

Privacy Principles for Digital Watermarking

June 2, 2008

Policy Posts are in-depth analyses on current tech policy issues from CDT experts. Sign up to receive the latest Policy Posts [here](#):

CDT released a paper this week offering a set of principles for addressing potential privacy considerations when deploying digital watermarking technology. As explained in greater detail below, digital watermarking technology embeds information, in machine-readable form, within the content of a digital media file (for example, a movie, song, or photograph).

[\(1\) CDT Offers Privacy Principles for Digital Watermarking](#)

[\(2\) Basics of Digital Watermarking Technology](#)

[\(3\) CDT's Suggested Principles](#)

(1) CDT Offers Privacy Principles for Digital Watermarking

CDT released a paper this week offering a set of principles for addressing potential privacy considerations when deploying digital watermarking technology. As explained in greater detail below, digital watermarking technology embeds information, in machine-readable form, within the content of a digital media file (for example, a movie, song, or photograph).

Digital watermarking is a general-purpose technology with a variety of possible applications. Like many technologies, it could raise privacy issues if deployed in ways that fail to take privacy into account. CDT's paper is intended to promote awareness by those developing digital watermarking applications and to provide guidance on how to steer clear of possible privacy risks.

Privacy questions are most likely to arise when digital watermarking is used to associate a file with an individual consumer, transaction, or device. An example would be a movie file with embedded watermarks identifying the particular user to whom the file was sold and downloaded. (A contrary example would be a movie file embedded with watermarks identifying the name and version of the movie; none of that information would be specific to an individual consumer.)

Of course, digital watermarking is not the only possible means of recording or signaling this kind of individualized information in a digital media file. Many digital media files include file headers-- bits in addition to the bits needed to render the particular image, audio, or video--that could convey such information. Watermarking can be more difficult to discern and is intended to be more persistent (i.e., harder to strip out) than file headers or other types of metadata. But many privacy questions raised by digital watermarks may apply to non-watermark information contained in a file as well.

CDT's paper on watermarking and privacy is in some respects a follow up to its previous survey of the various metrics consumers may want to consider in evaluating digital rights management (DRM) technology. That earlier paper focused largely on encryption-based, technological "locks" designed to prevent unauthorized uses of copyrighted media. Since then, there has been a strong trend in music download services away from encryption-based DRM, and some industry observers have speculated that watermarking may come to play an increasing role in deterring and providing accountability for copyright infringement. In particular, watermarks can be used forensically, to try to determine the source of illegally distributed copies.

For many of the metrics suggested by the DRM paper, watermarking could rate favorably from a consumer perspective. For example, since watermarking merely records and communicates information, it should have little direct impact on the flexible use or interoperability of the watermarked files. Of course, the analysis could be different if watermarks are integrated with or

serve as a trigger for other DRM. But for watermarking itself, the biggest lurking question mark among CDT's metrics would appear to be the impact on privacy. CDT's new paper therefore explores the privacy considerations relating to digital watermarking in significant detail.

In developing its privacy principles for digital watermarking, CDT consulted with representatives of companies providing digital watermarking technology and with interested privacy advocates. The Digital Watermarking Alliance, an industry group representing companies involved in watermarking, endorsed the principles upon their release and announced that it will undertake outreach efforts to ensure that digital watermarking applications are designed with privacy principles in mind.

[CDT Paper, Privacy Principles for Digital Watermarking](#) [1]

[CDT Press Release](#) [2]

[CDT Paper, Evaluating DRM: Building a Marketplace for a Convergent World](#) [3]

2. Basics of Digital Watermarking Technology Watermarking

Digital watermarks encode information in a media file by making subtle changes to the image, audio, or video. Much like watermarks on stationary, these changes typically would not be noticeable to a person viewing or listening to the content. Indeed, digital watermarks often are not perceptible by humans at all, but rather are designed to be detected and decoded only by machines specifically programmed to do so. The content of the information conveyed by watermarks will depend on the application and intended use.

The general elements of a digital watermarking system are as follows:

--Embedding of watermark in content-- Every watermarking application starts by placing watermarks into digital content. This is done using a special algorithm, which translates the data to be conveyed into specific, subtle modifications to the content.

