Volume 40, Number 11
May 21, 2014

ACCESS REPORTS
FREEDOM OF INFORMATION

A Journal of News & Developments, Opinion & Analysis

In this Issue

Editor/Publisher:
Harry A. Hammitt
Access Reports is a biweekly newsletter published 24 times a year.
Subscription price is $400 per year.

1624 Dogwood Lane
Lynchburg, VA 24503
434.384.5334
FAX 434.384.8272
email: hhammitt@accessreports.com
website: www.accessreports.com

ISSN 0364-7625.

Washington Focus: Sen. Ed Markey (D-MA) and Sen. Orrin Hatch (R-UT) have proposed draft amendments to the Family Educational Rights and Privacy Act, which restricts disclosure of student information without consent, to deal with the proliferation of student data resulting from the increased use of technology. According to the New York Times, the draft legislation would require schools to maintain and make available a list of outside companies that have access to student information; give parents the right to review and correct personal information about their children collected by educational apps, online homework software, or any other school vendors; minimize the amount of data that could be transferred to companies; prohibit the use of students' information to market products or services to them; and require data security safeguards to product sensitive student data collected by companies. In announcing the draft legislation, Markey said in a news release that "the draft legislation would ensure that students are better protected when data is shared with and held by third parties, and parents are able to control the sensitive information of their children.". . .President Barack Obama signed the Digital Accountability and Transparency Act of 2014 (DATA Act) into law May 9 after the Senate passed an amended version of the legislation Apr. 10. The law requires agencies to disclose more information about federal spending and improve the quality of data.

D.C. Circuit Finds Bay of Pigs History Protected by Deliberative Process Privilege

In a decision that is defensible on the law but astonishingly bone-headed on the policy, the D.C. Circuit has ruled that the last volume of a projected five-volume internal CIA history of the Bay of Pigs operation is protected entirely by Exemption 5 (deliberative process privilege). Over the years, the CIA disclosed the first four volumes with minimal redactions, including, in response to the National Security Archive's FOIA request for Volume 4 and Volume 5 that formed the basis of this litigation, a slightly redacted

version of Volume 4. However, the agency contended that Volume 5, entitled "CIA's Internal Investigation of the Bay of Pigs Operation," was still in draft form and was protected by the deliberative process privilege. While the CIA had argued during litigation brought in 1987 by Jack Pfeiffer, the CIA staff historian who wrote the draft of Volume 5, that his draft remained under review within the agency and would surely serve as the basis for future internal deliberations for a finalized Volume 5, in the present litigation the CIA made no effort to claim the draft of Volume 5 was still under review. Rather, the agency suggested Pfeiffer's draft was rejected early on as being too polemic and was never pursued beyond its initial stages. Nevertheless, the agency insisted that the document was a draft that was both predecisional and deliberative and thus easily fell within the deliberative process privilege. At the district court level, the agency also claimed the draft was protected by Exemption 1 (national security) and Exemption 3 (other statutes), but Judge Gladys Kessler accepted the agency's assertion that it was protected entirely by Exemption 5.

Writing for the majority, Circuit Court Judge Brett Kavanaugh agreed, rejecting all the arguments put forward by the National Security Archive. The Security Archive pointed out that there had been no final version of Volume 5, suggesting the draft was the agency's final action. Noting that "we do not see the relevance of the point," Kavanaugh explained that the deliberative process privilege was meant to provide confidentiality to agency reflections regardless of whether the process resulted in a final decision. "A Presidential speechwriter may prepare a draft speech that the President never gives. A Justice Department aide may give the Attorney General a draft regulation that the Attorney General never issues. Those kinds of documents are no less drafts than the drafts that actually evolve into final Executive Branch actions. Moreover, the writer does not know at the time of writing, whether the draft will evolve into a final document. But the writer needs to know at the time of writing that the privilege will apply and that the draft will remain confidential, in order for the writer to feel free to provide candid analysis. A privilege contingent on later events—such as whether the draft ultimately evolved into a final agency position—would be an uncertain privilege, and as the Supreme Court has said, an uncertain privilege is 'little better than no privilege at all.' In short, to require release of drafts that never result in final agency action would discourage innovative and candid internal proposals by agency officials and thereby contravene the purposes of the privilege."

The Security Archive claimed that the agency had disclosed similar information in the past. But Kavanaugh noted that "an agency does not forfeit the benefit of a FOIA exemption simply because its prior decision to voluntarily release other similar information. Indeed, penalizing agencies in that way would discourage them from voluntarily releasing information, which would thwart the broader objective of transparent and open government." Kavanaugh rejected the notion that the agency had not shown any harm that would occur from disclosure. He pointed out that "the harm from release is, among other things, the harm to the candor of present and future agency decisionmaking." Nor did the age of the document affect Kavanaugh's analysis. He observed that "premature release of material protected by the deliberative process privilege would have the effect of chilling current and future decisionmaking because agency officials—realizing that the privilege evaporates over time—would no longer have the assurance that their communications would remain protected. And without that assurance, they in turn would not feel as free to advance the frank and candid ideas and advice that help agencies make good decisions." He added that "premature release of privileged information would risk embarrassment of individuals who had put forth certain ideas on the understanding and assurance that their communications would remain confidential. To avoid such an unfair bait and switch, among other reasons, the Supreme Court has recognized that a privilege designed to encourage candid communications must be durable and lasting." Finally, Kavanaugh dismissed the Security Archive's contention that the agency was required to disclose factual materials from the draft history. Kavanaugh explained that "our cases have made it clear that a draft agency history may not be dissected by the courts in the manner suggested by the FOIA requester here."

