POSNER ON CLINTON — A BOOK REVIEW

DELAWARE LAWYER

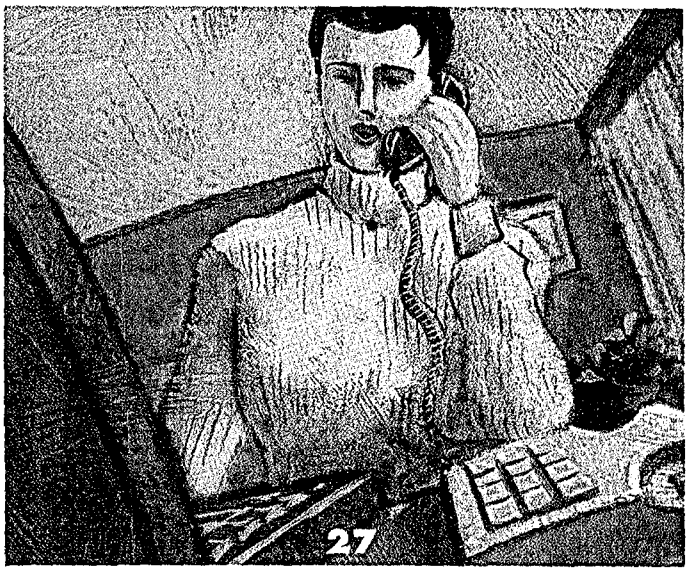
A PUBLICATION OF DELAWARE BAR FOUNDATION
Volume 18 Number 2
$3.00 Summer 2000

CONFIDENTIAL

ENDANGERED PRIVACY

CONTENTS

FEATURES



The right to privacy is not absolute but must sometimes yield to the rights or interests of others.

Cover illustration by Lynne Gangewere

DELAWARE LAWYER
A publication of Delaware Bar Foundation
Volume 18, Number 2
3301 Lancaster Pike, Suite 5-C
Wilmington, Delaware 19805

DELAWARE LAWYER
Attention: Chairman, Board of Editors
c/o **TODAY MEDIA, INC.**
3301 Lancaster Pike, Suite 5-C
Wilmington, Delaware 19805
(302) 656-8440

Editorial inquiries should be directed to:
Megan M. F. Everhart, Associate Editor
ext. 211
Requests for information about advertising should be directed to:
Chris Joyce, Project Manager ext. 221
Subscription orders and address changes should be directed to:
Today Media, Inc. at
302-656-8400

Delaware Lawyer is published by Delaware Bar Foundation as part of its commitment to publish and distribute addresses, reports, treatises, and other literary works on legal subjects of general interest to Delaware judges, lawyers, and the community at large. As it is one of the objectives of *Delaware Lawyer* to be a forum for the free expression and interchange of ideas, the opinions and positions stated in signed material are those of the authors and not, by the fact of publication, necessarily those of Delaware Bar Foundation or *Delaware Lawyer*. All manuscripts are carefully considered by the Board of Editors. Material accepted for publication becomes the property of Delaware Bar Foundation. Contributing authors are requested and expected to disclose any financial, economic, or professional interests or affiliations that may have influenced positions taken or advocated in the articles. That they have done so is an implied representation by each author.

Most of us easily define those aspects of our life that are private. In the not so distant past, that boundary was breached only by an affirmative act on our part—seeking public office, courting fame or notoriety, committing a crime, or publishing a memoir. This presumption of privacy is no longer valid. In the "Information Age" our financial, employment and medical lives are routinely translated into bits and bytes, with the potential that private information might be freely shared among or sold to interested third parties. Will our seemingly minor acts of compliance with the information demands of a modern world come with a large cost to our privacy?

The theme that runs through this issue is whether such concern is misplaced and what constraints exist on employers, doctors, financial institutions and governments to guard against disclosure. Three articles anchor this discussion, examining privacy concerns in the realms of banking, medicine and employment. We believe you will find the articles uniformly interesting, varied in tone but consistent in scholarship. An excellent article on genetic privacy and paternity, a controversy nationally, ameliorates concern about inappropriate use of the genetic material (or the test results) used to establish relationships.

As family law practitioners and attorneys for employers are well aware, the federal Office of Child Support Enforcement operates the Federal Parent Locator System. With the generous assistance of OCSE, this issue contains something new: a reference tool that explains who, how and for what purpose data on this computerized, national location network can be obtained. While we recognize that attorneys keep all back issues of Delaware Lawyer close at hand, the center spread may be easily removed and retained for quick reference.

Finally, we cannot help but note that the latest review by our resident book critic, Joel Friedlander, serves as a particularly apt end point for this edition. We thank our authors for being so generous with their time and expertise. We hope you find this edition illuminating and thought-provoking. We anticipate future discussion of this topic in these pages and elsewhere for many years to come.

Susan Friedman Paikin
Center for the Support of Families

Teresa Cheek
Young Conaway Stargatt & Taylor, LLP

CONTRIBUTORS

Sheila Hackney Bradley is a Senior Associate with the Center for the Support of Families. A graduate of Catholic University of America, Columbus School of Law, she performs various research functions for the Federal OCSE.

Eileen M. Brooks is team leader for FPLS and interstate policy at the Federal Office of Child Support Enforcement.

Teresa A. Cheek, Esquire is a partner with Young Conaway Stargatt & Taylor, LLP. She practices management side employment law and chairs the DSBA Labor and Employment Section.

Lawrence S. Drexler Between stints as a youth athletic coach, Lawrence S. Drexler, Esquire is working for a start-up internet financial services company in Wilmington.

Joel Friedlander is a partner with Bouchard Margules & Friedlander, where he practices corporate law litigation. He also serves on the Board of Editors of this magazine.

Nancy W. Law, Esquire is an associate with the law firm of Morris, James, Hitchens & Williams. Her practice focuses on the defense of health care providers in medical negligence and health care fraud and abuse litigation.

George C. Maha, JD, Ph.D., MT(ASCP) is a Director of Laboratory Operations, Department of Parentage Evaluation, Laboratory Corporation of America(tm) Holdings. A member of the N.C. Bar, he is an observer to the NCCUSL Draft Committee revising the Uniform Parentage Act, and was Vice Chair of the Paternity Committee of the ABA Family Law Section.

Dr. James M. Mason received his Ph.D. in 1972 from the University of Tennessee, Memphis, the Health Sciences Center, where he majored in pathology. An expert in immunogenet-

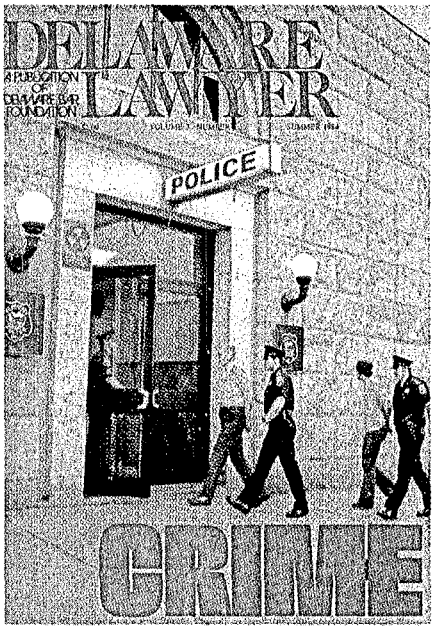
Continued on page 5

CHAIRMAN'S NOTES

The nefarious types shown below have made significant advances in their life styles. The undersigned is the (outgoing) chairman of the Board of Editors. His companion in crime, editor Thomas L. Ambro, will have ascended the Federal bench by the time you read this.

The occasion for the photograph was our 1984 issue on criminal law. We think Tom's thuggish cap adds verisimilitude to our portrayal of wrongdoers. Photography by Eric Crossan.

WEW



CONTRIBUTORS

ics, he has testified in disputed parentage and criminal cases. He is an Associate Vice President at Laboratory Corporation of America Holdings (LabCorp) where he directs the Identity Testing Laboratory.

Joseph R. Slights, III, Esquire is a partner with Morris, James, Hitchens & Williams and practices health law litigation, including malpractice defense and fraud and abuse investigations.

LETTER TO THE EDITOR

Ladies and Gentlemen:

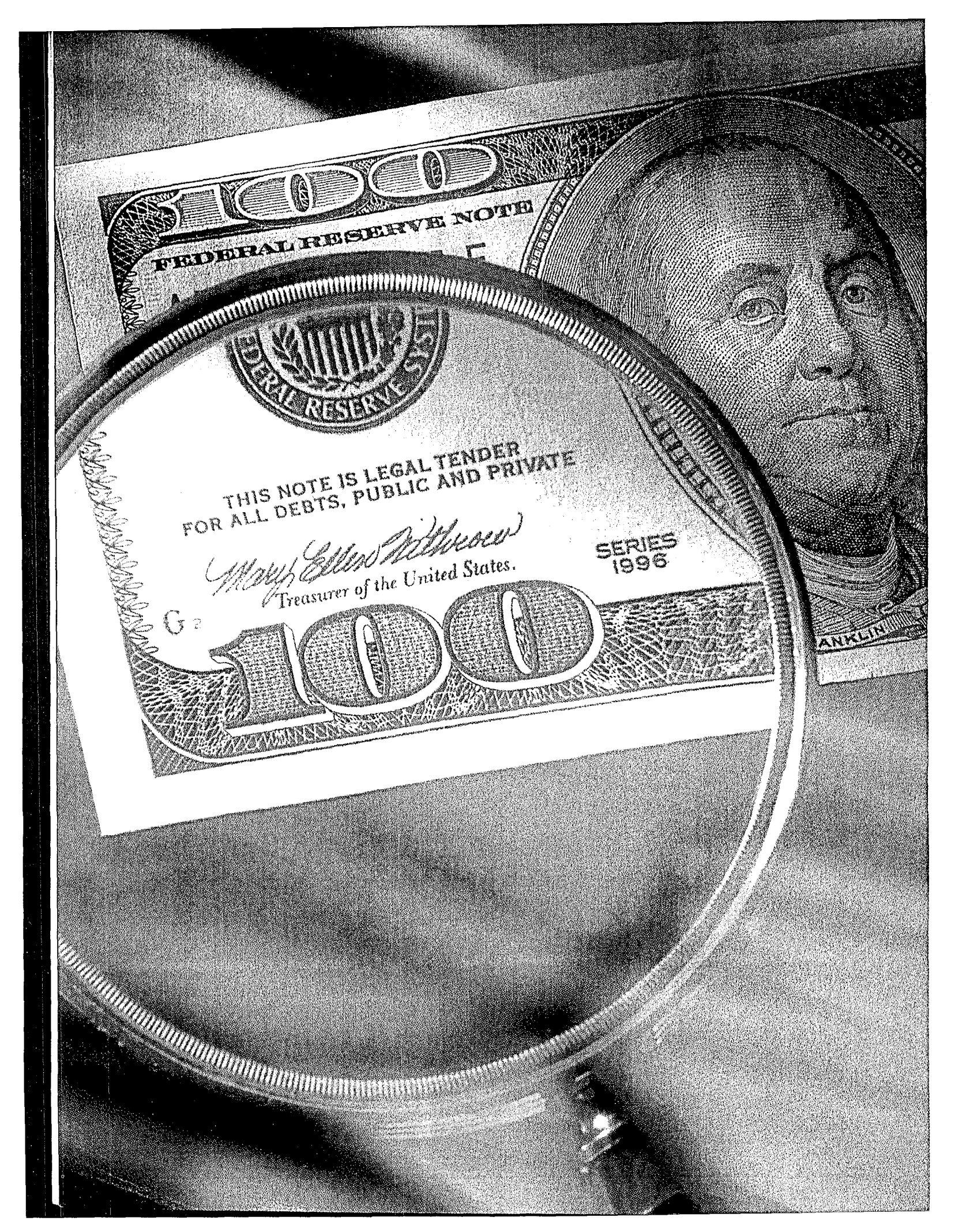
Several members of our section read with interest the article *Some Highlights of the Past Century* in the Winter 1999/2000 issue of the *Delaware Lawyer*. Unfortunately, the article contains an omission and some inaccuracies, which we believe, should not be overlooked. The article omitted the fact that Roxana C. Arsht became the first female judge in the State of Delaware when she was appointed to Family Court in 1971.

