee, a large amount of public information about an individual, Butler Lampson, Microsoft Corporation, questioned the need for concern over disclosure of personally identifying information. Apart from special cases like Ashley Madison, he contended that disclosure of identifying information does not constitute a significant harm. In his presentation, James Harvey, Alston & Bird, suggested that having a credit card number stolen may not in itself constitute tangible loss if the consumer does not have to pay for any fraudulent charges and only has to have the credit card replaced. Others, including Fred Schneider, Cornell University, and Anita Allen, University of Pennsylvania, countered that the costs and harms in these situations are indeed real, even if the victim does not pay money out of pocket, not least because of the time it takes to update credit card numbers and take other necessary steps or protect one's finances or identity following a breach. Several participants commented that technological advances could help to reduce these burdens by allowing consumers to more easily replace a credit card and update all of their routine or automatic charges.

Not everyone is equally equipped to understand and appropriately respond to becoming the victim of a data breach.

To fully understand the harms of data breaches and build better models for remediation, it may be important to consider the specific circumstances of the victims. Allen pointed out that not everyone is equally equipped to understand and appropriately respond to becoming the victim of a data breach, suggesting that some groups, such as intellectually disabled adults, younger people, and the elderly, may be particularly vulnerable. "I think that a lot of us just don't have the means, the resources, to cope with the results of someone getting ahold of our data," she said.

Allen also shared her view that the conversation about defining harm from the legal perspective has stagnated over the past several years, with continuing debates over whether harm should be defined broadly, as it is throughout the rest of privacy law, or more narrowly to restrict liability, and whether or when a "no harm/no foul" approach might be appropriate.

# DATA BREACH ANALYSIS

The need for better mechanisms and incentives to prevent data breaches was a recurrent theme throughout the workshop, and discussants also noted the importance of learning from breaches so that aftermath and remediation work can help prevent future breaches.

Tony Sager, Center for Internet Security, emphasized the importance of learning lessons from previous incidents to implement good practices before another incident occurs. For example, he said it can make a big difference what parties are assigned administrative rights and who controls privileges. Poor security practices not only leave openings for a breach to occur, they also make it impossible or extremely costly to respond quickly when one does occur, Sager said. As Deirdre Mulligan, University of California, Berkeley, put it, “Your security practices upfront are about prevention, but they’re also basically the architecture for instant response.”

Suggesting that preventing data breaches should be thought of as an infrastructure issue, Fred Cate, Indiana University, expressed his view that there has been an inappropriate reliance on complicated password systems, which he called “silly infrastructures.” “We have been giving and listening to presentations for what, a decade now, about how worthless passwords are—so what does every company and government agency represented in [this workshop] do? It requires a password,” he said.

In her wrap-up comments, Mulligan pointed to a general sense among workshop attendees that “we’re standing on a pretty faulty [technical] foundation” and that systems need to be re-architected with an eye toward preventing breaches. Paul Kocher, Cryptography Research, Inc., described current systems as being “in the middle of a scaling problem.” Our technical foundations are expected to hold up an ever more complex array of data and systems, and they are cracking under the weight, he said, adding that this burden will only increase in the future. With the advent of the Internet of Things, individuals may have to update and maintain dozens of connected devices in their homes rather than just a few; a similar process is under way at the levels of companies and governments, he observed. “There’s this path that we’re kind of on by default, where more and more balls are going to get handed to the juggler, and we’re dropping some, and we’ll drop more,” Kocher said.

A partial solution, in Kocher’s view, is to invest more time and money in data protection at the early stages by investing in basic technical components that can have a big impact. For example, he said, instead of designing processors “where every device driver is one bug away from compromising the whole device,” software architectures need to be built so that some portions of data security stay intact even in the face of inevitable human error on the part of developers.

Steve Lipner built on these themes. In his view, conducting a thorough root cause analysis after a breach is not only crucial to fixing the weakness behind the current breach, but essential for learning how to avoid making the same mistake again. Whether the incentives to conduct such analyses come from the insurance industry or from standards bodies or other sources, "I think that feedback loop, given that security is imperfect, is super important and something that organizations ought to be building in," Lipner said.

## DATA BREACH REMEDIATION

Perhaps more than on any other issue, workshop attendees expressed broad agreement that current remediation measures are insufficient to address the harms caused by today's data breaches.

Credit monitoring is the overwhelmingly predominant remediation, a measure that many attendees viewed as not only inadequate protection against financial and identity theft—since it can only help victims detect identity theft but not prevent that theft from occurring—but completely inappropriate for a wide variety of other types of harms that can result from data breaches. David Vladeck, Georgetown University, reiterated the fact that there is no pathway for remediation of medical identity theft, for example, and emphasized the need to address such gaps. Schneider expanded on this point, suggesting that prevention, deterrence, and remediation might need to be wielded in different ways for different types of breaches. "We should stop thinking that data breach and identity theft are coupled—we should start thinking that there are lots of harms that could happen," Schneider said. "There are lots of remediations that are possible. Some harms may not have remediation, [in which case] you have to count on prevention and deterrence."

