University of Groningen

A dynamic view on secrecy management

Bos, Brenda; Broekhuizen, Thijs L. J.; de Faria, Pedro

Published in:
Journal of Business Research

DOI:
[10.1016/j.jbusres.2015.04.009](https://doi.org/10.1016/j.jbusres.2015.04.009)

IMPORTANT NOTE: You are advised to consult the publisher's version (publisher's PDF) if you wish to cite from it. Please check the document version below.

Document Version
Publisher's PDF, also known as Version of record

Publication date:
2015

[Link to publication in University of Groningen/UMCG research database](#)

Citation for published version (APA):

Bos, B., Broekhuizen, T. L. J., & de Faria, P. (2015). A dynamic view on secrecy management. *Journal of Business Research*, 68(12), 2619-2627. <https://doi.org/10.1016/j.jbusres.2015.04.009>

Copyright

Other than for strictly personal use, it is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), unless the work is under an open content license (like Creative Commons).

The publication may also be distributed here under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license. More information can be found on the University of Groningen website: <https://www.rug.nl/library/open-access/self-archiving-pure/taverne-amendment>.

Take-down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from the University of Groningen/UMCG research database (Pure): <http://www.rug.nl/research/portal>. For technical reasons the number of authors shown on this cover page is limited to 10 maximum.

A dynamic view on secrecy management

Brenda Bos, Thijs L.J. Broekhuizen *, Pedro de Faria

Department of Innovation Management and Strategy, Faculty of Economics and Business, University of Groningen, PO Box 800, 9700 AV, The Netherlands

ARTICLE INFO

Article history:

Received 2 January 2014

Received in revised form 16 April 2015

Accepted 17 April 2015

Available online 16 May 2015

Keywords:

Secrecy

Innovation

Appropriability

Secrecy management lifecycle

ABSTRACT

Purpose – The current study provides a literature review on secrecy as mechanism for appropriating value from innovation. It synthesizes previous findings into a framework that can explain the advantages of exercising secrecy versus patenting. It also examines the management lifecycle of secrecy. **Design/methodology/approach** – It takes a dynamic perspective and suggests a four-stage secrecy management lifecycle: creation of secret, installation of preventive mechanisms, protection and exploitation, and minimization of leakage. **Findings** – Based on the four stages, the study highlights under-researched areas, and develops a future research agenda for secrecy management. **Originality/value** – Despite the managerial and academic relevance of this topic, extant research does not offer a comprehensive framework for the concept of secrecy. This study provides a dynamic perspective to highlight the important aspects of secrecy management during the lifecycle of secrets.

© 2015 Elsevier Inc. All rights reserved.

1. Introduction

Firms can gain competitive advantages from innovation activities only by effectively appropriating value from the related knowledge, which requires the protection of knowledge from uses by competitors. From the range of protection mechanisms, patenting attracts the most attention in management research (Blind, Cremers, & Mueller, 2009; Levitas & McFadyen, 2009; McGahan & Silverman, 2006), at the expense of theoretical and empirical investigations of mechanisms such as copyrights, lead time, or secrecy. This study focuses on secrecy as a knowledge protection tool, noting that secrecy offers one of the most important appropriability mechanisms for firms of all sizes and industries (Arundel, 2001), especially for industries where value depends on knowledge creation and exploitation activities (Hannah, 2007). However, secrecy also is complex and difficult for modern firms, due to increased employee mobility (Delerue & Lejeune, 2010, 2011), the digitalization of content, the ease of recording and distributing information through mass communication technologies and social media (Harris, 2009), the wider uses of open innovation and strategic alliances in R&D activities (Bogers, Afuah, & Bastian, 2010; Drechsler & Natter, 2012), and greater reliance on cross-functional teams (Carbonell & Rodriguez, 2006; Sethi, Smith, & Park, 2001). In today's information-rich, dynamic environments, secrecy management is strategically relevant (Cohen, Nelson, & Walsh, 2000) and a source of competitive advantage (Hannah, 2005).

In classifying the advantages and disadvantages of secrecy relative to patenting, prior studies list many contextual factors that determine the

effectiveness of secrecy efforts (Amara, Landry, & Traoré, 2008; Hanel, 2006; Harabi, 1995; Hurmelinna-Laukkanen & Puimalainen, 2007). The piecemeal approach in most of this research limits understanding of how secrecy works in varying circumstances though (for a notable exception, see Hall, Helmers, Rogers, & Sena, 2012). Considering the increasing importance of secrecy, this research stream requires a comprehensive literature review, to establish what researchers know, what remains to be uncovered, and what insights researchers should pursue to expand the broader understanding of secrecy. Although previous research cites factors that influence the effectiveness of secrecy, most studies take a narrow or static perspective and address secrecy as a knowledge protection tool that firms decide to apply or not in a one-time decision.¹ The present article seeks to provide a broader, more dynamic view, focused on secrecy management as a continuous management process comprised of four stages – creation of the secret and choice of protection strategy; installation of preventive mechanisms to protect the secrets; protection and exploitation of the secret; and minimization of the negative effects of leakage – dealing with different firm goals and activities. This proposed secrecy management lifecycle thus incorporates aspects that static paradigms cannot address, such as methods for dealing with contingencies. In turn, the framework provides managerially relevant insights into how to manage secrets across different stages. By linking extant literature with these identified stages, the study also reveals critical directions for further research by highlighting under-researched areas.

¹ Literature on product piracy (Berger et al., 2012), imitation (Ordanini, Rubera, & DeFillippi, 2008), and causal ambiguity (King, 2007) also addresses the challenges firms face when trying to appropriate value from knowledge. Such findings complement but are outside the scope of this literature review; the insights inform the further research section of this article.

* Corresponding author. Tel.: +31 50 363 3777

E-mail addresses: b.h.bos@rug.nl (B. Bos), t.l.j.broekhuizen@rug.nl (T.L.J. Broekhuizen), p.m.m.de.faria@rug.nl (P. de Faria).

Table 1
Article sample.

Database	Keywords	Initial pool	Duplicates	Errors	No focus on secrecy (based on abstract/text)	Net Sample
EBSCO	Innovation & secrecy	33	–	–	11	22
ISI Web of knowledge	Innovation & secrecy	43	21	–	16	6
Top journals (ISI Web of knowledge)	Secrecy, trade secrets, knowledge protection, appropriability & innovation	–	–	–	–	10
Google Scholar search of top journals	Secrecy & innovation	783	18	20	702	43
Total						81

Note: Scholar Google identified more articles but is not necessarily superior to traditional searches; this method failed to identify five relevant articles that emerged from top journals using librarian searches. The use of Scholar Google is complementary, not substitutive.

The next section describes the research method and synthesizes the findings of previous studies. Section 3 links the findings of previous studies with the stages of the secrecy management cycle and introduces a research model to specify the role of secrecy in innovation management. Finally, this article concludes with an overview of areas that should guide further research.