The article indicates that in 1972, Jane (Richards) Roth became the first female partner in a major Delaware law firm. In fact, Brereton Sturtevant was the first female partner in a large firm. Ms. Sturtevant became a partner in the early 1960s with the firm now known as Connolly, Bove, Lodge and Hutz. The article also indicates that Patricia W. Griffin became the first female magistrate appointed to the Justice of the Peace Court. Our research shows that Hattie E. Sylvia holds that distinction. Ms. Sylvia became a magistrate in 1962. Although this was prior to the Justice of the Peace system coming under the Delaware Court system, she remained a magistrate when that occurred in 1966.

We appreciate that had you been aware of this information, it would have been accurately reported in the article. Please do not hesitate to contact me if you have any questions.

Very truly yours,

Claire M. DeMatteis
Chair, Women and the Law Section
Delaware State Bar Association


FEDERAL RESERVE NOTE
THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES
1996

FEATURE

Lawrence S. Drexler

PRIVACY IN FINANCIAL SERVICES: "A HARD RAIN'S GONNA FALL"

The financial industry is in a state of siege over privacy. The industry is facing legislative battles over privacy in Congress and virtually every state. State Attorneys General are individually and collectively investigating various banks' information handling practices, including those of the largest banks in the country. Two banks, US Bankcorp and Chase Manhattan Bank have each entered into consent orders regarding their information handling practices. By year's end the financial industry will be incurring as much as a billion dollars in expenses annually and blanketing the country in paper related to privacy and information handling practices.

Bad Moon Rising

Before 1999, privacy was taken for granted in the banking industry. The banks' sharing of information did not give rise to significant problems or issues. Banks, as a result of understanding the needs of their customers, were able to promote billions of dollars of goods and services to consumers without a significant privacy incident. The banks, to some extent, policed the offers being extended to their customers, thereby providing a comfort level to the buyers. In this period of relative calm, the industry failed to appreciate, recognize, respond to or understand the politically charged storm clouds on the horizon. To most, privacy was an issue for the internet, telemarketers and the healthcare industry, not banks. Most banks voluntarily created privacy policies for their websites describing the banks' information handling policies. Banks believed they were acting responsibly and were not a target on the privacy radar screen.

Unfortunately, the financial industry misread the tea leaves. Banks failed to realize that because they are repositories of vast amounts of information, people hold them to a high standard. Increased competition among credit card issuers also led to the industry becoming the largest user of direct mail and telemarketing which in turn increased public animosity. Increased competition also led banks to look to alternate sources of income, including partnering with marketers to make offers of goods and services available to their clients. These offers were also communicated by direct mail and telephone, further eroding the industry's good will. The offering of third party products, which involved the legal sharing of certain consumer information with the marketers, deeply offended the commentators and legislators. Privacy was building as a key political issue transcending traditional political boundaries, attracting support from liberals, moderates and conservatives alike. The public's trust and confidence in banks was further eroded by banks' newfound reliance on fee income and other charges (e.g. late fees) to offset low interest rates. At the same time, politicians were looking for an outlet to prove their bona fides on privacy.

Eye of the Hurricane

The flash point for banking privacy became the legislation to modernize the banking regulatory scheme which had been under consideration in various forms for 20 years. The purpose of financial modernization was to amend the Banking Act of 1933 (the Glass-Steagall Act) to allow banks to affiliate with other financial service providers such as insurance and securities firms. The primary impediment to financial modernization had been a tug of war over which federal regulator would become the primary regulator of the expanded bank holding companies in the new regime. In the first half of 1999 the focus changed. A solution on the regulatory scheme appeared to be achievable. Privacy advocates began to lobby for a privacy provision to balance against one of the consequences of financial modernization: information sharing among affiliates. The privacy lobby contended that information would be used to the detriment of the consumer. The oft-cited example was that medical information made available to an insurer would thereafter be shared with a banking affiliate and shared to make lending decisions adverse to the applicant. The arguments were fueled by polling

data that showed that privacy resonated very well with voters who expressed an overwhelming concern about the impact of the information age on privacy.

The privacy ripples in the pond gained momentum, and, in retrospect, critical mass in June 1999, when the Minnesota Attorney General filed suit against U.S. Bankcorp challenging Bankcorp's information handling practices. The heart of the suit, which was quickly resolved by a consent order, was U.S. Bankcorp's sharing of information with third party marketers in a manner inconsistent with the bank's privacy policy. The bank allegedly shared information regarding credit card and savings accounts including account numbers, aggregated account use data and social security numbers. Significantly, the complaint did not allege specific harm to the bank's customers, nor was any evidence revealed that the recipient of the information used the information improperly or for a purpose other than the marketing contemplated by the information exchange. Moreover, while the complaint alleged that certain information provided may have contravened state and federal law, the heart of the complaint was failure to adhere to the bank's own privacy policy.

By fall 1999, each house of Congress had passed its own version of financial modernization. The Senate version did not have a privacy provision. The House version had a modest one. The bill went to Conference Committee at the end of the summer with U.S. Bankcorp fresh in the legislators' minds. The press began, on almost a daily basis, to focus on privacy, not just in regard to financial institutions but also concerning privacy on the internet, in healthcare, and in government. In the Conference Committee privacy quickly became a make or break issue. The debate focused on whether banks would be subject to an "opt-in" or "opt-out" regime. Under "opt-in," the customer must expressly agree to sharing information in advance of the sharing. "Opt-out" allows the consumer to elect not to participate in the sharing of information. The real difference between the regimes is what occurs in the absence of consumer information. In "opt-out," silence is consent, and begets marketing. The depth of passion on the issue is best exemplified by the fact that a number of banks threatened to scuttle a decade of work in promoting the cause of financial modernization and oppose the bill if an acceptable compromise on privacy was not achieved. In retrospect, banks may now regret their decision to compromise on privacy to save the bill.

The privacy advocates, sensing opportunity, rallied support by citing misfortunes which could occur as a result of banks having and sharing social security numbers, account numbers and certain information about credit card transactions. The privacy advocates' position was premised on several myths that were advanced in the press and back halls, to which the banks have had no meaningful opportunity to respond.

Contrary to one of these myths, credit card banks do not share details of transactions with third party marketers. To the extent the credit card is a MasterCard or Visa, the only information possessed by the credit card company is when and where a consumer shops and how much was spent. In any event, according to the U.S. Bankcorp and Chase consent orders, that type of information was not shared by banks. Rather, banks provided aggregated information regarding use of a particular account, and only that aggregated information was provided to assist the marketer in identifying prospects. Further, as a general rule, the data was used in the marketer's back room, and was not available to the actual phone representative marketing the product.

Privacy was building as a key political issue transcending traditional political boundaries, attracting support from liberals, moderates, and conservative alike.

The second myth that permeated the debate was the idea that merchants who offer goods and service by phone have access to account numbers, thereby perpetuating or facilitating fraud. In fact, the opposite is true. First, access to the account number helps combat fraud because the risk of loss in the event of misuse of the number is on the bank. Second, by creating a process in which the account number is not given over the phone, the recipient is able to distinguish between legitimate marketers and fraudulent marketers. In fact, most Attorneys General advise citizens not to give credit card numbers to telemarketers. Third, the account number does not appear on the phone representative's computer screen. Rather, the number is encrypted by the bank and generally unencrypted by computer after a transaction has been authorized by the consumer.

Finally, the privacy provisions were motivated by an unspoken yet more formidable issue: No one likes to receive phone calls at dinner-time offering a wide variety of products, most notably credit cards or products associated with credit cards. As competition among credit companies became more intense, telemarketing increased, causing a simultaneous increase in ill will towards credit card banks. Thus, the debate was shaped as much by annoyance as anything else. The public's low opinion of credit card banks severely hindered the bank's ability to educate Congress on these issues.

The uproar that followed the U.S. Bankcorp litigation in Minnesota led to enormous pressure on Congress to "do something on privacy." The need for quick action, low public perception of banks and political expedience combined to make the privacy an above-the-fold issue. Thus, the Conference Committee met under the most unusual of conditions. The success of the financial modernization effort which was shaped by five decades of debate, would hinge on four months of Conference Committee negotiations turning on privacy. The banking industry did not have the time or forum to counteract the passion created by perceived threats to privacy. Rather, negotiations began with political horse trading. Nonetheless, the financial industry had a hand in creating the rules of the privacy road and so it cannot be without some blame for the result. In this environment, it makes perfect sense that the final privacy provisions would aspire to noble and lofty goals of informing consumers and providing choices but lack practical grounding.

Wake of the Flood

In October 1999, Congress enacted

and the President later signed into law the Gramm-Leach-Bliley Act amending the Banking Act of 1933 (Glass-Steagall Act) to permit banks to affiliate with other financial institutions. The final version contained privacy provisions (Title V) premised on notice and the opportunity to opt out of the sharing of information. Title V requires 1) that each financial institution have and publish its policies on information handling; 2) that the privacy policy should be readily available to the public and distributed to customers; and 3) that to the extent information provided to the bank is used for a purpose other than that for which it was provided to the bank, the consumer should be able to opt out of sharing information. Specifically, Gramm-Leach-Bliley requires each bank's privacy policy to include policies and practices relating to:

1) Information provided to affiliates and non-affiliated third parties other than agents of the bank (Sec. 503(a)(i)):

a) Categories of persons to whom information may be disclosed (Sec. (503(b)(i)(A)); and

b) Policy related to former customers (Sec. 503 (b)(i)(B)).

2) The categories of information collected (Sec. 503 (b)(2)); and

3) Its policies to protect confidentiality and security (Sec. 503(b)(3)).

Aside from setting forth these standards, much of the detail was left to the combined, or if they choose individual, efforts of the primary regulators of the financial world, the Office of the Comptroller of the Currency (OCC), the Board of Governors of the Federal Reserve (the Fed), the Federal Deposit Insurance Corp. (FDIC), the Office of the Thrift Supervision (OTS), the National Credit Union Administration, and the Securities and Exchange Commission (SEC). The Federal Trade Commission is empowered to regulate any financial institution not otherwise regulated. Finally, state insurance regulators were tasked with creating regulations for insurance companies. The federal agencies are working together to draft implementing regulations. The draft regulations were circulated for comment in February 2000. Comments were due March 31, 2000. Unless the present deadlines are extended, the regulations will become effective on November 12, 2000. Unfortunately, the privacy language in Gramm-Leach-Bliley and the regulatory zeal that has followed have resulted in proposed Regulation P. Unless it is altered after the comments period, Regulation P will not advance privacy and choice, but rather, will simply be anti-consumer, anti-environment and anti-business.

