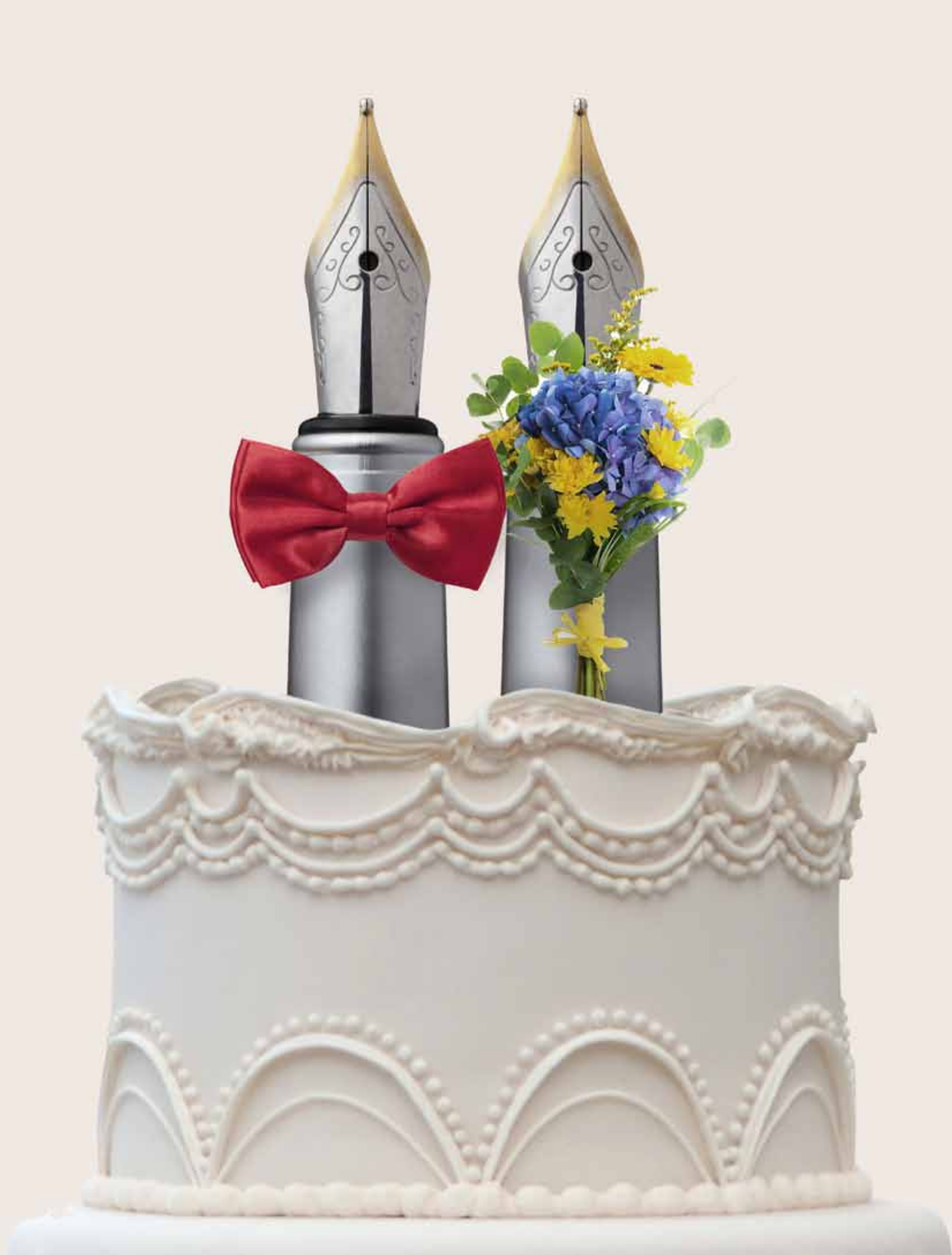

Employment Agreements:

DRAFTING THE NEW PRENUP

By Kevin Cranman, John F. Baum and Jason D'Cruz

There are two times in the employer–employee relationship when the employer is in a stronger and more advantageous position to outline obligations and duties with its employees: at the start (often called "on-boarding") and at the end (often called "off-boarding") of the employment relationship. These are the two junctures to get it right regarding issues the employer wants to address with employees — and usually when the employee has some incentive to agree (e.g., wanting to start new job; wanting to arrange departure, including, perhaps, separation-related benefits). At the start of any relationship between parties, it is important to have clear agreement as to who does what, what is the this-for-that, who owns what, etc. Indeed, this is a best practices approach we would recommend for all clients in all endeavors (and what our litigation colleagues would say, after problems arise, they wish we had done better at the outset); employee engagement is no different. The importance of confidential information and intellectual property (IP) has grown dramatically, and the capture and maintenance of information, IP and related assets is even more relevant today.