Cate suggested that in designing remediation measures, there is a need to be more specific about the type of data involved and the context of the breach. Lumping all breaches together, as is typically done in relevant laws, he said, fails to adequately address the variety of breaches that occur and also contributes to breach fatigue among victims, who likely routinely ignore notices and don't take steps to protect themselves because they simply do not pay attention to breach notices anymore.

Because it is challenging to identify harms from a breach, it is similarly challenging to quantify losses for the purposes of informing remediation. Bob Blakley, CitiGroup, Inc., raised the question of whether it is best to focus on losses to individuals or losses in the aggregate and whether the tort process or the statutory damages framework is better suited to addressing remediation. Although it is difficult to quantify the damage from a data breach, Reidenberg, Fordham University, noted that the ability to do so could open up consumer remediation via individual payouts, provide the basis for a new type of insurance to cover losses from data breaches, or help a court set statutory damage criteria. The outcome of a case currently with the Supreme Court, *Spokeo, Inc. v. Robins*, could influence some of these issues, he noted.

In terms of describing harms, designing remediation, and assigning liability, Mulligan posited that some types of information may need to be considered under the legal standard of strict liability because there is no way for a victim to fully recover from the repercussions of the breach. She cited as an example the Ashley Madison breach, which she said could be viewed as the equivalent of "an inherently dangerous product." She noted that in that case, the company had actually encrypted all of its customers' financial data, but the financial information did not constitute the totality of the sensitive information they were sitting on.

Allen contended that even breaches like Ashley Madison can and should be remedied in some way. "Privacy law in general has always, [in] the last 100 years, been there to deal with embarrassment, humiliation, shame. So we lawyers have a lot of examples and a lot of precedent to build on for why we should take this kind of harm very seriously and why we can address it through law." Mulligan noted that one of the weaknesses of this approach is that it requires the injured party to publicly acknowledge private matters in court, which can present a barrier, and she wondered whether it would be possible for such victims to be made whole in some other way.

Circling back to the question of companies' motives in disclosing or concealing information following a breach, Eric Grosse, Google, Inc., underscored the viewpoint that many companies do or should notify victims after a breach, not only because they "have to" in certain circumstances, but because it's the right thing to do—a point Heather Adkins, Google, Inc., had emphasized in her presentation. Of course, companies also listen to the guidance of their legal teams about what must be said and when it's perhaps wiser to minimize communications. But Grosse contended that companies ought to notify victims whenever possible because doing so helps them understand the cyber risks we all live with every day, helps to alleviate uncertainty, and perhaps more importantly, it allows victims a chance to respond. "I sort of resent the fact that it seems like the legal system is forcing us to minimize what we say," Grosse said. "I think that is not the right policy outcome."

Cate emphasized that there is a long way to go to adequately address breaches: "I'm not sure anyone has much to be proud of," he said of the current system. Offering a pointed analogy, he highlighted the inadequacy of breach notifications toward resolving the harms suffered by victims. "Our first and primary response, as a matter of legal systems or our society, has been to tell the person who has been victimized that they have been victimized," he said. "Imagine that in any other area—imagine we had a law for murder that said the first thing we're going to do is not try to arrest the person, not prosecute him, but let's tell the person who has been killed they have been killed."

Cate also expressed disappointment in the government's ability to appropriately respond to breaches, citing the federal Office of Personnel Management breach as an example. "The most extraordinary breach of our lives of the most sensitive information of a group of people to whom the government owes the most, and [the government] has done nothing, absolutely nothing," he said. "It took [the government] 3 months to admit it had even happened. For the next 3 months, it argued over how big it was. And now, it has offered credit monitoring!" Based on this track record, he said that in his view it would not be productive to rely on the government to provide adequate remedies. He recognized that the FTC may provide some solutions in the consumer space, although he noted that it lacks the necessary regulatory authority. Moreover, the discussion throughout the day made clear that there is no clear consensus on what the remediable harms are.

# MECHANISMS FOR CHANGE

Given the general sense among attendees that the current information security framework has not been effective at preventing, deterring, or adequately remediating data breaches, participants explored how the situation could be improved. In her closing comments, Mulligan noted that while there has been "a lot of money changing hands" and many lawyers and insurance companies getting involved in addressing data breaches, there is still a sense that there hasn't been much progress on the day-to-day protection of information. To move forward, she called for deeper thinking about harms and how problems develop, to allow the field to focus on creating incentives and infrastructure improvements where they can have the greatest impact.

## Understanding the Problem

Attendees discussed different conceptual frameworks for viewing data breaches and explored the need for data collection, sharing, and research.