The simple premises of notice and opt-out have mushroomed into a complex statement of information handling practices. Gramm-Leach-Bliley prohibits sharing of non-public personal information unless the consumer is given notice and the opportunity to opt out of the sharing. The Act further requires that each financial institution have a privacy policy and distribute it to its customers at least once a year. In addition, the policy must be given to every customer at or before the time the person becomes a customer.

The Devil is in the details and Congress delegated the details to the combined efforts of the regulators. The regulations they have proposed would make the privacy policy statement onerous and extremely detailed. The statement would include:

1) categories of non-public personal information collected, including examples;

2) categories of non-public personal information that the bank discloses, by source of information, including examples;

3) categories of affiliates and non-affiliated third parties to which non-public personal information is disclosed, other than entities processing and servicing transactions;

4) categories of information disclosed regarding former customers and the categories of non-affiliated recipients of the disclosures;

5) categories of information provided to service providers and joint marketers and categories of service providers and joint marketers with which the bank has contracted (not covered by another exception);

6) a statement of policies and practices to protect information security including an explanation of the measures employed by the bank to protect against reasonably anticipated threats and hazards; and

7) the institution's policy regarding opting out of sharing of information.

In place of the simple notion of notice and opportunity to opt out, banks would be required under Regulation P to create complex statements revealing vast amounts of information about the financial institution's practices. Given the purpose of the privacy policy, the legislative and regulatory requirements, and the legal consequences (litigation and/or government action), each privacy policy will likely be a dense, lawyer-written document that is neither plain nor simple. This complicated disclosure would be expensive and not reasonably calculated to promote privacy.

Snowbound

Regulation P would unleash a torrent of paper that would result in consumers receiving hundreds of pages of legal notices, each packaged differently, in the last two months of 2000 and annually thereafter. Banks and insurance companies would not be the only companies sending out privacy policies, since financial institutions are broadly defined in Gramm-Leach-Bliley as "any institution engaged in financial activities described in Section 4(k) of the Bankholding Co. Act of 1956." Section 4(k) defines financial activity as traditional banking activity, insurance activity and matters closely related to such activities as well as matters "complementary" to a financial activity. The Federal Trade Commission's commentary on the proposed regulation states that entities that may be subject to Gramm-Leach-Bliley privacy requirements include: stores that issue credit cards to their customers, appraisers, career counselors for employees in financial occupations, digital signature services, courier services, real estate settlement services, manufacturers of computer software and hardware and certain travel agencies.

Upon the Gramm-Leach-Bliley privacy provisions' effective date, a family with one car loan, a house with a mortgage and a life insurance policy will receive at least 5 privacy policies: one from the car loan lender, one from the mortgage lender and one each from the life, automobile and homeowners insurance carriers. The number quickly multiplies when credit cards, loans, other insurance and other related activities are factored into the mix. Assuming an average of 10 existing relationships for each of the 103 million U.S. households, more than one billion annual notices will be distributed in the last 6 weeks of 2000 and then annually thereafter. Your postal carrier thought the Christmas rush was bad.

Commentators Peter Gray and Duncan MacDonald suggest that the average person will receive 40-50 notices a year resulting in up to 3.5 billion notices costing as much as $1.25 billion. This is before the associated administrative expenses are factored in, driving expenses to over $2 billion a year. Obviously, this surge of paper will in and of itself have a significant impact on the environment. It is difficult to conceive that anyone will read the material. A society that routinely avoids

reading documents such as leases and loan documents is unlikely to read privacy policies. When did you last read a rental car agreement? Rather than becoming more sensitive to privacy, people will become jaded and indifferent to privacy concerns.

No Shelter from the Storm

The rigid and detailed privacy provisions of Regulation P will hinder business development. The proposed regulations require notice of changes to the privacy policy before the changes become effective. This requirement can be anti-competitive and retard growth and consumer access to products to the extent it may inhibit a financial institution from offering a product or partnering with another financial institution because of the need to make an amended disclosure even if the new venture is entirely consistent with existing policy although not expressly described and/or the consumer would not have the right under the law to opt out. For instance, to the extent two financial institutions agree to a joint marketing program for a new product, it is likely that the program will not be able to commence until both provide amended privacy policies. The regulations thus will create a cumbersome process which will be at least a hurdle if not a road block to bringing new and competitive products to market.

Crawling from the Wreckage

I propose a simple alternative. Require each financial institution to maintain a complete privacy policy as required by Gramm-Leach-Bliley. The privacy policy must be readily available and provided free of charge upon request. It should be a dynamic document, allowing change to promote competition and flexibility on privacy. Require an annual notice to be sent to each customer whose information could be shared with affiliated companies or unaffiliated third parties. The brief notice would in summary form describe the information practices of the institution and the options available. The notice would also include a convenient method for the consumer to opt out. An information sharing notice currently in use by one financial institution reads as follows:

> Bank does not share information about you or your Account, except 1) to process your transactions; 2) to service and handle repayment of your

Account; 3) to update your credit reports; 4) to help our affiliates serve you; 5) to assist carefully selected merchants who offer you goods and services that we believe may be of interest to you; 6) to respond to a court order or similar legal request; 7) to further a program with a partner; or 8) to implement special program features you have approved (e.g. mileage and other rewards programs). When we share information we only share information that is appropriate to accomplish the particular task. We maintain your information in accordance with strict security standards and require the same of anyone we use to administer our relationship with you. We require those entities never to use the information we provide for other purposes. When we arrange an offer of goods or services, we disclose only your name, address and how to contact you but never your Account number. We provide your Account number to the merchant only when you make a purchase. If you do not want to receive offers from non-affiliate merchants, just write us at _____ _____ and be sure to include your name, address and Account number. _____'s complete Privacy Policy is available on the Web at http://_____.

Information may only be shared with unaffiliated third parties, not otherwise covered by one of exception in Gramm-Leach-Bliley, if the opt out notice has been provided to the consumer in the prior 12 months and the customer has had a chance to chose to opt-out. The notice would also include information to allow the consumer to obtain the full policy. Thus, notices would only come from entities which seek to avail themselves of the Section 502 opt out. The truncated notice provides consumers with options that impact their day-to-day lives and gives consumers control over contacts with both the bank and third party marketers. The privacy policy allows the regulators to examine the financial institution's policies and ensure that information is being handled appropriately in terms of both the consumer and the financial institution's safety and soundness.

Finally, this solution creates an environment in which the information handling practices of financial institutions can be an area of differentiation and competition which can be meaningful to the consumer. ◆

George C. Maha
James M. Mason[1]

GENETIC PRIVACY AND PATERNITY TESTING

Concern for genetic privacy is a new and highly emotional fear sweeping the country.[2] Unfortunately, such fear has begun to spill over into genetic testing in paternity and criminal issues. For example, the State of New York recently amended its statute governing the felon database, making it a felony to disclose a person's DNA record.[3]

Paternity testing and felon databasing are non-health related activities.[4] The DNA testing results from paternity evaluations do not have diagnostic or prognostic value in health or employment. Even the older genetic tests, such as HLA or blood types,[5] while having medical uses, were not by themselves diagnostic or prognostic indicators of health. As such these genetic tests do not come under the Delaware Health Information Network (DHIN).[6] Yet, concern over potential use of the test results and the genetic material gathered to conduct such tests has led to legislative action in some jurisdictions.

Discussion about the potential for misuse of test samples and results has increased over the past several years due to two related circumstances: the increased use of paternity testing in the national child support enforcement (IV-D) program; and the pending revision of the Uniform Parentage Act. In the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA, also known as the Welfare Reform Act) Congress tied continued receipt of federal child support funds to enhanced paternity establishment services by the states.[7] These federal requirements have complimentary provisions: increased use of voluntary paternity acknowledgments[8] and streamlined access to genetic testing to determine parentage. It is the latter "quasi-mandate" that is relevant here. The state agency providing services under Title IV, Part D of the Social Security Act (here the Delaware Division of Child Support Enforcement) now has authority to order genetic testing in a case where the agency is providing services.[9]

As to the Uniform Parentage Act, the National Conference of Commissioners on Uniform State Laws will consider passage of a totally revised UPA at its meeting this summer. The Act has expanded its genetic testing article from 1 (in the 1972 version) to 10 to accommodate the wide use of testing to establish relationships.[10] Although the UPA addresses the genetic privacy issue in its most recent draft, a discussion of the appropriateness or efficacy of legislative approaches taken by other states is timely.

By way of example, Michigan's legislature has recently modified their paternity statutes, with the apparent motive of protecting "genetic privacy."[11] We believe, for the reasons discussed below, that Michigan's paternity legislation is an example of overreaction to genetic privacy concerns, resulting in a statute that actually provides less protection where there are real documented concerns. When enacting genetic privacy statutes, members of Delaware's legislature should be careful not to make the same mistakes as Michigan.

Michigan's first mistake was in the definition section of their paternity statute. Here, they provide a definition of "DNA identification profile"[12] and "DNA identification profiling."[13] While the definitions are correct, these are not terms normally applied to paternity testing. In the scientific community these terms are generally used to refer to DNA testing done for felon databases. The testing for felon databases, generally stored in the FBI's CODIS system (Combined DNA Identification System) or a state's equivalent, is different from that used for paternity testing. The results of paternity tests are usually referred to as "phenotypes" or "genetic markers."[14] The use of the term "DNA identification profiling" is misleading as it could give the impression that persons are being tested for the CODIS system, which is not what is done in paternity testing. The felon database requires the testing of certain genetic markers using specific technologies. Paternity testing may use some of the same genetic markers, but the paternity laboratories do not have a mechanism to enter the results, and under the statutory systems regulating CODIS

systems it would be extremely difficult to enter outside results. Thus, for those concerned about their genetic testing, the term "DNA Identification Profiling" may cause unnecessary apprehension over routine paternity testing. Paternity test results are not maintained in a national database and there is no plan to create one. These tests are generally not health care related, so they are not part of one's medical history.

In a strange statutory scheme the Michigan statute provides a definition of a "summary report."[15] While this section generally reflects current practice, it leaves out the genetic markers[16] and "prior probability." The prior probability is used in the calculation of the probability of paternity. Both the prior probability and the genetic markers are required by all accreditation agencies including the American Association of Blood Banks, the American Society for Histocompatibility and Immunogenetics, and the New York State Department of Health.

There are many problems in leaving the genetic markers off of the report. The most common practical problem arises where a tested party wants the report reviewed by another expert, and the expert has nothing to review. Given that many persons tested cannot afford an attorney to file discovery motions to get the results from the laboratory, this requirement is puzzling. Even if the party has an attorney who wants a quick review to see if it is necessary to obtain a discovery request, the expert still has nothing to review. On a day-to-day basis, laboratory errors may be detected because the genetic markers are on the report and other experts can easily review them. For example, an outside expert may determine that there is insufficient evidence to conclude that a man is excluded or that if the mother and child are switched the exclusion goes away, indicating a possible error in the testing or in the chain of custody.

