Privacy: Computing, IT and Digital Media

Helen Nissenbaum
New York University

Privacy has been a critical social issue associated with computing, information technology (IT) and digital media for as long as these technologies have been in existence. Today, headlines in the news media and deliberations in DC – with a focus on online and mobile media, abridgement of the Fourth Amendment, and "big data" – attest to an enduring interest and concern.

The range of technologies and systems that draw attention has rapidly expanded and diversified, to include GPS, RFID, biometrics, pervasive sensory networks, networked video and audio capture, cookies, data aggregation and mining, social computing, email, and mobile media. Privacy concerns are triggered not because these technologies diminish control over personal information, nor because they provide greater and easier access to this information. Rather, these concerns arise because information technologies disrupt "normal," or expected, flows. IT and digital media have extended capacities to obtain information, through monitoring, capture, and surveillance of data and communications. They have enabled novel ways of utilizing the information collected: storing it, aggregating it, and analyzing it through advances in hardware and software, statistical methods, and protocols. Finally, epic advances in the technologies and systems of networks and media have brought with them radical changes in the modes of information distribution and disclosure.

In the 1960s, when privacy in the digital world was first embraced as an important public issue, it was predominantly understood as political and ethical, the bailiwick of pundits, politicians, public interest advocates, judges and academics in law, the humanities and social sciences. By the 1970s, even as some technologists were drawn into these discussions, solutions to privacy problems were still sought mainly outside of the technical domain in ethics, law and regulation. To the extent technologists engaged, it was as conscientious citizens with particular expertise in the offending systems, not through the systems themselves.

The thirty-year crypto wars, beginning in the 1970s, can be viewed as a transition because they engaged a cohort of technologists in their capacities as technologists, invoking technology in service of privacy and liberty. Although the research and development focus on ethical, legal, social implications (ELSI) of technology had encouraged scientists to bring humanists and social scientists aboard large projects to evaluate their impacts upon societal values, including privacy, it was with the rise of privacy-inspired science and technology that we begin to see greater integration of privacy into technology and a broader-based population of technologists embracing privacy as their

own problem and not something to be tossed over the fence to the “softer” areas of research and activism.

As a result, researchers have developed richer formal languages to express privacy rules; new metrics to evaluate data release, such as differential privacy; more secure data storage; more effective cookie management; a deeper understanding of anonymization and its limits; more targeted techniques for data obfuscation, and a myriad privacy-enhancing technical systems to protect mobile transactions, web search, private browsing, and more. A great many of these advances in the last 20 years have been enabled through Federal Networking and Information Technology Research and Development (NITRD) Program investments. In constraining, containing, restricting, modulating and diverting information flows, the association of computing and IT with erosions of and threats to privacy has been challenged as their power to protect privacy has been demonstrated by leading technologists.

Looking ahead, the sustained public attention on privacy and ongoing support from the R&D community will continue to yield great scientific and technological innovation. The existing research paradigms have much to offer, but, in addition, there exists promise in a more thoroughgoing hybridity of effort between technologists on the one hand and humanists, social scientists, and policy makers on the other to produce systems based on keener conceptual fidelity, more nuanced privacy threat modes, and a better coordinated handoff between technical and political modes of regulation and enforcement.