Boston Bar Journal
A Peer Reviewed Publication of the Boston Bar Association
FALL 2015 | Volume 59, Number 4

Special Privacy Edition

Foreword from the Editors

In our digital age, technology has brought attention to "privacy" in unprecedented ways. And privacy, although a term frequently used, has no set meaning. Ready electronic access to information, for instance, raises questions about the misuse of public records (and, more broadly, whether one can or should ever be forgotten), while lack of access raises concerns about government abuse going unobserved. Near-daily stories of data breaches now have a connection to matters that are surprisingly close to home, as the "internet of things" means that even our home appliances are collecting and sharing our goings-on. Businesses need to consider not only whether they are adequately protected against cyberattacks, but also whether they have adequate cyber insurance in place. In this special issue, we reflect on these timely and compelling questions.

– The Boston Bar Journal Board of Editors

Cyberattack Risk: Not Just For Personal Data

by Mark Szpak, Seth Harrington and Lindsey Sullivan

Practice Tips

In August, the United States Department of Justice ("DOJ") and the Securities Exchange Commission ("SEC") unsealed complaints alleging a scheme to hack into computer systems of newswire services in order to steal material nonpublic information, which the hackers then allegedly used to place trades.

This case is strikingly different than many other recently reported data-breach cases. Typically such cases have involved an attacker breaking into a company's network to access personal nonpublic information (e.g., credit card numbers, medical history, social security numbers) that potentially could be sold to other criminals who would use it to attempt to commit identity theft or fraud. This hack involved information concerning publicly traded companies, obtained not from the companies themselves, but third-party newswire services. These complaints highlight that cyberattack risk is not limited to the theft of personal information but extends to any confidential information that hackers may seek to exploit for financial gain – trade secrets, insider information, customer prospects, bid packages, marketing data, business plans, etc. Companies need to understand this risk as well as how to prevent it and manage it if it occurs.

The Alleged Hacking and "Insider" Trading Scheme

The criminal complaints filed by the DOJ allege that nine individuals hacked into the computer systems of newswire services Marketwired, PR Newswire, and Business Wire, accessed nonpublic information, and allegedly used it to generate $30 million in illegal profits. The civil complaint, brought by the SEC against 32 individuals, alleges that the defendants generated more than $100 million in illegal profits by trading on the stolen nonpublic information in violation of federal antifraud laws and related SEC rules.

These newswire services were engaged by major publicly traded companies to publish corporate releases and, as a result, received confidential information hours and even days before the information was publicly released. By infiltrating the computer systems of these newswire services, the criminals were able to access – and act upon– the releases ahead of the market.

Few are surprised that the newswire services were targeted, but the extent of the scheme is drawing attention. The hacking allegedly lasted five years, during which the criminal attackers allegedly accessed over 150,000 press releases. In one instance, according to the SEC complaint, the hackers and traders were able to act within the 36-minute period between when the press release was provided to the newswire service and public disclosure of the release, executing trades that resulted in $511,000 in profit.

Potential Exposure

Compared to other cybercases, these complaints represent the relatively rare occurrence in which claims are brought against the *perpetrators* of the data breach and the individuals who seek to use and profit from the stolen information. As this article goes to press, no litigation is known to have been initiated against either the newswire services or the companies whose information is alleged to have been stolen in this attack. Yet, based on trends in litigation and regulatory enforcement efforts in matters involving data breaches of personal information, one can expect that claims against hacked entities or their clients may begin also to arise even where only nonpersonal information is involved.

With respect to private litigation, potential claims could face a number of hurdles. Any potential plaintiff would have to allege a cognizable injury as well as the breach of a duty owed by the defendant to the particular plaintiff. Many courts in breach cases have dismissed claims (under both tort and contract theories) based on the attenuated relationship between the plaintiff and defendant regarding an alleged duty to safeguard information for the benefit of the plaintiff. As we move beyond personal information, each new digital information context will raise questions regarding whether a duty to anticipate and protect against criminal cybertheft can be fairly imposed, in what circumstances, pursuant to what standards, and, if so, to whom is it owed.

With respect to regulators, the SEC has made clear its position regarding the importance of cybersecurity. **In March 2014**, Chair Mary Jo White explained that "the SEC have been focused on cybersecurity-related issues for some time" because "[c]yber threats [] pose non-discriminating risks across our economy to all of our critical infrastructures, our financial markets, banks, intellectual

property, and, as recent events have emphasized, the private data of the American consumer." Other regulators (most notably the FTC) have also staked out a position of overlapping jurisdiction.

Best Practices for Companies

In a world where the electronic landscape and the sophistication of cyberhackers are both moving at high speed, here are nonetheless a few best practices that companies facing an actual or potential data security incident (i.e., all companies) can follow to mitigate potential risk:

- *Think carefully about third-party vendors*— Companies rely on numerous third parties for everything from corporate disclosures to marketing advice. Thoughtful contracting and training can go a long way to reducing the risk of loss or misuse.
- *Supplement perimeter detection systems*— According to the indictments in the newswire case, the criminal hackers were resident in the victims' systems for years. The case illustrates the potential significance of taking a "defense-in-depth" approach to security and system monitoring.
- *Be realistic about law enforcement and regulators*— Notifying and cooperating with law enforcement can be important for many reasons, and the same is true for governmental regulators. But law enforcement usually focuses on getting the criminal attacker, while regulators (by comparison) often focus instead on examining any role the company had in having been criminally attacked. Keeping that difference in mind can be significant in dealing simultaneously with these respective governmental actors.
- *Involve outside experts (both legal and forensic) at the earliest sign of a possible problem*— Never guess or assume what may have taken place. Forensic experts can help your team assess whether an attack or breach has occurred, the actual scope of the breach, and how to contain it, while legal experts (both internal and outside counsel) can direct that forensic review and assess potential legal obligations involving notification, public statements, remediation, responding to law enforcement, dealing with regulators, preparing for litigation, and protecting the record.
- *Carefully draft external statements*— When an incident occurs, all outward facing statements should be carefully crafted to say only what is necessary, and to avoid committing to specifics until facts are definitely known. Before an incident occurs, promising any level of protection is risky because, if a hacker makes it into the system, the company's statements will inevitably be second-guessed.
- *Check your insurance*— For the sake of planning, assume that erstwhile attackers will be able to access any system in your network. Consider, then, what kind of attack or what kind of data loss could cause the most exposure or disruption. Then make sure your insurance will actually cover those costs and that any related exposure to liability is indeed included. Evaluate your incident response preparedness through "tabletop exercises" to confirm that you have identified the potential risks and expenses.
- *Avoid creating a bad record*— Preservation of evidence after discovering a data breach often involves much more than just the usual email and paper files. In a network attack, the relevant

evidence may include large groups of servers, firewall configuration records, network access logs, security management databases, vulnerability scan results, software hotfix schedules, or any number of other forensic or technical data sources that in most litigation rarely come into play. Identifying that relevant forensic and technical evidence and then maintaining it, while preserving applicable privileges and minimizing the interruption of critical ongoing company operations, can in many cases pose enormous challenges.

The panoply of costs that a cyberhack can impose make it clear that a well-developed program to secure all types of business information, not just personal information, can provide a competitive advantage. And when data thieves strike, regardless of the type of data they target, following a prompt and careful response protocol can pay significant legal dividends.

Mark Szpak is a partner in Ropes & Gray's privacy & data security practice. He focuses on the wide range of challenges that arise after a computer network intrusion, including defending against multidistrict class actions in the U.S. and Canada, handling forensic investigations and responding to regulators.

Seth Harrington, also a partner in Ropes & Gray's privacy & data security practice, represents clients in all aspects of the response to a privacy or data security incident, and he regularly advises clients on indemnification and insurance matters, including cyber risk insurance.

Lindsey Sullivan is an associate in Ropes & Gray's business & securities litigation practice, where she focuses on assisting clients through forensic investigations and preservation efforts around privacy and data security breaches.

Cyber/Privacy Insurance: A Very Brief Primer

by Alan M. Reisch

Practice Tips

"If you don't know where you are going, you might wind up someplace else."
— Attributed to Yogi Berra

Massachusetts has one of the country's most stringent statutory and regulatory schemes relating to data privacy and security. The complexity and scope of available insurance products dealing with "cyber" exposures, in Massachusetts and throughout the business world, has dramatically increased over the past several years and is now as fractured and complicated as is the law, which differs from state to state and from country to country. Insurance underwriters, insurance brokers, technologists, security professionals, pundits and others offer conflicting advice about how to best move through this maze of insurance policies, technology, and the many potentially applicable state and federal regulations that often conflict. Imagine that there is growing apprehension that a company is at risk. At some point, a lawyer is called to advise on insurance protection. What is that lawyer to do?

The first step is to establish a team of professionals and client representatives who will, together, work through the issues that will allow the development of a meaningful strategy. The team should include the lawyer, an insurance professional, a technology resource (internal to the client's business operations or external), and a representative of the client who is sufficiently vested with authority so that access to required information will be facilitated. Once the team is in place, the following should happen, in more or less this sequence:

1. The team should develop a realistic understanding of the client's cyber/privacy and data risk profile. It is important to analyze not just electronic exposures, but traditional paper-based exposures as well. Among the many factors to consider are the following:

> A. **The type and location of protected information that is procured, handled, managed and stored by the client.** Protected information includes, but is not limited to, private personal information (which is defined differently in various jurisdictions and under different regulatory schemes but often consists of an individual's first name, last name, and either a social security number, bank account number or other similar data point), and confidential business information.
>
> B. **The federal, state, and local statutory and regulatory schemes that impact the client's obligations with respect to protected information.** Most states have adopted data privacy regimes that are grounded in statutes (in Massachusetts the applicable statute is Mass. Gen. Laws ch. 93H) and implemented through a series of regulations. Several federal agencies, including the

FTC and the SEC, are focused in meaningful ways on the security of personal and other confidential information that is handled by businesses. Courts are, in most instances, finding statutory and regulatory support for robust enforcement actions by these agencies. It is important to keep in mind that many states, Massachusetts among them, have taken the position that their privacy schemes are meant to be protective of their citizens wherever those citizens conduct commerce.