In dissent, Circuit Court Judge Judith Rogers did her best to argue that the agency had failed to make the necessary showing as to why the draft history fell within the deliberative process privilege. She started by noting that "of course, an agency does not 'waive its right to claim an exemption from disclosure simply because it has released information similar to that requested.' But at this point the agency's FOIA-related release of the draft of Volume IV appears from the record to be 'fundamentally inconsistent with [the agency's categorical] claim that release of [the draft of Volume V] would threaten the decisionmaking process of the agency.' Even assuming the draft of Volume V is predecisional, there is neither a final version of Volume V nor anything in the record to suggest that comparing the draft with the other four volumes would implicate the rationale *Dudman Communications v. Dept of Air Force* and *Russell v. Dept of Air Force* [two earlier D.C. Circuit decisions on draft histories]. The draft of Volume V. moreover, was rejected at the first stage of the agency's review process and was not part of the agency 'give-and-take of the deliberative process by which the decision itself is made.'"

Rogers complained that "the majority reads *Dudman Communications* and *Russell* as calling for a *per se* rule of Exemption 5 protection for draft agency histories." She pointed out that "it is one thing to conclude that disclosure of a draft could 'stifle. . .creative thinking and candid exchange of ideas' where it is possible to identify editorial judgments by comparing the draft and the final version, and quite another to conclude stifling could occur where there is no final version and the agency has identified the requested document as reflecting no more than the individual staff historian's view." She observed that strong criticisms of the draft made by the Chief Historian "while denying any opportunity for the work to speak for itself (even in redacted form)" also had an impact on future candor. She indicated that "these circumstances, no less than disclosure, could cause current and future staff historians to curtail the candor and creative flair that the agency values as part of its History process."

Rogers criticized the majority's apparent reliance on *Dudman Communications* and *Russell* to conclude that agency draft histories were not subject to the statutory segregability requirement. Pointing out that "the agency has provided this court no basis to conclude that all factual materials in the draft history reflects deliberative judgments" and that the district court had not conducted an independent segregability review, Rogers called for a remand of the case to the district court to conduct such a review. (*National Security Archive v. Central Intelligence Agency*, No. 12-5201, U.S. Court of Appeals for the District of Columbia Circuit, May 20)

Thoughts from the Outside…

The following is one in a series of views and perspectives on FOIA and other information issues. The views expressed are those of the author.

The Return of Practical Obscurity: The Google Spain Case at the European Court of Justice

By Robert Gellman

Last month, the European Court of Justice decided the Google Spain case involving privacy and search engines. The court's decision is like an onion in that it has many layers, and it may take some time before we can identify, let alone evaluate, all of the layers. The decision interprets the European Union's Data Protection

ACCESS REPORTS

Directive.[1] A casual observer might conclude that the decision is not important for the United States, but it will directly affect US companies, may give US citizens limited rights, and may be a bellwether for regulation of privacy and of search engines on the Internet.

Let's begin with the facts. A Spanish citizen brought the action, objecting that entering his name in Google's search engine produced links to legal notices in an online Spanish newspaper about his debts from 1998. The Spaniard was unhappy that anyone searching for his personal information would find an old and irrelevant item, long since resolved.

The original complaint objected to the newspaper's maintenance of the information and to Google's providing the link to anyone searching the plaintiff's name. The Spanish courts rejected his request that the newspaper remove or alter the old story, and that part of the case disappeared, but it sent other issues on to the European Court of Justice, the highest court for European Union law.

The European Court of Justice focused on the second part of the complaint, the one addressed to Google, or to be more specific, Google Spain. The plaintiff asked that Google Spain be required to remove or conceal the personal data relating to him so that the links to the newspaper no longer appeared in the search results. The Court upheld this request, and therein lies our tale.[2] The Court was not shy in offering broad and sweeping conclusions about both privacy and the Internet.

The Court's first holding was that the operator of a search engine collects personal information within the meaning of the EU Data Protection Directive. It did not matter that the search engine merely provided links to information that others published elsewhere on the Internet. If a search engine processes personal data in the way that search engines do, then it is a data controller under the EU Directive. Thus, a search engine must comply with the Fair Information Practice requirements for data controllers set forth in the Directive (as implemented in national law), and data subjects have rights that they can pursue with search engines. Search engines are not neutral or passive processors of data held by others. Search engines are responsible for what they do with personal information.

Next, the Court found that Google and Google Spain are establishments in Europe, so that the EU Data Protection Directive applies to them, along with all of its substantial privacy protections. This is an important jurisdictional finding. Google argued that it did not process personal data in Europe, but the Court disagreed. The Court observed that Google Spain sold advertising to support the search facility, and the processing was accomplished in that context. The Court looked at Google's and Google Spain's activities as a whole, and it refused to allow the foreign processing of data to be bifurcated from the local advertising operations in Spain. For other Internet companies located in the United States or elsewhere outside Europe, this jurisdictional finding may significantly extend the reach of the EU Data Protection Directive. Any local EU activities may bring a formerly "foreign" processor under the Directive. It remains to be seen just which local activities will be enough to do the same in other contexts.