2. Literature review

2.1. Method

To understand the view of secrecy as a knowledge protection strategy, the literature review for this study adopted a management perspective, such that the selected articles focus on the strategic management of secrecy in relation to value appropriation. The review intentionally excludes articles from economics and law (Somaya, 2012), unless a contribution provides valuable insights about a firm's use and effectiveness of secrecy. The selection process followed the methodology that Crossan and Apaydin (2009) propose, starting with two commonly used search engines (EBSCO Business Source Premier and ISI Web of Knowledge) that identified available, scholarly, peer-reviewed journal articles. This initial keyword search for “secrecy” and “innovation” resulted in an initial pool of 76 papers, including 21 duplicates. Excluding articles that did not explicitly focus on the use of secrecy, according to their abstracts, that did not appear in journals with impact factors greater than .50, or that did not receive any citations resulted in a sample of 28 peer-reviewed articles (Table 1).

To ensure the inclusion of important articles published in the top journals, a subsequent search of the publications in top innovation² and management research journals³ relied on a broader set of keywords, including both “secrecy” and “innovation” but also related concepts such as “trade secrets,” “appropriability,” and “knowledge protection.” This search revealed 10 additional articles.

Finally, Google Scholar (Advance Search) complemented the previous search. Despite some criticisms of its reliability and transparency, Google Scholar enables searches of complete texts (Schultz, 2007). The combined key terms “innovation” and “secrecy” across all the top innovation and management research journals produced a list of 783 articles. After removing duplicates and errors, a net sample of 745 articles remained available for further analysis. The criteria for relevance required that articles mention secrecy in the text, in combination with other protection mechanisms, or deal with value appropriation. Irrelevant texts might mention secrecy only in footnotes or references; pertain to not-for-profit innovations; refer to military secrecy; involve withholding information from customers (e.g., ingredients), employees

(e.g., wages), or financial institutions (e.g., bankruptcy); or cite secrecy in relation to sensitive data collection. Of the 745 articles, 307 (41%) met the minimum requirements. Of these, 43 relevant articles met the sample inclusion criteria but had not been identified by the traditional search methods. The net sample of 81 journal articles covered 1989 to 2014 and contained 24 theoretical and 57 empirical papers, 43 of which relied on survey data.

2.2. Definition, forms, and use of secrecy

Secrecy is the intentional withholding of a piece of knowledge, information, or behavior by one or more persons from the view of others (Bok, 1984) and an important mechanism to protect valuable information (Dufresne & Offstein, 2008). The main aim of secrecy is to make imitation as costly and unpredictable as possible (Arundel & Kabla, 1998), by concealing chemical formulae, recipes, customer files, machinery designs, or other types of information that are important to a firm and that may be valuable to third parties (Hannah, 2005). Most extant literature studies the relative advantages of secrecy relative to other protection mechanisms. Table 2 provides an overview of commonly cited advantages and disadvantages compared with patenting, a formal protection method that imposes a punishment on the imitator. Secrecy instead functions as a preventive measure, to avoid or at least delay the imitation process from ever starting.

A major advantage of secrecy relates to cost: The costs for design, monitoring, and rule enforcement are relatively low (De Faria & Sofka, 2010), and the approach does not require large upfront investments or maintenance costs (Hussinger, 2006; Leiponen & Byma, 2009). Patenting instead requires huge upfront investments, annual payments to the patent office, and other indirect enforcement costs, such as active monitoring for infringement and legal costs to defend patents (Arundel, 2001). Secrecy also helps firms gain extra time to develop their products prior to product launch (Hurmeliina-Laukkanen & Puumalainen, 2007), and potentially, secrecy can last in perpetuity (Arundel & Kabla, 1998; Hannah, 2005).

The main disadvantage of using secrecy is that firms run the continuous risk of leakage (Hannah, 2005); most forms of secrecy (excluding trade secrets and employee mobility constraints) do not provide any legal protection against accidental disclosures or reverse engineering (Arundel, 2001; Hussinger, 2006; Von Hippel, 1988). If a secret leaks, a company may lose advantages over competitors and other parties. Especially in cooperative relationships, trade secrets are difficult to maintain (Delerue & Lejeune, 2010), and incurred losses are hard to recoup. Restricting the flow of information in cooperative partnerships also may constrain desired information spillovers that foster innovation, inhibit organizational learning, and create employee discontent (James, Leiblein, & Lu, 2013). Moreover, secrecy is generally less effective in achieving strategic benefits beyond knowledge protection, such as blocking advantages, reputational or signaling benefits, exchange advantages, and incentives (Blind, Edler, Frietsch, & Schmoch, 2006). Patents can block competitors (Hussinger, 2006) while also signaling innovativeness to external parties (Harabi, 1995) and enhancing firm value (Blind et al., 2006). Because of formal protection, patents are

² According to the Centre for Development of Entrepreneurs of the UniSA, the top innovation journals in 2005 were *Research Policy*, *Technovation*, *Journal of Product Innovation Management*, *Long Range Planning*, *International Journal of Innovation Management*, *Creativity and Innovation Management*, *European Journal of Innovation Management*, *Technological Forecasting and Social Change*, *Technology in Society*, and *World Development*.

³ The top management journals are *Academy of Management Journal*, *Academy of Management Review*, *Administrative Science Quarterly*, *Management Science*, *Strategic Management Journal*, *Journal of Management*, and *Journal of Management Studies*.

Table 2
Advantages and disadvantages of secrecy and patents.