30-SECOND SUMMARY

When an employee first comes on board at a new company, that individual must review numerous documents, policies and forms. In addition to covering a variety of topics, such as initial title, compensation, location and manager, these documents should also focus on issues regarding confidential information, trade secrets, IP and related issues. The employer should define what its data/information is and inform the new employee what constitutes employer property. Before a separating employee leaves the organization, it is important to remind the employee that there is an ongoing obligation to protect the employer's IP and confidential information through the non-disclosure agreement or comparable document that the employee signed during the on-boarding process.

On-boarding basics

A successful on-boarding process often requires coordination among HR, legal and IT, and possibly sales, operations or other home departments. Because the modern work world is drastically different from days gone by, employers are smart to think of the on-boarding process as a way to secure a "pre-nuptial" agreement with a new hire, and explain that the "prenup" will be amended as technology advances (and/or, perhaps, as other workplace aspects change). Of course, one of the ongoing challenges for the legal department will be to determine which law(s) will govern the various advances in technology.

Listed below is an on-boarding checklist of and guidance regarding documents, agreements and policies employers should consider giving their prospective employees.

1. Offer letter

- Do not create a contract for a term of employment; instead, include at-will language.
- Maintain flexibility by using "initial" when describing pay, title, manager, duties, etc.
- Describe prospective employee's status under the Fair Labor Standards Act (FLSA): exempt or non-exempt.
- Summarize benefits but note that plan documents govern.
- Confirm prospective employee is not bound by any agreement prohibiting prospect from performing duties, and if necessary, request confirmation from outside counsel after reviewing any previously signed commitments.
- Tell prospective employee not to bring third-party information.
- Require prospective employee to complete a I-9 form (confirm whether your company is required to e-verify; if not, decide whether to e-verify anyway; see *www.uscis.gov/e-verify*), and sign pre-employment screening authorizations and Employment Covenant Agreement.

2. Pre-employment screening authorizations

- criminal background check authorization form
- drug testing authorization form
- Fair Credit Reporting Act disclosure and summary of rights
- applicable state and federal laws.

3. Employment covenants/ new employee agreement

- Include:
  - intellectual property assignment clause,
  - return of company property,
  - non-competition (if allowed under state law),
  - non-disclosure of confidential information/trade secrets,
  - non-solicitation of customers, and
  - non-recruitment of employees.
- Check state laws regarding enforceability of each clause.
- Some companies prefer to have a more general document covering the protection, non-use and nondisclosure of confidential information as the way to manage employee behavior, and to rely generally on trade secrets laws, instead of specifically focusing on issues like non-compete.

4. Employee acknowledgement, receipt and consent

- setoff agreement if property is not returned or amounts owed to employer are not paid upon termination (rules will differ by state)
- setoff agreement for employer to withhold or recapture monies while employee is employed (e.g., improper overpayment or other obligation)
- receipt of employer property:
  - detailed list of property/serial numbers
  - acknowledgment of what is expected upon termination
- receipt of employer information;
- consent permitting employer to monitor any device with employer information
- notices/employee confirmation regarding the scope or limit (or non-existence) of an expectation of privacy, if any, of communications through employer systems (e.g., email, phone/voice message, personal email accounts accessed, voice or text messages via employer account)

Kevin Cranman is general counsel for Ericsson Television's Americas Region. He handles commercial transactions for sales, R&D and supply chain; IP development and protection; HR and employment issues; litigation and dispute management; and whatever else darkens the doorway. *kevin.cranman@ericsson.com*

John F. Baum is a partner with Hirschfeld Kraemer LLP in San Francisco. He represents employers in all aspects of employment law, including litigation, counseling and advice, training and investigations. *jbaum@hkemploymentlaw.com*

Jason D'Cruz is a partner with Morris, Manning & Martin, LLP, in the firm's Atlanta office. He practices in the areas of executive compensation, employment law and restrictive covenants litigation. D'Cruz is also a Fellow, College of Labor and Employment Lawyers. *rjd@mmmlaw.com*[1]

The authors thank the following (in alphabetical order) for their comments on drafts of this article: Dan Fellner, Rani Garcia, Greg Gaugler, Tara Hittelman and M. Yusuf M. Mohamed.