Lampson suggested refocusing the discussion from data breaches in particular to the broader issues of "data flow"—a framework that encompasses all of the pathways through which data collected by one entity can be transferred to other entities—and how such flows can be traced and controlled. "You might take the view that data breach is just one extreme case of data flow, where there's a minimal amount of control involved," he said. Lampson also emphasized the "fractal" nature of information security, noting that the difficulty of solving subsets of the problem often seems just as difficult as solving the entire problem. As a result, making progress will require taking the broad view and being "much more ruthless" about setting priorities and addressing weaknesses, he said.

William Sanders, University of Illinois, Urbana-Champaign, and others emphasized the need for more data to fully understand the problem. He pointed to the illuminating data that had been presented at the workshop and said more studies were needed to understand both the policy and technical issues and how they fit together. Lampson expressed agreement but noted that there is a question about who is going to pay for collecting the needed data, because such an undertaking is likely to be difficult and potentially expensive. Vladeck noted that there is currently no comprehensive requirement to report data breaches to the government and suggested that some system of mandatory reporting could help address data collection issues as well as facilitate better remediation.

While attendees broadly expressed support for collecting more data and conducting more research on breaches, several noted inherent weaknesses in such research. For example, in data breaches and other cyber events, there are a lot of unknown unknowns—potential events that go undetected or unreported and cannot be appropriately accounted for. In reference to Sasha Romanosky's research on the costs and causes of cyber incidents, Grosse pointed out that phishing might account for a much higher percentage of breached data than the analysis recognized. In addition, Kocher said that comparing the costs of cyber incidents to other sources of loss, such as stolen intellectual property or bad debt, relies on a variety of studies using different methodologies and different data sources, which makes for a comparison that is, perhaps, at best an approximation.

Mulligan summarized the general viewpoint that thorough root cause analyses after breaches would be beneficial in identifying harms, risks, and threat models, but that these analyses are not conducted often enough. Another key issue, participants noted, is how to transfer lessons learned from one breach to help inform standards or practices that can help others avoid the same mistakes. At several points, workshop attendees discussed the potential role of Information Sharing and Analysis Centers (ISACs) in facilitating such exchange, but views on the merits of ISACs were mixed, and some favored other frameworks for information exchange.

## Setting Standards

Bob Belair, Arnall Golden Gregory, LLP,  noted that while workshop attendees expressed widespread agreement that reforms are needed to better address data breaches—for example, "as to what standards folks that are holding data ought to adhere to, what the process ought to be in terms of auditing and compliance with the policies, and then what happens if there is a breach and remediation"—he expressed doubts that these reforms would come in the form of federal legislation. The question then becomes, What is the right venue for these changes?

Belair suggested that giving rulemaking authority to the Federal Trade Commission

(FTC) would be one obvious approach, but in the absence of that, there are still ways for the FTC to take leadership by convening a multiagency effort, perhaps involving the National Academies of Sciences, Engineering, and Medicine, to give the private sector guidance. Lampson also noted that a consensus study from the Academies could help bring clarity on data breach harms, prevention, and remediation and help to establish standards. "I think it has been clear from this discussion that it would be good for the National Academies to undertake a study that can produce recommendations on this subject," he said.

Mulligan said there was enthusiasm for developing guidance about technical data security protection, such as configurations, defaults, and management. Belair concurred: "Really, you know, the truth is, except for outliers who you don't need to worry about, the private sector wants guidance. They want rules. They may not entirely like those rules, but getting rules creates certainty and is far better than being in a situation where you don't quite know what constitutes an appropriate approach to data security and to avoiding breaches," he said.

Allen said it is likely that the solution lies in some combination of technical fixes and strong incentives for the business sector. Allen and others noted that the increasing role of the insurance industry in incentivizing and even developing data security standards is an interesting recent development that warrants more consideration.

Cate reiterated that it seems clear that incentives are needed to help industry bear the cost of their breaches. It is only natural, he said, that industry and government would fail to adequately protect data when breaches do not have a major impact on the bottom line. Lampson agreed with this point but noted that there was no clear consensus on what form those incentives ought to take. One challenge, Lampson said, is that "there is this conflict between the desire to punish people for behaving badly and the desire to not stamp out innovation. And because a lot of this stuff is so new, it's extremely unclear, in my mind anyway, about how you can reconcile that conflict," he said.

Many agreed that a more thorough empirical and theoretical understanding of the problem would help to reconcile the difficult questions surrounding standards, incentives, and technology for better data breach prevention and response. Moving forward, Schneider said, "I believe we're going to probably come up with some principles that would justify remediations for different classes of harms." He noted that "if we got to that point, then we would really have a more powerful way to talk about laws that might compel people to do the right thing."