---

[1] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, http://eur-lex.europa.eu/legal-content/en/ALL/;jsessionid=53ChTGVDjDVdFJhGgXDzpfy26K3n0QqGKrSkKC0WXvtf1QGTKWST!-1548291755?uri=CELEX:31995L0046.

[2] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Court of Justice of the European Union* (13 May 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=129807.

The Court's decision firmly established the first two points. But the Court's other holdings are less definite and call for more judgment in application, making it much harder to determine just how the new rights found by the Court will apply in practice.

Because Google is a data controller subject to the EU Directive, the Court ordered that Google, in certain circumstances, must remove links to third party webpages that have information from results based on a search by an individual's name. We are now at the practical obscurity element of the case. In other words, the collection, maintenance, and presentation of old information by search engines affect privacy interests of a data subject in a way that is actionable under the EU data protection rules.

The search engine's obligation to remove a link applies even if the original publication is lawful and is not subject to removal on privacy or other grounds. It is here that the Court recognized the importance of search engines today. In its opinion, the Court said that a search engine plays:

> … a decisive role in the overall dissemination of those data in that it renders the latter accessible to any internet user making a search on the basis of the data subject's name, including to internet users who otherwise would not have found the web page on which those data are published.

Those of us who use a search engine everyday cannot deny the importance of search engines in pointing to information that would not be available without the index that the search engine provides. For personal information, it is the search engine that allows any Internet user to pull together a profile of any individual or entity. A search engine readily available to all is a tool that is unprecedented in human existence. Whatever you think of the rest of the Court's opinion, it is hard to deny that search engines have radically changed the way we acquire information, personal or otherwise.

Under the EU Directive, privacy is not the only interest recognized, and the Directive calls for balancing of privacy with other interests. In this case, however, the Court did not find that the economic interests of the search engine or the interests of other Internet users were sufficient to outweigh the privacy interests of the data subject. However, in another case, the Court might reach a different conclusion. If the information in question were about a public figure, the public's interest would be greater, and a public figure might lose a privacy fight that a more unknown individual might win.

In the end, the Court ruled that the EU Directive allows a data subject to ask that links pertaining to him or her be removed from search engine results after a certain time if continuing to provide the links generally would be "incompatible with the directive" because the data was no longer relevant or necessary for the purpose for which they were originally collected or processed by the search engine in its role as data controller. The initial lawful and accurate publication by the original source may not be relevant to the judgment that falls on the search engine. The search engine must accept and consider a request by a data subject that links be taken down.

Implications of the Ruling

Until now, search engines have avoided privacy responsibilities as data controllers under EU privacy regulations. The Court focused on take down notices, but its ruling may go further, and search engines in Europe will have to address other privacy obligations of data controllers. Search engines may be obliged to offer different search results to users in different countries, although they could decide that personal information that must be taken down in Europe will be taken down everywhere.

Search engines will have to make decisions on take down requests by an unknown number of individuals. Those already familiar with Freedom of Information and privacy laws recognize that the processing of individual requests requires formal procedures and, eventually, clear standards that can be applied uniformly to those requests. Responding to requests will not be simple or without cost. Search engines may be held accountable for their actions by EU data protection authorities. The denial of a request may force a search engine to defend its decision in extended legal proceedings. It may take a long time before data protection authorities and courts turn the vague standards that the Court established for taking down links into useful and consistent rules.

The Court's reservation about taking down information on public figures is understandable. In practice, however, it remains to be seen how that will work. Consider a 20-year old arrested and convicted of drunk driving. At age 35, he asks that Google remove the link to the conviction, and Google takes down the link. At age 50, that individual runs for public office. Will the old information lose its obscurity? Can Google now reactivate the link or will the individual be entitled to notice and a hearing? Will it matter that the obscure story circulates freely outside of Europe?

For an individual, asking Google to remove a link may just be the start of a long process. An individual's burden may not stop with the takedown of a single link. The same information may reappear at a different link, and another takedown request may be needed. Further, there are many search engines, and the same request may have to be repeated at each one. Given Google's prominence, it may be that action by Google will satisfy most individuals.

We come at last to the Court's revival of practical obscurity. As old FOIA hands recall, in *Department of Justice vs. Reporters Committee*, the U.S. Supreme Court decided a Freedom of Information Act case involving disclosure of criminal history records ("rapsheets").[3] The FBI centralized rapsheets for individuals by collecting records from federal and state law enforcement agencies. A reporter requested the rap sheet of a particular individual.

All of the information in his rapsheet was presumptively public in police stations and court houses throughout the country. Nevertheless, the Court found that the centralized records were exempt from disclosure on privacy grounds. The decision turned in part on the practical obscurity of the records in their original location and in part on the insufficiency of the FOIA's public interest in disclosure of government activities to overcome the privacy interest of the individual.