--Subsequent reading of watermark by device/software -- Recognizing the watermarks requires knowledge of the algorithm used to embed them, so that the reader device or software knows what to look for. Therefore, readers are system- or vendor-specific. There are no readers capable of deciphering all watermarks.

--Back-end database for determining meaning of watermark -- Most watermarking applications involve a database for storing data associated with specific watermarks. The watermark itself contains a serial number or coded message, and determining what that number or message means requires consulting the database.

--Actions triggered upon reading of watermark -- In many applications, the recognition or reading of a watermark will trigger or enable some type of action. For example, upon detecting a watermark in a media file, a device could record the fact that it encountered the watermark; display specific information or messages to the device's user; or enable or disable access to particular files or capabilities.

3. CDT's Suggested Principles Watermarking

Perhaps the most frequently raised privacy concern regarding digital watermarks is that they could enable increased monitoring, recording, or disclosure of an individual's media purchases or usage. The fear, in other words, is that watermarking could compromise an individual's ability to use and enjoy lawfully acquired media on a private, anonymous basis. Other possible privacy issues include the risk that watermarks could contain personal information that could be exposed to third parties, and the risk that errors in or manipulation of watermark data could paint a false picture of an

individual's behavior and perhaps lead to adverse consequences, including potential legal liability.

CDT's paper suggests the following principles, in the spirit of "best practices," for minimizing such risks.

1. Privacy by design -- Companies should address privacy considerations in the early design and planning phases of digital watermarking applications, not late in the process as an afterthought. Where applications involve multiple partners, contracts should include appropriate privacy-related commitments for each.
2. Avoid embedding independently useful identifying information directly in watermarks -- Companies should seek to ensure that even if unauthorized parties learn how to read the watermarks, no meaningful information will be exposed. For example, for most applications, the data actually embedded in the watermark should consist merely of a random serial number or other code, and the use of a consistent code to correspond to a specific individual should be avoided wherever practical.
3. Provide notice to end users -- When media files contain individualized watermarks, end users should be provided with notice disclosing key information such as the presence of the watermarks, the data they convey, and the purpose for which that data will be used. The prominence of notice should be proportional to the extent and likelihood of any privacy impact.
4. Control access to reading capability -- Members of the public who happen to obtain a watermarked file generally should not have easy access to the devices or software needed to read the watermarks. Nor should government or law enforcement authorities; if authorities need to decipher watermarks deployed for non-governmental purposes, they can obtain that information through appropriate legal process.
5. Respond appropriately when algorithms are compromised -- Companies should reconsider how much reliance to place on watermarking systems whose workings have been exposed, particularly if there is a risk that watermarks could be altered or forged.
6. Provide security and access controls for back-end databases -- Companies deploying watermarking applications should carefully protect the security of and control access to any back-end databases containing information about individuals.
7. Limit uses for secondary purposes -- The design of watermarking applications should seek to limit, not facilitate, future use of watermark information for purposes not related to the application's original mission. Information should be collected, retained, and disclosed only as necessary for the original mission; back-end databases should avoid unnecessarily centralizing all information about an individual in one place; and companies should refrain from using watermarks to "unmask" anonymous speakers who happen to incorporate some marked content into commentary or criticism.
8. Provide reasonable access and correction procedures for personally identifiable information -- Where watermarking applications cause personally identifiable information to be collected and stored, individuals should have reasonable means of accessing information that pertains to them for purposes of contesting inaccuracies.

In CDT's view, implementing and adhering to these principles in good faith should address the main potential privacy concerns relating to digital watermarking and promote consumer confidence in the current marketplace for digital media.

The copyright © 2013 by the Center for Democracy & Technology. CDT can be freely copied and used as long as you make no substantive changes and clearly give us credit. [Details](#).

Source URL: <https://www.cdt.org/policy/privacy-principles-digital-watermarking>



Links:

[1] <http://www.cdt.org/copyright/20080529watermarking.pdf>

[2] http://www.cdt.org/pr_statement/cdt-releases-privacy-principles-digital-watermarking

[3] <http://www.cdt.org/copyright/20060907drm.pdf>