# Appendixes

# A Workshop Agenda and Participants List

## WORKSHOP ON DATA BREACH AFTERMATH AND RECOVERY FOR INDIVIDUALS AND INSTITUTIONS

**January 12, 2016**
**Keck Center of the National Academies of Sciences, Engineering, and Medicine**
**Washington, D.C.**

## AGENDA

12:30 p.m. Welcome and Overview

Fred B. Schneider, Forum Chair

12:45 Empirical, Consumer, and Data Holder Perspectives

Joel Reidenberg, Fordham University
Sasha Romanosky, RAND Corporation
Beth Givens, Privacy Rights Clearinghouse
Tom Murphy, University of Pennsylvania
Heather Adkins, Google, Inc.

2:50 Break

3:15 Legal and Policy Perspectives

Bob Belair, Arnall Golden Gregory, LLP
James Harvey, Alston & Bird
David Vladeck, Georgetown University
Aaron Burstein, Federal Trade Commission

4:55 Wrap-up Reflections and Discussion

Deirdre Mulligan, Forum Member

5:30 Reception

# PARTICIPANTS LIST

Heather Adkins, Google, Inc.
Anita Allen, University of Pennsylvania
Christina Ayiotis, Georgetown Cybersecurity Law Institute
Robert Belair, Arnall Golden Gregory, LLP
Robert Blakley, CitiGroup, Inc.
Shenae Bradley, National Academies of Sciences, Engineering, and Medicine
John Breyault, National Consumers League
Aaron Burstein, Federal Trade Commission
Fred H. Cate, Indiana University
David D. Clark, Massachusetts Institute of Technology
Richard J. Danzig, Center for a New American Security
Janel Dear, National Academies of Sciences, Engineering, and Medicine
Donna F. Dodson, National Institute for Standards and Technology
Ann Drobnis, Computing Community Consortium
Jon Eisenberg, National Academies of Sciences, Engineering, and Medicine
Eric Fischer, Congressional Research Service
Robert Fortson, Department of the Treasury
Beth Givens, Privacy Rights Clearinghouse
Eric Grosse, Google, Inc.
Emily Grumbling, National Academies of Sciences, Engineering, and Medicine
James Harvey, Alston & Bird
Paul C. Kocher, Cryptography Research, Inc.
Tadayoshi Kohno, University of Washington
Butler W. Lampson, Microsoft Corporation
Steven B. Lipner, Independent Consultant
Clifford Lynch, Coalition for Networked Information
William B. Martin, National Security Agency
Keith Marzullo, Networking and Information Technology Research and Development Program
Lynette I. Millett, National Academies of Sciences, Engineering, and Medicine
Deirdre K. Mulligan, University of California, Berkeley
Tom Murphy, University of Pennsylvania
Joel R. Reidenberg, Fordham University
Sasha Romanosky, RAND Corporation
Tony W. Sager, Center for Internet Security
William H. Sanders, University of Illinois, Urbana-Champaign
Fred B. Schneider, Cornell University
Lisa Singh, Georgetown University
Peter Swire, Georgia Institute of Technology
Scott Tousley, Department of Homeland Security
Charlie Tupitza, Global Forum to Advance Cyber Resilience
David C. Vladeck, Georgetown University
Helen Wright, Computing Research Association
Mary Ellen Zurko, Cisco Systems, Inc.

# B Planning Committee Biographies

**FRED B. SCHNEIDER**, *Chair*, is the Samuel B. Eckert Professor of Computer Science at Cornell University and chair of the department. He joined Cornell's faculty in Fall 1978, having completed a Ph.D. at Stony Brook University and a B.S. in engineering at Cornell in 1975. Dr. Schneider's research has always concerned various aspects of trustworthy systems—systems that will perform as expected, despite failures and attacks. Most recently, his interests have focused on system security. His work characterizing what policies can be enforced with various classes of defenses is widely cited, and it is seen as advancing the nascent science base for security. He is also engaged in research concerning legal and economic measures for improving system trustworthiness. Dr. Schneider was elected a fellow of the American Association for the Advancement of Science (AAAS;1992), the Association of Computing Machinery (1995), and the Institute of Electrical and Electronics Engineers (IEEE; 2008). He was named a professor-at-large at the University of Tromso (Norway) in 1996 and was awarded a doctor of science (honoris causa) by the University of Newcastle-upon-Tyne in 2003 for his work in computer dependability and security. He received the 2012 IEEE Emanuel R. Piore Award for contributions to trustworthy computing through novel approaches to security, fault-tolerance and formal methods for concurrent and distributed systems. The U.S. National Academy of Engineering (NAE) elected Dr. Schneider to membership in 2011, and the Norges Tekniske Vitenskapsakademi (Norwegian Academy of Technological Sciences) named him a foreign member in 2010. He is currently a member of the National Academies of Sciences, Engineering, and Medicine's Naval Studies Board and Computer Science and Telecommunications Board and is founding chair of the Academies' Forum on Cyber Resilience.