The EU Court and our Supreme Court weighed more than just privacy in reaching their conclusions. Both Courts considered the interest of the public at large in having access to information. Under FOIA, the courts have found that the public interest in oversight of government is relevant to some disclosure decisions. In Europe, both the general public interest in access to information and the economic interest of the data controller were relevant factors. In the end, both courts reached similar conclusions, although the Supreme Court's decision was much narrower in scope than the European decision. An important difference is that the case in Europe involved a company and not a government agency. It is doubtful at best that the First Amendment to the U.S. Constitution would allow a court here to order a search engine to take down a link to truthful information otherwise accessible online.

The Supreme Court's reliance in *Reporters Committee* on the difficulty of locating and consolidating criminal history information has faded in importance because the Internet has almost completely destroyed the

[3] 489 U.S. 749 (1989), http://supreme.justia.com/cases/federal/us/489/749/case.html.

notion of practical obscurity. Rapsheets remain unavailable under the FOIA, but the obscure sources of criminal history information are not so obscure today. Data brokers collect records of arrests and convictions, and they effectively compile their own rapsheets. Some companies offer to sell you criminal history records about your neighbor or your daughter's boyfriend. Some companies want to sell you the right to suppress your own criminal history, a pointless activity given the widespread availability of the information from multiple sources.

In a recent D.C. Circuit case involving privacy, Judge Janice Rogers Brown offered a stark assessment of practical obscurity today:

> The touchstone of informational privacy—the right to be let alone—has long rested on the degree to which an allegedly private fact has been disseminated, and the extent to which the passage of time has rendered it private. Nevertheless, technological advances seem to presage the death knell for this previously workable standard. In today's echo chamber of big data, metadata, and the Internet, the once wholly forgotten memory of some unsavory, minimally broadcast misdeed is resurrected for global consumption.[4]

In Europe where privacy laws are broadly applicable to nearly everyone, the decision by the European Court of Justice revived practical obscurity. The Court recognized the central role that search engines play in the retrieval of personal information and refused to let search engines off the privacy hook. Because search engines prevent practical obscurity, they must restore it when appropriate.

There is additional context relevant to the EU decision. The EU is working on broad changes to its privacy regulatory regime. On the table is a proposal to create a formal right to be forgotten. The proposal has attracted considerable worldwide attention and debate. There seems to be some general recognition that individuals should be able to control information that they originally posted online, but there does not appear to be any consensus beyond that. The EU Court short-circuited the ongoing debate by finding a right to be forgotten in the current EU Directive, something that no one thought was there. How the decision will affect the future of EU privacy legislation remains to be seen, but it will certainly provide new fodder for lobbyists. I expect that there will be new pressure to revise the current draft privacy regulation to overturn some if not all of the Court's decision. I shall not hazard a prediction.

Nevertheless, the discussion of this issue is important. Too much personal information about everyone exists in the hands of hundreds or thousands of companies that few know about. Unlike Europe, the U.S. does not have a generally applicable privacy law, and much processing of personal information is wholly unregulated. The information industry has been able for the most part to do whatever it pleases with personal information until a scandal or horror story brings a particular activity to the front pages and compels attention by legislators. Then it becomes possible to pass a privacy law.

I do not think we need a right to be forgotten law in the United States today. We first need to apply fair information practices to more private, public, and non-profit actors. If we ever get that far – and I'm not holding my breath – there will be plenty of time to consider the right balance between personal privacy, free

[4] ACLU v. Department of Justice (D.C. Cir. 2014), http://www.cadc.uscourts.gov/internet/opinions.nsf/C093507F31A9E09485257CD3004EC615/$file/13-5064-1492222.pdf.

ACCESS REPORTS

speech, and the value of practical obscurity. In the meantime, there will be much to learn from Europe as data protection authorities struggle to implement the striking new decision of the European Court of Justice.

(*Robert Gellman is a privacy and information policy consultant in Washington, D.C. He can be contacted at www.bobgellman.com)*

Views from the States…

The following is a summary of recent developments in state open government litigation and information policy.