Client Choice USA & Canada 2013

The leading lawyers
and law firms for client service

Winners Announced

To view the full list of winners, please visit
www.clientchoiceawards.com

In association with LEXOLOGY® | International Law Office®

5. Employee handbook/ employer policies

- acknowledgment of receipt of handbook/policies
- Include:
  - data security policy;
  - technology usage policy;
  - employer property/resources policy;
  - social media policy;
  - anti-harassment policy;
  - anti-discrimination policy; and
  - driving policy (prohibit use of devices while driving or limit use to hands-free in accordance with state law).

The mechanics of the on-boarding process have changed dramatically. No longer is it a stop in the personnel office for new hires to receive standard employer-issued property: uniforms, keys and tools. Now, the human resources representative and the information technology representative meet, whether in person or virtually, with new hires to review the numerous documents, policies and forms required before employment commences, and before sophisticated and expensive electronic equipment is issued. Much of this information may now be reviewed online and acknowledgments are sent electronically. It is also common for employers to refer new hires and employees to policies (often in online or other repositories), and require that they read and remain current on them. While offer letters should set out a variety of topics, such as initial title, compensation, location and manager, they should also focus on issues regarding confidential information, trade secrets, IP and related issues. The offer letter and other on-boarding materials should direct new hires not to bring the property of others, especially trade secrets and confidential information, to the work environment. Prudent employers should have new hires, if appropriate based on duties, sign agreements that assign work product, inventions and related IP to the employer, while also imposing restrictions on employees, such as non-competes, non-disclosures of confidential information, non-solicitation of customers and/or non-recruitment of employees. Different states have different rules regarding the scope and enforceability of IP assignment and related restrictions. For example, California generally prohibits non-competes. (See Cal. Bus. & Prof. Code §16600 et seq.) However, some states will allow a court to "blue pencil" or judicially reform an overly broad covenant. For example, Georgia allows blue penciling as of May 11, 2011. (See O.C.G.A. § 13-8-53(d).) Because of state-specific enforceability issues, a best practice is to use the state in which the employee lives and works for governing law and forum selection clauses.

To protect its property, an employer needs to deploy, maintain, review and update its forms, agreements, policies and procedures in four main areas: data/information, property, usage and work environment.

Companies now strive to provide the proper technology and tools for successful communication and collaboration among employees. Employees are now potentially connected 24/7 from anywhere in the world. But by allowing such unprecedented access, companies also make it easier for their property to be compromised, whether inadvertently (e.g., poorly managed or simply left accessible to others), by improper actions of third parties (e.g., theft, hacking or espionage), and/or by improper use by employees. During the on-boarding process and regularly thereafter (e.g., when employees access databases, are granted broader or higher level access, and annually) companies now set expectations on the use of technology — receipt, return, access, monitoring and security of the property. In addition, at the commencement of employment and periodically thereafter, companies should notify employees (often in policies, such as a "use of employer resources" policy) and, if needed by the jurisdiction, secure appropriate employee consent for access, use, monitoring and recapture of its information.

To protect its property, an employer needs to deploy, maintain, review and update its forms, agreements, policies and procedures in four main areas: data/information, property, usage and work environment.

Data/information

Defining what constitutes employer data has become far more difficult. Once limited to the 1s and 0s on the employer's mainframe computers or hard-copy files in cabinets and drawers, today's "data" is housed everywhere (and nowhere — i.e., the cloud) and is not limited to the 1s and 0s of yesterday. Information that companies should protect can be found in employer emails, text messages, instant messages, social media accounts (such as Facebook, Twitter and LinkedIn), databases (such as customer relationship management or sales), computer code (code is not limited to software companies anymore; many companies have proprietary software), lists, marketing materials, reports, forms, templates, etc. It is imperative that companies broadly define what constitutes data or information. More important, companies need to educate new employees about what they deem to be employer information. Employment Covenant Agreements and acknowledgments should define

what information the employee may access, who owns that information (presumably, mostly the employer) and what should happen to that information when the employment relationship ends. While some companies may require employees to certify on a regular basis what data/information has been provided to them, such an approach may also be too cumbersome to manage. Finally, at the onset of employment, companies need to address with new hires expectations regarding security concerns, privacy expectations (if any; these may differ by state or country), passwords, encryption and what level of access the employee may have to employer information.