These are practical concerns that do occur, as opposed to hypothetical genetic privacy concerns about a test that does not have diagnostic or prognostic value in health or employment. A valid concern might be that somehow someone might take the results and compare them to someone else. For example, President Clinton's DNA genetic markers from the stain on Monica Lewinski's dress were published in the popular press. Theoretically, one could use the genetic markers to compare to some mother and child's result for the same tests and make an assertion of paternity. Aside from the fact that the tests used in President Clinton's forensic DNA analysis are not commonly used in paternity testing, the expectation is that a man who is not the father will be excluded. The chance of false inclusion is extremely low. Even if this happened, the opposing person could seek additional testing and pursue the privacy violation using current applicable laws.

Such sensational cases are extremely rare and it is unrealistic to expect the publication of a paternity test. The second problem is that the individuals involved have to actually be tested using the same tests. As there is no national database of paternity testing results and the tests used vary from laboratory to laboratory, obtaining and matching the results is not realistic.

Adding confusion to the issue, in a later section of the Michigan statute the results of the "DNA identification profile" and the summary report are served on the alleged father and mother.[17] Whereas the legislature provides a specific definition of a summary report that excludes the genetic markers, it now appears that some other unspecified report is needed. Only the summary report is filed with the court. But later the statute provides for admission of the "DNA identification profile" and the "summary report" if there is no objection. As the unspecified DNA identification report is not filed with the court, how it gets admitted is puzzling.

The most unusual requirement is the destruction and expunging of records. In a apparent attempt to protect the genetic privacy of men (but not women and children), the statute provides for the destruction of the excluded man's sample and expunging of all records of the excluded man's testing.[18] This requirement is contrary to all national standards that require the maintenance of records for at least five years.[19]

There are excellent public policy reasons for keeping both the samples and records of the excluded man. The immediate destruction of the records and samples of excluded men will, in fact, cause a disservice to the very persons the law seeks to protect. Specifically, there are cases where the excluded man turns out to be an imposter. By destroying the records, the laboratory, prosecutor, the mother or other interested person cannot properly investigate the potential false exclusion. Under this statutory scheme, the records would most likely be destroyed before anyone could investigate.

Another problem that has arisen are cases where the report, issued as an exclusion, is altered by the mother (or another person) so the man appears included as the biological father. We know of several cases where these altered reports made it through the court systems causing men who were actually excluded to pay child support. Without laboratory records, these alterations would not be detectable and could not be investigated. Here men are actually harmed by Michigan's scheme to protect their genetic privacy.

It also harms the laboratory, which could not defend itself against a malpractice suit, as it would have no records.[20] An exclusion is the expected result if there is an error either in chain of custody or in the testing. By destroying the samples and records it becomes impossible not only to investigate possible imposters, forgeries and altered reports, but also the laboratory cannot investigate to see if a potential error has occurred. We cannot see any rational reason to treat an excluded man's samples and records any differently from those of a man (or of a women or child) who has not been excluded. Further, this section does not discuss what the laboratory is supposed to do if the alleged father is tested with two children and one child is excluded and one child is not excluded. Does the laboratory destroy all his records or just the fact he was excluded as the father of one child? The national standards for record retention were developed to provide protection for all tested persons and as such it is unfortunate that Michigan's rush to genetic privacy provides a lesser standard for its citizens.

Is there a reason to fear misuse of the samples? Of the expressed concerns, this is at least rational, although the authors could not find any example of a paternity laboratory performing testing other than paternity testing or releasing identifiable genetic samples to another laboratory without authorization. This fear may be sensibly handled by prohibiting a laboratory from transferring the samples or performing unauthorized testing. An approach might be statutory language such as "An individual commits a [appropriate level misdemeanor] if the individual intentionally releases an identifiable specimen of a person for any

Continued on page 32

FEATURE

Eileen M. Brooks
Sheila Hackney Bradley[1]

FEDERAL PARENT LOCATOR SERVICE:

ACCESS AND PRIVACY

In the United States today, nearly one-third of all children are growing up in single-parent homes. Of all families owed child support, only half receive the full amount due, and a quarter of these families receive no support. The goal of the child support enforcement program, established in 1975 under Title IV, Part D of the Social Security Act,[2] and thus referred to as the IV-D program, is to ensure that children receive financial and emotional support from both parents.

Designed as a Federal, State, and local partnership, the national child support program involves 54 State and territory programs, each with its own unique laws and procedures, in addition to the federally prescribed laws and procedures. The program is usually administered by State and local human service agencies, often with the help of prosecuting attorneys and other law enforcement officials as well as officials of family or domestic relations courts. The Division of Child Support Enforcement, Department of Health and Social Services is the Delaware IV-D agency.[3] The Office of the Attorney General provides legal representation.

At the Federal level, the Department of Health and Human Services provides policy guidance on Federal mandates, technical assistance and funding to the States through the Office of Child Support Enforcement, which also operates the Federal Parent Locator Service (FPLS). The FPLS is a computerized, national location network designed to assist States in locating non-custodial parents, putative fathers and custodial parties for the establishment of paternity and the establishment, modification and enforcement of child support obligations. Under specified circumstances, information from the FPLS may also be available in parental kidnapping cases, as well as custody and visitation matters. The FPLS also identifies support orders or support cases involving the same parties in different States.

The FPLS was dramatically expanded in scope and utility by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PRWORA).[4] Developed in cooperation with the States, employers, Federal agencies, and the judiciary, the expanded FPLS now includes two new databases: the National Directory of New Hires (NDNH)[5] and the Federal Case Registry (FCR).[6] These databases reside on the Social Security Administration's mainframe computers in Washington, D.C. The FPLS is also linked to databases maintained by Federal agencies such as the Internal Revenue Service, the Department of Defense, and the Department of Veteran Affairs.[7]

The following chart titled *Requests for Information from the Federal Parent Locator Service* identifies "authorized persons" who may request available information from the FPLS and the "authorized purposes" for which these entities may obtain information as identified in the sections 453 and 463 of the Social Security Act. With limited exceptions, all requests for FPLS information must be made through the State IV-D agency's State Parent Locator Service. The chart may be easily removed from this volume and retained as a quick reference tool.

The FPLS system provides confidential information that requires protection from unauthorized disclosure. There are safeguards built in at the Federal level to ensure the privacy of FPLS data and to prevent unauthorized access to the data. Each State's statewide automated child support enforcement system must be capable of exchanging information with the FPLS and each State's IV-D agency must have in effect safeguards on the

Continued on page 21

Requests for Information from the Federal Parent Locator Service

The Federal Office of Child Support Enforcement in the Administration for Children and Families, Department of Health and Human Services, operates the Federal Parent Locator Service (FPLS) that includes the National Directory of New Hires (NDNH), that became operational October 1, 1997 and the Federal Case Registry of Child Support Orders (FCR), that became operational October 1, 1998. The NDNH database contains new hire information on employees, quarterly wage data on employees, and information on unemployment compensation benefits. The FCR database contains information on all individuals subject to a child support order established or modified after October 1, 1998 and information on all individuals involved in cases where the state is providing child support services pursuant to title IV-D of the Social Security Act (the Act), whether or not an order has been established. The FCR contains information with respect to each case and order maintained by the state child support agencies in their state case registries.

The purposes for which information in the FPLS may be requested are specified in §453 and §463 of the Act.

Requests for Information for Child Support Purposes

Who May Request	Why	Information Available
Agent/attorney of a state with authority/duty under the state IV-D plan approved by OCSE to collect child support. (§453(c)(1)) Court with authority to issue an order for child support, or to serve as the initiating court in an action to seek a child support order, or any agent of such court. (§453(c)(2)) Resident parent, legal guardian, attorney or agent of a child not receiving title IV-A benefits. (§453(c)(3))	Establish parentage, establish the amount of, modify or enforce child support obligations. (§453(a)(2))	Information (including SSN, address, and name, address and federal employer identification number of employer) on, or facilitating the discovery of, the location of any individual: ◆ who is under an obligation to pay child support, ◆ against whom a child support obligation is sought, ◆ to whom a child support obligation is owed, or ◆ who has or may have parental rights with respect to a child. Information on the individual's wages, other income from and benefits of employment (including group health care coverage). Information on the type, status, location and amount of any assets of, or debts owed by or to the individual (asset information is currently derived from IRS and is available only to title IV-D agency). (§453(a)(2))

Requests for Information for Title IV-B & Title IV-E Purposes

Who May Request	Why	Information Available
State agency administering a program under title IV-B or title IV-E of the Social Security Act. (§453(c)(4))	Locate an individual who has or may have parental rights with respect to a child. (§453(a)(2)(A)(iv))	Same as for child support purposes. (§453(a)(2))

Requests for Information for Child Custody, Visitation & Parental Kidnapping Cases

Who May Request	Why	Information Available
Agent/attorney of a state with authority/duty under state law to enforce a child custody or visitation determination. State must have a written agreement with the Secretary of DHHS. (§463(d)(2)(A))	Make or enforce a child custody or visitation determination. (§463(a)(2))	Most recent address and place of employment of parent or child. (§463(c))
Court with jurisdiction to make or enforce a child custody or visitation determination, or any agent of such court. (§463(d)(2)(B))	Make or enforce a child custody or visitation determination. (§463(a)(1))	
Agent/attorney of the U.S. or a state with authority/duty to investigate, enforce or prosecute the unlawful taking or restraint of a child. (§463(d)(2)(C))	Enforce any federal or state law regarding unlawful taking or restraint of a child. (§463(a)(1))	
U.S. Central Authority (under Hague convention on international child abduction). (§463(e))	Locate any parent/child on behalf of an applicant to Central Authority, Department of State in a child abduction case. (§463( ))	
U.S. Attorney General (Office of Juvenile Justice & Delinquency Prevention). (§463(f))	Enforce any state/federal law with respect to unlawful taking or restraint of a child, or make or enforce a child custody, or visitation determination. (§463(f))	

Requests for Information for Other Purposes

Who May Request	Why	Information Available
Secretary of Treasury (§453(h)(3) and (i)(3))	Administration of the specified federal tax laws. (§453(h)(3) and (i)(3))	Federal Case registry data or National Directory of New Hires data, depending on purpose for which data is sought. (§453(h)(3) and (i)(3))
Social Security Administration (§453(j)(1))	Verification of information supplied to the Secretary of DHHS. (§453(j)(1))	The name, social security number and birth date of such individuals and employer identification number. (§453(j)(1))
Social Security Administration (§453(j)(4))	Administration of Social Security programs. (§453(j)(4))	NDNH data (§453(j)(4))
Secretary of Education (§453(j)(6))	For collection of the debts owed on defaulted student loans, or overpayment of grants, made under title IV of the Higher Education Act of 1965, after removal of personal identifiers. (§453(j)(6)(D)(i) and (ii))	Matches to compare NDNH information and information on individuals who are borrowers of loans that are in default or who have an obligation to refund an overpayment on a grant under title IV. (§453(j)(6)(A)(i) and (ii), §453(j)(6)(C)(i), (D))
Researchers (§453(j)(5))	Research purposes found by the Secretary of DHHS to be likely to contribute to achieving purposes of the titles IV-A/IV-D programs. (§453(j)(5))	Data in each component of the FPLS for research purposes found likely to contribute to achieving the purposes of titles IV-A and IV-D but without personal identifiers. (§453(j)(5))
State IV-A agencies (§453(j)(3))	Administration of title IV-A program. (§453(j)(3))	Compare the information in each component of the FPLS determined to be effective in assisting states in their operation of the title IV-A program. (§453(j)(3))

How to Request Information

1. Authorized state agencies, courts and private parties must request FPLS information through a State Parent Locator Service (SPLS) after paying an established fee in accordance with §453(e)(2). The state PLS will contact the FPLS and return the information provided to the requestor.