	Secrecy	Patents
Application costs	No large investments (Hussinger, 2006; Leiponen & Byrna, 2009).	High application costs, uncertain outcome of patenting process (Hall et al., 2012).
Maintenance, monitoring, and infringement costs	Relatively low costs for design, monitoring, and enforcement (De Faria & Sofka, 2010).	High application costs with uncertain outcome, and lengthy application process. High legal costs to monitor and handle infringement (Arundel, 2001; De Faria & Sofka, 2010).
Strategic information costs	Moderate costs for not sharing strategic information restricts organizational learning (James et al., 2013).	Low costs. Legal protection allows for organizational learning in collaborative and open innovation, because technology is protected (Somaya, 2012).
Duration of protection	Long duration. Can last in perpetuity (Hannah, 2005). Firms gain time to further develop the product (Hurmelinna-Laukkanen & Puumalainen, 2007).	Restricted to around 20 years (Blind et al., 2006).
Disclosure effects	No disclosure, but a continuous risk of leakage (Arundel & Kabla, 1998; Hannah, 2005).	R&D cost savings for competitors (Arundel, 2001; Delerue & Lejeune, 2010; Harabi, 1995; Hussinger, 2006), who can start early with inventing around patent (Harabi, 1995).
Legal protection benefits	No legal protection (Delerue & Lejeune, 2010; Hall et al., 2012). Protection by withholding valuable information.	Excludes competitors from using the patent. Legal protection obtained by sharing patent information (Blind et al., 2006).
Blocking advantages	No blocking possible, because no legal protection against imitation (Arundel, 2001; Hussinger, 2006). Danger of being blocked by competitors' patent development.	Offensive and defensive blocking possible through legal protection (Hussinger, 2006) and right to sue for infringement (Amara et al., 2008; Hussinger, 2006).
Reputation or signaling benefits	Limited. Signaling may occur by disclosing parts of the secret information (Ndofor & Levitas, 2004).	Signaling of patent information to other companies (Harabi, 1995); improve customer image (Cohen et al., 2000; Jansen, 2011), attract potential research collaborators, and increase company value (Blind et al., 2006).
Exchange advantages	Limited. Difficult to protect secrets in cooperative relationships (Brockhoff, Gupta, & Roterling, 1991; Leiponen & Byrna, 2009). Exchanging secrets facilitates cooperation in informal networks (Schrader, 1991) and reduces the possibility of holdup (Delerue & Lejeune, 2010).	License income and improve power in interfirm negotiations, facilitate cooperation and technology trading, and patent pool participation (Blind et al., 2006; Cohen et al., 2000; Hall et al., 2012; Hussinger, 2006). Coordination device in partnerships (Pénin, 2005). Learning and cooperation when waiving patents in open innovation projects (Henkel et al., 2014).
Incentive advantages	Limited. Employees feel important when given secret information but can hold that information against the firm (Dufresne & Offstein, 2008; Haas & Park, 2010). Employees may become dissatisfied if secrets are withheld from them (James et al., 2013).	The number of patents, as an internal performance indicator, may motivate staff and provide a performance evaluation tool (Blind et al., 2006).

more effective for achieving exchange advantages, including license income or greater bargaining power in interfirm negotiations (Cohen et al., 2000). Patents also facilitate cooperation, increase a firm's ability to participate in patent pools (Blind et al., 2006; Hall et al., 2012), and stimulate openness and learning in open innovation projects when firms waive some of their patents (Henkel, Schöberl, & Alexy, 2014). Although the ability of secrecy to achieve these strategic aspects remains insufficiently explored, initial evidence implies that exchanging secrets can facilitate cooperation across informal networks (Schrader, 1991) and interfirm negotiations (Harabi, 1995). Finally, patents motivate staff as internal indicators of performance. Although the disclosure of secrets to certain employees might motivate them or increase their sense of importance, employees also can use this knowledge to hold the organization hostage (Dufresne & Offstein, 2008; Haas & Park, 2010).

2.3. Contextual factors shaping the use and effectiveness of secrecy

Extant research demonstrates the context-specific nature of effective secrecy (Hall et al., 2012; James et al., 2013). Fig. 1 accordingly delineates key contextual factors related to innovation, organization, industry factors, and intellectual property protection.

2.3.1. Innovation factors

Innovation characteristics and the type of information embedded in an innovation determine the use and effectiveness of secrecy. Secrets work well when innovations cannot be observed and replicated easily, such as those that contain tacit knowledge elements. Patents work well to protect codified elements (Arora, 1997). Secrecy also is more effective for services than goods, because services embody more tacit knowledge and are harder to patent (Delerue & Lejeune, 2010). Service

knowledge often is heterogeneous, intangible, and client specific, so companies likely cannot protect it with formal protection methods (Amara et al., 2008). Secrecy also is more effective for protecting new processes than products, which tend to be hidden within the firm (Gonzalez-Alvarez & Nieto-Antolin, 2007). In contrast, patents are less effective for process innovations, for which possible infringements are difficult to detect (Gallié & Legros, 2012). Patents instead provide more protection for innovations in sectors such as pharmaceuticals, chemicals, and machinery, where the cost of copying an innovation is substantially lower than the initial cost of inventing the product (Arundel & Kabla, 1998; Encaoua, Guellec, & Martinez, 2006). Secrecy works better for incremental than for radical innovations, especially if consumer switching costs are high and market lead time is critical. Some research suggests that secrecy benefits radical innovations, because patent applications must disclose valuable information before product launch that competitors can use to start inventing around the innovation (Zaby, 2010), but the wider consensus suggests that radical innovations more easily meet the non-evident improvement requirement, and patent protection advantages outweigh the benefits created by market lead times (Cohen et al., 2000). Finally, secrecy is a more effective appropriation method for products with relatively short life cycles (Blind & Thumm, 2004).

2.3.2. Organizational factors

Firm size, focus on R&D or cooperative partnerships, and organization culture also influence the effectiveness of protection mechanisms. Theoretically, small firms might benefit more from patents because of their disadvantageous position related to alternative protection mechanisms and appropriation (Arundel & Kabla, 1998; Blind et al., 2006) and greater need for patent signaling. Most empirical results instead indicate that larger firms find patenting more important and apply for

Fig. 1. Determinants of the use and effectiveness of secrecy (Zhao, 2006).

more patents (Arundel, 2001; Cohen et al., 2000; Gonzalez-Alvarez & Nieto-Antolin, 2007; Hussinger, 2006; Leiponen & Byma, 2009). Large firms can carry out specific functions within their own organizations and maintain patent departments that actively seek out patents (Blind et al., 2006). Small firms instead rely on secrecy because they lack the resources to obtain and defend patents (Cohen et al., 2000; Gonzalez-Alvarez & Nieto-Antolin, 2007; Katila, Rosenberger, & Eisenhardt, 2008; Leiponen & Byma, 2009; Milesi, Petelski, & Verre, 2013; Neuhäusler, 2012). Only in high-tech, information-intensive industries (e.g., biotech) small firms tend to use patents as negotiation tactics in acquisitions and mergers (Blind et al., 2006). Furthermore, R&D-intensive firms attribute more importance to secrecy than firms with lower R&D investments (Blind & Thumm, 2004; Cassiman & Veugelers, 2006; Neuhäusler, 2012), and secrecy is more important for firms that perform in-house R&D than those that outsource R&D (Gooroochurn & Hanley, 2007). Firms that actively form cooperative relationships also make more use of patents to protect valuable knowledge (Leiponen & Byma, 2009), provide observable proof of research quality, and support selective knowledge sharing with partners through licensing. Cooperative relationships instead make the protection of secrets more difficult and less desirable, because a partnering strategy requires knowledge sharing and goal alignment, which may not be compatible with deliberately withholding knowledge (Milesi et al., 2013; Slowinski, Hummel, & Kumpf, 2006). Cooperating firms tend to favor patenting, because patents provide an observable proof of the quality of the research activities of the firm and allow a selective sharing of knowledge with partners via licensing. Finally, firms' national cultures influence preferences for a particular protection strategy: Firms

operating in countries with lower collectivism and uncertainty avoidance make more frequent use of secrecy (Delerue & Lejeune, 2011).

