The Difference between Data Security and Privacy

Mark R. Heckman, Ph.D., CISSP, CISA
Professor of Practice
Shiley-Marcos School of Engineering
University of San Diego

Security and privacy are related, but distinct concepts. That may seem obvious to many people, but relatively few can clearly explain the difference. Privacy, moreover, is impossible without security, but not the other way around, and the reason why that is true is often missed. Without a clear understanding of the difference, security and privacy may be conflated in ambiguous and imprecise policies, leading to confusion among developers, administrators, and users. This article demonstrates the difference using a simple, abstract model.

The International Association of Privacy Professionals (IAPP) defines the difference between security and privacy in this way:

> *Data privacy is focused on the use and governance of personal data—things like putting policies in place to ensure that consumers' personal information is being collected, shared and used in appropriate ways. Security focuses more on protecting data from malicious attacks and the exploitation of stolen data for profit. While security is necessary for protecting data, it's not sufficient for addressing privacy.* [1]

This definition says that privacy is "focused on the use and governance of personal data", while "security focuses more on protecting data". Both of those statements are true, but the difference between security and privacy in this definition is fuzzy (does "focuses more" mean that security also focuses on the use and governance of personal data?) and the relationship between the two is not obvious.

A better definition is given by the U.S. Department of Health and Human Services (HHS) in an explanation about the difference between the Health

Information Portability and Accessibility Act (HIPAA) Security and Privacy Rules with respect to electronic protected health information (EPHI):

> *The Privacy Rule sets the standards for, among other things, who may have access to PHI, while the Security Rule sets the standards for ensuring that only those who should have access to EPHI will actually have access.*[2]

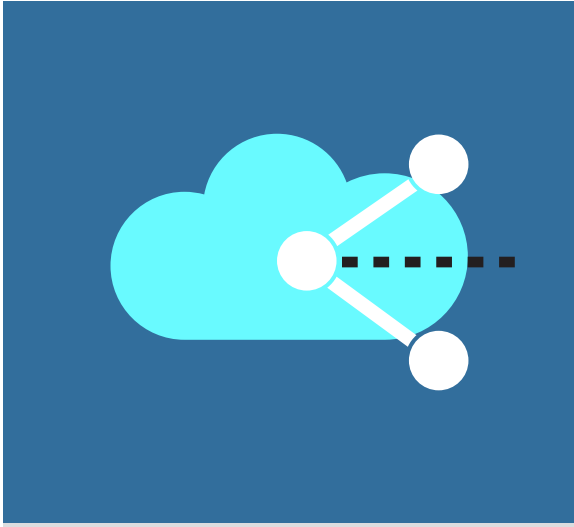
The Privacy Rule grants certain parties (e.g., health care plans and providers) access to PHI and gives individuals the right to control access to their own personal information by parties not granted access by the law. The key distinction here is that the Security Rule requires protection of sensitive data against unauthorized access, while the Privacy Rule specifies who is granted authorization or has the right to grant authorization.

