ITIF
The Information Technology & Innovation Foundation

The Need for an R&D Roadmap for Privacy

BY DANIEL CASTRO | AUGUST 2012

A research and development roadmap for privacy would help ensure that federal research dollars are directed to the most pressing privacy challenges.

The increasing use of data by the public and private sectors has put privacy issues at the front and center of many policy debates, including on health care, home energy efficiency, cyber security, transportation, and of course, e-commerce. Learning how to properly collect, manage and use data is an important challenge for many organizations. If privacy concerns are not adequately addressed, they may stall or disrupt the deployment of new technologies that offer many potential economic and quality-of-life benefits to consumers. But at the same time, if policymakers promulgate overly strict privacy regulations, they may stall or disrupt these same technologies. Effectively addressing privacy concerns in ways that do not block innovation will require a mix of new technologies and policies to ensure that data is properly safeguarded and consumers are protected.

Privacy regulations typically involve restrictions on the use of information. While regulations may be intended to protect consumers, ultimately restrictions on the use of information may also limit beneficial uses of information. Various government organizations, including the U.S. Department of Commerce and the Federal Trade Commission (FTC), as well as the White House, have recently focused on developing a stronger regulatory framework for addressing privacy concerns through policy. However, relatively little effort has gone into considering how new technology might address many of the same privacy challenges.[1] In part, this reflects a tendency among government policymakers to promote privacy, even at the expense of other goals such as beneficial sharing of information.[2] But it also indicates poor awareness of the potential benefits of

using technology to protect privacy. This is unfortunate because technology has an important role to play in improving privacy.

Consumers today benefit from many privacy-enhancing technologies that allow them to better manage and protect their personal data. These technologies are either integrated in other products or offered as standalone products or services. For example, Internet users can purchase virtual private network (VPN) or web proxy services that encrypt and anonymize Internet traffic, or use online services such as Personal or Reputation.com to manage aspects of their online identities.

While many privacy-enhancing technologies exist today, development of additional tools could positively impact consumer privacy. Additional development of privacy tools could also have a positive economic impact. Investments in developing technological solutions to privacy problems would help create a network of developers with expertise in this domain. Developers of such tools would likely be even more competitive in countries with strict privacy regulations, where there may be a stronger market for privacy-enhanced products and services.

Rather than block potentially harmful uses of technology, government should find ways to address known challenges so as to enable further innovation and adoption of technology. For example, if there are limits to what policymakers believe the public and privacy sector should do with data (because of limitations in the current state of the art in technology), then policymakers should direct more investments in R&D to overcome these challenges.

Advances in privacy research and technology could strengthen consumer trust and better protect consumer privacy while enabling continued innovation. For example, better privacy tools would help ensure that organizations could better manage data and give regulators more options for protecting consumer privacy. While some type of privacy metrics exist today (e.g. k-anonymity, l-diversity, t-closeness), more robust metrics would help organizations (and regulators) assess how well data has been anonymized. If new technology better addresses the concerns of regulators, then organizations may be able to continue to use data to develop new products and services.

The U.S. government funds millions of dollars of research in computer science and related disciplines, a portion of which is directly relevant to the privacy concerns of the public and private sectors. Many areas of privacy research would be useful across many different domains. For example, every government agency that uses personally identifiable information (PII) might benefit, either directly or indirectly, from advances in privacy-preserving data mining or new techniques to securely de-identify data. Similarly, industries such as health care and financial services would benefit from this research as well.

However, a set of clear research goals and objectives is needed to maximize the social and economic benefits of federal funds for privacy research. Given the potential benefits of more coordinated research in this field, stakeholders from the public and private sectors facing privacy challenges should work together to define shared objectives and direct funds to find solutions to common challenges. To that end, the U.S. government should create and fund a research and development (R&D) roadmap for privacy.

THE BENEFITS OF AN R&D ROADMAP FOR PRIVACY

Many countries have created R&D roadmaps for various industries including automotive, cybersecurity, photovoltaics, health care, nanotechnology and unmanned systems.[3] For example, the U.S. Department of Energy has created a roadmap to guide R&D activities for nuclear energy to address four specific challenges to expanding the use of nuclear power.[4] Similarly, an R&D roadmap for privacy would establish a common vision for privacy R&D and better align R&D activities with strategic objectives necessary to improve privacy across multiple sectors.