Connecticut

A trial court has ruled that the FOI Commission used an improper definition of the term "customer list" in finding that the Town of Trumbull did not have a proprietary interest in a list of Trumbull residents who used Trumbull's sanitary sewer system. The neighboring Bridgeport Water Pollution Control Authority signed an agreement in 1997 with the Town of Trumbull to treat wastewater from 9,600 Trumbull properties connected to Trumbull's sewer system. The Bridgeport WPCA told Trumbull officials that it was terminating the agreement and would negotiate a new agreement in its place. Trumbull disagreed and the contractual dispute is currently being arbitrated. The Bridgeport WPCA requested the names and addresses of all Trumbull property owners using the Trumbull sewer system so that it could bill them directly. Trumbull refused to release the names and addresses, claiming they were trade secrets and that they were covered by the exception for strategy and negotiation in respect to pending claims. The FOI Commission found that neither exemption applied, and Trumbull filed suit. Rejecting the strategy and negotiations claim, the court pointed out that "it is true that the names and addresses of property owners connected to the Trumbull sanitary sewer system are at the heart of the legal dispute, currently being arbitrated between Trumbull and the Bridgeport WPCA. . .That reality, however, does not transform the names and addresses into records of either strategy or negotiations with respect to that legal dispute. . .Trumbull's maintenance of a list of names and addresses of customers neither reflect the devising of plans or stratagems for their dispute with the Bridgeport WPCA nor an attempt to negotiate or compromise any claims between the parties." But the court found that the FOI Commission's use of a definition from an online financial dictionary was inadequate. The online dictionary defined a customer list as a "list of buyers from a company that a company maintains in order to continue the business relationship and promote customer loyalty." The FOI Commission found that Trumbull did not maintain the list to promote customer loyalty and added that "the [Bridgeport] WPCA and Trumbull are not competitors with respect to wastewater service; indeed, the [Bridgeport] WPCA provides a service that the respondents are unable to provide themselves." But the court pointed out that "the definition of the phrase 'customer list' imposed by the commission imports an added notion of business loyalty that is not suggested by the plain meaning of the words employed by the legislature. Moreover, such a definition is far too narrow in the context of governmental entities, particularly with reference to the commission's conclusion that such a list must be created in order to maintain loyalty to the town's services." Instead, the court observed, the standard was whether the list had independent economic value. The court noted that "like for-profit sector companies, governmental entities sell goods and services, and persons who purchase those goods and services from a governmental entity are customers of that entity for purposes of trade secret customer list analysis." The court sent the case back to the FOI Commission for application of the correct standard. (*First Selectman, Town of Trumbull v. Freedom of Information Commission*, No. HHB-CV-13-6021690S, Connecticut Superior Court, Judicial District of New Britain, May 16)

Michigan

A court of appeals has ruled that the records of the Michigan Catastrophic Claims Association, created by the legislature to indemnify no-fault auto insurers from catastrophic loss arising from an insurer's obligation to pay lifetime medical expenses, are specifically exempt from FOIA and that the trial court erred when it found a combination of constitutional and common law rights of access that allowed the Coalition Protecting Auto No-Fault Brain Injury Association of Michigan to request records from the association. After the association cited the provision in its enabling statute indicating that "an association or facility shall be exempted from disclosure pursuant to section 13 of the freedom of information act" and identified the "catastrophic claims association" as falling within that prohibition to deny the coalition's request, the coalition filed suit, claiming the association was subject to FOIA. The trial court agreed and the association appealed. The appeals court noted that "applying the plain language of [the association's enabling statute], we conclude that the trial court erred as a matter of law by holding that MCCA's records were not exempt from FOIA. Here, Subsection (4) unambiguously exempts 'a record of an association or facility' from disclosure and Subsection (6)(c) defines an 'association or facility' to include MCCA. Thus, when read together, the subsection provides that 'a record of [MCCA] *shall be exempted* from disclosure pursuant to section 13 of [FOIA].'" The court observed that "there is no ambiguity in these provisions." The appeals court rejected the trial court's finding that the reference to section 13 of FOIA meant that MCCA was able to protect records that were subject to an exemption, not that it was exempt entirely. But the appeals court noted that "nothing in § 13 of FOIA precludes the Legislature from exempting all records of a particular entity from FOIA and we will not read such a restriction into § 13." The coalition argued that a 1928 Michigan Supreme Court case suggested a common law right of access, but the appeals court pointed out that FOIA superseded any common law right of access. Relying on several federal cases in which courts found plaintiffs did not have a common law right of access beyond the rights granted by FOIA, the appeals court explained that "here, like its federal counterpart, Michigan's FOIA provides a comprehensive statutory scheme that governs requests for public records held by public bodies. . .It would be illogical to conclude that this comprehensive legislation has no effect on plaintiffs' pre-existing common law right to access MCCA's records." (*Coalition Protecting Auto No-Fault Brain Injury Association of Michigan, et al. v. Michigan Catastrophic Claims Association*, No. 314310, Michigan Court of Appeals, May 20)

New Jersey

A court of appeals has ruled that the Open Public Records Act does not authorize agencies to withhold records they decide are non-responsive to a request and that the onus to clarify the dimensions of a request lie with the agency and not the requester. The ACLU of New Jersey requested records from the Division of Criminal Justice concerning the use of Automatic License Plate Recognition technology. The Division of Criminal Justice disclosed 79 pages of redacted records with the notation that "redacted information not relevant to request." The ACLU sued, and the trial court found the agency's response appropriate because the redacted portions were not germane to the ACLU's request. The court further found that if the ACLU wanted to pursue the redactions, it should submit another request. The ACLU appealed. The appeals court reversed, noting that "the redaction protocol adopted by the DCJ here cannot stand because it is not grounded on any of the statutorily recognized exemptions to disclosure in OPRA or on a claim of confidentiality under the common law. Absent a legally recognized exception to disclosure, a citizen's right of access to public information is unfettered." The appeals court pointed out that "the fact-sensitive approach employed by the trial court here authorizes the custodian to unilaterally determine what sections of an indisputably public document falls within the scope of a request, and thereafter deny access to that record without 'attempting to reach a reasonable solution with the requestor that accommodates the interests of the requestor and the agency.' We discern no legal basis to expand the custodian's role beyond what the Legislature specifically

ACCESS REPORTS

described [in the statute]." The court added that "shifting the burden to the requestor to make a follow-up request, as suggested by the trial court here, imposes a bureaucratic hurdle that runs counter to our State's strong public policy favoring 'the prompt disclosure of government records.'" (*American Civil Liberties Union of New Jersey v. New Jersey Division of Criminal Justice*, No. A-3381-12, New Jersey Superior Court, Appellate Division, May 13)

