Jon David on Privacy (2)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

In the first part of his essay on privacy, my friend and colleague Jon David reviewed some fundamentals of privacy in the world of electronic communications. In this second part of two, he looks at some relatively recent developments in US law that makes privacy mandatory in certain applications.

* * *

HIPAA, the Health Information Portability and Accountability Act, has specific security requirements devoted to what is known as personally identifiable information. This means, for example, that if information that a hospital was testing a new drug on 50 patients was to get out, that might not be ideal from the researchers’ point of view, but at least it wouldn’t be illegal. However, revealing the fact that John Smith was one of those patients would be a direct violation of HIPAA. Revealing his participation would imply that John might be suffering from an affliction treatable by that medication. If you want to imagine the consequences of such a data leakage for a participant, imagine that the drug were directed at treating, say, a sexually-transmitted disease.

There are severe penalties for both individuals and organizations set forth in the HIPAA security regulations. HIPAA is the concern of the entire healthcare industry, not just hospitals. This includes doctors in private practice, pharmacies, medical labs and test facilities, insurance providers, etc.

The Gramm-Leach-Bliley (GLB) Act treats financial privacy. Again, the orientation seems to be towards individually identifiable information. Hayes, Judy and Ritter, in Chapter 52 of the _Computer Security Handbook, 4th Edition_ have summarized the core of the GLB as follows:

“[I]t requires every ‘financial institution’ to protect the security and confidentiality of its customers’ nonpublic personal information, disclose its privacy policies to consumers, and provide consumers with an opportunity to direct that the institution not share their nonpublic personal information with unaffiliated third parties.”

With most major financial services concerns having facets of their operations which deal in banking, securities (e.g., stocks, bonds, etc.), insurance, real estate and the like, this law governs a huge population of data subjects and data users.

It is important to note that both laws are directed towards the custodians of the information to be kept private. When personal information is offered to third parties (e.g., marketing firms), the custodians must inform each data subject of the proposed transfer and must provide the opportunity to refuse the transfer of his or her particular data before any of the data are divulged. Failing to offer each individual the right to opt-out of such transfers is a violation of the law.

Although the United States isn't the whole world, and while healthcare and financial services

...
aren't the majority of business activities even within the US, both HIPAA and GLB are having a significant impact on the ways organizations treat personal information they possess. It is likely that similar laws will be enacted for other industries.

* * *

Jon David < jon@securitymeister.com > has been a security advisor to industry and government for more than 20 years.

* * *

Further reading on the Web:

HIPAA Central < http://www.smed.com/hipaa/index.php >
HIPAA Information from the Centers for Medicare & Medicaid Services < http://cms.hhs.gov/hipaa/>
History and Overview of HIPAA < http://www.hipaadvisory.com/regs/HIPAAHistorybyZon.htm >
HIPAA Primer < http://www.hipaadvisory.com/regs/HIPAAprimer1.htm >

GLB Compliance Checklist < http://www.wrf.com/publications/publication.asp?id=1451315312001 >
GLB links from the Federal Trade Commission < http://www.ftc.gov/privacy/glba.ct >

* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see < http://www.norwich.edu/msia > for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at < mkabay@norwich.edu >; Web site at < http://www.mekabay.com/index.htm >.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to _Network World_ to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.