Equally important is to instruct the new employee in the on-boarding process what information the employer does not want the employee to bring into the work environment. With today's mobile workforce, the number of lawsuits filed when an employee moves from one employer to another has increased exponentially (from Mark Hurd leaving Hewlett-Packard for Oracle, to lower level "pre-sales" representatives going to competitors). At the heart of most of these lawsuits is whether the individual took information from the last employer. If information has been downloaded from a prior employer and provided to the new employer, a judge may allow a forensic expert to determine what information was downloaded and what has been done with that information since — a lengthy and expensive process for the new employer.

Companies need to be vigilant in the on-boarding process to tell the new employee what is, and what is not, permissible. For example, companies should forbid new employees from bringing any other employer's data/information (defined as broadly as the employer defines its data/information) with them to their new position. This means individuals should not upload any information onto the employer's database, computer devices (including handheld devices), storage devices, email accounts, etc.

Many times, new employees assume ownership of their contact database (Outlook or similar) from their last employer. The new employer should be careful not to allow automatically the "Outlook Download," because that database may actually belong to the previous employer. Likewise, new employees should be directed not to use information, forms, templates, forecasts or reports from any other employer when preparing deliverables for their new employer. Vigilance in this area will serve the new employer well if there is a dispute with the former employer.

Property

After the employer has defined what its data/information is, it must also inform the new employee what else constitutes employer property. Employer-issued property, like traditional office equipment and supplies, is generally recognized to be owned by the employer. More confusing, however, is ownership of handheld devices, tablets, laptops, home desktops, fax machines, printers and storage devices (especially if the employer allows the employee to use their own devices for employer business). For all of these devices (whether employer-issued or personal), it should be clear at the onset of employment who owns the devices and the data/information sent to or stored on those devices. Detailed records should be kept of serial numbers, makes and models of each device so that the employer can recover its property upon termination. Acknowledgment forms should be signed setting forth how these devices are to be returned and the consequences of not doing so (e.g., setting off the value of the device against amounts owed to the employee if allowed under applicable state law; note that many states, such as Connecticut, New York, and Texas, require a specific written agreement signed by the employee authorizing any such set-off).

It is imperative that companies broadly define what constitutes data or information. More important, companies need to educate new employees about what they deem to be employer information.

More difficult in the "property" genre are things like telephone numbers, email addresses, websites and LinkedIn or Facebook accounts (if the employee is allowed to use these for employer business). Although the law is developing in these areas, employer policies and agreements should set out clearly who owns this property, and what the procedure will be to provide passwords and access to such property upon termination of employment.

Usage

Back in the good old days, employers were concerned about how much time employees were spending on the employer telephone. Detailed policies were devised to set appropriate limits (emergency use only, lunch breaks, etc.) and what discipline was appropriate for infractions. Then came the internet. If the employee was even given internet access, similar policies were implemented. Today's workplace is light years ahead of then.

Although many of today's technological advances enable employees to communicate and collaborate on work issues more effectively, these same advances also are susceptible to employee abuse. Thus, the new employer must set forth which tools employees are allowed to use, which tools they are not allowed to use and appropriate limits on personal usage. In addition,

Because of the global economy, employees are communicating regularly with coworkers, vendors and customers in other states and countries. Privacy laws must be reviewed with employees who are working across state and country lines to ensure compliance with applicable laws.

companies should secure the employee's consent for monitoring devices and content. If appropriate, companies should also seek permission to install software on an employee's device to monitor for compliance and security measures (wiping data) if the device is lost or employment ends.

Equally important is educating employees on the proper use of employer property. If appropriate, companies should prohibit employees from copying, sending to personal accounts or downloading to personal storage devices any employer information/data. Companies should list the types of approved devices on which employees are allowed to view and work on employer information. Companies should also state what security measure must be in place prior to such usage. Finally, companies should define the procedures to follow if a device is misplaced, stolen or replaced.