C. **The commercial obligations that have been assumed by the client by contract or otherwise in connection with data security and privacy.** These should be charted, and compliance measured.

D. **The security of non-electronic records that contain protected information.**

E. **The client's network and electronic information storage infrastructure. As with non-electronic records, this infrastructure should be assessed** by qualified professionals, and a plan should be established for correction of deficiencies.

2. Next, insurance coverage that is already in place should be reviewed. Among the policies to be reviewed are:

A. General Liability policies

B. Directors and Officers Liability policies

C. Errors and Omissions policies

D. Fiduciary policies

E. Crime policies

F. Professional Liability policies

G. Commercial Property policies

The risk profile that has been developed should be reviewed in the context of the insurance coverage that is present in these policies (there are no true "standard forms" and careful, term-specific analysis is required). The insurance professional who is part of the team should assist in identifying potential exposures that are not within the scope of the existing coverage.

3. Having established a risk profile, assessed the protection afforded by the insurance coverage in place and begun the process of correcting deficiencies, the team should next consider whether existing coverage should be supplemented, including whether stand-alone cyber/privacy coverage should be procured. **The policy wordings that might be employed to supplement existing policies, and the policy forms that**

are available as stand-alone products, are not standard forms of insurance. Nearly all wordings can and should be specially negotiated.

As the stand-alone cyber/privacy insurance market has evolved, these general coverage types have become "standard" in most offerings (with the caveat that while the coverage "type" may be standard, the implementation varies from insurer to insurer, and from product to product, in meaningful ways):

A. **Third party coverage against claims asserting a "data privacy wrongful act," a "network security wrongful act," or other similar coverage grant.** This coverage affords the cyber/privacy equivalent of general liability coverage. A client purchases this coverage to protect against third party claims alleging damages due to the client's handling of protected information.

B. **Third party coverage for claims relating to violation of intellectual property rights or copyright.**

C. **Various types of first party coverages** (coverage that will pay an insured for loss that the insured suffers itself, rather than indemnifying an insured for claims asserted by others), such as:

1. Notification and related expense coverage;

2. Coverage for regulatory fines and penalties;

3. Coverage for the expense of recreating information that is damaged, compromised or destroyed as the result of a data security incident, or other covered occurrence;

4. Coverage for the expense resulting from the inability to use a network or other asset as the result of a covered event; and

5. Coverage for fines and penalties payable as the result of a failure to maintain appropriate levels of Payment Card Industry compliance in connection with credit or payment card exposures (this is not as generally available).

There are, of course, additional issues that will arise in the course of developing an appropriate mitigation strategy and insurance structure. For example, it may be necessary to allow an insurer, or several insurers, to independently audit a client's infrastructure. It may be that an insurer adds exclusions to a policy that render otherwise appropriate coverage difficult to accept – for example, adding an exclusion that would allow an insurer to avoid payment obligations in the event that there is a change in network structure, levels of security protection, or the like. These types of potentially devastating exclusions, sometimes based on ambiguous terms that are difficult to either understand in an operational sense or manage, can make otherwise meaningful protection unacceptable.

So, dealing with the structure of an effective cyber/privacy insurance program requires knowing what you've got, knowing what's lacking, and filling gaps in a targeted way. Know where you're starting, understand the potential end points, and you'll get where you're going and not someplace unexpected.

Alan M. Reisch is a Director in the Litigation Group at Goulston & Storrs, as well as a Founder of the firm's risk management affiliate Fort Hill Risk Management, and counsels clients in connection with insurance coverage and portfolio analysis, risk assessment and management, fraud, data privacy and other related issues.

Public Access to Electronic Judicial Records

by Jonathan M. Albano

Legal Analysis

In February 2015, the Supreme Judicial Court authorized Massachusetts trial and appellate courts to conduct pilot projects on electronic filing and service.**[i]** The Court also issued Interim Electronic Filing Rules for the pilot projects.**[ii]** Before the Interim Rules were issued, Trial Court Chief Justice Paula Carey appointed a 24-member Trial Court Public Access to Court Records Committee to develop a uniform policy for court records in written and electronic form.**[iii]** The Committee will publish proposed rules for public comment and, after considering the public comments, present the proposed rules to the Trial Court and the Supreme Judicial Court for their consideration.

Although electronic filing and service is familiar to federal practitioners who use the PACER system, because Massachusetts state courts have far more expansive jurisdiction than the federal courts, additional study was required to determine how best to administer a state court electronic court record system. This article considers three of the many issues raised by the Commonwealth's transition from paper to electronic court records and offers the following conclusions:

1. The public has a constitutional and common law right of access to electronic court records;

2. The public has a commensurate right of access to electronically maintained alphabetical indices of criminal cases; and

3. Permitting remote access to criminal case files would not violate the Criminal Offender Record Information Act ("CORI"), **G.L. c. 6, § 167,** ***et seq***.

Public Access to Electronic Court Records

The shift to electronic court files is not likely to alter the public's well-recognized constitutional and common law rights to on-site access to court records. The Supreme Court repeatedly has held that the

First Amendment grants the public a right of access to criminal proceedings. *See Globe Newspaper Co. v. Superior Court*, **457 U.S. 596**, 600, 610-11 (1982) (striking down Massachusetts statute imposing mandatory closure of sex-offense trials during the testimony of minor victims).**[iv]** Several Circuit Courts of Appeal (including the First Circuit) have held that the public's First Amendment access rights extend to judicial documents filed in criminal cases. *See, e.g., In re Globe Newspaper Co.,* **729 F.2d 47**, 52 (1st Cir. 1984); *Globe Newspaper Co. v. Pokaski*, **868 F.2d 497**, 505 (1st Cir. 1989). The Supreme Judicial Court similarly has stated that "the public has a First Amendment right of access to court records such as the transcripts of judicial proceedings and the briefs and evidence submitted by the parties." *The Republican Co. v. Appeals Court*, **442 Mass. 218**, 223 n.8 (2004).**[v]**

The SJC also has recognized a *common law* right of access to judicial records in both criminal and civil cases. *See, e.g., Boston Herald, Inc. v. Sharpe*, **432 Mass. 593**, 604 (2000); *Republican*, 442 Mass. at 222. *Cf. Commonwealth v. Winfield*, **464 Mass. 672**, 672-73, 679 (2013) (no constitutional or common law right to court reporter's "room recording" that is not the official record of the trial, is not filed with the court, and is not referenced in the court file). Many of these principles are incorporated into the recently amended Uniform Rules on Impoundment Procedure, which now apply to criminal and civil case records. *See* C.J. Paula M. Carey and Joseph Stanton, *Amendments to the Uniform Rules of Impoundment Procedure*, **BBA Journal Summer 2015 Vol. 59**.

None of these cases or rules establish an *absolute* right of access to judicial records. Judges are authorized to impound court records on a case-by-case basis or if required by statute or court rule, provided that the governing constitutional or common law standards are met.**[vi]** "Under the First Amendment to the United States Constitution, '[t]he burden falls on the party seeking closure to demonstrate that (1) there exists a substantial probability that permitting access to court records will prejudice his fair trial rights; (2) closure will be effective in protecting those rights, and that the order of closure is narrowly tailored to prevent potential prejudice; and (3) there are no reasonable alternatives to closure.'" *Republican*, 442 Mass. at 223 n.8 (quoting *Sharpe*, 432 Mass. at 605 n.24). The common law right of access similarly permits impoundment of judicial records upon a showing of "good cause," a standard which the Supreme Judicial Court has said "take[s] into account essentially the same factors as required by the First Amendment: 'the competing rights of the parties and alternatives to impoundment.'" *Id.**[vii]***

Given these well-established constitutional and common law principles, there should be little doubt that the public's right of access to electronically maintained court files is comparable to its historical right to inspect conventional court records. In both situations, "[i]t is desirable that [judicial proceedings] should take place under the public eye . . . because it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed." *Republican*, 442 Mass. at 222 (quoting *Cowley v. Pulsifer*, **137 Mass. 392**, 394 (1884) (Holmes, J.)). As discussed below, however, other questions remain about the manner in which the public will be allowed to access electronic records.

Public Access to Electronically Maintained Alphabetical Indices of Criminal Cases

Alphabetical indices of criminal case files have been available to the public since at least the 18th century. *See Globe Newspaper Co. v. Fenton*, **819 F. Supp. 89**, 91-93 (D. Mass. 1993). *See also* ***Massachusetts Body of Liberties***, art. 48 (1641) ("Every inhabitant of the Country shall have free liberty to search and review any rolls, records or registers of any Court or office…."). Although converting to electronic records will make it unnecessary for clerks to continue to keep conventional, hard-copy alphabetical indices, clerks still will be required under Massachusetts law to maintain alphabetical indices (even if in electronic form). *See* **G.L. c. 221, § 23** ("Each clerk shall keep an alphabetical list of the names of all parties to every action or judgment recorded in the records and a reference to the book and page thereof…."). As a practical matter, moreover, some form of an alphabetical index or search function will be needed to efficiently organize and retrieve case information. Will the public have a right to use the newly created electronic indices of criminal cases? Case law concerning public access to conventional alphabetical indices and docket sheets suggests that the answer is yes. *See Fenton*, 819 F. Supp. at 90-91 (public has First Amendment right of access to alphabetical indices of criminal cases); *Hartford Courant Co. v. Pellegrino*, **380 F.3d 83**, 86 (2d Cir. 2004) (First Amendment right of access to docket sheets).