2. Authorized federal entities may request FPLS information by contacting the Federal Office of Child Support Enforcement directly. Information is generally provided under the terms of an agreement.

3. The SPLS must distinguish requests for purposes of child custody, visitation determination or in cases of the unlawful taking or restraint of a child from requests made for child support purposes, so that the FPLS may return only authorized information.

Exception to Information Release

Information from the FPLS may not be disclosed:

1. Where the disclosure of information would contravene the national policy or security interests of the United States or confidentiality of census data (§453(b)(2)); or

2. If the state has notified the Secretary that it has reasonable evidence of domestic violence or child abuse and the disclosure of such information could be harmful to the parent or the child of such parent (§453(b)(2)); information can only be disclosed to a court or an agent of a court upon further request. If, upon receipt of the information from the Secretary, the court determines that disclosure to any other person of that information could be harmful to the parent or the child, the court and its agents shall not make any such disclosure. (§§453(b)(2)(A), (B) and 454(26)(D), (E))

References are to sections in title IV-D of the Social Security Act, Pub. L. No. 93-647, 88 Stat. 2337 (1974) (codified as amended at 42 U.S.C. §651 et seq (1999)).

The Federal Office of Child Support Enforcement may be contacted at:
FPLS ACCESS@OCSE.CONTR@ACF.WDC

BROOKS/BRADLEY

continued from page 16

integrity, accuracy, access to, and the use of data in the automated system.[8] Additionally, if a State has placed a Family Violence Indicator in its State Case Registry on a participant, the FPLS will not release information on that parent or child except to a court or an agent of a court of competent jurisdiction.[9]

All partners in the child support community recognize that ensuring the security of FPLS data is vital to the success of IV-D child support programs, and for protecting the privacy of American citizens.

FOOTNOTES

1. The accompanying chart was designed by William Reese, Associate, Center for the Support of Families, based on content provided by the Federal Office of Child Support Enforcement.

2. Pub. L. No. 93-647, 88 Stat.2337 (1974) (codified as amended at 42 U.S.C. §651 *et seq* (1999)).

3. All requests for locate services should be made through DCSE's customer service unit: 577-7171 (New Castle County); 739-8299 (Kent County); or 856-5386 (Sussex County).

4. Pub. L. No. 104-193, 110 Stat. 2104 (codified as amended in scattered sections of 42 U.S.C.) (1996), (popularly known as the Welfare Reform Act). An original component of the IV-D program, the FPLS was established to provide address and Social Security Number (SSN) information to State and local child support enforcement agencies seeking to locate noncustodial parents. In response to locate requests submitted by State IV-D agencies, OCSE accessed its external locate sources to search for the requested information.

5. The NDNH is a central repository of employment and wage data from the State Directories of New Hires and the State Employment Security Agencies (SESA) and Federal agencies, operational since October 1, 1997. The National New Hire Reporting Program requires all employers to report information on newly hired employees to a State Directory of New Hires (SDNH) within 20 days of hire. States then match new hire reports against their child support records. Within five business days of receiving new hire reports from employers, States must enter the information on the SDNH and then must submit its new hire reports to the NDNH within three business days. SESAs are required to report unemployment insurance and quarterly wage data to the NDNH as well. Federal agencies report new hire and quarterly wage data directly to the NDNH.

6. The FCR is a national database that contains every State's IV-D cases. The FCR also contains each State's non-IV-D support orders that are established or modified on or after October 1, 1998.

7. 42 U.S.C. §653(e).

8. 42 U.S.C. §§653, 654, 654a; 5 U.S.C. §552a; 26 U.S.C. §6102, 7213, 7431.

9. 42 U.S.C. §653(b)(2). ◆

FEATURE

Joseph R. Slights, III
Nancy W. Law

THE PRIVACY OF MEDICAL RECORDS: ARE PATIENTS PROTECTED?

Introduction

Most of us expect our personal affairs to remain private. While we may choose to allow access to our personal information in certain circumstances, we should like to think that we can control who sees our personal information and how much those people will see. Of course, in the electronic age, we have been conditioned to expect that certain personal information will be easily accessible despite our wishes that the information remain private. For instance, I recently sat across the desk from a fresh-out-of-college car salesman who, before running lease rates on a car I hoped to lease, ran a credit check on me from his desktop computer. No request for my permission; no offer to let me see it first before he studied it. I sat helplessly watching him review my credit history, a history which I must acknowledge started inauspiciously when I was first turned loose on my own in Harrisonburg, Virginia. Would this young man see that I didn't always pay my bills on time when I was in college? Had we paid our bills on time last month? It was a very strange feeling; I didn't like the invasion into my private affairs one bit.

Although conditioned to accept that credit histories, consumer lists (with addresses, buying habits, etc.), and other consumer-oriented information may be available to outsiders, most of us feel confident that our medical information—perhaps our most private information—will remain confidential and protected from disclosure. We all have a sense, perhaps not clearly defined, that doctors and other health care practitioners are prohibited from disclosing our medical information. Lawyers especially identify with this notion of patient privacy because we practice every day under the umbrella of the attorney-client privilege. Is our confidence misplaced? What protections exist for patients who wish to keep their medical information private and how effective are they? This article will summarize the professional and legal measures that are intended to regulate the disclosure of this most sensitive information.

The Landscape Before the Electronic Age: Professional Regulation and State Law

The idea that medical information should be protected from disclosure is as old as the practice of medicine itself. The Hippocratic Oath, which continues to provide the moral framework upon which medical doctors around the world practice, states in pertinent part:

> Whatever, in connection with my professional practice, or not in connection with it, I see or hear in life of men, which ought not to be spoken of abroad, I will not divulge as reckoning that all such should be kept secret.

The American Medical Association's guidelines for medical ethics embrace the Hippocratic Oath by providing that "[a] physician shall respect the rights of patients, . . . and shall safeguard patient confidences within the constraints of the law." 1992 *Code of Medical Ethics: Current Opinions of the Council on Ethical and Judicial Affairs of the American Medical Association.* Delaware's Medical Practices Act, 24 *Del. C.* § 1701, *et seq.*, actually codifies the Hippocratic Oath by defining unprofessional conduct, *inter alia*, as the "willful violation of the confidential relations and communications of a patient." *Id.*

Delaware's Uniform Rules of Evidence also codify the Hippocratic Oath by recognizing a physician-patient privilege specifically in the context of litigation:

> A patient has the privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of diagnosis or treatment of his physical, mental or emotional condition, including alcohol and drug addiction, among

himself, his physician or psychotherapist,[1] and persons who are participating in the diagnosis or treatment at the direction of the physician or psychotherapist, including members of the patient's family.

The patient bears the burden of establishing the existence of the physician-patient privilege and its application to the facts of the given case. *Secrest v. State*, Del. Supr., 679 A.2d 58 (1996).

There are, of course, exceptions to almost every rule, including the time-honored rule of confidentiality in our medical affairs. For instance, a patient can waive his expectation that his medical information will remain confidential by placing his medical condition at issue in litigation. D.U.R.E. 503(d)(3); *Green v. Bloodsworth*, Del. Supr., 501 A.2d 1257 (1985). Likewise, a parent's psychiatric and psychological history will be discoverable in the discretion of the court where the parent's fitness is raised by a petition for visitation or where the records are relevant to an evaluation of fitness in connection with a petition to terminate parental rights. *Betty J. B. v. Division of Social Services*, Del. Supr., 460 A.2d 528 (1983). Additionally, a court-ordered examination of an individual's physical, mental or emotional condition will waive the privilege with respect to communications between the patient and physician or psychotherapist which relate to the particular purpose for which the examination is ordered. D.U.R.E. 503(d)(2).

Delaware law also recognizes certain situations where a physician must violate his oath to maintain patient confidences by reporting otherwise confidential information to public authorities. In these instances, the Delaware General Assembly has determined that public interest "outweighs the duty of confidentiality, and it requires the physician to breach these confidentialities." *Martin v. Baehler*, Del. Super., C.A. No. 91C-11-008, mem. op. at 6, Lee, J. (May 20, 1993). Examples of these statutory exceptions to a patient's privacy include the duty to report certain wounds, injuries and poisoning, 24 *Del. C.* § 1762(a), communications relevant to child abuse cases or the appointment of a guardian, 12 *Del. C.* § 3901, 16 *Del. C.* ch. 9, and information regarding contagious diseases, 16 *Del. C.* § ch. 5.[2]

While exceptions to medical privacy do exist, they are construed narrowly by most courts, including Delaware courts. For example, in *Martin, supra*, the Court was confronted with a physician's seemingly innocent disclosure of a patient's confidential medical information. The physician had just informed a patient that she was pregnant. *Martin*, mem. op. at 1. In order to confirm insurance information, the physician's receptionist phoned the patient's grandmother without the patient's consent and, in the course of the discussion, advised the grandmother that her granddaughter was going to have a child. *Id.* at 1-2. The patient, unaware of the disclosure, had already decided to terminate the pregnancy. As a result of the receptionist's unauthorized disclosure, the plaintiff alleged she suffered emotional distress from the irreparable damage to her family relations. *Id.* at 2.

We have a sense, perhaps not clearly defined, that doctors and other health care practitioners are prohibited from disclosing our medical information.

The court concluded that the statutory exceptions to confidentiality and corresponding immunity from suit implied exposure to liability when an exception is not implicated. *Id.* at 6. Accordingly, the court held that, in the absence of an applicable statutory exception to confidentiality, the physician was liable to the patient for violating the duty of confidentiality all Delaware physicians owe to their patients. *Id.* at 6-7.[3] The controversy was resolved at trial with a jury verdict in favor of the plaintiff for $75,000. *See Martin v. Baehler*, Del. Super., C.A. No. 91C-11-008, Del Pesco, J. (July 7, 1993) (upholding the jury award).

Delaware courts are not alone in their strict interpretation of a patient's right to keep medical information confidential. Most state and federal courts rigidly enforce this entitlement. For instance, last November, the Eleventh Circuit, interpreting Georgia law, held that the unauthorized disclosure of a physician's own psychiatric and psychological records to a state licensing board violated the physician's expectation of confidentiality. *Hicks v. Talbott Recovery Sys., Inc.*, 11th Cir., No. 98-08821, 1999 WL 1054595 (Nov. 22, 1999). The licensing board was investigating charges that the physician was abusing alcohol. *Id.* The records disclosed to the board also contained references to treatment of certain sexual disorders. *Id.* This disclosure prompted the board to expand its investigation. *Id.* The plaintiff-physician was awarded damages by a jury for the wrongful disclosure of confidential information and the resulting emotional distress caused by the expanded investigation of him. *Id.* Some courts have concluded that disclosure of treatment records without patient identification can still violate the patient's right of confidentiality. For instance, a Michigan court recently opined that the physician-patient privilege protects the unauthorized disclosure of medical records even where the patients' names have been redacted. See *Baker v. Oakwood Hosp. Corp.*, Mich. Ct. App., No. 206407 (Jan. 18, 2000).