2.3.3. Industry factors

Lifecycle, competitiveness, and structure are industry factors that influence secrecy's effectiveness. Secrecy is most effective in the premarket development phase (Arundel, 2001; Cohen et al., 2000), providing innovators with additional time to make modifications to the original design before commercializing the product (Hurmelinna-Laukkanen & Puumalainen, 2007). Firms often use secrecy first, to protect an invention during the development phase, then rely on patents or other appropriation methods when the invention enters the market (Arundel, 2001; Hussinger, 2006). Industries vary in their competitive pressure and thus in the degree to which information spillovers or leakages occur. Companies tend to use patents in highly competitive markets with neck-a-neck competition, where firms build on other firms' innovations and products have greater substitutability (Jansen, 2011). Conversely, secrecy is desirable if competitors are unlikely to devise a similar innovation (Kultti, Takalo, & Toikka, 2007), because patent blocking then is less likely.

2.3.4. Intellectual property protection

Several factors govern the innovator's ability to capture value from its innovation through formal protections, related to intellectual property regime costs and benefits of patenting and other formal protection mechanisms. These factors differ across nations and regions (Cohen, Goto, Nagata, Nelson, & Walsh, 2002). The relative advantages of secrecy versus patenting depend strongly on the ease of obtaining a patent

(e.g., disclosure requirements, initial fixed costs, costs of confidentiality agreements, possibility to patent services), legal costs of maintaining and enforcing the patent, and the benefits patents create in terms of the duration and effective protections of a temporary monopoly (Amara et al., 2008), as well as strategic benefits, such as improving interfirm negotiations (Cohen et al., 2002). Firms often use secrecy in countries with weak property rights (Anton, Greene, & Yao, 2006), because the legal protection provided by patents is limited. Although firms seemingly should patent more in effective patent systems, empirical evidence does not support this causal link (Brouwer & Kleinknecht, 1999), possibly because stricter intellectual property regimes also increase patent litigation costs (Gallini, 2002).

In summary, existing literature delineates advantages and disadvantages of secrecy compared with formal protection means, such as patenting. Studies also have identified several innovation, organizational, industry, and intellectual property protection factors that enhance or impede the (perceived) effectiveness of secrecy as a value appropriation mechanism. Yet extant literature has not provided a systematic, dynamic view of secrecy. The next section seeks to fill this research gap and introduces a secrecy management lifecycle.

3. Managing secrecy

Secrecy management aims to create, protect, and exploit secrets to increase value appropriation from innovations.⁴ Thus, the method does not halt with the initial decision to keep valuable information secret but rather involves a continuous, nonlinear process that requires adjustments to changing market circumstances or contingencies. Secrecy management also is not linear; some steps must be rerun (or skipped) when they are not executed well or when changes occur in the intraorganizational (e.g., leaving employees), interorganizational (e.g., cooperative partner defects), or external (e.g., competitor patents similar technology) environment. Treating secrecy as one-time decision neglects the uncertainty of managing innovations; contingencies in later stages can challenge assumptions that informed initial decisions and demand actions to maintain the secrets' value or limit the negative consequences of information leakages. Furthermore, the goals and activities of secrecy management differ with the stages. By distinguishing distinct stages' goals and activities (Table 3), managers can gain a better understanding of how to manage secrecy over time, and scholars can identify under-researched topics.

Fig. 2 displays the dynamic approach, in which secrecy management is an ordered process with potential feedback loops that also incorporates contingencies. Rather than asking "When should firms use secrecy?" research should address "How can firms manage secrecy and react to contingencies?" In addition, the secrecy management lifecycle helps structure investigations of preliminary answers to questions beyond the initial choice of a protection mechanism (Stage I), to include "How can firms install preventive mechanisms to protect secrets?" (Stage II), "How can firms protect and exploit secrets?" (Stage IIIa), and "How can firms minimize the negative effects of leakage?" (Stage IIIb).

3.1. Stage I: Creation of a secret and choice of protection strategy

After deciding to protect valuable information, managers must determine how to do so. The goal is to find appropriate protection mechanisms that provide effective protection at low costs. Firms can use formal, informal, or a combination of both protection mechanisms (Encaoua et al., 2006), and use them simultaneously or sequentially.

In addition to answering the key questions in Table 3, finding a cost-effective secrecy strategy requires firms to understand the effectiveness of available formal and informal protection mechanisms and the value of the secret (i.e., costs of leakage).

Existing research largely ignores the potential for complementarity and synergies achieved by using different protection methods (Hall et al., 2012). Arora (1997) cites the example of the organic chemical industry, which combines secrecy (for tacit elements such as specific combinations of different compounds) and patents (for codified elements such as individual compounds) to protect inventions and innovations. Amara et al. (2008) also show that legal and informal mechanisms can complement each other (patents, registered design patterns, trademarks, secrecy and market lead time are complements), or else act as substitutes (patents and design complexity are substitutes). Sofka, Shehu, and de Faria (2014) assume that legal knowledge protection instruments, such as patents, can be complemented by organizational knowledge protection measures, such as secrecy, in multinational subsidiaries' knowledge protection strategies. The lack of knowledge about simultaneous uses of different protection strategies or the effectiveness of combined strategies reveals an interesting avenue for research. Little research attempts to explain how different protection strategies induce organizational performance differences either. For example, are organizations that restrict their secrets more capable of appropriating value from innovations than open organizations?

3.2. Stage II: Installation of preventive mechanisms to protect the secret

When firms install preventive mechanisms to protect a secret, the goal is to design products and organizational procedures that effectively prevent valuable knowledge from leaking, thus increasing the stickiness of information, so the costs of obtaining and understanding those secrets increase for outsiders. Firms can increase product complexity or the tacitness or specificity of information embedded in the innovation to hinder the transfer of secrets (e.g., via reverse engineering) to rivals and make imitation more difficult (McEvily & Chakravarthy, 2002; Thomä & Bizer, 2013). Organizational procedures also should show employees how to protect secrets embedded in human capital (Delerue & Lejeune, 2010). Employees not only possess valuable know-how acquired through experience but are also often the sources of leakage (Hurmelinna-Laukkanen & Puumalainen, 2007). Delerue and Lejeune (2011) conclude that the biggest leakage threat is current and former employees, not spying competitors. Whether to share a secret often gets left to the interpretation of employees, who use their personal judgment to decide if information is confidential (Bouty, 2000). In addition, the likelihood of disclosures increases when more employees know the secret, such that managers must control the number of informed people (Steele, 1989), as well as specify which valuable information is secret and install mechanisms that ensure this information remains within the company. In addition to answering the important questions in Table 3, firms should implement measures that allow the flow of secrets to important decision makers who need to know while restricting access to others who might capitalize on secret knowledge (Haas & Park, 2010).

