Companies Must Update Confidentiality Agreements and Practices in Compliance with Current Trends

By Kristin Biedinger*

For many companies, executing Non-Disclosure Agreements (commonly referred to as "NDAs") is common practice when sharing confidential information with third parties.[1] While companies may recognize the need to put these types of agreements in place, there is often little thought as to the scope of the agreement or what additional steps need to be taken for the NDA to be enforceable.[2] Recent trends with respect to NDA practice highlight the importance of carefully considering these issues. For instance, a failure to do so can not only lead to a false sense of security with respect to the confidentiality of the information shared but also present the significant risk that the information will not be considered confidential at all.[3]

There is particular risk for companies sharing Personally Identifiable Information ("PII"). Recently, there has been a tremendous shift in how companies store data, including PII of their employees and customers, with more and more data being stored remotely and through cloud-based solutions.[4] The "Internet of Things" and "Big Data" trends have resulted in a significant increase in the amount of data companies collect, store, and utilize, not only as part of their daily business operations but also as part of their product offerings.[5] In fact, data is becoming a valuable company asset in and of itself.[6]

It is critical for companies to update their NDA practices to reflect theses changes. To do so, the scope of NDAs must be expanded to include PII regardless of how it is acquired. Traditionally, NDAs were designed to protect the disclosure of confidential information, which is typically defined as information relating to a company's intellectual property, business operations, or other information that would give one a competitive advantage.[7] This definition is further narrowed by a number of carve outs, information that the Parties agree will not be considered confidential information.[8] For example, it is customary to exclude information in the public domain, information that was in a party's possession prior to the NDA, or information that a party freely acquires from another source.[9]

---

* Kristin Biedinger is an associate with Tucker Arensberg, P.C. Kristin's practice includes all areas of

[1] Jodi L. Short, *Killing the Messenger: The Use of Nondisclosure Agreements to Silence Whistleblowers*, 60 U. PITT. L. REV. 1207, 1207 (1999) ("Nondisclosure agreements are a common feature of corporate life.").

[2] *See, e.g.*, nClosures Inc. v. Block & Co., Inc., 770 F.3d 598, 602 (7th Cir. 2014) (noting that "[a]greements [are] only enforceable when information . . . is actually confidential and reasonable efforts were made to keep it confidential").

[3] *Id.*

[4] *See* Tim Prosky, *Dear Data Analytics . . . Thank You for the Spam*, HB LITIG. CONFS. http://litigationconferences.com/dear-data-analytics/ (last visited Mar. 8, 2015).

[5] *Id.*

[6] *See* Steve Kroft, *The Data Brokers: Selling Your Personal Information*, 60 MINUTES (Mar. 9, 2014), http://www.cbsnews.com/news/the-data-brokers-selling-your-personal-information/.

[7] *See* David V. Radack, *Understanding Confidentiality Agreements*, JOM, http://www.tms.org/pubs/journals/JOM/matters/matters-9405.html (last visited Mar. 8, 2015).

[8] *Id.*

[9] *See, e.g.*, Raven Indus., Inc. v. Lee, 783 N.W.2d 844, 849 (S.D. 2010) ("Non-disclosure agreements are unenforceable if: '(1) a trade secret or confidential relationship does not exist; (2) the employer discloses the

Under this framework, there is risk that PII would not fall within the definition of confidential information or that PII would fall under one of the exclusions. NDAs must be updated to provide a definition of what information constitutes PII and must also provide language that clearly extends the confidentiality obligations of the NDA to this PII.[10]

Protecting only information that is *disclosed* to the other Party is also risky. With Software as a Service ("Saas") solutions and cloud-based storage of company data, a Party may have access to PII or even store or transmit PII on behalf of a company without the PII being *disclosed* in the traditional sense.[11] Therefore, to fully protect the PII, confidentiality obligations must be extended beyond PII to any PII that is also stored, accessed, transmitted, or received by a Party on behalf of a company.[12]

Companies must also ensure that PII is protected by obligation of confidentiality for a sufficient period of time. Under old NDA practice, it was not uncommon for obligations of confidentiality to have an expiration date, usually three to five years after termination of the NDA.[13] This is not sufficient for protecting PII.[14] Confidentiality obligations under the NDA must remain in effect so long as a Party can access, store, transmit, receive, or disclose the PII.[15]

To fully protect Confidential Information, including PII, companies cannot stop at a well-drafted NDA. For NDAs to be enforceable, companies must also impose reasonable internal security measures to ensure confidential information remains confidential.[16] The importance of these security measures was highlighted in the recent case of *nClosures, Inc. v. Block and Company, Inc*. nClosures and Block entered into a business relationship where nClosures would design and Block would manufacture certain electronics enclosures, such as covers for iPads and electronic tablets.[17]

---

information to others not in a confidential relationship; or, (3) it is legitimately discovered and openly used by others.'").