The Landscape in the Electronic Age: Enter The Federal Government

Protecting the privacy of a patient's medical information has traditionally been a matter governed by state law. In the electronic age, however, where national and multinational companies have entered the health care delivery market and have placed the latest information storage and transmission technology into physician offices and hospitals, the federal government has become sensitive to the prospect of abuse and has recognized the need for sweeping regulation to ensure the protection of medical information.

The concern that the electronic storage and transmission of medical information increases the likelihood of unau-

thorized disclosure is certainly well founded. In 1995, twenty-four people in Maryland were indicted for selling confidential patient information obtained from the state's Medicaid data base to four HMOs. Valentine, *Medicaid Bribery Alleged: HMOs, Md. Agency Implicated by State,* Washington Post, June 14, 1995, at B1. In Boston, a convicted rapist acquired a computer password and gained access to nearly a thousand patients' medical records. For months he used the records to make repeated phone calls to children and their parents during which he would often refer to medical treatment they had received. Brelis, *Patients' Files Allegedly Used for Obscene Phone Calls,* Boston Globe, Nov. 23, 1995, at A1. "In a 1993 Harris poll, more than a quarter of those surveyed said that their own [electronically stored] medical information had been improperly disclosed." *Who is Reading Your Medical Records,* Consumer Reports, Oct. 1994, at 628. And it is now common practice in connection with the application for life, health and disability insurance for the insurance carriers to provide the information disclosed in these applications to sophisticated data banks often referred to as "Medical Information Bureaus." *Id.*

In recognition of the widespread abuse of patient confidentiality, Congress included in its comprehensive healthcare reform measure, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), a specific directive that federal healthcare privacy legislation be enacted by August 21, 1999. In default of this deadline, the Secretary of the U.S. Department of Health and Social Services (the Secretary) was directed to issue a proposed rule that would establish standards to protect the privacy of health information. Public Law 104-191 (Section 261). Congress apparently bit off more than it could chew; it failed to meet the August 21 deadline.[4] Accordingly, the Secretary issued her proposed rule on November 3, 1999 (hereinafter, the Rule). 64 Fed. Reg. 59918. One need only take a cursory glance at the extensive guidelines to appreciate the ambitious undertaking of the Secretary in formulating it.

The parameters of the Rule are quite broad. It covers "individually identified healthcare data" that is or has been electronically maintained or transmitted by healthcare providers, healthcare clearinghouses, and health plans. *See* Steven L. Page et al., *Proposed Federal Privacy Rules: Locking the Electronic File Cabinet,* The Health Lawyer, Vol. 12, No. 2, Dec. 1999 at 2. "Electronically transmitted" healthcare data is information exchanged with a computer using electronic media. 64 Fed. Reg. 59918, 60053. Examples of covered data include information transmitted by floppy disk, over the Internet, Extranet, dial-up lines and private networks as well as telephone voice response systems and "faxback" systems. 64 Fed. Reg. 59918, 59938.

Under the Rule, patients have the right to access, correct and amend their healthcare information and receive an accounting of that information. *Id.*

The promulgation of effective protective measures is by no means a simple task, as evidenced by Congress' inability to meet its own deadlines for action.

Healthcare organizations, such as health insurers, may not use or disclose a patient's medical information without the patient's authorization, and the Rule provides detailed criteria which must be followed to secure the authorization. *Id.* The Rule also requires healthcare providers to provide for so-called "fire walls" (electronic buffers) and other protective measures to block access to electronically stored medical information. *Id.*

Importantly, the Rule provides for substantial penalties for violations of the confidentiality requirements including civil monetary penalties of up to $25,000 for each standard that is violated. Public Law 104-191 (Section 262). The Rule does not, however, provide for a private right of action on behalf of patients who are damaged by violations of the Rule. *Id.*

The Rule establishes several defenses to efforts to enforce civil penalties. For example, where the provider, plan or clearinghouse shows that it could not have known, even with reasonable diligence, that a standard had been violated, it will not be penalized. Public Law 104-191 (Section 262). Likewise, a penalty will not be imposed if the provider, plan or clearinghouse rectifies a failure to comply within thirty days of determining, through self-audit, that the violation has occurred. *Id.* HHS may waive or reduce the penalty if it determines that the failure to comply can reasonably be explained or that a penalty would be considered excessive. *Id.*

HIPAA also sets forth criminal penalties for wrongful disclosure of an individual's private healthcare information. These include imprisonment up to ten (10) years and a maximum fine of $250,000.00, depending upon the severity of the crime. *Id.*[5] Clearly, Congress intends to place the healthcare industry on notice that it is taking the protection of patient privacy very seriously.

The response to the Rule has been mixed. While patients' rights groups certainly appreciate greater control over their constituents' private medical information, healthcare providers and organizations argue that the costs of implementation far outweigh any privacy benefits to the public. The healthcare industry maintains that the Rule will cost providers between $30-$40 billion dollars over the next 5 years to implement. Page, *Proposed Federal Privacy Rules,* at 3. Further, industry experts claim that the cost of responding to patient requests to correct healthcare information will exceed $2 billion during the implementation period. *Id.* The federal government, on the other hand, estimates that the cost of implementing and enforcing the Rule will approximate $3.8 billion. Robert Pear, *Rules on Privacy of Patient Data Stir Hot Debate,* N.Y. Times, Oct. 29, 1999, at A1, A9. Healthcare organizations are required to achieve compliance with the Rule within two years of its promulgation. 64 Fed. Reg. 59918, 60064.

The Rule will preempt a state law that is contrary to its specifications but

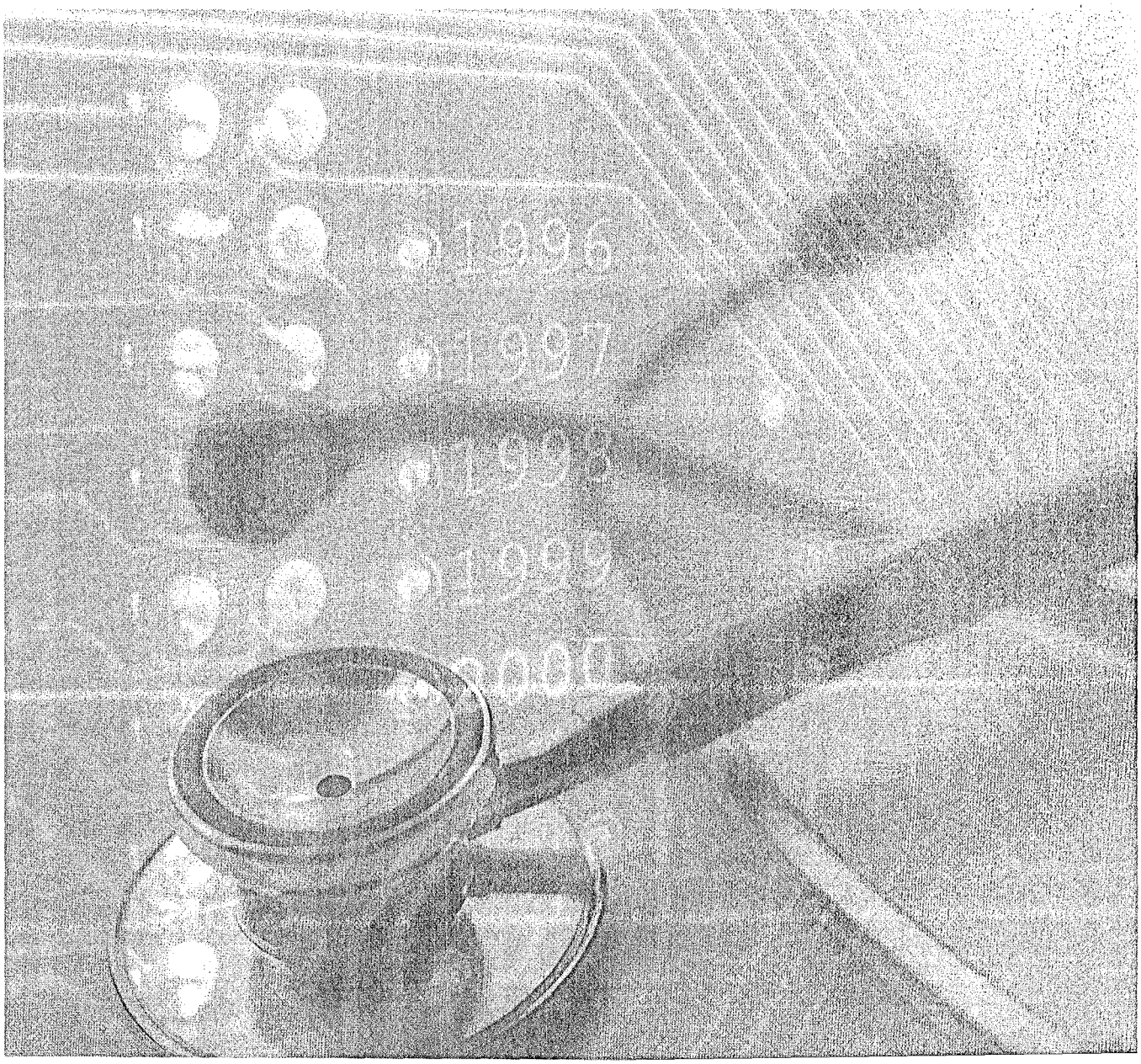
will not nullify a state law which provides greater protection. 64 Fed. Reg. 59918, 60051. A state law is considered contrary to the Rule when a party: "(i) would find it impossible to comply with both the state law and the Rule, or (ii) the state law is an obstacle to the execution of the objective of Part C of Title IV of the Social Security Act or Section 264 of HIPAA." 64 Fed. Reg. 59918, 60050. The Rule does not preempt state law if HHS finds that the state law: (i) addresses controlled substances; (ii) is necessary to prevent fraud and abuse; (iii) insures proper state regulation of health and insurance plans; (iv) enables reporting on health care costs or delivery; or (v) improves Medicare or Medicaid programs in that state. *Id.*

Clearly, it is intended that the Rule merely supplement more restrictive existing state law. The Secretary has openly encouraged states to continue aggressively to restrict access to private medical information and to use the Rule as a foundation upon which to build their own medical privacy protections. *Id.* Many states are heeding the Secretary's call to action. In 1999 alone, legislators in 35 states introduced more than 300 bills relating to the confidentiality of medical records. Bowman, *Uneven State Medical Records Laws Offer Potential Pitfalls for Health Plans*, BNA Health Law Reporter, Nov. 11, 1999, at 1787.

