Micah Stargel

Dr. Songhui Yue

CSCI 415 Algorithms

3 January 2023

Privacy and Anonymity

With the technological developments of the past century, there has been a massive increase in the digitization of records. Though this is often more convenient, a significant security matter has gained attention by individuals: the access and distribution of personal information. Two ways of addressing data utilization are privacy and anonymity, which have subtle yet drastic nuances in their definitions, implications, and applications.

There has been much deliberation throughout the years about the definitions of privacy and, more recently, anonymity. Whether physical, digital, or social, both privacy and anonymity stem from and build upon information security, which implies certain attributes that are prerequisites for privacy and anonymity but lack the full scope of both. The data characteristics are confidentiality—it can only be accessed by an authorized user; integrity—it is not altered unless by the author; and availability—the author can request it at any time (Wright 3). Two common additions to these elements to better distinguish privacy are that privacy constitutes control over personal information or that it involves restricting access to personal information, even in public. These allude to an individual being able to pick and choose who, what, when, where, why, how, and how much of their personal information is collected, viewed, and disseminated. According to Wright, there are four types of privacy, the first of which is information privacy (4). This is closely related to security as it is the protection of data but also covers “the collection and handling of personal information, such as medical, credit, residential information, but also government records, etc." (4). The second form of privacy is bodily privacy referring to "the protection against invasive procedures such as genetic tests, drug testing, and cavity searches" (4). Third, "privacy of communication…covers the security of mail, telephones, email, and other forms of communication" (4). Lastly, Wright lists "territorial privacy which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance, and ID checks" (4). This paper discusses mainly information and communication privacy and minorly the surveillance aspect of territorial privacy. Anonymity is slightly different than privacy in that, while privacy invokes the right to control or restrict data usage, anonymity entails that a user and their information is untraceable. "Anonymity does not imply that no information at all is released, but requires that information released be non identifiable" (Ciriani 5). Ciriani goes on to say that anonymity guarantees that any set of data cannot uniquely identify an individual, meaning each subset must be kept private from the other subsets (5). Wright draws a distinction, however, between two types of anonymity: total anonymity and pseudonymity (5). The first term is comparable to the first definition of anonymity discussed in conjunction with the fact that the origin of communication is completely untraceable as well (5). The term "pseudonymity" refers to concealing one's true identity by using false information (name, address, etc.) to communicate on one or more networks. The implications of privacy as well as the ability to be anonymous can have very crucial implications.

Without getting into the legal definitions and requirements of privacy and anonymity, one's rights, at a very basic level, must preserve their constitutional rights without endangering others. A couple common examples of privacy issues are the use of cookies and using contact information for advertisements (email and phone). The trouble arises when individuals' information is gathered and distributed without their knowledge. Many websites now have you agree to cookies, but many people either don't read these terms or the "contract" doesn't inform them that they are allowing their "clickstream" (internet search history to assist in recording interests and even financial history to gauge spending habits) to be sent to a cookie software that many different websites use, which allows them to see that information, communicate together, and taper advertisements to that unique user (Woo 955). Similarly, when one agrees to the terms of a certain company when creating an account (often commercial or social media websites), this often includes subscribing to receiving communications from them via text, email, or physical mail. Though many have the option to unsubscribe from this correspondence, a similar linkage happens to that of the cookies and that user's information is shared among similar companies to alter ads to that individual. Some companies are even able to access a list of many or all active emails, phone numbers, and and/or addresses to send individuals information or to link users by area or by identity (like family members). This is often referred to as spam mail, email, or calls. Point being, most users are unaware that when they agree to cookies or privacy terms, they are agreeing to that sharing of identifying information. Even if a government or similar "big brother" wants to use or monitor an individual's information or profile by collecting it and surveying them to ensure there is no suspicious activity, this could, and often is viewed as overstepping privacy boundaries. Ironically, many users, even if they are aware and contentious about their internet privacy, often agree anyways, justifying their choice because the compensation and convenience supersedes their privacy concerns (Woo 950). The question becomes then, is this tactic exploiting users for financial gain and breaching their privacy or assisting them by providing convenience?

Now, consider the implications of anonymity. Recall that it is largely referring to the fact that a user cannot be identified by their internet activity, whether because their information cannot be compiled to form a profile; they are innately untraceable; or they use a false identity. In its most honest use, anonymity's purpose is to discuss or receive counseling about sensitive topics such as politics, medical practice/treatment, sexual preferences and/or orientation, and other volatile subjects. In this situation, anonymity, especially, as well as privacy provide a certain level of protection to the user, preserving their identity, reputation, and documentation. However, both privacy and anonymity are very easily utilized for malicious purposes. One can abuse these rights to steal others' information and pose as that person or plant false records; launder or plunder money to and from personal and company accounts; or collect an individual's, government's, or corporation's classified or intimate data with the surety that they, the thief, will be extremely difficult to track. So, where is the balance between granting any user on the internet enough privacy and anonymity to ease their concerns without compromising security and protection of data from fraudulent users?

First, though this is largely a personal initiative, users should start by educating themselves on the definitions and types of privacy, anonymity, and security so their ignorance cannot be exploited. Similarly, they should be careful about which websites they visit and grant certain privileges and access, their social media presence, as well as ensuring emails and phone calls are legitimate. These can all become security issues for finances and identity theft. Another step to finding a solution on the corporate level is requiring users and employees to agree to an ethical code that addresses privacy. For example, the Institute of Electrical and Electronics Engineers states in their code of ethics that their members will strive "to hold paramount the safety, health, and welfare of the public, to strive to comply with ethical design and sustainable development practices, to protect the privacy of others, and to disclose promptly factors that might endanger the public or the environment;" (I.1.). Likewise, sections 1.6 and 1.7 of the ACM Code of Ethics are entitled "Respect Privacy" and "Honor Confidentiality." These two passages talk about only using information for "legitimate ends" (1.6) and not disclosing it unless absolutely necessary (1.7). For a Christian, the highest authority on the matter is Jesus when he says in Matthew 7:12, "So whatever you wish that others would do to you, do also to them" (*The Holy Bible*, ESV). Ideally, though unrealistic, if everyone lived by this principle, no one would try to dishonestly obtain or use someone else's personal data.

In conclusion, today's world is extremely digital which makes data storage and access more convenient than ever. With this luxury, however, comes many threats to the acquisition and dissemination of personal information. The contrast between a user's ease-of-use and vulnerabilities on the internet is the double-edged sword of privacy and anonymity, which are remarkably comparable, yet distinct in particular aspects of their expositions, ramifications, and utilizations.

Works Cited

Wright, Thomas. “Security, Privacy, and Anonymity.” *XRDS: Crossroads, The ACM Magazine for Students*, vol. 11, no. 2, 2004, https://doi.org/10.1145/1144403.1144408.

Ciriani, Valentina, et al. “Theory of Privacy and Anonymity.” *Research Gate*, Jan. 2009. University of Milan

Woo, Jisuk. “The Right Not to Be Identified: Privacy and Anonymity in the Interactive Media Environment.” *New Media & Society*, vol. 8, no. 6, Dec. 2006, pp. 949–967., https://doi.org/10.1177/1461444806069650.

“IEEE Code of Ethics.” *Institute of Electrical and Electronics Engineers*, IEEE Board of Directors, June 2020, https://www.ieee.org/about/corporate/governance/p7-8.html.

ACM Code 2018 Task Force. *ACM Code of Ethics and Professional Conduct*, Association for Computing Machinery Council, 22 June 2018, https://www.acm.org/code-of-ethics.

The Holy Bible. English Standard Version, Crossway, 2001.