A growing concern in this area is where the device or information is used, sent or accessed. Because of the global economy, employees are communicating regularly with coworkers, vendors and customers in other states and countries. Privacy laws must be reviewed with employees who are working across state and country lines to ensure compliance with applicable laws. Most US states have enacted data breach notification laws in some form. Many of these laws are identity-theft protection measures that generally impose an obligation to protect Social Security numbers and similar personal data against unauthorized use or disclosure, and require secure destruction of such data. The laws of each state may vary, sometimes significantly. For example, since March 1, 2010, Massachusetts requires most companies to adopt a written security policy that meets certain standards to protect a broad range of personal data collected from customers and employees who reside in the state. A compliant plan requires not only security measures, such as encryption of personal data stored on portable devices, but also training and oversight of vendors who have access to the data. In addition, US federal statutes protect specific types of personal information. The most important of these for employers are:

1. Health Insurance Portability and Accountability Act (HIPAA), covering certain health-related information (although employers that do not provide health services are not generally covered by the HIPAA rules, they may nevertheless be subject to the Act's restrictions in their capacity as administrators of a health plan).
2. Genetic Information Nondiscrimination Act (GINA), which applies specifically to genetic information.
3. Americans with Disabilities Act (ADA), which applies to information about an employee's disability.
4. Fair and Accurate Credit Transactions Act (FACTA), designed to protect consumer credit information.

Work environment

Because of technological advances, work can now occur 24 hours a day, seven days a week and in many different time zones. With the ability to access the employer's systems remotely, work occurs in trains, planes, automobiles and everywhere else imaginable (or at least where there is cell coverage or internet access). Work also occurs during "normal business hours," before and after hours, on the weekends, on vacation and on leave. Employees toggle back and forth between work and personal matters using devices, email accounts and social media sites. As a result, employers need to review exempt and non-exempt classifications under state and federal wage and hour laws to ensure that non-exempt employees understand the parameters of permitted work (e.g., companies should make clear whether overtime work is permitted and under what circumstances [e.g., prior, written approval]) and the necessity for keeping accurate time records so employees can be compensated for hours worked. In addition, companies need to review their security and encryption procedures to make sure their employer information is secure on approved devices anywhere in the world.

After doing good preparation on the front end to address information protection, behavior management and IP assignment, there are steps employers can take when employees depart, whether voluntarily or involuntarily, to continue this important asset protection and management.

Off-boarding in the digital age

An employer in the digital age must now consider issues that were not considered years ago in regard to off-boarding employees. Those issues center on the protection of IP and confidential information of the employer and the myriad ways that information can be compromised. Given the rapid advancement of technology, the protection against the improper migration of such information should be an important consideration in every separation.

The basics of the transition

The nuts and bolts of the separation

CALIFORNIA EMPLOYMENT LAW FOR BUSINESS

SAN FRANCISCO
LOS ANGELES

proven strategic collaborative cost effective trial ready

Miller
LAW GROUP

Our practice is focused exclusively on employment law and related litigation, representing start-ups to Fortune 500 companies doing business in California.

WWW.MILLERLAWGROUP.COM
415.464.4300

Certified WBENC Women's Business Enterprise

LAW 2013 GO-TO TOP 500 FIRM

Certification for continuing duty of confidentiality

I understand that I have a continuing obligation not to disclose, use or retain the confidential and proprietary information and trade secrets of the employer. This obligation, fully set forth in the attached confidentiality and non-disclosure agreement that I signed at the beginning of my employment with the employer, remains in effect and survives the end of my employment with the employer. I agree to abide by its terms.

_____

Date

_____

Employee's Signature

_____

Employee's Name Printed/Typed

Letter to a new employer

Dear _____:

We understand that our former employee, [employee name], has accepted employment with [new company name]. This letter is to advise you that [employee name] signed a confidentiality and non-disclosure agreement ("agreement") with [company name], which remains in full force and effect. At the time of the employee's departure from our company, we advised her of her continuing obligations under the agreement.

Employee's obligations under the agreement include maintaining the confidentiality of the confidential and proprietary information and trade secrets of [company name] (collectively "company confidential information") in her work for any subsequent employer. Collectively, this company confidential information may include, but is not limited to, documents, reports, manuals, notes, presentations, PowerPoint slides, client or financial information that she created, worked on or used while at [company name]. Under no circumstances should you now or in the future ask or allow employee to disclose, rely upon, refer to or otherwise use company confidential information or other property of [company name] during her employment with you.