[10] It is important to note that at the time of this article's publication, there was no federal law governing PII. Each state has its own laws defining PII and imposing notification requirements in the event of a security breach. In addition to the general provisions provided herein, companies should carefully review the applicable law of their state.

[11] For an in-depth illustration of the practices of compiling, storing, and sharing PII, see Paul M. Schwartz & Daniel J. Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable nformation*, 86 N.Y.U. L. REV. 1814, 1836–65 (2011).

[12] ERIKA MCCALLISTER ET AL., GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) 4-2 (drft. 2009), *available at* https://www.illinois.gov/bccs/news/Documents/Security/Guide_to_protecting_PII.pdf.

[13] *See* Mike Tobin, *Time Limits in Confidentiality Agreements: Traps for the Unwary*, SEC. & CORP. GOVERNANCE GROUP (Oct. 30, 2013), http://scgg.parkerpoe.com/commercial-contracts/time-limits-in-confidentiality-agreements-traps-for-the-unwary/.

[14] *See id*.

[15] *See id*.

[16] nClosures, Inc. v. Block & Co., Inc., 770 F.3d 598, 602 (7th Cir. 2014) (holding that a failure to "engage in reasonable steps to protect the confidentiality of proprietary information" renders a confidentiality agreement unenforceable).

[17] *Id.* at 600.

nClosures and Block executed an NDA in which the Parties agreed to use the confidential information solely for engaging in discussions and evaluating a potential business relationship with respect to iPad enclosures.[18] Block began manufacturing enclosures based on nClosures' disclosed designs and also started manufacturing its own competing product.[19] Block eventually terminated its relationship with nClosures, and nClosures filed suit against Block for, among other things, breach of contract.[20] The District Court granted summary judgment for Block, which was affirmed on appeal by the United States Court of Appeals for the Seventh Circuit.[21]

On appeal, the court stated that confidentiality agreements will only be enforced if the "information sought to be protected is actually confidential."[22] The issue of whether an enforceable contract existed between the Parties turned on whether or not nClosures took reasonable steps to maintain the confidentiality of its information.[23]

The court found several deficiencies in nClosures' treatment of its confidential information, which can provide a framework for companies to follow when updating their current practices.[24] First, although nClosures entered into a confidentiality agreement with Block, it did not require any individuals who accessed their designs to sign confidentiality agreements.[25] Second, nClosures did not mark their designs with words such as "confidential" or "proprietary."[26] Third, the designs were not kept in a secure location, such as a locked cabinet.[27] Based on these failures, the Court found nClosures did not take reasonable steps to maintain the confidentiality of its information, and therefore, the confidentiality agreement with Block was unenforceable. [28]

While implementing internal security safeguards may seem like common sense, it is very easy for companies to become complacent with respect to enforcing these measures. Therefore, it is best practice for companies to periodically audit the security measures that are in place and update or modify these measures as needed to maximize protection. Learning from nClosures's mistakes, companies should have all employees sign NDAs and restrict which employees have access to confidential information.[29] Only the employees that need to know the confidential information to perform their job functions should be granted access. Records should be kept in order to identify what information the company considers confidential, and appropriate legends such as "CONFIDENTIAL" and/or "PROPRIETARY" should be used to mark these materials

---

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.* at 600, 602.

[22] *Id.* at 602 (quoting Tax Track Sys. Corp. v. New Investor World, Inc., 478 F.3d 783, 787 (7th Cir. 2007)).

[23] *Id.* at 602.

[24] *Id.*

[25] *Id.* ("While nClosures and Block did sign a confidentiality agreement at the outset of their business relationship, no additional confidentiality agreements were required of individuals who accessed the design files for the Rhino or Rhino Elite devices.").

[26] *Id.* ("Additionally, neither the Rhino nor the Rhino Elite drawings were marked with words such as 'confidential' or 'contains proprietary information.'").

[27] *Id.* ("Furthermore, the drawings were not kept under lock and key, nor were they stored on a computer with limited access.").

[28] *Id.* (holding that failure to "engage in reasonable steps to protect the confidentiality of proprietary information" renders a confidentiality agreement unenforceable).

[29] *See id.* at 602.

appropriately.[30] In addition, care should be taken as to how confidential information is stored.[31] Paper copies should be kept in a locked cabinet, and electronic copies should be saved to a secure network.[32] Restricting access to this electronic information is also critical.

The *nClosures* case is a good indication of how courts will address the enforceability of NDAs in the future. Companies must take reasonable steps to protect the confidentiality of their information.[33] While "reasonable steps" may depend on the facts of a given case, most companies, regardless of their size or industry, can easily implement the Court's guidance in *nClosures*.[34] Without these security measures, executing NDAs becomes futile and companies risk giving up some of their most valuable assets.[35]

[30] *See id*.

[31] *Id*.

[32] *Id*.

[33] *See id*.

[34] *See id*.; Tax Track Sys. Corp. v. New Investor World, Inc., 478 F.3d 783, 787; Rockwell Graphic Sys. Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).

[35] *See nClosures, Inc*., 770 F.3d at 602.