An R&D roadmap can also help ensure that privacy research is adequately funded. Comprehensive data on the amount and focus of privacy research do not exist. While the National Science Foundation (NSF) is likely the principle funder of this type of research, other agencies, such as the U.S. Department of Health and Human Services (HHS), the Defense Advanced Research Projects Agency (DARPA) and the Department of Homeland Security, also fund important related research. For example, the U.S. Naval Research Laboratory funded the initial development of the Tor Project, a system that allows users to anonymously route their network traffic to avoid surveillance. The Tor Project has also been funded by multiple U.S. agencies, including the Broadcasting Board of Governors and the NSF.[5] The U.S. Department of State and USAID jointly spent $76 million between 2008 and 2011 on "Internet freedom" programs, which include the development of anonymous communication technologies to avoid surveillance; they have committed an additional $25 million for 2012.[6] Similarly, the National Institute of Standards and Technology (NIST) funded development of online identity solutions as part of the National Strategy for Trusted Identities in Cyberspace (NSTIC).[7]

To enable this information to be better aggregated, funding agencies should start identifying and tabulating the research they fund on privacy-related topics. Initially, this information could be used simply to gain a baseline understanding of what privacy-related research is currently being funded. In the future, it could be used to identify progress toward specific privacy-research objectives. Monitoring privacy R&D funding will help avoid duplicative research and allow agencies and businesses facing privacy-related challenges to identify the latest research on particular topics. Researchers in the field could also more easily locate funding opportunities, while developers could learn of new research to integrate into new products and services.

A roadmap will also enable funders and researchers to identify potential resource gaps that must be addressed to meet certain priorities. There may, for example, be a need to develop and make available a set of test data for researchers, to provide appropriate training and support for new researchers, and to ensure sufficient support for underfunded research, including areas that currently lack sufficient market-based demand but that could yield important tools in the future.

AREAS FOR FURTHER RESEARCH

Technology is changing rapidly and these changes introduce new privacy challenges. For example, GPS and mobile devices have presented new concerns about the privacy of personal movement. Improvements in facial recognition technology have presented new

concerns about the privacy of biometric data. Social networking and ubiquitous computing have created concerns about the increased risk of surveillance. As technologies changes, new research is needed to better understand how to effectively protect consumer privacy. For example, research on differential privacy could improve the accuracy of queries from statistical databases while preserving the privacy of individual records; enhanced algorithmic and statistical approaches to de-identifying data could better preserve the utility of the data, especially for sparse data sets or data sets containing geo-location data. Similarly, additional research into computer-readable privacy policies could result in the ability to create policies bound to data so that, for example, data that has been de-identified stays de-identified. Or additional research on chains of trust could establish accountability among multiple parties that share data, such as in cloud-based systems. And just as federal-funded research on information security focuses on both "offensive" and "defensive" capabilities, privacy research should include research that not only finds weaknesses with current systems but also proposes solutions to improve consumer privacy.

Some of the research areas where further technology-based R&D could have wide-reaching implications for improving consumer privacy are

- Data de-identification
- Privacy-preserving data mining
- Usability and accessibility of privacy-enhancing technologies
- Secure, multi-party authentication
- Interoperable digital credentials
- Privacy metrics

In addition, many privacy problems are interdisciplinary in nature. For example, advances in human-computer interaction can improve the usability of privacy controls on mobile devices and social networks. Finding solutions will require bringing together researchers from different disciplines outside of computer science, including design, economics, behavioral sciences, and law.

NEXT STEPS

The next step for creating an R&D roadmap for privacy is to bring the research community and interested stakeholders together to define key priorities. To help facilitate this process, the Information Technology and Innovation Foundation has created "The Privacy R&D Roadmap" (www.privacyroadmap.org), a freely accessible website now available to the research community for collaboration on creating an R&D roadmap for privacy. This website allows stakeholders to easily engage in developing a preliminary list of illustrative real-world examples of where R&D research is needed and to describe the potential beneficiaries of this research. Using this website, registered users can submit their ideas on what should be included in the Privacy R&D Roadmap.

Collecting initial ideas for the Privacy R&D Roadmap is only the first step. In addition, stakeholders need to be brought together to begin developing the roadmap. This process should be led by a federal government agency. The NSF, working in partnership with the National Telecommunications and Information Administration (NTIA) and NIST in the Department of Commerce, and the FTC, should convene stakeholders to identify critical

priorities in privacy research and explore a variety of views about how they might best be addressed. This needs assessment should include representatives from agencies involved in both the collection and use of information from diverse fields such as health care, financial services and law enforcement. For example, it should draw on the expertise of various government agencies, such as HHS, the Internal Revenue Service (IRS), the Federal Bureau of Investigation (FBI), the Census Bureau, and the Securities and Exchange Commission (SEC). It should also build off of established interagency working groups in the federal government, such as the Open Government Working Group.