**FRED H. CATE** is vice president for research at Indiana University. He is the distinguished professor and the C. Ben Dutton Professor of Law at the Indiana University Maurer School of Law. He also serves as the managing director of the Center for Law, Ethics, and Applied Research in Health Information and a senior fellow and former founding director of the Center for Applied Cybersecurity Research. Professor Cate specializes in information privacy and security law issues. He has testified before numerous congressional committees and speaks frequently before professional, industry, and government groups. He is a senior policy advisor to the Centre for Information Policy Leadership at Hunton & Williams, LLP, and is a member of Intel's Privacy and Security External Advisory Board, the Department of Homeland Security's Data Privacy and Integrity Committee Cybersecurity

Subcommittee, and the National Security Agency's Privacy and Civil Liberties Panel. He serves on the board of directors of The Privacy Projects, the International Foundation for Online Responsibility, and the Kinsey Institute for Research in Sex, Gender and Reproduction. Previously, Professor Cate served as a member of the Academies' Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention, as counsel to the Department of Defense Technology and Privacy Advisory Committee, as a reporter for the third report of the Markle Task Force on National Security in the Information Age, as a member of the Federal Trade Commission's (FTC's) Advisory Committee on Online Access and Security, and on Microsoft's Trustworthy Computing Academic Advisory Board. He chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities. He served as the privacy editor for IEEE's *Security & Privacy* and is one of the founding editors of the Oxford University Press journal *International Data Privacy Law*. He is the author of more than 150 books and articles, and he appears frequently in the popular press. Professor Cate attended Oxford University and received his J.D. and his A.B. with honors and distinction from Stanford University. He is a senator and fellow (and immediate past president) of the Phi Beta Kappa Society, an elected member of the American Law Institute, and a fellow of the American Bar Foundation.

**ERIC GROSSE** is a senior member of the Google Security Team and previously vice president, Security and Privacy Engineering, at Google, Inc., in Mountain View, California, leading a team of 512 who ensure systems and data stay safe and users' privacy remains secure. Improved and wider use of SSL, stronger consumer authentication technology, detection and blocking of espionage, transparency on legal requests for data, sophisticated malware analysis, and tools and frameworks for safer building of web applications are among the achievements of the Google Security Team. Before Google, Dr. Grosse was a research director and fellow at Lucent Bell Labs where he worked on security, networking, algorithms for approximation and visualization, software distribution, and scientific computing. He has a Ph.D. in computer science from Stanford University.

**SUSAN LANDAU** is a professor of cybersecurity policy in the Department of Social Science and Policy Studies at Worcester Polytechnic Institute. Dr. Landau has been a senior staff privacy analyst at Google, Inc., a distinguished engineer at Sun Microsystems, and a faculty member at the University of Massachusetts, Amherst, and at Wesleyan University. She has held visiting positions at Harvard University, Cornell University, Yale University, and the Mathematical Sciences Research Institute. Dr. Landau is the author of *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (2011) and co-author, with Whitfield Diffie, of *Privacy on the Line: The Politics of Wiretapping and Encryption* (1998, rev. ed. 2007). She has written numerous computer science and public policy papers and op-eds on cybersecurity and encryption policy and testified in Congress on the security risks of wiretapping and on cybersecurity activities at the National Institute of Standards and Technology's Information Technology Laboratory. Dr. Landau currently serves on the Academies' Computer Science and Telecommunications Board. A 2012 Guggenheim fellow, she was a 2010-2011 fellow at the Radcliffe Institute for Advanced Study, the recipient of the 2008 Women of Vision Social Impact Award, and also a fellow of AAAS and the ACM. She received her B.A. from Princeton University, her M.S. from Cornell University, and her Ph.D. from the Massachusetts Institute of Technology.

**DEIRDRE K. MULLIGAN** is an associate professor at the University of California, Berkeley, School of Information and formerly a clinical professor of law at the University of California, Berkeley, School of Law. She was the founding director of the Samuelson Law, Technology and Public Policy Clinic, which she led from 2001 to 2008. Before coming to Berkeley, she was staff counsel at the Center for Democracy and Technology in Washington, D.C. Professor Mulligan's current research agenda focuses on information privacy and security. Current projects include qualitative interviews to understand the institutionalization and management of privacy within corporate America and the role of law in corporate information security policy and practice. Other areas of current research include digital rights management technology, privacy and security issues in sensor networks and visual surveillance systems, and alternative legal strategies to advance network security. Professor Mulligan is currently participating in a multistakeholder initiative, the Global Network Initiative, to advance and preserve freedom of expression and privacy through collaborative efforts aimed to resist government efforts that seek to enlist companies in acts of censorship and surveillance in violation of international human rights standards. During the summer of 2007, Professor Mulligan was a member of an expert team charged by the California Secretary of State to conduct a top-to-bottom review of the voting systems certified for use in California elections. This review investigated the security, accuracy, reliability, and accessibility of electronic voting systems used in California. Professor Mulligan was a member of the Academies' Committee on Authentication Technology and Its Privacy Implications; the FTC's Federal Advisory Committee on Online Access and Security, and the National Task Force on Privacy, Technology, and Criminal Justice Information. She was a vice chair of the California Bipartisan Commission on Internet Political Practices and chaired the Computers, Freedom, and Privacy Conference in 2004. She is currently a member of the California Office of Privacy Protection's Advisory Council and a co-chair of Microsoft's Trustworthy Computing Academic Advisory Board. She serves on the board of the California Voter Foundation and on the advisory board of the Electronic Frontier Foundation.