The *Fenton* court struck down on First Amendment grounds a provision of CORI (since repealed) that prohibited public access to the alphabetical indices of criminal cases in order to promote privacy and rehabilitation interests. *Fenton*, 819 F. Supp. at 93.**[viii]** *See generally New Bedford Std.-Times Pub. v. Clerk, Third Dist. Ct.*, **377 Mass. 404**, 412, 413 (1979); J. Brant, *et al.*, *Public records, FIPA and CORI: how Massachusetts balances privacy and the right to know*, 15 Suffolk U. L. Rev. 23, 59-60 (1981). *Fenton* held that the historical tradition of access to alphabetical indices, combined with the positive role access has on public oversight and understanding of the courts, required that alphabetical indices to criminal cases be publicly available absent case-specific findings that a restriction on access was narrowly tailored and effectively served a compelling state interest. 819 F. Supp. at 91-99.

Throughout the courts a sprawling amalgam of papers reflects action in connection with judicial proceedings. It is not misleading to think of courthouse papers as comprising a vast library of volumes for which docket sheets are the tables of contents. Without the card catalogue provided by alphabetical indices, a reader is left without a meaningful mechanism by which to find the documents necessary to learn what actually transpired in the courts. The indices thus are a key to effective public access to court activity. And the importance of public access to the proper functioning of our judicial system cannot be overstated.

Id. at 94. *Fenton* has been cited approvingly by the SJC. *See Globe Newspaper Co. v. Dist. Attorney for Middle Dist.*, **439 Mass. 374**, 382 n.12 (2003) ("[a]s a result of [*Fenton*], the public has access to court clerks' alphabetical indices of defendants' names and may thereby obtain access to court records concerning an individual defendant"); *Roe v. Attorney General*, **434 Mass. 418**, 435-436 (2001)

(citing*Fenton* for the proposition that the "denial of public access to court alphabetical indices of criminal defendants violated First Amendment to the United States Constitution").

These decisions provide strong support for the proposition that the public should have a commensurate right of access to electronically maintained alphabetical indices (or "card catalogues") of criminal cases. Absent recognition of such a right, the modernization of court files would have the unintended consequence of reducing public oversight of the courts.

Remote Electronic Access to Criminal Case Records and CORI

Recognizing a public right of access to electronic court records ensures that the computerization of judicial records will not diminish the public's longstanding right to obtain information about the functioning of the judicial system. Other questions remain, such as whether the public should have remote access to case files over the World Wide Web. PACER, for example, permits registered users to remotely search court records by a party's name in individual federal district courts, courts of appeal and bankruptcy courts to obtain both civil and criminal case records.**[ix]** **Federal Rule of Civil Procedure 5.2** addresses some privacy concerns raised by online access by requiring PACER users to redact certain personal identifying information from their electronic filings. Similar requirements are contained in the **Supreme Judicial Court's proposed new Rule 1:24**, Personal Identifying Information. Despite such safeguards, privacy advocates have concerns about the difference between, on the one hand, requiring members of the public to travel to individual courthouses to examine a court record and, on the other hand, permitting the public to access records online either on a court-by-court, county-by-county, or state-wide basis. In addition to these public policy issues, online access to court records also raises a legal issue unique to Massachusetts law: would permitting remote web access to electronic court records in criminal cases violate CORI?

As initially enacted, CORI restricted public access to certain criminal record information held by the executive and judicial branches. *See generally New Bedford Std.-Times*, 377 Mass. at 412, 413; *Public records, FIPA and CORI, supra,* 15 Suffolk U. L. Rev. at 58-60. The statutory provision that prohibited public access to alphabetical indices of criminal cases was struck down by *Fenton* and, thereafter, repealed as part of the 2010 amendments to the statute. *Compare* **St. 1977, c. 841** and **G.L. c. 6, § 172**(m). *See generally* G. Massing, *CORI Reform–Providing Ex-Offenders with Increased Opportunities without Compromising Employers' Needs*, **55 Boston Bar Journal 21**, 22 (Winter 2011).

The combination of *Fenton* and the 2010 amendments to CORI have led some to conclude that CORI no longer has any application to court records. *See* ***Guide to Public Access, Sealing & Expungement***, Administrative Office of the District Court Department of the Trial Court (Rev. Ed. 2013) at 8 ("The CORI Law Does Not Limit Access to Clerk's Records"); *see also id.* at 8 n.27, 11 & n.34. This conclusion is supported by **G.L. c. 6, § 172(m)(2)**, which provides in relevant part: "[n]otwithstanding this section . . ., the following shall be public records: . . . chronologically maintained court records of public judicial proceedings." *Id. See also Middle Dist.*, 439 Mass. at 382 ("[d]ocket numbers are

assigned chronologically and maintained by courts as part of their court records, criminal proceedings against adult defendants are public proceedings, and docket number information thus falls squarely within the second listed exception to the CORI statute."); *id.* at 385 ("There is no violation of the CORI statute when the search specifications consist of information that would also be revealed on the court's records accessible to the public.").

Privacy advocates argue that remote access to electronic court records would provide the public with the type of aggregated criminal history information still protected by CORI. The 2010 amendments to CORI authorized the Department of Criminal Justice Information Services ("DCJIS") to create an electronic database of criminal offender record information and strictly limited access to that database to enumerated persons and entities. *See* **G.L. c. 6, § 172(a)**. *See also id.* at §§ **167(e)**, **G.L. c. 6, § 168A**,**G.L. c. 6, § 168C**, **172(29), (30)**. The statute also makes it a crime to knowingly obtain or attempt to obtain criminal offender record information under false pretenses or to knowingly communicate such information "except in accordance with [CORI]." **G.L. c. 6, § 178**.

A discussion of the public policy arguments for and against online access to court records of criminal cases is beyond the scope of this article.**[x]** As a matter of statutory construction, however, it is difficult to argue that CORI forbids remote access to court records (whether on a state-wide, county-wide, or court-by-court basis), particularly given the unintended consequences of such an interpretation. For example, the statute draws no distinction between electronic and conventional court records. If CORI applies to accessing electronic court records remotely, then it also would apply to accessing conventional records in a courthouse, a conclusion that would upend centuries of tradition and raise significant constitutional issues of free speech and separation of powers. *See generally Fenton*, 819 F. Supp. at 98-99; *Opinion of the Justices*, **365 Mass. 639**, 645-647 (1974) (executive branch agency that controlled electronic data processing in the judicial branch would violate art. 30 of the Declaration of Rights). Nor does the statute distinguish between remote and on-site access, or between state and federal courts. Broadly interpreting CORI as applying to court records thus would implicate PACER users as well. Under these circumstances, the criminal penalties imposed for obtaining criminal offender record information under false pretenses or communicating such information except in accordance with the statute seem best understood as protecting the DCJIS database, not court files. *See* **G.L. c. 6, § 178**.

Electronic court records represent a great technological advance for the delivery of legal services and justice. But that advance should not render obsolete a far greater innovation — the Founders' vision of a presumptively public judicial system. There may be many issues to consider before permitting remote Web access to court records, but violating CORI most likely is not one of them.

Jonathan M. Albano is a partner at Morgan Lewis & Bockius LLP in Boston. He represents the press in courtroom access and privacy matters and was counsel on behalf of media interests in some of the cases cited in this article.

Endnotes

[i] *See* **http://www.mass.gov/courts/case-legal-res/rules-of-court/sjc/efiling-order.html**.

[ii] *See* **http://www.mass.gov/courts/case-legal-res/rules-of-court/efiling-rules.html#rule11**.

[iii] Committee members include representatives of the Trial Court, the Superior Court, the Boston Municipal Court, the Housing Court, the Land Court, the Probate and Family Court, the Appeals Court, and the Supreme Judicial Court. A transcript of a June 15, 2015 public hearing held by the Committee, as well as written comments received from 36 persons and organizations, is available at**http://www.mass.gov/courts/court-info/commissions-and-committees/tc-access-records.html**.

[iv] *See also Richmond Newspapers v. Virginia*, **448 U.S. 555**, 580 (1980); *Press-Enterprise Co. v. Superior Court*, **464 U.S. 501**, 513 (1984); *Press-Enterprise Co. v. Superior Court*, **478 U.S. 1**, 10 (1986).

[v] Other courts also have recognized a First Amendment right of access to civil proceedings and records. *See generally Publicker Ind., Inc. v. Cohen*, **733 F.2d 1059**, 1070 (3d Cir. 1984). The Supreme Judicial Court has not yet addressed whether Article 16 of the Declaration of Rights of the Massachusetts Constitution grants the public a comparable right of access to court records.

[vi] The Massachusetts Appeals Court maintains a list of materials that are not available for public inspection. *See* **http://www.mass.gov/courts/docs/appeals-court/impoundment-sources.pdf.** *But see Commonwealth v. Jones*, **472 Mass. 707**, 731 (2015) (despite statutory requirement of **G. L. c. 233, § 21B** that rape shield hearings must be held *in camera*, Constitution requires trial court to make case-specific findings before closing hearing).