[Company name] is not accusing you or [employee name] of any wrongdoing. We merely wish to inform you of [employee name]'s continuing obligations to [company name] so that any conflict with those obligations can be avoided during her employment with you. As you can imagine, the protection of [company name]'s property is very important to us. We expect that you will take appropriate steps to ensure that [employee name] is directed not to use any company confidential information, or other [company name] property that she retained from her employment at [company name].

We have no interest in interfering with [employee name]'s right to pursue her business interests or in [new company name]'s ability to lawfully operate in the marketplace. However, [company name] will take the appropriate steps to protect its rights, if necessary.

If you have any questions about this matter, please contact me.

Best practices suggest that an exit interview is scheduled and is held separately from the administrative meeting regarding termination paperwork. They are two different tasks with very different objectives.

remain unchanged from years ago. The employer should explain the terms of the final pay and the last day of benefits coverage, preferably in a face-to-face meeting. Some jurisdictions require final checks to be available and accrued, unused vacation or paid time off to be provided on the last day of employment (see, e.g., California Labor Code Sections 201, 227.3).

The physical property of the employer should be collected. Keys, access cards, credit cards, cell phones and laptops should be recovered. The employer may need to arrange for the recovery of physical property that is not in the employee's possession and may be in the employee's vehicle or home.

At times, it becomes critically important to ensure there is an appropriate knowledge transfer. The location of project information, client or customer data, and work in progress must be transferred to the organization. Often, the information has been stored electronically, and the knowledge transfer must be very specific as to the location of electronic files and the manner of access, especially if the information has been password-protected or encrypted.

Many employers believe that an exit interview is an opportunity to obtain honest information about the organization. The departing employee who resigns is no longer bound by considerations of power or limited by the fear of retaliation. Best practices suggest that an exit interview is scheduled and is held separately from the administrative meeting regarding termination paperwork. They are two different tasks with very different objectives. The tone of the exit interview is to attempt to establish an environment such that a departing employee feels comfortable explaining the advantages and disadvantages of the workplace so that the employer identifies issues that can be addressed. For many organizations, the individual with the employee relations expertise and sensitivity may be very different than someone who is ensuring that the administrative side of the transaction is discussed (i.e., explaining the employer's benefits, stock plan and 401(k) program). Many larger organizations provide a written survey to gather the information.

Protecting your intellectual property and confidential information

Before the separating employee leaves the organization, it is important to remind the employee of the obligations

Certification for return of all company property

This is to certify that I have returned all property of the company. This includes all physical property, including but not limited to keys, access cards, credit cards, phones, tablets, laptops, computers, computer disks or storage devices. This obligation also includes the return of all originals and copies of documents, records, data, information, notes, notebooks, reports, memoranda, manuals and presentations obtained by me or accessed by me during the course of my employment with the company. It also includes the property and information of a customer or client obtained during the course of the company's business. This is collectively referred to as "company information."

I understand that this obligation extends to company information and property that has been stored on my home computer, any personally owned storage device used by me (including storage in the cloud), my phone, tablet or laptop. I have followed the instructions of the company's information technology department and have returned all hard copies and electronic copies. I have permanently deleted such company information from any personally owned, held or able to be accessed storage device. I understand that I must not retain, disclose or use any such company information.

Date

Employee's Signature

Employee's Name Printed/Typed

to the employer that survive the termination. The employee should be told that there is an ongoing obligation to protect the employer's IP and confidential information through the non-disclosure agreement (NDA) or comparable document that the employee signed during the on-boarding process. Further, depending on the jurisdiction, there can be ongoing obligations pursuant to restrictive covenants, most particularly non-compete and non-solicitation (generally regarding employees and/or customers) agreements.

In addition to orally explaining these ongoing obligations, it would be a best practice to provide the employee a document that explicitly states these obligations. (See sidebar, "Certification for continuing duty of confidentiality.") The employee should be required to sign an acknowledgement of the document and be given a copy of the original NDA and restrictive covenant they signed.

Some employers take the further step and send a letter to the departing employee's new employer and state the ongoing obligations even after the employee has left, especially where there are no restrictive covenants applicable that would prohibit the departing employee from working for a competitor. The letter should explicitly state that the prior employer is not interested in interfering with the employee's ability to work in the marketplace, but the new employer should understand that the new employee has continuing obligations. (See sidebar, "Letter to a new employer.")