For its part, Delaware passed legislation creating the Delaware Health Information Network (DHIN) for the purpose of providing a public instrumentality to control and monitor the public and private use of health care information. 16 *Del. C.* § 9920. Under the DHIN, "all persons providing information and data to the DHIN shall retain a property right in that information or data . . .." 16 *Del. C.* § 9924(a).

Similarly, patients' rights to the confidentiality of their information and its disclosure for medical purposes only has been codified in Title 16, Chapter 11 of the Delaware Code. 16 *Del. C.* § 1121. Under this statute, patients and residents in sanatoria, rest homes, nursing homes, boarding homes and related institutions are guaranteed privacy and confidentiality with respect to their medical care, discussions, consultations and treatment. 16 *Del. C.* § 1121(b). The patient's information shall not be made public without the consent of the patient. *Id.*

Consumers of medical care have every reason to be concerned. Nearly every day, some newspaper somewhere will report another disturbing story of sensitive medical information being disclosed inappropriately. Nevertheless, state and



federal lawmakers have placed the protection of medical information near the top of their priority lists. Of course, the promulgation of effective protective measures is by no means a simple task, as evidenced by Congress' inability to meet its own deadline for action. The flurry of activity in states across the country, however, does suggest that progress is being made. In the meantime, the consumer beware: with a few strokes of the keyboard, someone out there whom you've never met may be looking at information even more sensitive than your not so perfect credit history.

FOOTNOTES:

1. A "physician" is a person authorized to practice medicine in any state or nation, or reasonably believed by the patient to be authorized to practice medicine. A "psychotherapist" is (a) a person authorized to practice medicine in any state or nation, or reasonably believed by the patient to be so authorized, while engaged in the diagnosis or treatment of a mental or emotional condition, including alcohol or drug addiction, or (b) a person licensed or certified as a psychologist under the laws of any state or nation, while similarly engaged. D.U.R.E. 503(a)(1), (2).

2. Each of these statutory disclosure requirements is accompanied by immunity from suit protections for the physician. *See, e.g.*, 16 *Del. C.* § 906 ("Anyone participating in good faith in the making of a report pursuant to this chapter shall have immunity from any liability, civil or criminal, that might otherwise exist and such immunity shall extend to participation in any judicial proceeding resulting from such report.").

3. The court rejected the contention that the disclosure of confidential medical information constituted an "invasion of privacy" and, instead, recognized an independent cause of action for breach of confidentiality. *Id.* at 3. The court also held that the disclosure by the physician's receptionist could be ascribed to the physician under the doctrine of *respondeat superior*. *Id.* at 7.

4. Senator Jim Jeffords, R-VT, "postponed a privacy bill marked-up four times as law makers and their staffs argued behind the scenes over such issues as patient's right to sue for compensatory and punitive damages when the confidentiality of their medical file is breached." *Privacy Legislation Stalled*, Health Lawyers' News, Vol. 3, No. 8, Aug. 1999 at 30. At the same time legislators battled over the language of the Act, several GOP lawmakers wrote HHS Secretary Donna E. Shalala, requesting that she hold off proposing any new medical privacy regulations until Congress had an opportunity to act upon the proposed legislation. *Id.* The request went unanswered; HHS promulgated the Rule in November 1999 and made its final revisions to the Rule on February 21, 2000.

5. In the spectrum of culpability, HIPAA distinguishes between knowingly disclosing protected health information and doing so under false pretenses or for financial gain, the latter infractions being penalized most severely. ◆

FEATURE

Teresa Cheek

PRIVACY IN THE WORKPLACE

When hiring new employees, monitoring employee performance and investigating suspected employee misconduct, employers commonly ask their employment counsel about the scope of lawful inquiries. Employers may want employees and applicants to answer questions about their health, submit to medical examinations, and take lie detector, drug, alcohol and psychological tests. Employers often want information about an applicant's criminal, credit and work record. Employers may wish to listen to their employees' telephone calls, watch their employees over video cameras, and read their employees' e-mail. They may want to hire private investigators to observe their employees or search their employees' persons or property. They may want to question their employees about alleged misconduct. All such actions involve not only the familiar common law causes of action for invasion of privacy, but also may implicate constitutional principles and state and federal statutes designed to protect individual privacy. Employers in general have broad authority to obtain information about their employees and applicants. This article will briefly explore the limitations on that authority.

Constitutional and Common Law

Public sector employers, unlike private employers, are subject to federal constitutional constraints because the conduct of governmental employers constitutes "state action" for constitutional purposes. Private employers are not subject to constitutional claims unless their investigations become intertwined with the state's investigatory activities. For example, a private employer could be subject to constitutional limitations if it becomes involved in a cooperative search or investigation with the police.

Constitutional issues frequently surface when public sector employers institute drug tests, which are considered searches and seizures under the Fourth Amendment. Body searches and searches of employees' offices and desks have also been held to implicate the Fourth Amendment. Searches by governmental employers are evaluated under a "reasonableness" standard that balances the level of intrusion of the search against the extent to which it serves a legitimate governmental interest. *See, e.g., Treasury Employees v. Von Raab*, 489 U.S. 656, 665 (1989) (applying the Fourth Amendment to random drug testing); *O'Connor v. Ortega*, 480 U.S. 709, 726-729 (1987) (reasonableness test rather than warrant requirement applies to search of employee's office). Governmental employees may have a reasonable expectation of privacy in their persons, property, offices, desks and file cabinets, according to *Ortega*. The reasonableness and extent of such expectations depend on the context, including, in particular, what the employer has done to increase or decrease them: "Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." 480 U.S. 717. The lesson for public sector employers from *Ortega* is that announcing policies affecting employee privacy goes a long way toward insulating employers from liability under the Fourth Amendment.

As in the public sector, searches in private work places may prompt litigation. Whether such claims are successful depends on what the employer has done to create or defeat employees' legitimate expectations of privacy. Both written and unwritten employer policies and practices may create an expectation of privacy. Employers thinking about searching an employee's work area, desk, car, locker, person or possessions should first review the company's written policies. Before undertaking a search, the company should have given employees unambiguous notice that it reserves the right to search any and all persons, locations and property in its work place, including their lockers, files, desks, handbags, brief cases, and so on.

Employers must balance their need to make such searches against the possible negative impact on employee morale that a far-reaching search policy might have. Notice of the policy can be given by conspicuously posting it in the work place, printing it in the employee handbook, and/or by requiring employees to sign consent forms authorizing searches as a condition of employment. Even if the employer has a clear written policy, of which employees have been informed, it is wise to obtain the employee's written permission to search his or her person, work area or possessions before beginning the search. If there is no written policy or practice of conducting searches, and the employee will not consent to the search, the employee should be suspended without pay pending the company's decision about what action to take. Failure to cooperate with the employer's investigation can be grounds for discipline, including termination.

The theory under which most private sector employees proceed is "intrusion upon seclusion." Delaware, like most other states, recognizes claims for intrusion into the plaintiff's private concerns or seclusion. *Barbieri v. News-Journal Co.*, Del. Supr., 189 A.2d 773, 774 (1963). Intrusion into seclusion occurs when "'one...intentionally intrudes upon the solitude of seclusion of another or his private affairs or concerns...if the intrusion would be highly offensive to a reasonable person.'" *Restatement (Second) of Torts*, § 652B, *quoted in Beckett v. Trice*, Del. Super., C.A. No. 92C-08-029, Graves, J. (Nov. 4, 1994).

In *Beckett*, a former employee of one of the defendants was fired after she was arrested for selling marijuana and maintaining a dwelling for the purpose of delivering and keeping a controlled substance. The arrest was the result of an investigation by an undercover detective originally hired by the employer. The detective confirmed the employer's suspicion that there was a drug problem at the company. He then agreed to work as an agent of the Delaware state police to investigate drug use at the company. In the course of his investigation he began a sexual relationship with the plaintiff. He eventually bought marijuana from her and turned her in to the police. The state dropped the charges against her after it found out about her sexual relationship with the investigator. The court held that she had no claim for intrusion into seclusion because (even though it was based on deception) she had consented to the investigator's intrusion into her private life.

In a similar more recent case in Illinois, on the other hand, the court held that the deceptive nature of undercover investigators' relationships with employees and the broad range of personal information they disclosed in their reports to the employer raised a jury question as to whether the employer's investigation would be offensive or objectionable to a reasonable person. *Johnson v. K-Mart Corp.*, Ill. App., 15 IER Cases (BNA) 1605 (2000). Given that the investigators were posing as employees, the court questioned whether the disclosures employees made to the investigators were truly voluntary. The plaintiffs told the investigators about their family matters, sex lives and romantic interests, employment plans, complaints about the employer and other personal matters, all of which the investigators reported to the employer. Although the employer was trying to prevent theft, sabotage and drug use, it never instructed the investigators to confine the information in their reports to these topics.

Drug testing has led to many lawsuits against employers, most of which result in decisions in favor of the employer. Indeed, the Delaware District Court recently held that even having monitors directly observe urination during urine drug tests on firefighters did not constitute an invasion of their privacy. *Wilcher v. City of Wilmington*, 60 F. Supp. 2d 298 (D. Del. 1999). Noting that the right to privacy is not absolute but must sometimes yield to the rights or interests of others, the court set forth factors for determining whether an intrusion into a person's privacy would be highly offensive to a reasonable person, the standard under Delaware law. The factors include: (1) the degree of the intrusion; (2) the context, conduct, and circumstances surrounding the intrusion; (3) the intruder's motives and objectives; (4) the setting into which the intruder invades; and (5) the expectations of those whose privacy is invaded. In other words, the court looked at all the circumstances surrounding the drug test and then balanced the individual firefighter's right to privacy during urination against the employer's need for accurate and unadulterated test results. The court noted that firefighters work in a heavily regulated industry and that their function is to protect and promote public safety. A firefighter with an undetected drug problem accordingly poses a greater than normal risk to himself and to the public at large. Therefore, firefighters have a diminished expectation of privacy, even in settings that are generally regarded as private. In addition, the monitors stood in back of or beside the firefighters and only looked in the general direction of the firefighters and did not directly observe their genitals. In its analysis, the court distinguished between the male and female firefighters based on the fact that men often urinate at exposed urinals in public restrooms, while women do not. In the court's view, women require more substantial measures to protect their privacy. SODAT's procedure, in which female monitors stood to the side of the women being tested was adequate protection. The same court had previously held that the testing procedure did not violate the Fourth Amendment, and the Third Circuit had agreed.

Courts have also upheld claims for intrusion into seclusion in cases of sexual harassment. For example, in *Cunningham v. Dabbs*, Ala. App., 703 So. 2d 979 (1997), an employer who was a physician allegedly subjected the plaintiff to sexual propositions and inappropriate physical contacts (he acted as though he was going to whisper something to her and then stuck his tongue in her ear) and then fired her when he found out she was about to get married. The court held that this conduct was sufficient for a reasonable jury to conclude that he had unreasonably intruded into her private affairs.