Most extant research treats secrecy as a single, firm-level protection tool without distinguishing between different secrecy instruments. Some recent research examines specific instruments that protect secrets but not their effectiveness. Formal instruments include trade secrets, nondisclosure agreements, and noncompetition agreements (Hannah, 2005, 2007). Hannah (2005) investigates the degree to which employees feel obliged to protect a secret when firms use trade secret access or handling procedures, which have negative and positive effects, respectively, on felt obligation. Both instruments also are more effective when supported by organizational actions. In turn, Hannah (2007) discusses three types of agreements that firms use to retain protected knowledge: nondisclosure agreements restrict the use and disclosure of trade secrets, noncompete agreements impede employees

⁴ This article does not address firms' responses to the (il)legitimate copying by third parties. Actions aimed at fighting counterfeits and product piracy generally rely on formal mechanisms, such as trademarks, copyrights, patents, and design rights (Levin, Klevorick, Nelson, & Winter, 1987), performed after the exposure of valuable information that is no longer secret.

Table 3
Stages, goals, and activities in the secrecy management lifecycle.

	Goal	Key questions	Required knowledge/activities
Stage I: Creation of secret and choice of protection strategy	To determine the scope of the secret and how to protect the secret.	How to protect the secret? How effective are formal and informal protection mechanisms, given the nature of the secret and organization? With whom and when to share information? What parts need to be shared and what parts need to be protected by other mechanisms? How should the firm disclose secrets to outsiders in time?	Firms should understand the effectiveness of the available formal and informal mechanisms and the value of secrets to come up with a protection strategy.
Stage II: Installation of preventive mechanisms to protect secret	To install the preventive mechanisms and agreements to protect the secret.	Which preventive mechanisms can protect secrets? How can products be designed so they are not easy to imitate? How can the firm limit the disclosure of secrets, while allowing the dissemination of strategically relevant information to decision makers? What culture motivates employees to protect secrets?	Firms should install protection mechanisms, assign individual responsibility for the protection of secrets, and motivate employees to protect secrets.
Stage IIIa: Protection and exploitation of secret	To increase the lifetime value of a secret by scanning for opportunities and threats that determine (future) costs and benefits, and react to changes.	How can the firm maintain and exploit the value of a secret? How should the firm react to internal and external changes that affect the likelihood of leakage and the value of secrets? How should the firm exploit the value of secrets by releasing some parts of them?	Firms need knowledge about the effective (combination of) implementation techniques, monitoring, and take corrective actions. Firms can increase the value of a secret by exploiting it in exchange situations and for marketing purposes.
Stage IIIb: Minimization of negative effects of leakage	To reduce the negative impact of leakage.	How can the firm reduce the impact of leakage of information? What actions prevent further distribution of the leakage?	Firms need knowledge about problem solving and should take effective measures to minimize the negative consequences of disclosures.

from working for direct competitors, and assignment provisions assign legal rights to the ideas that employees developed during their employment to the company. Violations of any of these contractual agreements expose employees to the risk of dismissal or a lawsuit. [Sussman \(2008\)](#) finds that formal communication prohibitions are more effective if firms also create an organizational culture that supports the prohibitions and minimizes employee resistance. Employees adhere to prohibitions that appear reasonable, warranted, equitable, and legal.

Formal measures to control knowledge flows between workers and the external environment are generally less effective though ([Gallié & Legros, 2012](#)), so many firms turn to informal measures, such as fair compensation to restrict employee mobility ([Deleue & Lejeune, 2010](#)), administrative or operational protection procedures that reduce

chances of leakage ([Hannah, 2005](#)), and compartmentalization, which allows slicing secrets into parts so no employee can put the secrets together to understand the bigger picture ([Dufresne & Offstein, 2008](#)). Research also suggests that in collaborative projects, it pays off to provide trainings focused on the protection of sensitive information during the course of collaboration to the employees of the constituent firms ([Slowinski et al., 2006](#)).

Thus some research identifies formal and informal instruments available to protect secrets but has not assessed their relative effectiveness, whether their effectiveness differs in different circumstances, or if formal and informal mechanisms complement and reinforce each other. Nor does existing research provide answers about how to install and maintain such instruments, how firms should balance the

Fig. 2. Secrecy management lifecycle.

dissemination of strategically relevant information with increased leakage chances, or how to motivate employees to continuously protect information.

3.3. Stage IIIa: Protection and exploitation of the secret

In the third stage, the goal is to protect and exploit the secret to its full extent. During the development and commercialization phases of the innovation, companies face challenges and opportunities that might require adjustments to initial protection strategies. Failing to respond adequately to new environmental challenges means that firms' existing protection strategy might not be sufficient to prevent the secret from leaking or losing value. At the same time, apart from the protection benefits that secrets generate, firms seek to use their secrets to attain strategic advantages and increase the value of the secret further. Ideally, firms continue to protect and further develop their secret (as long as the costs of protection and development are lower than the future benefits), so that the firm can exploit the secret in exchange situations or for marketing purposes.

A limited set of studies examines ways to protect secrets over time, including investigations of how firms secure and exploit secrets in collaborative relationships and respond to critical incidents. Secrets are difficult to protect, and in cooperative relationships, the partners must update protection strategies (Leiponen & Byma, 2009). Slowinski et al. (2006) find that firms use sequences of protection strategies to extend the lifetime of a secret. Managers also tailor legal agreements, such as nondisclosure agreements, to collaborative project stages or form new agreements when a project enters a subsequent product phase.

Another important challenge arises when employees leave the firm. Hannah (2005) finds that exiting employees face a dilemma: The new employer might benefit from the secret, but sharing that secret would be a betrayal of the previous employer and potentially risk a lawsuit. The likelihood of sharing then depends on the employee's relative loyalty toward the old and new employer.

In terms of strategic advantages from secrets, research shows that exchanging secrets facilitates cooperation in informal networks through reciprocity (Schrader, 1991) and reduces the possibility of holdups (Deleue & Lejeune, 2010). Yet no research has investigated how and in what circumstances firms might gain more by disclosing rather than keeping a secret. By revealing some parts of the secret, firms might signal to the market that they have valuable technology or information; this signal could alter the beliefs of or convey information to market actors about the firm's unobservable attributes and intentions (Ndofo & Levitas, 2004). Anecdotal evidence indicates that firms with publicly visible signals can generate effective marketing campaigns by releasing parts of the secret, such as when Apple discloses a snapshot of a new iPhone model.

Despite this evidence about the dynamic nature of secrecy management, a strong need persists for research that describes how firms should react to critical events and changes and thereby optimize the value of secrets. Further research should investigate the necessary reactions and firm capabilities required to reduce potential leakages caused by contingencies, as well as how firms can capitalize on the strategic benefits associated with releasing parts of the secret (e.g., promote new products to customers, promote research projects to partners, create exchange benefits during interfirm negotiations).