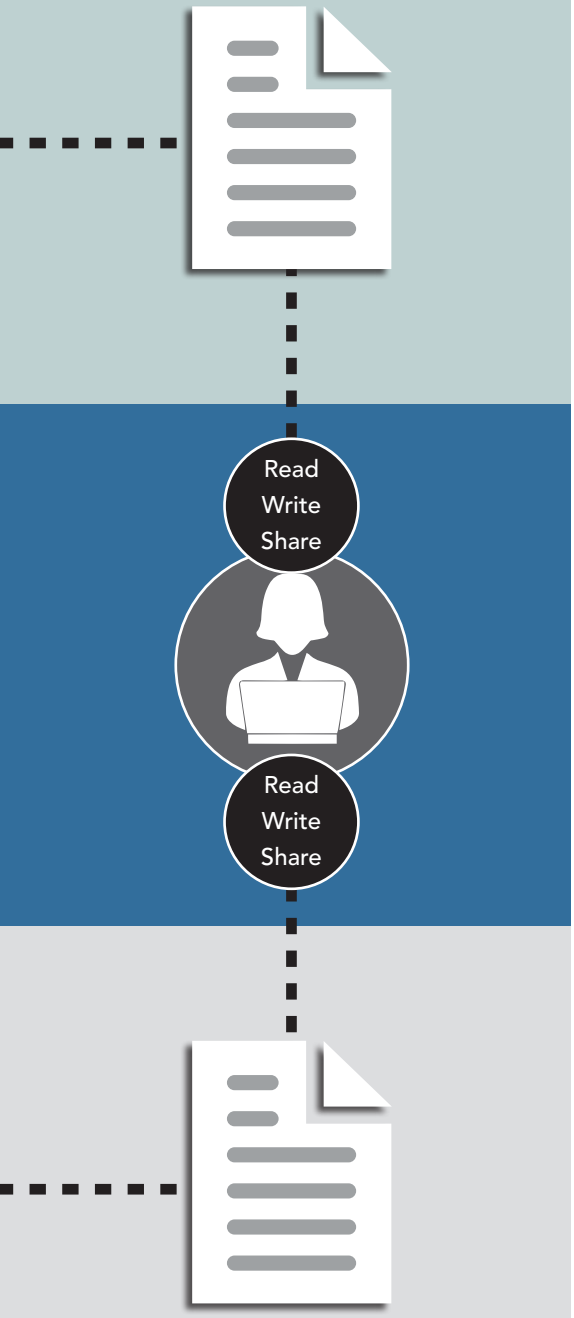
We can represent the protection state of a system using the access control matrix model.[3] The model consists of a set of *objects* that contain information (such as files) and a set of *subjects*, which are active entities (such as users) that access the objects. There is also a set of access rights (read, write, etc.) that a subject may have to an object. The access rights that subjects have to different objects are represented in the form of a table, where the rows of the table correspond to the subjects and the columns correspond to objects. The cell that is the intersection of a subject row and an object column contains the access rights that that subject is authorized to have to the object. The access rights in the table constitute the system's security policy. An example is shown in Figure 1.

	Bob's File 1	Bob's File 2	Carol's File 1	Carol's File 2
Bob	Read, Write, Share	Read, Write. Share		
Carol			Read, Write. Share	Read, Write, Share
GFC	Read, Write	Read, Write	Read, Write	Read, Write

Figure 1- Access Control Matrix

Consider that the access control matrix in Figure 1 represents the protection state for a new, free cloud storage system managed by the "Giant Faceless Corporation" (GFC). The privacy policy for the system is that only owners have access to their files, unless an owner explicitly grants another user access to a file. An object owner has a "share" access right that permits the owner to grant another user access to the object. Currently in beta testing, there are only two users of this system, Bob and Carol, each with two files. Initially, Bob has no access to Carol's files and Carol has no access to Bob's files. A user grants the GFC authorization to access that user's files when the user signs up for the free service (for advertising purposes), but the GFC does not "own" the files and does not have the right to grant a user access to another user's files.





Security is enforcement of the authorized access rights currently in the access table. The system is secure with respect to the security policy represented by the table as long as subjects can only access the objects with the authorized rights in the table. If Carol were able to access any of Bob's files given the current permissions in the table, for example, the system would not be considered secure.

Privacy, on the other hand, is a policy on control over where and when authorized access rights appear in the table. The privacy policy for the cloud system states that users have full control over who is allowed to access that user's files, except that the GFC by default has the ability to read all files stored in the system. The information in the system would be considered private with respect to the privacy policy if only Bob, for example, has control over granting access authorization to Carol and Carol does not have the ability to grant herself authorization to access Bob's files.

Let's say that Bob has decided to let Carol read one of his files. That results in a change to the protection state of the system – to the security policy that the system must enforce. The updated protection state would be as shown in the matrix in Figure 2, where Carol now is authorized to have read access to Bob's File 2.