Pennsylvania

A trial court has ruled that delinquent sewer accounts for the Borough of Lemoyne must be disclosed in response to a Right to Know Law request by the *Patriot News*. The borough refused to provide a list of delinquent accounts, arguing it was prohibited from disclosing them under the Fair Credit Extension Uniformity Act, which restricts disclosure of records for debt collection purposes. Cate Barron of the *Patriot News* appealed the borough's decision to the Office of Open Records, which found that the FCEUA did not apply and ordered the borough to disclose the records. The borough then challenged the OOR decision in court. The court recognized that the borough qualified as a debt collector, but that disclosure in response to a RTKL request did not constitute a debt collection action. The court pointed out that "Lemoyne is not seeking to release the records and, therefore, cannot be seeking to directly or indirectly take an action for the collection of the debt. In fact, Lemoyne is not taking *any* action 'in connection with the collection of a debt' but is simply responding to a valid RTKL request. The FCEUA is not intended to provide blanket protections to debtors, but, rather, is intended to protect them from oppression by the creditor. Responding to a valid RTKL request cannot be construed as oppression or harassment of a debtor." The court noted that similar information was readily available throughout the state and observed that "to deny the release of information would be to ignore the clear direction of the RTKL—all agency records are presumed to be public records—and the reality of this information age where most of this information is readily found in ordinary course and the remainder available for a RTKL fee." (*Borough of Lemoyne v. Pennsylvania Office of Open Records, et al.*, No. 13-6395, Pennsylvania Court of Common Pleas, Ninth Judicial District, May 16)

The Federal Courts…

Judge James Boasberg has ruled that the Justice Department cannot issue a *Glomar* response neither confirming nor denying the existence of records concerning a confidential source because the identity of the confidential source has been publicly disclosed. David Wilson, a Washington, D.C. gang member, was convicted of participating in a double homicide in 1998. Wilson allegedly drove the car while Antonio Roberson actually killed two passengers in a parked car. By the time Wilson was tried in 2007, Roberson had died and the government relied on a confidential informant named Bobby Capies, who testified that he had recorded Roberson confessing to the crime and implicating Wilson. Convinced of his innocence, Wilson made a FOIA request to EOUSA for records of the taped conversation between Roberson and Capies. The agency said it could neither confirm nor deny the existence of records without either consent or proof of death. Wilson appealed to OIP, which upheld EOUSA's decision. At trial, however, Wilson produced two documents referring to Capies and the wire recording, as well as Roberson's obituary. Boasberg observed that the question before him at this point was whether "DOJ's *Glomar* response [was] appropriate in this case, in light of the information that it had *already* disclosed at Wilson's trial. Put another way, does any privacy interest remain in concealing the recording's very existence, or is the metaphorical cat already out of the FOIA bag?" He then pointed out that "Capies [the informant] may indeed have a privacy interest in protecting the *content* of documents related to his cooperation here. As a confirmed government informant in Wilson's case, however, he does not have a privacy interest in concealing this status or the *existence* of Wilson-related documents." Boasberg noted that Roberson also had a possible privacy interest in the contents of the recorded

conversation, but not its existence. Boasberg explained that "he has no privacy interest in concealing that this already-acknowledged conversation took place." He added that EOUSA's privacy policy apparently did not apply when an individual was deceased. DOJ argued that "the Government should be able to avoid disclosing whether Capies was the informant involved in *this particular* recording." However, Boasberg indicated that "what the revelation of an informant's status *does* prevent is the Government's issuance of a *Glomar* response refusing to confirm or deny the fact that records related to the informant exist—particularly when those records are connected to the very case in which the informant's assistance has been openly acknowledged." Saying that ordinarily he would need to balance the privacy interest against the public interest, but "here, however, DOJ has identified no privacy interest adequate to justify its *Glomar* response. Accordingly no balancing is necessary. . .DOJ must—at a minimum—confirm or deny whether the record Wilson is seeking exists. If it does, DOJ must either turn it over or explain the reasoning behind its withholding." (*David Wilson v. United States Department of Justice*, Civil Action No. 13-2053 (JEB), U.S. District Court for the District of Columbia, May 21)

In a good example of the saying that "you can't win for losing," a magistrate judge in California has ruled that the Department of Homeland Security did not violate the court's order enjoining DHS from requiring requesters to provide consent of individuals when requesting alien files when the agency decided to withhold all the requested files entirely under **Exemption 6 (invasion of privacy)** and **Exemption 7(C) (invasion of privacy concerning law enforcement records)**. The case involved a suit brought by Gonzales and Gonzales Bonds and Insurance Agency, a company that posted immigration bonds for aliens who had been detained for possible immigration violations. Gonzales and Gonzales argued that it had filed 571 requests for alien files but that the agency failed to process them without consent. The court enjoined the agency from using the consent provision, finding it violated FOIA's requirement that agencies actually review records before determining if an exemption applied. The requests were sent back to the agency for processing and DHS ultimately decided to withhold all the alien files under Exemption 6 and Exemption 7(C). Gonzales and Gonzales argued this was a violation of the court order. But Magistrate Judge Donna Ryu disagreed. Pointing out that "the order did not address whether any FOIA exemptions could be applied to prevent disclosure of the requested documents," she noted that "contrary to Plaintiff's assertion, the circumstances here do not present a 'never ending loop' of administrative obstinacy in which an agency refuses to follow a court order on remand." She observed that "instead, they raise questions that this court has not yet considered. Because the court finds that DHS has substantially complied with its order on summary judgment, it declines to hold DHS in contempt or require DHS to pay Plaintiffs attorneys' fees in bringing this motion." (*Gonzales and Gonzales Bonds and Insurance Agency, Inc. v. United States Department of Homeland Security*, Civil Action No. 11-02267, U.S. District Court for the Northern District of California, May 8)