3.4. Stage IIIb: Minimization of the negative effects of leakage

Finally, a secret may lose value over time and become obsolete. If espionage, bribery, or employee flows lead to the unwanted exposure of a secret, the firm must mitigate the negative effects. In the effort to minimize the negative effects of this leakage, firms hope to halt any further leakages and take affirmative action against the leakers, while limiting the degree to which external actors can benefit from the already disclosed information.

Firms engage in formal and informal responses to secret exposures. Hoti, McAleer, and Slottje (2006) describe the increasing uses of formal enforcements of intellectual property rights by U.S. firms, despite the substantial settlement costs. In this stage, firms might rely on the preventive mechanisms installed in Stage II, especially if the mechanisms can provide evidence of leakages or violations of procedures and roles. Sickles and Ayyar (2006) cite five measures to calculate damages in trade secret lawsuits: (1) the value of the trade secret at the time it was first misappropriated, (2) lost profits, (3) price erosion of the company's products, (4) the defendant's unjust enrichment in terms of the value of the trade secret when it was taken, and (5) the costs of legally licensing the trade secret.

A common informal measure is the distribution of disinformation, that is, strategic, intentional spreading of false or inaccurate information to deceive external parties (Karlova & Fisher, 2013). No management research has addressed how the timing, content, or intensity of such a strategy might steer attention away from the secret or undermine its credibility. In conclusion, though researchers identify some reactive measures to leakages, future research should come up with a taxonomy of measures and conduct empirical tests of the measures' effectiveness.

4. Discussion and further research

This study synthesizes extant research and provides a secrecy management lifecycle model that extends current research by highlighting important research areas, beyond the understanding of when to use secrecy. This lifecycle indicates the stages and activities involved in the management of secrecy, incorporates potential contingencies, and directs managerial decisions toward maximizing the value appropriated through secrecy. By categorizing previous research according to these stages, the present article elucidates the significant advances achieved by prior research for determining the effectiveness of secrecy relative to other protection means across various contexts. The results also denote which research areas deserve additional scholarly attention, including (1) strategic objectives beyond protection and limits of protection, (2) stages beyond the initial decision, and (3) methodological issues.

4.1. Strategic objectives beyond protection and the limits of protection

Although secrecy is a strategic asset, research rarely links it to strategic objectives. Just as patents can facilitate the attainment of strategic objectives (e.g., reputation or signaling benefits, exchange and incentive advantages; Connelly, Certo, Ireland, & Reutzel, 2011; Hall et al., 2012), secrecy may provide benefits beyond the protection of valuable information. For example, secrecy can be a signaling tool (Ndofo & Levitas, 2004). Rather than publicly revealing information protected by the patent, firms might strategically reveal some features of a secret and thus signal their innovative capacity. Apple frequently generates substantial buzz by intentionally revealing part of its secret to the public; using such signals, highly visible firms can often generate more excitement than via ordinary product announcements or expensive mass media campaigns. Also, Coca-Cola still benefits from the mystery surrounding its secret recipe. This strong, enduring signal would not be possible with a time-limited patent (The Economist, 2013). In addition, showing external partners that the company owns a secret (e.g., demonstration of end product but not the process) may create exchange benefits and facilitate cooperation. Additional research should assess the degree to which firms can reap strategic benefits across various firm characteristics (e.g., firm visibility, technology orientation) and circumstances. Other studies should investigate how to balance the flow of secret information to important insiders and outsiders during innovation management processes, while minimizing the chances of leakage. Such research opportunities require a temporal perspective, because the value of secrets and the benefits of sharing vary over time.

Most secrecy research cites the protection benefits, but secrecy also creates limitations, such that very strong protections might harm the firm's innovation success. Restricting the flow of valuable information to employees that are not the focal decision makers may effectively reduce the chances of information leakage (including the risk of human capital spillover when employees leave the firm), but also hinder knowledge exchanges that help employees develop human capital resources and innovative ideas (King, 2007). The nondisclosure of secrets to external cooperation partners also could backfire, because external knowledge search and cooperation activities imply some level of reciprocity, which may be hampered by a high level of secrecy. Research should investigate whether a trade-off exists between the degree of value appropriation and level of innovativeness in intra- and interorganizational settings.

4.2. Later stages of secrecy management

Most studies in the literature review focused on the initial stage, when firms determine which protection strategy to use. The less studied subsequent stages remain poorly understood. A comprehensive understanding of secret management requires investigations of the entire process, including installing the preventive measures (Stage II), protecting and exploiting secrecy (Stage IIIa), and minimizing the negative effects of leakage (Stage IIIb), and the effectiveness of the related measures. This requirement indicates important research avenues. Researchers still know relatively little about how and to what degree firms install secrecy mechanisms (e.g., training, administrative protection), monitor and react to information leakages, and update or further develop secrets.

4.3. Methodological issues

The reviewed articles suggest that researchers struggle to collect valid data about the use, effectiveness, and value of secrets. Several studies cite concerns about the measurement of secrecy and the validity of the findings. Secrecy is difficult to measure, because by definition it relies on the nondisclosure of information to external parties. Obtaining reliable data about the management of secrecy at the firm level thus is very difficult. Similar to other fields that depend on sensitive information, such as product piracy literature that addresses an illegal activity (Berger, Blind, & Cuntz, 2012), limited data are publicly available, and firm-level surveys seem to offer the most reliable data collection method.

Accordingly, empirical studies mainly use firm-level survey data, whether from the Community Innovation Survey (CIS) or self-constructed surveys (Arundel, 2001; Harabi, 1995; Hurmelinna-Laukkanen & Puumalainen, 2007; Leiponen & Byma, 2009), even though secrecy decisions generally occur at the project level (Gonzalez-Alvarez & Nieto-Antolin, 2007; Hussinger, 2006). The collection of firm-level data obscures the link between the knowledge protected and the types of protection methods, so researchers cannot disentangle the individual from the joint effects of knowledge protection mechanisms (Hussinger, 2006) or establish the potential complementarity effects between secrecy and other formal protection mechanisms (Amara et al., 2008). To overcome the potential subjective reporting biases in surveys, researchers can turn to retrospective studies that likely can obtain more objective data and documents (e.g., content analysis to investigate leakage rates prior product launch) and assess the effectiveness of secrecy. Other studies can also use indirect measures to infer the use and effectiveness of secrecy, such as the percentage of patent-protected products released in a market or by a firm, which could reflect the importance of secrecy, or the degree to which the competitors can imitate innovators' unpatented products faster than average, to assess secrecy effectiveness. Both retrospective studies and indirect measures rely on proxies for secrecy that require certain assumptions. Valid inferences demand clear assumptions or

additional information about firms' secrecy strategies (e.g., motivation and capacity to use secrecy), capacity to innovate (e.g., R&D intensity, number of patents), and market sector characteristics (e.g., likelihood of imitation). To overcome the limits of static measures and better understand the dynamics of secrets, researchers could use case studies or use experiments to create artificial settings to observe managers' reactions to secrecy leakage and secrecy exchanges, though the generalizability of such studies is a concern. Researchers also face problems in finding metrics to assess the value of secrets. Firms choose secrecy as a protection mechanism on the basis of the trade-off between the relative costs and benefits, as well as the importance or value of the secret, that is, the costs of information leakage. The means decision makers use to achieve this trade-off are unknown, including whether the decision is intuitive or calculated. Researchers should try to help managers develop metrics or use existing indicators (e.g., clearance levels that define access to the secret) to assess the value of secrets and thereby enhance understanding of why certain secrets remain protected and further developed, whereas others get neglected and no longer protected.