[vii] "The exercise of the power to restrict access, however, must recognize that impoundment is always the exception to the rule, and the power to deny public access to judicial records is to be strictly construed in favor of the general principle of publicity." *Republican*, 442 Mass. at 223 (quotation and citation omitted).

[viii] *See* **St. 1977, c. 841** ("the following shall be public records: … (2) chronologically maintained court records of public judicial proceedings, *provided that no alphabetical or similar index of criminal defendants is available to the public, directly or indirectly*") (emphasis added).

[ix] The more than one million users of PACER, which is an acronym for Public Access to Court Electronic Records, include attorneys, *pro se* filers, government agencies, trustees, data collectors, researchers, educational and financial institutions, commercial enterprises, the media, and the general public. *See* **https://www.pacer.gov/**.

[x] *See, e.g.*, N. Gomez-Velez, *Internet Access to Court Records – Balancing Public Access and Privacy*, 51 Loy. L. Rev. 365 (2005); P. Martin, *Online Access to Court Records – From Documents to Data, Particulars to Patterns*, **53 Villanova L. Rev. 855** (2008). *See generally U.S. Dep't of Justice v. Rep. Comm. for Freedom of the Press*, **489 U.S. 749**, 764 (1989).

The Misuse of MassCourts as a Free Tenant Screening Device

by Esme Caramello and Annette Duke

Heads Up

"If I see that a prospective tenant has ever had a lawyer in any proceeding at **http://www.masscourts.org** as of this case forward I no longer take them as a tenant. This is a free country. They certainly have a right to hire a lawyer and I have a right to not take them as tenants because of that." **Massachusetts Landlords Blog**, June 12, 2015.

The Trial Court's Electronic Case Access system (MassCourts) was not intended to be a direct, online "free tool for tenant screening." But that is how it is increasingly being promoted and used:

"After years of lobbying from rental housing groups, the Massachusetts Housing Court has finally announced a powerful new and free tool for tenant screening: public internet access to all Summary Process, Small Claims, Civil and Supplementary Process case types…. This new system will enable landlords to research whether a potential or current tenant has been a party to a previous eviction, small claims or related housing case." The Massachusetts Real Estate Law Blog, "**Massachusetts Housing Court and Tenant Eviction History Now Online**," April 24, 2013 (emphasis added).

While careful, conscientious tenant screening can help landlords avoid problems with new tenants, the automatic refusal to rent to anyone whose name appears in an online court database is a dangerous form of tenant blacklisting. Tenants are sometimes forced by absentee or unscrupulous landlords to access the courts to protect their families from unsafe conditions. For example, one tenant, 8½ months pregnant and shoveling the walkway in front of her unheated apartment, turned to the court to force an unresponsive bank that owned her building to pay its bills and maintain the property. Another faced a retaliatory eviction lawsuit after reporting a building-wide bedbug infestation affecting the health of her neighbors, families, and friends. Still another was brought into court after her landlord discovered she had a female partner. Blacklisting tenants like these merely because their names are online in MassCourts erects unfair barriers to finding an apartment for anyone who has ever been to court in a housing case – tens of thousands of people every year – and could place especially vulnerable people with limited housing options into a spiral towards homelessness.

While some landlords undoubtedly look beyond the mere fact of a tenant's appearance in MassCourts to the actual "Disposition" or docket itself, even this increased level of scrutiny may not elicit an accurate picture of a tenant. MassCourts was not designed as a tenant-screening tool. It is a case management database built to assist the court system in managing litigation, and it uses shorthand that suffices for that

purpose. It does not tell the real story behind any landlord-tenant dispute. Most summary process dockets, for example, ultimately reflect a judgment for the landlord. This does not equate to a finding the tenant was at fault. The vast majority of tenants are unrepresented, and the few who are lucky enough to access legal assistance often do not agree to have a judgment enter against them, but instead secure dismissal of the case or a straight agreement (with no judgment of eviction) in which the parties make commitments to each other, such as payment of rent in exchange for repairs.

To make matters worse, there are inaccuracies in the MassCourts database. For example, a review of housing cases closed by the Harvard Legal Aid Bureau in 2013 showed that in nearly 10% of the cases, MassCourts incorrectly displayed a judgment of eviction against the tenant when there was none. In MassCourts, "no-fault" evictions are sometimes miscoded as "cause" cases. Cases that have been dismissed may appear as open, active cases or even judgments in favor of the landlord. Minor children may erroneously appear as parties in their parents' eviction cases, potentially hurting their creditworthiness before they have a chance to enter the adult world. MassCourts remote access takes these errors and turns them into major barriers to housing, with no way for a tenant to even know that this information is being used by a landlord and no clear way to challenge its accuracy.

Other states have recognized the problems with court-enabled tenant screening and scaled back access. For example, in 2012, the Chief Administrative Judge of the New York State Office of Court Administration announced that the court would no longer include in the electronic data feed it sold to tenant screening companies the names of tenants involved in New York City Housing Court evictions.*See* Hon. Gerald Lebovits and Jennifer Addonizio, **The Use of Tenant Screening Reports and Tenant Blacklisting**, New York State Bar Association (2013). Applauding this action "to protect both New York's tenants and the integrity of the court system," one legislator explained: "When the fear of being 'blacklisted' causes many tenants to avoid the court and relinquish their legal rights, access to justice is fundamentally undermined." **Sen. Krueger Announces Courts to End Electronic Sale of Housing Court Data Used in "Tenant Blacklists"** (2012).

Massachusetts, through the Trial Court Public Access to Court Records Committee, can and should implement safeguards that protect tenants without impairing the public's right to open courts. A very limited change to how party identification information is displayed online could counteract the misuse of MassCourts: tenant names should be replaced with numbers or initials in the online database. Parties and attorneys would still be able to access case information online with docket numbers. The official case record would still be public, would still include parties' names, and could be accessed by going to court. This change would balance protecting tenants' rights with keeping court records public.

With 40,925 eviction cases filed in Housing and District courts across the Commonwealth in FY 2014 alone, the easy, online use of MassCourts as a free tenant screening tool has become a serious access to justice issue. Without reform, tenants will increasingly fear that the consequences of coming to court will

be that they won't be able to find housing in the future, and they will not see courts as a place to seek justice.

Annette Duke is a housing attorney at the Massachusetts Law Reform Institute, a statewide nonprofit poverty law and policy center. She specializes in public housing and landlord-tenant law and is currently working with the Massachusetts Access to Justice Commission and a broad coalition of organizations to expand housing courts statewide.

Esme Caramello is the Faculty Director of the Harvard Legal Aid Bureau, a century-old student-run legal services organization that represents low income clients in housing, family, wage and hour, and government benefits cases. She is also a Clinical Professor at Harvard Law School, where she teaches courses in housing law and policy and legal skills and ethics.

The Unwarranted Secrecy of Criminal Justice Information in Massachusetts

by Jeffrey J. Pyle

Legal Analysis

In the past year, the normally sleepy topic of public records law has caught fire in Massachusetts. Thanks to extensive reporting by the news media, the public has become aware of widespread problems accessing public records, including questionable denials of access, demands for exorbitant fees, and ineffective administrative oversight. The Center for Public Integrity has given Massachusetts an "F" grade for its public access to information, and our State Police recently won the 2015 "**Golden Padlock Award**," a national "honor" bestowed by Investigative Reporters & Editors to acknowledge "the dedication of government officials working tirelessly to keep vital information hidden from the public."

As a result of these embarrassments, the legislature is finally giving serious consideration to updating the Public Records Act, G.L. c. 66, § 10, long viewed as the weakest freedom of information act in the country. **House Bill 3665**, "An Act to Improve Public Records," addresses the substantial procedural obstacles to access, including high fees for production, slow response times, and the inability of courts to award attorneys' fees to requesters who prevail in court. As of this writing, the bill remains on hold as sponsors consider objections from some cities and towns to its limitations on search fees and copying costs.

Even if this important legislation is enacted, however, significant barriers to access will remain. Many have noted that the bill does not address the exclusion of the legislature and the courts from the Public Records Act, and the Governor's Office will be able to continue to declare itself exempt. Less remarked upon, but of arguably equal significance, the bill does not address the fact that in the last ten years, through statutory enactments and restrictive interpretation of existing law, vast categories of documents concerning the Massachusetts criminal justice system have been removed from public inspection. These changes have placed the Commonwealth well outside the norm of other states, and deprived the public of crucial information at a time of heightened public concern about criminal justice policies and police misconduct.

This article will focus on three categories of criminal justice records of particular concern.

Arrest Reports, the Investigatory Exemption and the CORI Statute

The Public Records Law, G.L. c. 66, § 10, provides that all records in the custody of covered governmental entities—including state agencies, municipalities, and law enforcement —are presumptively open to the public. The law also contains numerous "exemptions" to the statutory definition of "public record" that allow covered entities to withhold documents, but places the burden on the government to prove with specificity that an exemption applies. The exemptions are to be narrowly construed, and where possible, the government must redact sensitive material rather than deny records outright. *See Reinstein v. Police Comm'r of Boston*, 378 Mass. 281, 289-90 (1979).