	Bob's File 1	Bob's File 2	Carol's File 1	Carol's File 2
Bob	Read, Write, Share	Read, Write. Share		
Carol		**Read**	Read, Write. Share	Read, Write, Share
GFC	Read	Read	Read	Read

Figure 2- Updated Access Control Matrix

The system would still be secure now if it allowed Carol to read Bob's File 2, even though in the earlier protection state Carol was not allowed to read that file, because in the current protection state Carol is authorized to have read access. Information in the system is still private because, under the privacy policy, Bob has authority to grant Carol the right to access Bob's files.

Let us say, however, that the state of the system is as shown in Figure 3. The GFC has given itself "share" access to all of the user's files, so that the GFC could, if it wanted to, authorize users to access the files of other users without the approval of the file owners. This ability is in direct contradiction to the stated privacy policy of the system. In fact, the GFC (not Carol) has given Bob the right to read one of Carol's files. The information would still be secure if the system enforced the policy represented in the matrix, but it would not be private because the privacy policy says that only Carol can authorize other users to access her files and she was not the one who gave Bob access.

	Bob's File 1	Bob's File 2	Carol's File 1	Carol's File 2
Bob	Read, Write, Share	Read, Write. Share	**Read**	
Carol			Read, Write. Share	Read, Write, Share
GFC	Read, **Share**	Read, **Share**	Read, **Share**	Read, **Share**

Figure 3 - Privacy-violating protection state

Privacy is not the state of information being protected from unauthorized access. Information is not private because unauthorized users are prevented from accessing the data, but it is secure. People frequently conflate confidentiality – the property that only authorized users can read protected information – with privacy but, as the access control matrix model clearly shows, confidentiality is a security policy because it is determined by the system correctly enforcing read access rights in the access control matrix. The ability of an owner to control who is authorized to access the owner's information – where and when authorized access rights appear in the matrix – is what determines privacy.

Control over access rights, which defines privacy, is useless unless the system reliably enforces the access rights. If there is no enforcement, granting and revoking access has no meaning. That is why there can be no privacy without security. On the other hand, as Figure 3 shows, a system can reliably enforce the access rights in the access control matrix and therefore be considered secure, but information owners may have no ability to control who is authorized to access their data, so their data would not be considered private.

Conclusion

The access control matrix model, which represents the protection state of a system, is a simple method of demonstrating that difference and relationship between security and privacy. Information is "secure" when a system correctly enforces the access rights currently in the matrix. Information is "private" only when the owner of the information has control over changing the rights in the matrix for the owner's information. Furthermore, privacy is impossible to enforce in a system unless that system is secure, but the reverse is not true. A clear understanding of the difference and relationship between security and privacy is essential for developing and implementing unambiguous and precise security and privacy policies.

Sources

1. International Association of Privacy Professionals web site. https://iapp.org/about/what-is-privacy/ (Accessed: 22 November 2016)
2. HIPAA Security Series: Security 101 for Covered Entities, Center for Medicare and Medicaid Services, U.S. Department of Health and Human Services. Volume 2 /Paper 1. 11/2004:rev. 3/2007. http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/security101.pdf (Accessed 22 November 2016).
3. B. Lampson. Protection. Proc. 5th Princeton Conf. on Information Sciences and Systems, Princeton, 1971. Reprinted in ACM Operating Systems Rev. 8, 1 (Jan. 1974), pp 18-24. Available: http://research.microsoft.com/en-us/um/people/blampson/08-Protection/WebPage.html (Accessed 22 November 2016)

About the Author

Mark Heckman *has worked in the field of information security for over 30 years as an engineer, researcher, practitioner, and educator. His experience includes high-assurance, multi-level secure systems used by the military, intrusion detection and security event management systems, and IT security and compliance for commercial organizations in the financial and health industries. Heckman earned his Ph.D. in Computer Science at the University of California, Davis and is a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA).*

University of San Diego