Judge Ellen Segal Huvelle has ruled that the Justice Department properly withheld information in email discussions that inferred the sexual orientation of certain DOJ employees under both **Exemption 5 (deliberative process privilege)** and **Exemption 6 (invasion of privacy)**. Responding to a request from Judicial Watch for records concerning the Attorney General's speech to the National LGBT Bar Association, the Office of Information Policy disclosed 66 pages in full and 166 pages with redactions. Judicial Watch only challenged the category of records identified by OIP as "discussing the drafting of the Attorney General's speech which discuss/infer the sexual orientation of certain Department employees." Although OIP claimed the redactions were justified by Exemption 6, in a footnote it also indicated that it was claiming Exemption 5. Judicial Watch argued that OIP had failed to make the Exemption 5 claim in a timely fashion. Noting that as a general rule the government was required to make all its exemption claims in the original district court proceeding, Huvelle pointed out that "here, the disputed issue is somewhat different—whether it is sufficient

ACCESS REPORTS

for defendant to raise the objection in the supporting sworn declaration and not within the four corners of the motion itself. The Court believes that it is." In a footnote, Huvelle explained that "the presence of the footnotes in the [OIP] Declaration, as well as the legal discussion regarding the deliberative process privilege in the summary judgment motion, provided sufficient notice to the plaintiff that the disputed documents were protected under *both* Exemption 5 and Exemption 6. This case does not present any sort of gamesmanship by the government, but rather, at most a lack of precision." Judicial Watch scoffed at the idea that puerile speculation about sexual orientation could be privileged. But Huvelle indicated that "contrary to the plaintiff's assertion, the government's justification for withholding parts of the e-mail chain under Exemption 5 is not based on the content of the e-mails, but rather is based on the context in which the comments were made." She agreed with the agency that the redactions were also justified under Exemption 6. She observed that "based on the very small number of individuals referenced, their identities—which plaintiff agrees can be protected—could easily be determined based on the context of the e-mails. Balancing this privacy interest against, at most, the relatively inconsequential (if not non-existent) interests identified by the plaintiff, the Court concludes that summary judgment would be justified under Exemption 6 as well." (*Judicial Watch, Inc. v. United States Department of Justice*, Civil Action No. 13-0949 (ESH), U.S. District Court for the District of Columbia, May 12)

A federal court in Maryland has ruled that the Social Security Administration conducted an **adequate search** for records of Harry Bounel when it informed Orly Taitz that it could find no record for a social security number application for Bounel. Taitz, a prominent member of the birther conspiracy convinced that President Barack Obama is not actually a U.S. citizen, made a request to SSA for Social Security applications, known as SS-5s, for Bounel, Tamerlan Tsarnaev, and Stanley Ann Dunham, Obama's mother. The agency disclosed applications for Tsarnaev and Dunham, but could not find any record that Bounel had applied for a social security number. Taitz alleged that Obama is actually using Bounel's social security number. She described Bounel as an "immigrant from Russia, born in 1890, arrived in the U.S. in and around 1912, received Social Security number in the state of CT in and around March 28, 1977," included what Taitz alleged was Bounel's social security number and insisted that because of the 120-year rule the agency was required to disclose Bounel's records without proof of death. After the agency informed Taitz that it could not find any records on Bounel, she filed suit. District Court Judge Ellen Hollander ruled in favor of the agency, but allowed Taitz to amend her complaint to include a challenge to the agency's search for Bounel's records. The agency provided a detailed explanation of its search and Hollander indicated that "without question, this Declaration satisfies FOIA's requirements; it is reasonably detailed, sets forth the types and varieties of search performed, and states that all files likely to contain responsive materials were searched." Taitz argued that the agency's response to an earlier FOIA request for Bounel's records based on his alleged social security number explaining that the agency could neither confirm nor deny that there were records on Bounel under that SSN indicated that the agency indeed did have records. But Hollander pointed out that "SSA's practice of declining to confirm or deny a match when a requester provides only an SSN and a name is eminently sensible, as it prevents the inadvertent confirmation of an individual's SSN. . .Therefore, the [earlier response letter] does not cast any doubt on SSA's later statement, in response to plaintiff's more detailed FOIA request, that it was unable to locate records for Mr. Bounel." Hollander rejected Taitz's argument that the SSA database was unreliable and that the agency should have conduct a manual search. She noted that "plaintiff's unsubstantiated allegations that the Numident has been altered or is not comprehensive are insufficient to raise a material dispute about the adequacy of the agency's search." Taitz argued that because Obama had falsified a number of his identity documents the agency's search should be questioned. Hollander disagreed, noting that "these exhibits, important as they may be to plaintiff's overarching theory about President Obama, are irrelevant to the narrow question presented in this particular case—whether SSA adequately responded to plaintiff's FOIA request for the SS-5 of Harry Bounel. In other words, irregularities in President Obama's records would not support plaintiff's claim that SSA improperly withheld Mr. Bounel's SS-5 or otherwise

failed to comply with the FOIA." (*Orly Taitz v. Caroln Colvin*, Civil Action No. ELH-13-17878, U.S. District Court for the District of Maryland, May 13)