One exemption allows the government to withhold "investigatory materials," *only* if they are "necessarily compiled out of the public view by law enforcement or other investigatory officials" *and* their release "would probably so prejudice the possibility of effective law enforcement that such disclosure would not be in the public interest." G.L. c. 4, § 7 cl. 26(f). Plainly, this is no "blanket exemption" for all "records kept by police departments," and it does not permit "every document that may be placed within what may be characterized as an investigatory file" to be kept secret. *Bougas v. Chief of Police of Lexington*, 371 Mass. 59, 65 (1976). Rather, for the investigatory exemption to apply, there must be "specific proof" that the release of a particular record would prejudice the possibility of effective law enforcement. Because that burden can be established with a showing that release would expose confidential law enforcement techniques or discourage witnesses from coming forward in the future, the conclusion of an investigation does not necessarily eliminate protection. Nonetheless, courts have ordered the release of citizen witness statements,[i] police incident reports,[ii] and even the interview of a murder suspect,[iii] notwithstanding invocation of the exemption.

The language of the investigatory exemption reflects a legislative intent to balance the legitimate needs of the police against the substantial public interest to know about crime and law enforcement activities. However, in the last several years, law enforcement agencies have asserted that they need not contend with the narrowness of the investigatory exemption. They claim that routine police documents,

such as arrest reports, incident reports and mugshots are subject to the Criminal Offender Record Information (CORI) statute, G.L. c. 6, § 167 *et seq.*; that the CORI statute gives police the "discretion" whether to withhold or release such documents; and thus they are "specifically or by necessary implication exempted from disclosure by statute," in the words of another exemption.
These assertions are incorrect. While the CORI statute imposes restrictions on the dissemination of "criminal offender record information," it expressly limits the restriction to information "recorded *as the result of* the initiation of criminal proceedings." G.L. c. 6, § 167. Routine police documents like arrest reports and mugshots are prepared *before* and not "as the result" of the issuance of a criminal complaint. Accordingly, the CORI statute plainly "was not enacted to stop the release of police records," and does not—"specifically or by necessary implication"—exempt such records from release under the Public Records Act. This was the analysis of then-Supervisor of Public Records Alan Cote in 2003, in a memorandum deriding a "troubling" law enforcement trend of withholding pre-arrest incident reports under CORI.**[iv]**

However, in 2010, the Department of Criminal Justice Information Services (DCJIS), which is tasked with implementing the CORI statute, adopted the novel position that the "initiation of criminal proceedings" is not the issuance of a criminal complaint, but rather, the "point when a criminal investigation is sufficiently complete that the investigating officer takes actions toward bringing a specific suspect to court." That moment generally precedes arrest and the taking of a mugshot. The DCJIS later issued a regulation embodying this definition of "initiation." 803 CMR 2.03(4) and 7.02. Now, police departments—as well as the current Supervisor of Records—routinely rely on the DCJIS regulations to deny public access to routine police records.

This does not mean that police departments *never* release arrest reports or mugshots—they often do under another DCJIS regulation that permits, but does not require, the dissemination of CORI records "specifically related to, and contemporaneous with, an investigation or prosecution." 803 CMR 7.10. However, when the *Boston Globe* sought public records concerning the arrests of police officers for drunk driving, police departments almost uniformly relied on the CORI statute to deny the requests.**[vi]** Thus, in Massachusetts, reports of arrests—one of the most significant actions the government can take against an individual—are being released only at the discretion of the police, contrary to the strong presumption of openness at the heart of the Public Records Act.

The *Boston Globe* recently filed a groundbreaking lawsuit challenging the DCJIS regulations and the law enforcement interpretation of the CORI law. *Boston Globe Media Partners, LLC v. Dep't. of Criminal Justice Information Services*, Suffolk Superior Court, No. SUCV2015-01404D. A decision in the case could affect not only the press and the public, but also attorneys seeking to investigate prior incidents. If the courts rule in favor of the law enforcement agencies, Massachusetts would become the only state where police are vested with the unfettered discretion over whether and when to grant public access to arrest reports.[vii]

Domestic Violence Records

Massachusetts police departments have long been required to assemble a log of daily arrest reports and keep it open for public inspection. G.L. c. 41, § 98F. Journalists use the logs to inform the public about crime in the community and to determine which court proceedings to cover. But in 2014, the governor signed legislation requiring police departments to exclude from the logs all reports of domestic violence, sexual assault, and the violation of abuse protection orders pursuant to G.L. c. 209A. Before this change, no type of crime, but for a limited exception, was excluded from public inspection.[viii] At the same time a different statute, G.L. c. 41, § 97D, was amended to provide that the police must keep all incident reports concerning domestic abuse confidential—that provision had previously applied only to charges of rape and sexual assault.

These changes to the law, included in a larger domestic violence bill, were intended to encourage victims of abuse to report the violence without the risk of embarrassment. However, the expurgation of the logs can also result in protecting the alleged perpetrators of abuse from publicity, thus arguably removing a deterrent to abuse. The exclusion also may dampen public awareness about violence in the community,[ix] prevent the public from learning about violence perpetuated by public officials or other persons holding positions of trust, and mask other criminal charges that may accompany domestic violence arrests, such as drug and firearms possession. While the domestic violence bill did not purport to seal court records (and thus cannot promise true confidentiality to victims), the mandatory exclusion of the information from police logs may hinder the news media's efforts to learn about crimes in first place. It may also prevent the public from learning how the police respond to and otherwise handle reports of domestic abuse, thereby creating the risk that the crime could be driven further underground. This Massachusetts restriction appears to have no equivalent elsewhere in the United States.[x]

Sealing of Criminal Cases

In a celebrated "quartet" of decisions in the 1980s, the Supreme Court ruled that the public has a fundamental right protected by the First Amendment to attend criminal trials and pre-trial proceedings. One of the purposes of the First Amendment, the Court explained, is to assure "freedom of communication on matters relating to the functioning of government," and it would be difficult to identify any government function "of higher concern and importance to the people than the manner in which criminal trials are conducted." *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 575 (1980). Numerous federal courts of appeal have applied the Supreme Court's reasoning to hold that there is a First Amendment right of access to documents filed in criminal cases.

In 1989, the First Circuit held that a Massachusetts statute requiring the blanket sealing of records of cases resulting in not-guilty findings and other non-conviction dispositions was unconstitutional as written. *Globe Newspaper Co. v. Pokaski*, 868 F.2d 497 (1st Cir. 1989). The court held that records of dismissed or *nolle prossed* cases may be sealed only upon specific, on-the-record findings that sealing is necessary to effectuate a compelling governmental interest sufficient to overcome the public's First Amendment right of access to criminal proceedings. The Supreme Judicial Court followed suit a few years later, ruling in *Commonwealth v. Doe* that in order to seal such records, the defendant must demonstrate on the specific facts of the case, that "the value of sealing to the defendant clearly outweighs the constitutionally-based value of the record remaining open to society." 420 Mass. 142, 151 (1995). The value of open court proceedings is so weighty, and the First Amendment right so strong, that both the *Pokaski* and *Doe* courts anticipated that few defendants would be able to seal records under this standard. *Pokaski*, 868 F.2d at 506 n. 17; *Doe*, 420 Mass. at 150 n. 7.

In August 2014, however, the SJC departed sharply from this well-established case law. In*Commonwealth v. Pon*, 469 Mass. 296 (2014), the Court decided that the First Amendment does not apply after all, and that henceforth, defendants need show only "good cause," not a compelling interest, to seal the records of a case ending in dismissal or a *nolle prosequi*. *Id.* at 311-312. While it remains true that in order to seal these records, defendants must overcome a common-law based "general principle of publicity," the SJC invited motion judges to abandon the case-specific inquiry required by *Doe* (and, for that matter, the common law "good cause" test), and instead to "take judicial notice that the existence of a criminal record, regardless of what it contains, can present barriers to housing and employment opportunities." *Id.* at 315-316. *Pon* gives great weight to "the compelling governmental interests in reducing recidivism, facilitating reintegration, and ensuring self-sufficiency by promoting employment and housing opportunities for former criminal defendants," and only the barest acknowledgement of the public's "*general* right to know so that it may hold the government accountable for the proper administration of justice." *Id*. at 315 (emphasis supplied).

The SJC's ruling in *Pon* once again puts Massachusetts law at the vanguard of criminal justice secrecy, and in sharp conflict with not only the First Circuit's *Pokaski* decision but with every other federal court of appeals to have considered the standard for sealing criminal records. To be sure, the societal goals cited in *Pon* are important, but the articulated test makes it likely that many more criminal records—including in cases where the defendant admitted to facts sufficient to warrant a guilty finding in exchange for a continuance without a finding—will be shielded from the press and the public. While acknowledging in a footnote that a "different analysis may be necessary" if "the defendant is a public figure," the SJC failed to recognize that today's private figure can be tomorrow's candidate for election, and it could be highly relevant to voters that a candidate for office once admitted to a crime. Perversely, the *Pon* decision also makes it more likely that the public and the media will resort to third-party background check services, which are likely to be less complete and accurate than official court records that are now permitted to be sealed under *Pon.*

Conclusion

If there is any part of our government that deserves scrutiny by the press and the public, it is the criminal justice system. More than 130 years ago, then-Supreme Judicial Court Justice Oliver Wendell Holmes wrote: "it is of the highest moment that those who administer justice should always act under the sense of public responsibility, and that every citizen should be able to satisfy himself with his own eyes as to the mode in which a public duty is performed." *Cowley v. Pulsifer*, 137 Mass. 392, 394 (1884). We are in danger of abandoning that important principle in Massachusetts.