In addition to this discussion of the continuing obligations, the employer might also conduct a mini-investigation into the spread of IP and/or confidential information to sources outside the control of the employer. The employee should be asked the following questions and the employer should be prepared to follow the trail until all originals and copies (electronic and hard) have been recovered:

The employee should be told that there is an ongoing obligation to protect the employer's IP and confidential information through the non-disclosure agreement (NDA) or comparable document that the employee signed during the on-boarding process.

- Have you sent emails with employer IP and/or confidential information to your home computer, laptop, tablet, phone or other storage device?
- Have you provided or forwarded employer IP and/or confidential information to anyone outside of the employer?
- Have you worked on such information at home on any of these devices?
- Have you stored any such information in the cloud through any of these devices?
- Do you have copies of any such information on any storage device, such as a server, workstation, laptop, tablet, backup drive, thumb drive or disk?

If the employee has such originals or copies in existence, then the employer must decide how to arrange the recovery of that information (if the employer does not have complete copies) and/or how to destroy any extraneous copies for which the employer has an original or a copy of the organization's work product. At a minimum, the employee should be required to affirm in writing that no original or copy has been retained. (See sidebar, "Certification for return of all company property.")

On the last day of employment, the separating employee must be cut off from access to the employer's information technology system, voicemail and the physical property. Procedures should be put in place with the appropriate personnel that control such access to ensure that it is terminated immediately when the word is given. As always, the employer should consider any behavior or safety risks and plan appropriately (e.g., security).

New issues in the digital age

Bring your own device

If the explosion of technology does not present enough of a challenge, the management and recovery of an employer's IP and confidential information becomes increasingly complex in the age of "bring your own device" (BYOD). Many employers, especially in the high technology world, are finding that employees want to use their own smartphones, tablets, memory or other devices in the workplace. The employee comes into the workplace with an Android phone or iPhone and wants to have it synced to the organization's system to facilitate work being accomplished in a seamless fashion. Employers agree (or, sometimes, don't affirmatively object) to such an arrangement because they believe that the employee will be happier and more productive using her own device.

The challenge arises from the fact that the employee's work and personal information are intertwined on a single device. It is unavoidable that the employee will be retaining the device after employment with the enterprise ends. Consequently, the employer must take extra, more cumbersome steps to ensure the employer's IP and/or confidential information is not retained after employment ends.

It then becomes critical that the employer uses mobile device management software (MDMS) to allow more control over the employer's information on this personal device. The MDMS allows the employer to protect the IP and/or confidential information, control access to the employer's systems, and recover information when necessary.

These additional steps increase the burden on the employer's information technology department. The IT department must now be a more active manager of the BYOD hardware. That may mean broadening technical expertise among a wider array of platforms and providing helpdesk support among a correspondingly greater number of types of devices.

For those employers who adopt a BYOD environment, it is critical to have IT support at the beginning of the process, when the employee is coming

ACC EXTRAS ON…
Employment & HR practices

ACC Docket
The Nuts and Bolts of Employment Agreements for Foreign Employees Working Outside the United States (June 2012). *www.acc.com/docket/empl-agree-outUS_jun12*

Forms & Policies
Employment Agreement — Executive (May 2012). *www.acc.com/form/empl-agree_may12*

Employment Agreement — Sales Executive (May 2012). *www.acc.com/forms/empl-sales_may12*

Sample Interview Exit Form (May 2012). *www.acc.com/forms/exit-interview_may12*

Article
Nonprofit Executive Employment Contracts: Don't Overlook These Key Issues (Nov. 2009). *www.acc.com/nonprof-contracts_nov09*

Education
Review the basics of employment law by attending ACC's Corporate Counsel University®, May 19–21 in New Orleans. Designed specifically for lawyers new to in-house, this program includes sessions on employment law, contracts and compliance. Learn more about CCU and register to attend at *http://ccu.acc.com*

ACC HAS MORE MATERIAL ON THIS SUBJECT ON OUR WEBSITE. VISIT *WWW.ACC.COM*, WHERE YOU CAN BROWSE OUR RESOURCES BY PRACTICE AREA OR SEARCH BY KEYWORD.