**PETER SWIRE** joined the faculty of the Scheller College of Business, Georgia Institute of Technology, in the fall term of 2013 as the Nancy J. and Lawrence P. Huang Professor, in the Law and Ethics Program. At Georgia Tech, he has appointments by courtesy with the College of Computing and School of Public Policy. Professor Swire has been a leading privacy and cyber law scholar, government leader, and practitioner since the rise of the Internet in the 1990s. In 2013, he served as one of five members of President Obama's Review Group on Intelligence and Communications Technology. Prior to that, he was co-chair of the global Do Not Track process for the World Wide Web Consortium. He is a senior fellow with the Future of Privacy Forum and a policy fellow with the Center for Democracy and Technology. Under President Clinton, Professor Swire was the Chief Counselor for Privacy in the Office of Management and Budget. He is the only person to date to have U.S. government-wide responsibility for privacy policy. In that role, his activities included being White House coordinator for the HIPAA medical privacy rules, chairing a White House task force on how to update wiretap laws for the Internet age, and helping negotiate the U.S.-European Union Safe Harbor agreement for transborder data flows. Under President Obama, he served as Special Assistant to the President for Economic Policy. Professor Swire is author of five books and numerous scholarly papers. He has testified often before Congress and been quoted regularly in the press. Professor Swire has served on privacy and security advisory boards for companies including Google, IBM, Intel, and Microsoft, and for 8 years he was a consultant with the global law firm of Morrison & Foerster, LLP. Professor Swire graduated from Princeton University (summa cum laude) and the Yale Law School, where he was an editor of the *Yale Law Journal*.

# C Speaker Biographies

**HEATHER ADKINS** is an 11-year Google, Inc., veteran and founding member of the Google Security Team. As manager of information security, she has built a global team responsible for maintaining the safety and security of Google's networks, systems, and applications. The Google Security Team, now numbering in the hundreds, is involved in every facet of the business, including launching new products, mergers and acquisitions, building security infrastructure, responding to security threats, and evangelism. Ms. Adkins has an extensive background in systems and network administration, with an emphasis on practical security, and has worked to build and secure some of the world's largest infrastructure for web information systems. She now focuses her time primarily on the defense of Google's computing infrastructure and working with both the Google Incident Response Team and outside entities to tackle some of the industry's greatest security challenges.

**ROBERT R. BELAIR** is a partner and practice leader of the Privacy Practice and co-chair of the Government Relations Practice. Mr. Belair is the managing partner of Arnall Golden Gregory's Washington, D.C., office. He is an internationally recognized privacy lawyer with more than three decades of experience and is a frequent writer and speaker on privacy topics. Mr. Belair focuses his practice on advising clients with all aspects of the privacy policy cycle. This has included drafting legislative language, submitting public comments, and engaging congressional and agency staff on the development of privacy policy. With regard to existing privacy requirements, Mr. Belair has assisted clients to develop comprehensive privacy compliance programs, responded to data breaches, and defended against administrative actions and litigation. He served as deputy counsel to the White House Privacy Committee in the Ford Administration and as a lawyer in the Federal Trade Commission's (FTC's) Bureau of Consumer Protection doing Fair Credit Reporting Act and other privacy-related work. Later, Mr. Belair served as general counsel of the National Commission on the Confidentiality of Health Records. In private practice, he was a founding partner of Oldaker, Belair & Wittie. He has done work for numerous government entities on privacy matters, including the National Science Foundation, the National Academy of Sciences, Engineering, and Medicine, the Department of Transportation, and the Social Security Administration. Mr. Belair has served on the Judiciary Committee Advisory Committee for Chairman Joe Biden (D-DE) and as an advisor to Senator Bob Bennett's (R-UT) Health Privacy Task Force. Together with Alan Westin, he was the editor of a preeminent privacy periodical for the business community, *Privacy & American Business*.