Jeffrey J. Pyle is a partner at Prince Lobel Tye LLP in Boston, where he practices in the fields of First Amendment, media law, and litigation. He is a member of the BBA Council, and previously served as Chair of the Amicus Committee and co-chair of the Civil Rights and Civil Liberties Section.

Endnotes

[i] *Globe Newspaper Co. v. Police Comm'r of Boston*, 419 Mass. 852, 863 (1995).

[ii] *Reinstein*, 378 Mass. at 291; *Globe Newspaper Co. v. Evans*, No. CIV.A 97-4102-E, 1997 WL 448182, at *4 (Mass. Super. Aug. 5, 1997) (Burnes, J.).

[iii] *Rafuse v. Stryker*, 61 Mass. App. Ct. 595, 600 (2004).

[iv] SPR Bulletin No. 3-03, Nov. 21, 2003.

[vi] Todd Wallack, "Ruling Allows Police to Withhold Officers' Drunken Driving Records," *Boston Globe*, March 11, 2015.

[vii] *See* **www.rcfp.org**, last visited September 23, 2015. According to the Reporters Committee for Freedom of the Press (RCFP), which publishes a 50-state guide to access to public records, there is currently no state where police have unfettered discretion whether to withhold routine arrest reports.

[viii] The earlier exception provides that "any entry in a log which pertains to a handicapped individual who is physically or mentally incapacitated to the degree that said person is confined to a wheelchair or is bedridden or requires the use of a device designed to provide said person with mobility, shall be kept in a separate log and shall not be a public record nor shall such entry be disclosed to the public." G.L. c. 41, § 98F (2013).

[ix] After the amendment of G.L. c. 41, § 98F, the City of Waltham noted a significant drop in the overall number of incidents reported in the police log. *See* Eli Sherman, "Waltham Police Comply with New Domestic Violence Law; Logs Show Far Fewer Arrests," *Waltham News Tribune*, Aug. 28, 2014.

[x] Under California law, the names and addresses of victims of domestic assault may be withheld at the victim's request. Cal. Gov't Code, § 6254.

[xi] *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980); *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596 (1982); *Press–Enterprise Co. v. Superior Court*, 464 U.S. 501 (1984); *Press–Enterprise Co. v. Superior Court*, 478 U.S. 1 (1986).

Making Sense of the Internet of Things

by Peter M. Lefkowitz

The Profession

We have seen the marketing. According to a recent report by a top consulting firm, the Internet of Things will have an annual economic impact of between $4 trillion and $11 trillion by 2025. Another firm has announced that there will be 50 billion internet-connected devices globally by 2020. And companies already have rebranded in grand fashion, declaring the arrival of "Smart Homes," "Smart Cities," the "Smart Planet," the "Industrial Internet" (the contribution of the author's company), and even the "Internet of*Everything*." We also have seen the reality of Fitbits that record our activity and suggest changes to our exercise and sleep patterns, cars that accept remote software updates, and airplane engines that communicate maintenance issues from the tarmac. For all of this potential, and even greater claimed potential, our shared late-night admission is that none of us has a well-defined picture what, precisely, the Internet of Things is or does.

This combination of wide promise and shared confusion is not a trivial matter. Companies are setting long-term strategy based upon *Jetsons*-like glimmers of the future; consumer expectations and fears are being set in an environment of rapidly-evolving offerings and — most critically for attorneys providing advice to clients considering investments in this area — legislators and regulators are being asked to set legal and enforcement frameworks without a clear picture of the future product landscape or whether products still in their infancy will create anticipated harm. In order to advise properly in this area, and to avoid regulatory frameworks getting far ahead of actual product development, it is important that lawyers appreciate the scope of Internet of Things technology and the policy implications of internet-connected goods and the data they create and use.

So what is the Internet of Things? Simply put, the Internet of Things, or IoT, is a set of devices that connect to and send or receive data via the internet, but not necessarily the devices people most often think of as being connected to the internet. In the consumer world, IoT includes smart meters that measure home energy use, refrigerators that can report back on maintenance needs or **whether the owner needs more eggs**, and monitors that can record blood sugar results and communicate via Bluetooth to a connected insulin pump. It also increasingly includes cars that sense other cars in close proximity and record and report on driver speed, location and music listening choices. And in the industrial space, offerings include an array of sensors and networks that measure and manage the safety and efficiency of oil fields or the direction, speed and service life of wind turbines and airplane engines; X-ray and CT machines with remote dose monitoring; and badge-based radio-frequency identification systems that analyze whether medical providers are washing their hands in the clinical setting and the resulting impact on infection rates. This definition generally does not include computers, tablets and other computing

devices, although — with smartphone apps advancing to the point of measuring movement and heart rate and reading bar codes to compare prices at local retailers — one could argue that the iPhone and Android phone are the Swiss Army Knives of personal internet-based data collection and use. In turn, IoT devices generate large sets of sensor-based data, or Big Data, which can be aggregated and analyzed to generate observations concerning the world around us and to improve products and services in healthcare, energy, transportation and consumer industries.

These developments have not been lost on government. The White House has commissioned two major studies on the potential of Big Data. The Federal Trade Commission held a full-day workshop to discuss IoT in the home, in transportation and in healthcare, and FTC staff subsequently issued **a comprehensive report** discussing benefits and risks of IoT. Branches of the European Commission are encouraging companies to establish European research and development footholds for internet-based devices. The European Commission noted the development of internet-based devices and the prospect of a Digital Single Market as inspirations for the anticipated replacement of the European Data Privacy Directive. And European Data Protection Commissioners have boldly asserted their authority, **declaring** that in light of the risk presented by sensor-based devices, "big data derived from the internet of things . . . should be regarded and treated as personal data" under European data privacy law. Unfortunately, the Commissioners did not distinguish industrial uses such as wind turbines and oil wells from consumer goods that actively collect personal information.

The FTC report above summarizes many of the practical and policy challenges presented by emerging IoT technologies and the views of advocates for industry and consumers. Security is, for many, the most compelling issue. Internet-connected devices must collect data accurately; those data sets need to be communicated securely to data centers; and devices and back-end computing systems need to be protected against hackers, both to protect the data collected from devices and to protect the networks and devices against hijacking. Recent stories of rogue engineers using laptops to break into parked cars and controlling car brakes remotely, and the dystopian nightmare of a hacked pacemaker on the TV drama *Homeland*, have not helped mitigate these concerns. This risk is compounded by the prospect of "big data warehouses" that can store and analyze zettabytes of data in support of technological breakthroughs.

Separately, there is the question of notice and consent for the collection and use of IoT data. As the FTC staff report notes, it is significantly easier to provide notice about a company's data practices on a computer screen than on a piece of medical equipment or in a friend's car that already is collecting and reporting a wide array of data. This problem is compounded in industrial settings, for example, where passenger weight is analyzed to optimize airplane engine function, or where data sets from and surrounding an MRI machine are communicated to the hospital network to read the scan and to the device manufacturer to facilitate maintenance and product improvement.

Other questions abound. Will data from an internet-connected device be used for unanticipated purposes, such as devising large consumer medical or credit reports, without the consumer having the ability to know what is being done or how to correct or delete data? Will providers use data to discriminate improperly, or will better use of data create a more level playing field, facilitating new services at lower prices for a wider swath of consumers? And are some issues already addressed by current regulatory frameworks like HIPAA or the Fair Credit Reporting Act, related standards like the Payment Card Industry security rules, or extensive regulatory frameworks governing security and data use for government contractors, transportation providers and energy providers?

In turn, certain baselines have emerged. First, "security by design" and "privacy by design," the practices of building security and privacy protections into the development lifecycle of goods and networks, are essential. These requirements become even more compelling in light of the recent**decision of the Third Circuit** in *FTC v. Wyndham Corporation Worldwide*, holding, among other things, that the FTC has authority to bring claims alleging "unfairness" for a company's purported failure to properly secure networks and data. Second, companies collecting data from IoT devices must carefully consider how much data they need and whether it can be de-identified to minimize privacy risk, whether the data will be aggregated with other data, and whether consumer choice is needed to make specific use of the resulting data set. And in light of privacy and national security laws around the world — including recent data localization and national security laws in Russia and China — companies will need to evaluate where data is transferred globally and where to locate the associated databases and possibly even global computing, service and engineering staff.

Much of the promise and peril of the Internet of Things and Big Data are in the future. Google and Dexcom, a maker of blood sugar monitoring devices, recently announced an initiative to make a dime-sized, cloud-based disposable monitor that would communicate the real-time glucose values of diabetes patients directly to parents and medical providers. No date has been announced, although recent advances in remote monitoring suggest hope. And the journal Internet of Things Finland recently published an article announcing the proof-of-concept for a "wearable sensor vest with integrated wireless charging that . . . provides information about the location and well-being of children, based on received signal strength indication (RSSI), global positioning system (GPS), accelerometer and temperature sensors."

Thus far, rule-making has focused on security standards for connected devices and related computing networks. The FDA has issued detailed security guidance for connected devices and systems, and the Department of Defense has issued security standards for contractors that include an expansive definition of government data subject to coverage under the U.S. Department of Commerce's NIST 800-171 standard for protecting sensitive federal information. However, there has not been a push in the U.S. for comprehensive legislation governing internet-connected goods and services. As the FTC staff report explained: "[t]his industry is in its relatively early stages. Staff does not believe that the privacy and security risks, though real, need to be addressed through IoT-specific legislation at this time. Staff agrees

with those commentators who stated that there is great potential for innovation in this area, and that legislation aimed specifically at IoT at this stage would be premature."