The IT department must now be a more active manager of the BYOD hardware. That may mean broadening technical expertise among a wider array of platforms and providing helpdesk support among a correspondingly greater number of types of devices.

into the organization. That is when the MDMS must be installed on the employee's device and the parameters of use must be explained to the employee. A proper set-up will allow the employer to better protect its IP throughout the employee's tenure and especially at the point of separation.

Social media

Social media is the (newest) great frontier of communication, and employers are struggling with many aspects of its impact on the workplace. The control of and/or reaction to information posted on the internet is being addressed by employers through social media policies. State legislatures have reacted swiftly and decisively by passing laws that prohibit an employer from requiring the release of a password to find what an employee has posted on a social media site such as Facebook (e.g., Maryland Labor and Employment Law Section 3-712; 820 Illinois Compiled Statutes 55/10; California Labor Code Sections 980-982).

When an employee leaves a place of employment, there can be social media issues (e.g., who owns some, or all, of a social media profile, interactions and contacts). The employer has a strong argument that certain social media information was developed during employment for the purpose of advancing the work of the organization is the employer's property, arguing "it is just a sophisticated contact list of customers and prospects." The employee, in marked contrast, argues that the information is a combination of personal and professional contacts, is not confidential because it is often publicly available and is not the employer's property.

The courts are beginning to deal with this issue of ownership of social media content, and, as expected, the decision will rest on specific factual circumstances of the situation. In *Eagle v. Morgan* (E.D. Pa), the court is wrestling with a dispute over the ownership of the information in the LinkedIn account after Linda Eagle left the company. In that case, Eagle, the former CEO of EdComm, Inc., sued her former employer over the ownership of her LinkedIn account, which she started at the request of the company. In a case still being litigated, the court will be called to assess the unusual fact that the company controlled the content of the LinkedIn site while Eagle was employed, and had a claim to the content (as its property) after she left. In a second lawsuit, an employee who initiated a Twitter account at the direction of the employer for marketing purposes — developing over 17,000 followers — is being sued for ownership of the account by the employer in *PhoneDog v. Kravitz* (N.D. Cal.).

A best practices approach to avoid such a dispute and the operational and financial cost of a lawsuit would be to explicitly define the scope of the ownership of the social media property, including business contacts, blog content and other information posted on a social media site. A lawful social media policy clearly articulating that the use of social media sites for business purposes is allowed, and that the contact information and content developed, and other related client or customer information, is the property of the employer, will help to resolve any disputes in the future. Employers should be reviewing their social media policies to ensure language governing relevant issues and ownership is included.

What happens if an employee breaches her obligations?

Consistent with the "an ounce of prevention" adage, if employers establish good agreements and policies, they will be better able to mitigate risk. For example, having agreements and education in place should minimize bad acting (and, hopefully, inadvertent

When an employee leaves a place of employment, there can be social media issues (e.g., who owns some, or all, of a social media profile, interactions and contacts).

errors) by employees and former employees. If a former employee breaches (or threatens to breach) an ongoing obligation, employers have a variety of options, including: sending a cease-and-desist letter to the employee and/or her current employer; filing suit seeking an injunction or other enforcement of the obligations; and engaging her new employer to ensure compliance. Employers can rely upon their written agreements and policies, and statutory (e.g., trade secrets laws) and other common law protection (e.g., inevitable disclosure doctrine, where recognized) to seek compliance, minimize risk and seek remedies. Remember that many of the restrictions (especially regarding non-compete language) and related remedies (e.g., inevitable disclosure) vary significantly by governing law and jurisdiction, so, as always, be mindful of these issues in drafting and enforcement actions.

Not surprisingly, good planning will help our companies and clients manage employee behavior, especially regarding the capture and protection of confidential information and intellectual property. Setting forth expectations and agreements before employment starts keeps the relationship clean. Having a process to manage relevant issues also will help clarify what is expected and, if problems arise, how to remedy them. With agreements in place at the start of the employment relationship that identify ongoing, post-termination obligations — and with an exit interview or reminder process — we can better manage our valuable resources: human resources, property, financial, intellectual property and otherwise. **ACC**

NOTES

1 Mr. D'Cruz wishes to thank Tali Hershkovitz, a third-year law student at Duke University, for her contributions to this article. Ms. Herskhkovitz will be joining the offices of Morris, Manning & Martin, LLP in the summer of 2013.