Judge Beryl Howell has ruled that the FBI conducted an **adequate search** for records related to a search warrant that formed the basis for the arrest and conviction of Donald Paxson. Paxson requested the records and after a search of its Central Records System, the FBI indicated that it found no records. Paxson argued the records must have existed at some point, but Howell noted that "the mere fact that an agency's search failed to uncover a document that should or did exist is simply not enough to establish an inadequate search. . .[E]ven assuming *arguendo* that the plaintiff's incarceration 'proves' that a responsive search warrant existed 'at some point,' that 'does not mean that [the search warrant] remain[s] in the [defendants'] custody today or that the [defendants] had a duty under FOIA to retain the record.'" Paxson contended that a reference in records the agency found through a cross-reference search that it released even though it deemed them non-responsive indicated that Immigration and Customs Enforcement was involved and that agency should also have been searched. But Howell pointed out that "even if ICE had some involvement in the investigation of the plaintiff, this does not undermine the adequacy of the search undertaken by the defendants. Given the thoroughness of the defendants' search across the CRS, including in cross-referenced files, nothing in this reference to ICE suggests that the defendants held responsive records that would have warranted or triggered a referral to another agency." (*Donald L. Paxson v. United States Department of Justice*, Civil Action No. 13-00597 (BAH), U.S. District Court for the District of Columbia, May 14)

A federal magistrate judge in Ohio has recommended that Millie Howard's FOIA suit against the Railroad Retirement Board be dismissed because she did not ask for records but for an explanation of whether she was eligible for a widow's annuity because her deceased husband received a supplemental retirement annuity. The magistrate judge noted that "the record shows that Plaintiff repeatedly requested written explanations, legal advice, and other abstract information from the agency seeking to determine whether her husband had received a supplemental retirement annuity and, if he did not, the reason why. . .[O]n numerous occasions, USRRB explained that Mr. Howard did not receive a supplemental annuity because he did not meet the statutory and regulatory requirements to satisfy the 'current connection' standard at the time of his retirement. Notably, 'FOIA does not require agencies to provide explanations or answers in response to an individual's request for information.'" Further, the magistrate judge pointed out, Howard's attorney requested the agency to confirm whether her husband was ever paid a supplemental annuity and the agency responded by writing that "it does not appear that USRRB ever paid Mr. Howard a supplemental annuity." The magistrate judge observed that "attached to that correspondence was a screenshot from USRRB's Field Service Inquiry System database identifying, among other things, the details of Mr. Howard's annuity. Under the column marked 'SUP' for supplemental annuity, no amount was shown as paid." The magistrate judge concluded that "in light of the foregoing, the undersigned finds that Plaintiff's request falls far outside the purview of FOIA, and therefore fails as a matter of law." (*Millie Howard v. United States Railroad Retirement Board*, Civil Action No. 13-651, U.S. District Court for the Southern District of Ohio, May 14)

Judge Reggie Walton has rejected the Army's attempts to dismiss former Army Col. Malcolm Westcott's **Privacy Act** suit against the agency for removal or amendment of a letter of reprimand by the Vice Chief of Staff of the Army Reserve for negligent performance of his duties as a technical representative with respect to a $100,000 task order addition. Westcott sued after the Army Board for the Correction of Military Records rejected his claim that the allegations underlying the letter of reprimand were false. The Army claimed the court did not have jurisdiction to hear Westcott's suit for a variety of reasons. The agency argued

that opinions or judgments were not subject to correction, but Walton agreed with Westcott that he had provided considerable evidence showing that the facts upon which the letter of reprimand were based were demonstrably false. But Walton found "*removal* of the Reprimand is inappropriate because the plaintiff has not undermined the underlying basis for the judgment in its entirety." He noted that there was a combination of factors, including subjective judgments, that prevented Westcott from showing that he was entitled to have the letter removed. However, Walton pointed out that "as to whether *amendment* of any of the factual assertions contained in the Reprimand is warranted, the Court finds that genuine disputes of material facts preclude entry of summary judgment." (*Malcolm Bruce Westcott v. John M. McHugh*, Civil Action No. 09-0401 (RBW), U.S. District Court for the District of Columbia, Apr. 16)

■ ■ ■

Access Reports is no longer available in hard-copy and is available only via email in Word or PDF versions. Subscribers who have been receiving *Access Reports* in hard-copy need to provide an email address for future deliveries and identify the format in which they want to continue to receive the newsletter. Email addresses and choice of format can be sent to hhammitt@accessreports.com or by calling (434) 384-5334.