The marketplace for internet-connected goods and services surely will continue to expand, and the product and service landscape will advance rapidly. Whether we will see more than $10 trillion dollars of annual economic impact has yet to be determined. In this fast-moving environment, companies considering investment in the Internet of Things and Big Data and the attorneys who advise them would be well served to monitor the evolving regulatory and legislative landscape.

Peter Lefkowitz is Chief Counsel for Privacy & Data Protection, and Chief Privacy Officer, at General Electric. Mr. Lefkowitz previously served on the Boston Bar Journal's Board of Editors.

Assessing the Right to be Forgotten

by Daniel Lyons

Heads Up

From its inception the Internet has been disrupting business models, as once-ubiquitous brands like Blockbuster, Borders, and Encyclopedia Britannica can attest. But as more of our activities move online, society is beginning to realize how it can disrupt individual lives as well. In 2013, the tech world watched in real time as an ill-advised tweet to 170 followers began trending worldwide and cost 30-year-old PR director Justine Sacco her job while she flew from London to Cape Town, oblivious to the firestorm she had ignited below. More recently, the hack of the adultery facilitating website Ashley Madison has revealed financial information, names, and intimate details about millions of users online. Our lives increasingly leave digital fingerprints that can prove embarrassing or damaging when revealed on the network.

The "Right to be Forgotten" is the European Union's attempt to smooth these rough edges of cyberspace. The term originated with Mario Costeja Gonzalez of Spain, who defaulted on a mortgage in 1998. To foreclose on the property, the bank dutifully published a notice of default in Costeja Gonzalez's local newspaper and its online companion. Because Google indexed the site, the notice featured prominently in search results for Costeja Gonzalez's name, even years afterward. Embarrassed that his default was among the first facts the Internet recited about him, Costeja Gonzalez sued both the paper and Google under the EU Data Protection Directive, which governs the transnational flow of personal information in EU countries. He alleged that the notice infringed on his right to privacy and requested that the companies delete them.

The European Court of Justice ("ECJ") largely agreed, at least as to Google. Deciding the case on laws governing privacy and protection of personal data, the court explained in a decision dated May 13, 2014, an individual should have the right to request that a search engine remove links to information about an individual that are "inadequate, irrelevant or no longer relevant, or excessive." Importantly, the individual need not show the revelation of the information is prejudicial, because one's right to privacy should override a search engine's economic interests in listing search results. But the court was careful to note that there could be an exception if the individual's right to privacy was outweighed by the public's interest in having access to the information in question.

The *Costeja Gonzalez* opinion addresses an important digital-age problem. It is exceptionally easy to post false, misleading, or simply embarrassing personal information online, and once that information is posted, it is exceptionally difficult for the subject to remedy the situation. Costeja Gonzalez's embarrassment at a decades-old foreclosure may seem trivial. But the same dynamics plague countless others like Ms. Sacco who are forever tarred by a momentary lapse in judgment. It also affects wholly innocent victims whose private details are posted online, such as the subjects of so-called "revenge porn" sites.

Such incidents illustrate the dark side of the information revolution. The genius of the Internet is its ability to reduce information costs. Any information can be reduced to a series of 1s and 0s, replicated, and transmitted anywhere around the world, instantaneously and virtually without cost. This makes it an exceptional tool for communication and learning. But it can hurt those whose self-interest depends upon controlling the flow of information. Dictators have been hobbled by the Internet's ability to perpetuate ideas and information while connecting underground resistance groups. More benignly, record labels and movie studios have fought a decade-long war against online piracy. What copyright is to Universal, privacy is to the individual: a right to determine if and when certain information becomes public. The Right to be Forgotten is an attempt to force the Internet to respect these rights, by regulating one of the few bottlenecks in the Internet ecosystem: search engines that guide users to information online.

But the ECJ decision is an unworkable solution that risks doing more harm than good. First, the decision applies only to search engines, meaning the information in question is never actually "forgotten." Google must suppress links to Costeja Gonzalez's foreclosure notice, but the newspaper itself remains free to leave the notice available online. Second, the court's standard is astonishingly vague. The decision relies upon Google and other search engines to determine whether a particular link is "inadequate, irrelevant…or excessive," and if so, whether the "public interest" nonetheless requires the link to remain posted. The court envisions Google analysts assessing the harm that each item causes to the claimant, and carefully balancing that harm against the public's right to know a particular fact. In reality, Google faces liability for denying legitimate takedown requests but not for granting frivolous ones. This means that the company is

likely to err on the side of granting most requests rather than evaluating each request individually—especially when one considers the cost of evaluating potentially millions of such requests each year. Numerous commentators have criticized the similar selection bias evident in the Digital Millennium Copyright Act copyright takedown regime under US law, leading to the removal of a significant amount of non-infringing material.

More generally, the Right to be Forgotten decision raises broader questions about an Orwellian power to distort history. Unsurprisingly, media organizations are some of the decision's biggest critics, as they fear individuals will misuse the process to sanitize their pasts. There is some evidence to support this concern: among the first claimants was a British politician seeking to hide his voting record from the public and a convicted sex offender who wants his status kept hidden. In Massachusetts, it runs counter to the current push for broader public access to court proceedings, particularly in cases involving police officers and other public officials charged with criminal offenses. In this sense, the EU decision is only part of a broader social conversation about selective disclosure, which also includes the ethics of photoshopping models, contracts prohibiting users from posting negative reviews online, and the use of social media to present idealized images of ourselves online. As the merits of the "Right to be Forgotten" are debated in the United States, it is important that any dialogue, as well as any proposed solutions, carefully balance the rights of both the individual and society to open, accurate, and fair historical information.

Daniel Lyons is an Associate Professor (with tenure) at Boston College Law School, where he specializes in telecommunications, Internet law, administrative law, and property.

A Weak Expressio: In DaRosa v. City of New Bedford, The SJC Serves A Diluted Version Of An Established Statutory Interpretation Rule

by David S. Clancy and Marley Ann Brumme

Viewpoints

In *DaRosa v. City of New Bedford*, 471 Mass. 446 (2015), the Supreme Judicial Court made the Massachusetts Public Records Act ("PRA") a less effective tool for citizens seeking government records, just as the Massachusetts government faces sharp criticism from media outlets and good-government

groups for lack of transparency. In doing so, the SJC weakened something else: the established canon of statutory interpretation *expressio unius est exclusio alterius* (the expression of one thing is the exclusion of the other). This canon urges courts not to add "implied" terms to statutes. In its undiluted form, *expressio unius* is a strong constraint on judicial alteration of legislative enactments. But *DaRosa* dilutes it in a way that will affect future interpretation of the PRA, and maybe other statutes as well.

At issue in *DaRosa* was the status of attorney work product under the PRA. In an environmental dispute, the City of New Bedford was withholding such documents from third-party defendants. Those defendants had strong arguments for disclosure. The PRA states that all government records are public, unless they fall within one or more "strictly construed" exemptions from disclosure. *Att'y Gen. v. Ass't Comm'r of the Real Prop. Dep't of Boston*, 380 Mass. 623, 625 (1980). None of those exemptions explicitly protects documents that are attorney work product (or attorney-client privileged). And in *General Electric Co. v. Massachusetts Department of Environmental Protection*, 429 Mass. 798 (1999) ("GE"), the SJC — applying *expressio unius* — declined to add an "implied" exemption for attorney work product:

There is no ambiguity in the statute's explicit mandate that the public have access to all government documents and records except those that fall within the scope of an express statutory exception. As we said in construing an analogous statute, the open meetings law as it applied to municipal governments, G.L. c. 39, § 23B, 'exceptions are not to be implied. Where there is an express exception, it comprises the only limitation on the operation of the statute and no other exceptions will be implied.'

Id. at 805-806.

Despite all of this, the City of New Bedford won in *DaRosa*. The SJC did not go so far as to overrule *GE* and create an implied exemption for attorney work product — the Court entertained that possibility, but refrained. The practical result was largely the same, however. Reaching an issue that it did not address in *GE*, the SJC ruled that work product is almost always within an already-existing exemption anyway. That exemption — exemption (d) — covers "inter-agency or intra-agency memoranda or letters relating to policy positions being developed by the agency," except "reasonably completed factual studies or reports on which the development of such policy positions has been or may be based." *DaRosa*, 471 Mass. at 450-451. The Court held that attorney work product reflects "decisions regarding litigation strategy and case preparation" and thus amounts to development of policy. Id. at 458. (The Court acknowledged that a "reasonably completed factual study or report" would fall outside the scope of exemption (d), but hastened to add that the exemption applies to such work product if it is "interwoven" with "opinions" or "analysis." Id. at 459-460.)

To this point, *DaRosa* may seem to be merely a technical decision about the scope of one of the PRA's long-existing exemptions, with the SJC's conclusion at least plausibly supported by that exemption's text. But *DaRosa* is more than that because of the part of the decision where the SJC considered simply

adding an implied PRA exemption for attorney work product. As noted, the SJC refrained from doing so, but, in no uncertain terms, the SJC expressed a *willingness* to do so:

We no longer hold to the view declared in *General Electric* that there are no implied exemptions to the public records act, and that all records in the possession of a governmental entity must be disclosed under the act unless they fall within one of the exemptions identified [therein].

Id. at 453. This is a remarkable statement. It represents a sharp departure from *GE* and its forceful application of *expressio unius*. Moderating that departure, the SJC held that the judiciary should create "implied exemptions" only when necessary to "preserve the fair administration of justice." Id. at 454. But that malleable phrase is not a comforting restraint on a court which has so bluntly broken from *GE*.