5. Conclusion

This article provides a comprehensive review of research into the role of secrecy as a knowledge protection tool for innovation management. In addition to synthesizing the findings from previous studies into a framework, the present study presents a lifecycle model of the stages of secrecy management. Some weaknesses or gaps in prior research suggest possible solutions and research directions. In addition to contributing to a better understanding of the importance and meaning of secrecy, this study can help managers make well-informed, structured decisions about which protection strategy to choose, how to install preventive measures, how to protect and exploit a secret, and ways to deal with contingencies. This study stimulates scholars to build on these insights and calls for more research on secrecy management and clarifying the later stages of secrecy management, addressing the strategic objectives and limits of secrecy protection, as well as to overcome persistent methodological issues.

References^{5 6 7}

- *Amara, N., Landry, R., & Traoré, N. (2008). Managing the protection of innovations in knowledge-intensive business services. *Research Policy*, 37(9), 1530–1547.
- *Anton, J., Greene, H., & Yao, D. (2006). Policy implications of weak patent rights. *NBER Innovation Policy and the Economy*, 6.
- *Arora, A. (1997). Patents, licensing, and market structure in the chemical industry. *Research Policy*, 26(4–5), 391–403.
- *Arundel, A. (2001). The relative effectiveness of patents and secrecy for appropriation. *Research Policy*, 30(4), 611–624.
- *Arundel, A., & Kabla, I. (1998). What percentage of innovations are patented? Empirical estimates for European firms. *Research Policy*, 27(2), 127–141.
- †Berger, F., Blind, K., & Cuntz, A. (2012). Risk factors and mechanisms of technology and insignia copying – A first empirical approach. *Research Policy*, 41(2), 376–390.
- *Blind, K., Cremers, K., & Mueller, E. (2009). The influence of strategic patenting on companies' patent portfolio. *Research Policy*, 38(2), 428–436.
- *Blind, K., Edler, J., Frietsch, R., & Schmoch, U. (2006). Motives to patent: Empirical evidence from Germany. *Research Policy*, 35(5), 655–672.
- *Blind, K., & Thumm, N. (2004). Interrelation between patenting and standardisation strategies: Empirical evidence and policy implications. *Research Policy*, 33(10), 1583–1598.
- †Bogers, M., Afuah, A., & Bastian, B. (2010). Users as innovators: A review, critique, and future research directions. *Journal of Management*, 36(4), 857–875.
- †Bok, S. (1984). *Secrets: On the ethics of concealment and revelation*. London: Oxford University Press.
- *Bouty, I. (2000). Interpersonal and interaction influences on informal resource exchanges between R&D researchers across organizational boundaries. *Academy of Management Journal*, 43(1), 50–65.
- *Brockhoff, K., Gupta, A.K., & Rotering, C. (1991). Inter-firm R&D co-operations in Germany. *Technovation*, 11(4), 219–229.
- Brouwer, E., & Kleinknecht, A. (1999). Innovative output, and a firm's propensity to patent: An exploration of CIS micro data. *Research Policy*, 28(6), 615–624.

⁵ *reference part of sample and cited in text.

⁶ † reference not part of sample, but cited in text.

⁷ A full list of the 81 articles is available on request from the corresponding author.