**AARON BURSTEIN** is a senior legal advisor at the FTC to Commissioner Julie Brill. At the FTC, Mr. Burstein advises on enforcement and policy matters concerning privacy, data security, financial practices, and a range of other consumer protection issues. Before joining the FTC in 2013, he was a policy advisor at the National Telecommunications and Information Administration (NTIA), where he played a central role in drafting the Department of Commerce's privacy "green paper" and the Obama Administration's "Privacy Blueprint." Mr. Burstein also served as director for privacy and civil liberties in the Cybersecurity Directorate of the National Security Council at the White House. Before joining NTIA, he was a research fellow at the University of California, Berkeley, and a trial attorney in the Department of Justice's Antitrust Division. Mr. Burstein earned his law degree from the University of California, Berkeley, and his undergraduate degree from Brown University.

**BETH GIVENS** is founder and executive director of the Privacy Rights Clearinghouse (PRC), established in 1992. The PRC is a nonprofit consumer education and advocacy organization based in San Diego, California. Its mission is to engage, educate, and empower individuals to protect their privacy. The PRC invites consumers to submit complaints and questions via its website. Its online guides cover a broad range of topics, including credit reporting, identity theft, data breaches, online privacy, computer security, financial privacy, medical records, workplace monitoring, data brokers, employment screening, telemarketing, and smartphones. The PRC's "Chronology of Data Breaches" has tracked breaches since 2005. Ms. Givens and her colleagues represent the interests of consumers in public policy proceedings at the state and federal levels. They have served on several task forces and working groups and are often interviewed by the media. Prior to her work as a consumer advocate, Ms. Givens was a librarian specializing in resource sharing. She has a master's degree from the University of Southern California's Annenberg School for Communication and a master's degree in library and information services from the University of Denver. She is a member of the International Association of Privacy Professionals.

**JAMES HARVEY** is a partner at Alston & Bird, LLP, in the Technology and Privacy Group, and co-chairs the firm's Privacy and Security Task Force and its Cybersecurity Preparedness and Response Team. Mr. Harvey's practice involves board-level and enterprise-wide issues at the intersection of global cybersecurity, privacy, technology, and data initiatives. Given his decades-long experience in the technology space, he was one of the first lawyers in the United States to focus on the criticality of privacy and data management issues for global corporations. This immersion in technology and data matters motivated Mr. Harvey to found the task force and response team well before other firms realized these issues faced their clients. Today, Mr. Harvey and these teams assist multinational clients from a wide array of industries with a full spectrum of cyber, privacy, and technology issues and adversarial matters and transactions, including everything from preparing companies and their boards for cybersecurity risks; responding to network intrusion and other security incidents; collecting, storing, processing, and monetizing personal and corporate data around the globe; and acquiring technology and services in today's networked world.

**TOM MURPHY** is the vice president of information technology and the university chief information officer (CIO) at the University of Pennsylvania. Mr. Murphy brings a successful track record of creating a vision and mission for business and technology professionals and building strong, customer-focused teams. He provides leadership for the university's information technology (IT) and leads the central IT organization that is responsible for providing core administrative information systems, campus data, voice, and video networks. He advises the provost and executive vice president on information technology issues. Mr. Murphy previously held CIO and senior IT leadership positions at DaVita HealthCare Partners, AmerisourceBergen, Royal Caribbean Cruises, Bristol Hotels & Resorts, Cendant Corporation, Omni Hotels, Interstate Hotels Corporation, and Marriott Corporation. He was elected to the CIO Hall of Fame in 2010. In 2011 and 2008 he was recognized at the Global CIO Executive Summit as a Top Ten Global CIO for Breakaway Leadership and Leadership and Innovation, respectively. His teams have been recognized for innovation, resourcefulness, and for being best places to work. He holds a B.A from the University of Richmond.

**JOEL R. REIDENBERG** is the Stanley D. and Nikki Waxberg Chair and Professor of Law at Fordham University where he directs the Center on Law and Information Policy.  He was the inaugural Microsoft Visiting Professor of Information Technology Policy at Princeton University teaching in the Computer Science Department and, more recently, a visiting lecturer teaching cybersecurity policy at Princeton's Woodrow Wilson School. Dr. Reidenberg has also previously taught at the Universite de Paris-Sorbonne and the Institut d'etudes Politques de Paris. He publishes regularly on both information privacy and on information technology law and policy. He is a member of the American Law Institute and an advisor to its Principles of Law of Data Privacy project. Dr. Reidenberg has served as an expert adviser to the U.S. Congress, the FTC, the European Commission, and the World Intellectual Property Organization. At Fordham, he previously served as the associate vice president for academic affairs and, prior to his academic career, he was an associate at the law firm Debevoise & Plimpton. Dr. Reidenberg is a graduate of Dartmouth College and earned a J.D. from Columbia University and a Ph.D. in law from the Université de Paris–Sorbonne. He is admitted to the Bars of New York and the District of Columbia.