While startling, *DaRosa*'s "we no longer hold to" pronouncement did not come from thin air. In two prior cases — *Suffolk Construction Company v. Division of Capital Asset Management*, 449 Mass. 444 (2007), and *Commonwealth v. Fremont Investment & Loan*, 459 Mass. 209 (2011) — the SJC had already departed from the rationale of *GE*. But in both cases it had done so with greater delicacy.

Suffolk was effectively a companion case to *GE*. Recall that in *GE*, the SJC was asked whether the PRA contains an implied exemption for attorney work product, and answered "no." Eight years later, *Suffolk* raised a kindred question: whether the PRA contains an implied exemption for records that are attorney-client privileged. The SJC now answered "yes" — but it managed to do so without overturning GE or announcing a general judicial power to add PRA exemptions. How so? The Court explained that the need for an implied exemption was uniquely compelling in the particular circumstances of that case. The Court took pains to establish the importance and venerability of the attorney-client privilege, which it called "common law of fundamental and longstanding importance to the administration of justice." *Suffolk*, 449 Mass. at 458. The Court presented attorney work product as a doctrine of lesser status, referring to it as a mere "tool of judicial administration." Id. at 456. Further, the SJC persuaded itself that its decision was consistent with the Legislature's intent in enacting the PRA, which, according to the SJC, could not have been to "mandate[] that public officials perform their duties without access to legal advice protected by the attorney-client privilege." Id. at 458-459.

In the 2011 *Fremont* decision, the SJC again read an implied exemption into the PRA — but again without announcing a general power to do so. This time an individual requested documents from the Office of the Attorney General which it had obtained from the defendant in a civil lawsuit, and which were subject to a protective order issued in that lawsuit. The SJC decided that the PRA contains an implied exemption for such documents. To rule otherwise, held the SJC, would raise "serious constitutional questions about the validity of that law," because protective orders are within inherent judicial powers guaranteed by Article 30 of the Massachusetts Declaration of Rights. *Fremont*, 459 Mass.

at 214. In essence, the SJC narrowed the PRA in order to save it. *Fremont*, then, involved another unique situation where the need for an implied exemption was unusually powerful.

Suffolk and *Fremont* read as the decisions of a court that would add a PRA exemption only in an extraordinary situation, and perhaps only in the two particular situations addressed in those cases. *DaRosa* goes further.

This is not to say that *DaRosa* ends a golden age of judicial restraint in which *expressio unius* was rigidly applied. As humorist James Thurber observed, "[t]here is no exception to the rule that every rule has an exception." Historically, courts did read additional terms into statutes. But they did so circumspectly, usually where satisfied by the existing text that the addition was needed to effectuate the Legislature's purpose in passing the statute: "'The maxim [*expressio unius*] will be disregarded . . . where its application would thwart the legislative intent made apparent by the entire act.'" *Halebian v. Berv*, 457 Mass. 620, 628 (2010). *DaRosa* does not suggest that same fastidiousness about separation of powers. Adding "implied" exemptions for the "fair administration of justice" is, at least presumptively, to *frustrate* the PRA's "fundamental purpose to ensure public access to government documents." *GE*, 429 Mass. at 801.

Whether *DaRosa* is ultimately good or bad for citizens seeking government records is unclear. *DaRosa*'s holding about the scope of exemption (d) impairs the PRA as a tool for accessing government records, and the Court's statements about statutory interpretation threaten further diminishment. That said, the decision arrives just as public dissatisfaction with the PRA — which the Boston Globe recently called "anemic" — has reached a boiling point. In further weakening the PRA, the *DaRosa* decision could have the ironic effect of fueling the ongoing efforts to strengthen it.

DaRosa could also have a broader impact. The decision addresses the PRA only. However, attorneys will almost certainly use it to push for judicial revisions to other statutes, and practitioners could find judges more amenable to doing so. If so, in the courthouses of Massachusetts, a strong *expressio* may start getting harder to find.

David Clancy and Marley Ann Brumme are litigators at the Boston office of Skadden, Arps. Mr. Clancy represented GE in GE v. Massachusetts Department of Environmental Protection. Skadden also represented Fremont in Commonwealth v. Fremont Investment & Loan. The views expressed in this article are their own and do not necessarily represent the views of Skadden, Arps or its clients.

Making “Good” Laws Through the Ballot Initiative Process

by Tori T. Kim

Practice Tips

From marijuana legalization to campaign finance reform to a constitutional amendment to impose a “millionaire’s tax,” citizen groups turned to the initiative petition process this year to propose a variety of public policy measures. The process, governed by article 48 of the amendments to the state constitution, allows citizens to place measures directly on the ballot as an alternative to enacting legislation through elected representatives. Twenty-three other states permit similar forms of “direct democracy.” But compared to some systems (notably, the much-criticized California model), the Massachusetts process contains comparatively strict requirements to help ensure public support before a measure reaches the ballot and to make better law.

The initiative petition process is straightforward in theory but complex in its implementation. It begins with a filing with the Attorney General’s Office, usually by the first Wednesday in August of the year preceding a biennial state election. If the petition is “certified” by the Attorney General, the petitioners must then collect thousands of signatures by the first Wednesday in December in order to present the petition to the legislature. The legislature can choose to enact the petition in the same form or take no action by the following May, and, in the latter event, the petitioners must gather more signatures in order to place the petition on the November ballot. Proposed constitutional amendments follow a similar process, except that the measure must receive at least 25 percent support in joint sessions of two successive legislatures before it can appear on the ballot. Thus, a proposed constitutional amendment submitted in 2015 could not appear on the ballot until the 2018 election year.

Article 48 also restricts the types of initiative petitions that may appear on the ballot. Among the most litigated limitations is the requirement that the petition must contain “only subjects . . . which are related or [] mutually dependent.” Art. 48, The Initiative, II, § 3. In *Carney v. Attorney General*, 447 Mass. 218 (2006), the Supreme Judicial Court construed this phrase narrowly as requiring that a measure reflect an “operational relatedness among its substantive parts that would permit a reasonable voter to affirm or reject the entire petition as a unified statement of public policy.” Id. at 230-31. The Court applied this standard to deny certification of a petition seeking simultaneously to ban the dog racing industry and to increase penalties for the inhumane treatment of dogs. Although the Carney standard did not pose a hurdle for this year’s petition to legalize marijuana for adult users, similar petitions that address one “subject” broadly, but seek to make reforms in many “operationally” unrelated areas of the law, could be susceptible to challenge.

Importantly, article 48 bars petitions that are "inconsistent" with certain rights enumerated in the Declaration of Rights. See art. 48, The Initiative, II, § 2. For instance, the Supreme Judicial Court in *Bowe v. Secretary* of the Commonwealth, 320 Mass. 230 (1946), denied certification of a petition proposing to eliminate all forms of political spending by labor unions as "inconsistent" with unions' free speech and assembly rights. Id. at 252. However, the list of rights in article 48 is limited, reflecting a compromise among the members of the constitutional convention to prospectively allow voters to "override" decisions of the state's highest court only in certain areas. The members specifically had in mind Lochner-era cases declaring social welfare legislation invalid as violating "due process" as a type that could be addressed by an initiative petition, but they identified other "concrete" and "definite" rights enumerated in the Declaration of Rights that would not be subject to the initiative petition process. This compromise impacts advocates of all political persuasions, as is evident from this year's petition to roll back corporate political spending in a manner similar to that in the Bowe petition banning labor union spending.

In addition, article 48 bars initiative petitions that make a "specific appropriation of money from the treasury of the commonwealth." While this limitation preserves the legislature's exclusive authority to make appropriations, it does not prohibit a petition from specifying how funds may be spent once they are so appropriated. For instance, this year's petition imposing an additional 4% tax on incomes over $1 million states that the revenues collected under this provision shall be spent for the purposes of enhancing public education and transportation, but specifies that such spending is "subject to appropriation." While this could mean that the legislature may decline to appropriate the collected revenues for the stated purposes, the fact that the "millionaire's tax" is proposed as a constitutional amendment—which requires at least 25 percent support of the legislature—could reduce the chance of such a result. So too may the legislature's separate duty under article 48 to "appropriate such money as may be necessary to carry such law [if passed] into effect." Art. 48, The Initiative, II, § 2; see also *Bates v. Director of the Office of Campaign and Political Finance*, 436 Mass. 144, 154-61 (2002).

Whatever one's views on the effectiveness of the initiative petition process as a means of making public policy, everyone should agree that any measure that is destined to become law should be well-drafted. A few suggested guidelines in this regard include the following:

• Research the law to ensure consistency with existing provisions. Some changes proposed by a petition could be achieved through existing law or a more modest modification of such law.

• Consider the impact of the petition on other areas of the law. For instance, a change in the definition of a term could affect every provision of the General Laws where that term is used.

• Keep the legislative language succinct. An often-cited rule of thumb is to draft a summary of the petition as it would appear on the ballot, and then craft legislative language to match the summary.

• Consider issues that may subject the law to constitutional or other challenges if the petition were enacted, even if such issues would not bar certification. For instance, laws that have retroactive effect could raise due process issues.

These suggestions could help reduce duplication and confusion in the law, while also keeping issues succinct and clear for the voters. Overall, they further the goal of making "good" workable laws, in accordance with the overriding purpose of article 48.

Tori T. Kim is Deputy General Counsel in the Executive Office for Administration and Finance. Previously, as Assistant Attorney General, she co-directed the review of initiative petitions at the Attorney General's Office.