- *Carbonell, P., & Rodríguez, A. (2006). Designing teams for speedy product development: The moderating effect of technological complexity. *Journal of Business Research*, 59(2), 225–232.
- *Cassiman, B., & Veugelers, R. (2006). In search of complementarity in innovation strategy. *Management Science*, 52(1), 68–82.
- *Cohen, W.M., Goto, A., Nagata, A., Nelson, R.R., & Walsh, J. (2002). R&D spillovers, patents and the incentives to innovate in Japan and the United States. *Research Policy*, 31(8/9), 1349–1367.
- Cohen, W., Nelson, R.R., & Walsh, J. (2000). Protecting their intellectual assets: Appropriability conditions and why U.S. manufacturing firms patent (or not). *NBER Working Paper Series*. (pp. 7552).
- *Connelly, B.L., Certo, S.T., Ireland, R.D., & Reutzel, C.R. (2011). Signaling theory: A review and assessment. *Journal of Management*, 37(1), 39–67.
- *Crossan, M.M., & Apaydin, M. (2009). A multi-dimensional framework of organizational innovation: A systematic review of the literature. *Journal of Management Studies*, 47(6), 1154–1191.
- *De Faria, P., & Sofka, W. (2010). Knowledge protection strategies of multinational firms – A cross-country comparison. *Research Policy*, 39(7), 956–968.
- *Delerue, H., & Lejeune, A. (2010). Job mobility restriction mechanisms and appropriability in organizations: The mediating role of secrecy and lead time. *Technovation*, 30(5/6), 359–366.
- *Delerue, H., & Lejeune, A. (2011). Managerial secrecy and intellectual asset protection in SMEs: The role of institutional environment. *Journal of International Management*, 17(2), 130–142.
- *Drechsler, W., & Natter, M. (2012). Understanding a firm's openness decisions in innovation. *Journal of Business Research*, 65(3), 438–445.
- *Dufresne, R.L., & Offstein, E.H. (2008). On the virtues of secrecy in organizations. *Journal of Management Inquiry*, 17(2), 102–106.
- *Encaoua, D., Guellec, D., & Martinez, C. (2006). Patent systems for encouraging innovation: Lessons from economic analysis. *Research Policy*, 35(9), 1423–1440.
- *Gallié, E.P., & Legros, D. (2012). French firms' strategies for protecting their intellectual property. *Research Policy*, 41(4), 780–794.
- *Gallini, N.T. (2002). The economics of patents: Lessons from recent U.S. patent reform. *The Journal of Economic Perspectives*, 16(2), 131–154.
- *Gonzalez-Alvarez, N., & Nieto-Antolin, M. (2007). Appropriability of innovation results: An empirical study in Spanish manufacturing firms. *Technovation*, 27(5), 280–295.
- *Goorouchum, N., & Hanley, A. (2007). A tale of two literatures: Transaction costs and property rights in innovation outsourcing. *Research Policy*, 36(10), 1483–1495.
- *Haas, M.R., & Park, S. (2010). To share or not to share? Professional norms, reference groups, and information withholding among life scientists. *Organization Science*, 21(4), 873–891.
- *Hall, B.H., Helmers, C., Rogers, M., & Sena, V. (2012). The choice between formal and informal intellectual property: A literature review. *NBER working paper series* (pp. 17983).
- *Hanel, P. (2006). Intellectual property rights business management practices: A survey of the literature. *Technovation*, 26(8), 895–931.
- *Hannah, D.R. (2005). Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets. *Organization Science*, 16(1), 71–84.
- *Hannah, D.R. (2007). An examination of the factors that influence whether newcomers protect or share secrets of their former employers. *Journal of Management Studies*, 44(4), 465–487.
- *Harabi, N. (1995). Appropriability of technical innovation – An empirical analysis. *Research Policy*, 24(6), 981–992.
- *Harris, R.J. (2009). *Cognitive psychology of mass communication*. New York: Routledge.
- *Henkel, J., Schöberl, S., & Alexy, O. (2014). The emergence of openness: How and why firms adopt selective revealing in open innovation. *Research Policy*, 43(5), 879–890.
- *Hoti, S., McAleer, M., & Slottje, D. (2006). Intellectual property litigation activity in the USA. *Journal of Economic Surveys*, 20(4), 715–729.
- *Hurmelinna-Laukkanen, P., & Puumalainen, K. (2007). Nature and dynamics of appropriability: Strategies for appropriating returns on innovation. *R&D Management*, 37(2), 95–112.
- *Hussinger, K. (2006). Is silence golden? Patents versus secrecy at the firm level. *Economics of Innovation & New Technology*, 15(8), 735–752.
- *James, S.D., Leiblein, M.J., & Lu, S. (2013). How firms capture value from their innovations. *Journal of Management*, 39(5), 1123–1155.
- *Jansen, J. (2011). On competition and the strategic management of intellectual property in oligopoly. *Journal of Economics & Management Strategy*, 20(4), 1043–1072.
- *Karlova, N.A., & Fisher, K.E. (2013). A social diffusion model of misinformation and disinformation for understanding human information behaviour. *Information Research*, 18(1) (paper 573).
- *Katila, R., Rosenberger, J., & Eisenhardt, K. (2008). Swimming with sharks: Technology ventures, defense mechanisms and corporate relationships. *Administrative Science Quarterly*, 53(2), 295–332.
- *King, A.W. (2007). Disentangling interfirm and intrafirm causal ambiguity: A conceptual model of causal ambiguity and sustainable competitive advantage. *Academy of Management Review*, 32(1), 156–178.
- *Kultti, K., Takalo, T., & Toikka, J. (2007). Secrecy versus patenting. *RAND Journal of Economics*, 38(1), 22–42.
- *Leiponen, A., & Byma, J. (2009). If you cannot block, you better run: Small firms, cooperative innovation, and appropriation strategies. *Research Policy*, 38(9), 1478–1488.
- *Levin, R.C., Klevorick, A.K., Nelson, R.R., & Winter, S.G. (1987). Appropriating the returns from industrial research and development. *Brookings Papers on Economic Activity*, 3, 783–831.
- *Levitas, E., & McFadyen, M.A. (2009). Managing liquidity in research-intensive firms: Signaling and cash flow effects of patents and alliance activities. *Strategic Management Journal*, 30(6), 659–678.
- *McEvily, S., & Chakravarthy, B. (2002). The persistence of knowledge-based advantage: An empirical test for product performance and technological knowledge. *Strategic Management Journal*, 23(4), 285–305.
- *McGahan, A.M., & Silverman, B.S. (2006). Profiting from technological innovation by others: The effect of competitor patenting on firm value. *Research Policy*, 35(8), 1222–1242.
- *Milesi, D., Petelski, N., & Verre, V. (2013). Innovation and appropriation mechanisms: Evidence from Argentine microdata. *Technovation*, 33(2–3), 78–87.
- *Ndofo, H.A., & Levitas, E. (2004). Signaling the strategic value of knowledge. *Journal of Management*, 30(5), 685–702.
- *Neuhäusler, P. (2012). The use of patents and informal appropriation mechanisms – Differences between sectors and among companies. *Technovation*, 32(12), 681–693.
- *Ordanini, A., Rubera, G., & DeFillippi, R. (2008). The many moods of inter-organizational imitation: A critical review. *International Journal of Management Reviews*, 10(4), 375–398.
- *Pénin, J. (2005). Patents versus ex post rewards: A new look. *Research Policy*, 34(5), 641–656.
- *Schrader, S. (1991). Informal technology transfer between firms: Cooperation through information trading. *Research Policy*, 20(2), 153–170.
- *Schultz, M. (2007). Comparing test searches in PubMed and Google Scholar. *Journal of the Medical Library Association*, 95(4), 442–445.
- *Sethi, R., Smith, D.C., & Park, C.W. (2001). Cross-functional product development teams, creativity, and the innovativeness of new consumer products. *Journal of Marketing Research*, 38(1), 73–85.
- *Sickles, R., & Ayyar, A. (2006). Evaluation of damages in a trade secrets case. In D. Slottje (Ed.), *Economic damages in IP matters: A hands-on guide to litigation* (pp. 281–296). New York: Wiley.
- *Slowinski, G., Hummel, E., & Kumpf, R.J. (2006). Protecting know-how and trade secrets in collaborative R&D relationships. *Research Technology Management*, 49(4), 30–38.
- *Sofka, W., Shehu, E., & de Faria, P. (2014). Multinational subsidiary knowledge protection – Do mandates and clusters matter? *Research Policy*, 43(8), 1320–1333.
- *Somaya, D. (2012). Patent strategy and management: An integrative review and research agenda. *Journal of Management*, 38(4), 1084–1114.
- *Steele, J.M. (1989). Models for managing secrets. *Management Science*, 35(2), 240–248.
- *Sussman, L. (2008). Disclosure, leaks, and slips: Issues and strategies for prohibiting employee communication. *Business Horizons*, 51(4), 331–339.
- *The Economist (2013, March 16). *Can you keep a secret?*
- *Thomä, J., & Bizer, K. (2013). To protect or not to protect? Modes of appropriability in the small enterprise sector. *Research Policy*, 42(1), 35–49.
- *Von Hippel, E. (1988). *The sources of innovation*. New York: Oxford University Press.
- *Zaby, A.K. (2010). Losing the lead: The patenting decision in the light of the disclosure requirement. *Economics of Innovation and New Technology*, 19(2), 147–164.
- *Zhao, M. (2006). Conducting R&D in countries with weak intellectual property rights protection. *Management Science*, 52(8), 1185–1199.