**SASHA ROMANOSKY** researches topics in the economics of security and privacy, cybercrime, information policy, applied microeconomics, and law and economics. He is a policy researcher at the RAND Corporation. Dr. Romanosky holds a Ph.D. in public policy and management from Carnegie Mellon University and a B.S. in electrical engineering from the University of Calgary, Canada. He has published in the *Journal of Policy Analysis and Management*, the *Journal of Empirical Legal Studies*, and the *Berkeley Technology Law Journal*; coauthored two book chapters; and has written other works on information security. Dr. Romanosky was a Microsoft research fellow in the Information Law Institute at New York University and was a security professional for more than 10 years within the financial and e-commerce industries at companies such as Morgan Stanley and eBay. He holds a CISSP certification and is co-author of the Common Vulnerability Scoring System (CVSS), an open standard for scoring computer vulnerabilities.

**DAVID C. VLADECK** is a professor and co-director for the Institute for Public Representation at Georgetown Law School. Professor Vladeck holds a B.A. degree from New York University, a J.D. degree from Columbia University, and an LL.M. from Georgetown. Professor Vladeck teaches federal courts, civil procedure, administrative law, and seminars in First Amendment litigation and co-directs the Institute for Public Representation, a clinical law program. He recently returned to the Law Center after serving for nearly 4 years as the director of the FTC's Bureau of Consumer Protection. At the FTC, he supervised the bureau's more than 430 lawyers, investigators, paralegals, and support staff in carrying out the bureau's work to protect consumers from unfair, deceptive, or fraudulent practices. Before joining the Law Center faculty full time in 2002, Professor Vladeck spent more than 25 years with the Public Citizen Litigation Group, a nationally prominent public interest law firm, handling and supervising complex litigation. He has briefed and argued a number of cases before the U.S. Supreme Court and more than 60 cases before federal courts of appeal and state courts of law resort. He is a senior fellow of the Administrative Conference of the United States, an elected member of the American Law Institute, and a scholar with the Center for Progressive Reform. Professor Vladeck frequently testifies before Congress and writes on administrative law, preemption, First Amendment, and access to justice issues.

# OTHER RECENT REPORTS OF THE COMPUTER SCIENCE AND TELECOMMUNICATIONS BOARD

Continuing Innovation in Information Technology: Workshop Report (2016)
Future Directions for NSF Advanced Computing Infrastructure to Support U.S. Science and Engineering in 2017-2020 (2016)
Privacy Research and Best Practices: Summary of a Workshop for the Intelligence Community (2016)

Bulk Collection of Signals Intelligence: Technical Options (2015)
Cybersecurity Dilemmas: Technology, Policy, and Incentives: Summary of Discussions at the 2014 Raymond and Beverly Sackler U.S.-U.K. Scientific Forum (2015)
Interim Report on 21st Century Cyber-Physical Systems Education (2015)
A Review of the Next Generation Air Transportation System: Implications and Importance of System Architecture (2015)
Telecommunications Research and Engineering at the Communications Technology Laboratory of the Department of Commerce: Meeting the Nation's Telecommunications Needs (2015)
Telecommunications Research and Engineering at the Institute for Telecommunication Sciences of the Department of Commerce: Meeting the Nation's Telecommunications Needs (2015)

At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues (2014)
Emerging and Readily Available Technologies and National Security: A Framework for Addressing Ethical, Legal, and Societal Issues (2014)
Future Directions for NSF Advanced Computing Infrastructure to Support U.S. Science and Engineering in 2017-2020: An Interim Report (2014)

Geotargeted Alerts and Warnings: Report of a Workshop on Current Knowledge and Research Gaps (2013)
Professionalizing the Nation's Cybersecurity Workforce? Criteria for Future Decision-Making (2013)
Public Response to Alerts and Warnings Using Social Media: Summary of a Workshop on Current Knowledge and Research Gaps (2013)

Continuing Innovation in Information Technology (2012)
Computing Research for Sustainability (2012)
The Safety Challenge and Promise of Automotive Electronics: Insights from Unintended Acceleration (2012, with the Board on Energy and Environmental Systems and the Transportation Research Board)

The Future of Computing Performance: Game Over or Next Level? (2011)
Public Response to Alerts and Warnings on Mobile Devices: Summary of a Workshop on Current Knowledge and Research Gaps (2011)
Report of a Workshop on the Pedagogical Aspects of Computational Thinking (2011)
Strategies and Priorities for Information Technology at the Centers for Medicare and Medicaid Services (2011)
Wireless Technology Prospects and Policy Options (2011)

Limited copies of CSTB reports are available free of charge from:
Computer Science and Telecommunications Board
Keck Center of the National Academies of Sciences, Engineering, and Medicine
500 Fifth Street, NW, Washington, DC 20001
(202) 334-2605/cstb@nas.edu
**www.cstb.org**

*The National Academies of*
SCIENCES · ENGINEERING · MEDICINE

The nation turns to the National Academies of Sciences, Engineering, and Medicine for independent, objective advice on issues that affect people's lives worldwide.

**www.national-academies.org**