While the government should play a critical role as convener and facilitator, federal agencies should not try to use a "Manhattan Project"-style, top-down approach to privacy research. Instead, it should use a collaborative, multi-stakeholder approach to gain buy-in from both researchers and the private sector and to ensure that research findings are translated into practice. Working with stakeholders, the government can develop a list of key privacy research topics that are either not funded or under-funded by the private sector and government-sponsored research. Participants should also try to identify the most challenging problems in privacy. The NSF can work with academia and industry to link theoretical research with the most pressing applied problems. Stakeholders need not reach a consensus, but should work together to identify research goals of mutual interest. This will allow policymakers to craft a privacy R&D agenda that can help researchers identify key problems, research program managers allocate funds appropriately, and policymakers understand current technology challenges, limitations and opportunities.

Funding priorities can also be linked to short-term (1-3 years), medium-term (3-10 years) and long-term (10+ years) goals. The government must strike the right balance between basic R&D that has the potential to enable game-changing breakthroughs over the long term and applied research that tends to be more incremental and evolutionary.

Measuring innovation and research program effectiveness is difficult. It is not always possible at the beginning of a research project to identify what the outcomes will be or to guarantee that all projects will be successful. And many important research outcomes are by-products of research that was focusing on a different objective. For example, research on digital-rights-management technology was originally aimed at protecting intellectual property, but is now applied to preserve the privacy of medical records by preventing them from being copied. However, the federal government can identify key research areas, track how it allocates its research funds, and identify what research comes to fruition.

CONCLUSION

Organizations today routinely collect massive amounts of data. Information is at the core of many innovations, such as e-commerce, the smart grid, and use of electronic health records for health analytics. Policymakers should be encouraging data innovation and searching for opportunities to unlock the potential of the new era of "Big Data." While the federal government supports privacy research, the current approach to funding privacy-related research lacks coordination and direction. An R&D roadmap for privacy would help ensure that more federal research dollars are directed to the most pressing privacy challenges, and provide another tool for government to help protect consumer privacy.

ENDNOTES

1. Federal Trade Commission, "Protecting Consumer Privacy in an Era of Rapid Change," March 2012, http://www.ftc.gov/os/2012/03/120326privacyreport.pdf and The White House, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy," February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
2. Along these same lines, ITIF previously proposed that Congress should create a Data Policy Office within the Department of Commerce (rather than a Data Privacy Office solely focused on privacy) to create policies that would increase data sharing, reduce barriers to global information flows, and protect consumer privacy. See Daniel Castro, "Create a Data Policy Office not a Privacy Policy Office," Information Technology and Innovation Foundation, February 7, 2011, http://www.innovationfiles.org/create-a-data-policy-office-not-a-privacy-policy-office/.
3. See for example, "R&D Technology Roadmap," 2005, European Automotive Research Partners Association http://www.earpa.eu/docs/2005/furore_road_map_final.pdf, Chemical Industry Vision 2020 Technology Partnership, "Chemical Industry R&D Roadmap for Nanomaterials By Design: From Fundamentals to Function," October 2002, http://www.chemicalvision2020.org/nanomaterialsroadmap.html, David Infield, "A Roadmap for Photovoltaics Research in the UK," UK Energy Research Centre, August 2007, http://ukerc.rl.ac.uk/Roadmaps/Solar/A_Road_Map_for_Photovoltaics_Research_in_the_UK.pdf, "Health Research Roadmap: Creating innovative research for better health and health care," Canadian Institutes of Health Research, 2009, http://www.cihr-irsc.gc.ca/e/documents/strat_plan_2009_e.pdf, and Department of Defense, "Unmanned Systems Integrated Roadmap, FY2011-2036," 2011, http://www.fas.org/irp/program/collect/usroadmap2011.pdf.
4. U.S. Department of Energy, "Nuclear Energy Research and Development Roadmap," April 2010, http://www.ne.doe.gov/pdfFiles/NuclearEnergy_Roadmap_Final.pdf.
5. Tor. "Tor: Sponsors," n.d., https://www.torproject.org/about/sponsors.html.en.
6. U.S. Department of State, Office of the Spokesperson, "Internet Freedom Programs in the Middle East (Taken Question)," March 15, 2012, http://www.state.gov/r/pa/prs/ps/2012/03/185904.htm.
7. National Institute of Standards and Technology (NIST), "Pilot Projects," n.d., http://www.nist.gov/nstic/pilot-projects.html.

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing background information and ideas for this report: Rob Atkinson, Michelle Ash, Paul Bloom, Jeff Brueggeman, Lorrie Cranor, Sharon Grant, Susan Israel, Naomi Lefkovitz, Jeff Lenertz, Tim McNulty, Jon Peha, Javier Salido, Danny Sepulveda, Rob Sherman, Micah Sherr, Frank Torres, Sanjay Udani, and Jonathan Zuck. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

FOR MORE INFORMATION CONTACT ITIF BY PHONE AT 202.449.1351, BY EMAIL AT MAIL@ITIF.ORG, OR ONLINE AT WWW.ITIF.ORG.