In *Smyth v. The Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), the court held that an employee had no legitimate expectation of privacy in the content of e-mail correspondence between the employee and his supervisor, despite the fact that the company had assured employees that their e-mail correspondence could not be intercepted and was confidential. The employee's e-mail message about sales managers threatened to "kill the back-stabbing bastards" and referred to an upcoming company holiday party as "the Jim Jones Koolaid affair." The court also held that no reasonable person would consider the interception by the company of this e-mail message as a substantial and highly offensive invasion of the employee's privacy. The court explained that the employee had not been compelled to disclose personal or private information, but rather had voluntarily communicated his message, and that the company's interest in preventing unprofessional and inappropriate comments such as those voiced by the employee outweighed any

privacy interest he might have.

Another type of invasion of privacy recognized in Delaware is publication of private facts. *Barbieri,* 189 A.2d at 774 (also recognizing claims for "false light" invasion of privacy, and "misappropriation" of a plaintiff's name or picture). A recent Colorado case, *Ozer v. Borquez,* Colo. Supr., 940 P.2d 371 (1997), illustrates a claim for publication of private facts. Borquez, a law firm associate, learned that his domestic partner had just been diagnosed with AIDS. He was advised that he should immediately be tested for HIV. Fearing he would not be able to adequately represent his clients in a deposition that day and an arbitration on the following day, he contacted the office to find someone to handle these matters for him. In a telephone conversation with Ozer, a partner in the firm, Borquez disclosed that he was homosexual, that his partner had been diagnosed with AIDS, and that he needed to be tested for HIV, asking Ozer to keep the information confidential. Ozer then discussed Borquez' disclosures with his wife, the law office manager, and two secretaries. By the time Borquez returned to the office, everyone at the firm soon knew about his situation. One week later, Borquez was fired, allegedly because the firm's financial position was poor. Borquez sued, relying on a Denver ordinance forbidding discrimination on the basis of homosexuality and also for public disclosure of private facts. The jury rendered a verdict in favor of Borquez for $90,841. The court of appeals affirmed.

The Colorado Supreme Court affirmed in part and reversed in part, and remanded for a new trial. Joining the majority of other jurisdictions, the Court held that Colorado recognized a cause of action for unreasonable publication of private facts, outlined the elements of the claim: (1) private facts, (2) disclosure to the public, (3) a reasonable person would be highly offended by the disclosure, (4) the public has no legitimate interest in the facts disclosed, and (5) reckless disregard by the defendant of plaintiff's interest in keeping the facts private. The court held that facts regarding one's sexual relations and "unpleasant or disgraceful" illnesses are private facts. The number of people to whom facts must be disclosed to render the disclosure "public" depends on the circumstances, although disclosure to only one or a few persons would probably be insufficient, in contrast to defamation, when disclosure to one other person satisfies the "publication" element of that tort. A disclosure is deemed "highly offensive" if a reasonable person would find it emotionally distressing or embarrassing. The fourth element concerns the "newsworthiness" of the private information. The fifth, or "reckless disregard" element, is met when the person who disclosed the facts knew or should have known that they were private in nature. The case was remanded for a new trial because it was not clear whether the evidence would satisfy the publication element.

Other recent cases involving claims for invasion of privacy include *Stien v. Marriott Ownership Resorts, Inc.*, Utah App., 944 P.2d 374 (1997), in which the court held that an employer did not publicize private facts about employee's sexual relationship with his wife or place plaintiff in a false light by showing a "joke" video-

tape in which his statements about his most disliked household chore were made to appear to be response to question about what his sex life was like, where it was clear that he was not really talking about his sex life. In *Hart v. Seven Resorts, Inc.,* Ariz. App., 12 IER Cases (BNA) 1411 (1997), the court held that an employer who fired employees for refusing to take a drug test did not intrude on their seclusion or portray them in a false light before the public simply because the circumstances under which they were fired resulted in gossip about them.

Americans with Disabilities Act

The Americans with Disabilities Act (ADA) has caused employers to make major revisions in their hiring process to avoid unlawful inquiries about applicants' medical conditions. Under the ADA, employers may not ask applicants whether they have a disability or about the nature and severity of any disabilities. Employers are no longer allowed to ask, for example, "Do you have a handicap or disability that would prevent you from doing the job for which you are applying?" At the pre-offer stage, employers may no longer ask applicants to list illnesses, diseases, medical conditions, hospitalizations, and the like, or to disclose their workers' compensation history. When checking references given on an employment application, employers may not try to make an "end run" around the ADA's medical inquiry restrictions by asking the references if they know of any health or medical problems experienced by the applicant.

Employment interviewers may, on the other hand, ask applicants whether about their ability to do the job, a sometimes subtle distinction. For example, employers may ask, "Can you lift 50 pounds?" if lifting 50 pounds is required by the job. Employers may not ask how often an applicant will require leave for the treatment of a disability or how often he will use sick leave as a result of any disability, but the employer may specify the attendance requirements of the job and inquire whether the applicant can meet them. On the other hand, if an applicant has an obvious disability which may interfere with or prevent the performance of a job-related function, the employer is allowed to ask the applicant to describe or demonstrate how, with or without reasonable accommodation, he will be able to perform the job-related function, even if the employer does not routinely make such a request of all applicants. For example, an employer may ask an individual with one leg who applies for a position as a home washing machine repairman to demonstrate or to explain how, with or without reasonable accommodation, he would be able to transport himself and his tools down a customer's basement stairs. However, the employer still may not inquire as to the nature or severity of the disability. That is, for example, the employer cannot ask how the individual lost the leg or whether the loss of the leg is indicative of another underlying impairment such as diabetes or cancer. If the obvious disability of an applicant will not interfere with or prevent the performance of a job-related function, the employer may only request an explanation or demonstration by the applicant if such a request is routinely made of all applicants in the same job category. Therefore, for example, it would not be permissible for an employer to request that an applicant with one leg demonstrate his ability to assemble small parts while seated at a table, if the employer does not routinely make this request of all applicants.

As in the public sector, searches in private work places may prompt litigation. Whether such claims are successful depends on what the employer has done to create or defeat employees' legitimate expectations of privacy.

The ADA also restricts pre-employment medical examinations. They may be performed only after an offer of employment has been extended but before the employment begins. The employer may condition the offer of employment on the results of the physical examination, provided that all entering employees in the same job category are subjected to the same physical examination. In other words, the employer may not require only applicants suspected to have disabilities to submit to pre-employment medical examinations. On the other hand, the ADA does not restrict the scope of pre-employment medical examinations and, accordingly, an employee can be given a comprehensive examination regardless of the nature of the job. It should be noted, however, that Delaware state law provides that HIV tests may not be performed in the absence of informed consent under ordinary circumstances. 16 *Del. C.* § 1201-1204. If an employer withdraws an offer of employment because of the results of the medical examination, the employer must be able to demonstrate that the problem discovered would have prevented the applicant from performing the job.

The ADA also regulates medical examinations during employment, requiring them to be job-related and consistent with business necessity. The ADA requires that employee medical records be kept segregated from other personnel records and in a secure location. Finally, the ADA forbids the disclosure of medical information to anyone other than those who have a legitimate business-related need to know it.

Genetic Information

Since 1998, the Delaware Discrimination in Employment Act has included provisions protecting the privacy of emloyees' genetic information. 19 *Del. C.* § 710-718. An employee's genetic information is now treated as a protected characteristic, and employers are forbidden to discriminate against employees based on their genetic information. In addition, employers are not permitted to intentionally collect, either directly or indirectly, the genetic information of employees, job applicants or their families, unless the employer can demonstrate that collecting the information is job related and consistent with business necessity, or that the information is sought in connection with the employer's retirement policy or system or the administration of a bona fide employee welfare or benefit plan. 19 *Del. C.* § 711(e).

The Electronic Communications Privacy Act of 1986

Title III of the Omnibus Crime Control and Safe Streets Act ("Title III"), as amended by the Electronic Communication Privacy Act of 1986 ("ECPA"), generally prohibits the illegal "interception" of any "wire" or "electronic communication" or "oral communication" through aural or other acquisition of the contents of the communication by use of any "electronic, mechanical, or other device." 18 U.S.C. § 2510, *et seq.* The Act includes criminal penalties as well as a civil penalty of $100 per day for each day the Act is violated or $10,000, whichever is greater.

One case interpreting the ECPA in the employment context arose in Delaware. In *Wesley College v. Pitts*, 974 F. Supp. 375 (D. Del. 1997), the court held that simply reading an e-mail while it was displayed on a computer screen was not an "interception" of an electronic communication. Even if an e-mail is retrieved from storage, such a retrieval does not constitute an interception of the communication, the court said. The e-mail must be intercepted while it is in transit in order for the ECPA to be violated.

In a Tennessee case, four employees of a county rabies control office sued under the ECPA after they learned that their supervisor had surreptitiously tape recorded some private conversations between them at work, including some harsh negative comments about the supervisor. *Dorris v. Absher*, 959 F. Supp. 813 (M.D. Tenn. 1997). The court held the supervisor liable and assessed a civil penalty of $80,000 against him. The court of appeals affirmed the supervisor's liability, holding that the employees had a legitimate expectation that their conversation would not be intercepted, but remanded for a new decision on the amount of the civil penalty, which the court of appeals felt was too high. *Dorris v. Absher*, 179 F.3d 420 (6th Cir. 1999).

There are some significant exceptions to the ECPA's prohibitions. The provider exception allows an employer who is a network provider to access, disclose and use employee e-mail if it is a "necessary incident" to servicing the network, or if such access is necessary to protect the company's rights or property. Some commentators and courts have interpreted this provision to mean that an employer-provider is free to examine anything on its computer system. Alexander I. Rodriguez, *Comment: All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector*, 47 Emory L.J. 1439, 1451 (1998). It is possible, however, that an employer that contracts with a third party such as Compuserv or MCI Mail to provide internet service will not be considered a "provider" of the e-mail service so as to qualify for the provider exception.

A second exception is the business extension or business use exception, which applies when the interception of the communication is made by the employer in the ordinary course of the employer's business using equipment provided by a communications carrier as part of the communications network. Under this exception, for example, employers may ask the telephone company to install a device to permit the employer to monitor conversations between its employees and customers for legitimate business reasons such as protecting employees from abuse by customers and vice versa. If an employer wishes to monitor telephone calls or e-mail for quality control or other legitimate business reasons, it should advise employees in advance that it may do so. In addition, a monitor should stop listening as soon as he realizes that the employee's call is personal. *See, e.g., Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1994); *Watkins v. L. M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983); *James v. Newspaper Agency Corp.*, 591 F.2d 579 (10th Cir. 1979); *United States v. Harpel*, 493 F.2d 346 (10th Cir. 1974); *Ali v. Douglas Cable Communications*, 929 F. Supp. 1362 (D. Kan. 1996).

Employers must balance their need to make such searches against the possible negative impact on employee morale that a far-reaching search policy might have.

The final exception to the ECPA is consent. This exception has spawned some litigation over the circumstances under which consent may be implied. An interesting example is *Deal*, in which an employer (a husband and wife who owned a liquor store) decided to tap their own phone to try to catch their employee, a store clerk, in an admission that she had participated in a burglary of the store. The installed a recording device the husband bought at Radio Shack on a telephone extension in their mobile home (the same line was used for the store and the owners' home). The husband tape recorded and listened to 22 hours of telephone conversations, including conversations between his employee and her lover. His wife also listened to some of the tape recording. They didn't get the incriminating information they wanted, but they did learn that the employee had violated store policy by selling her lover a keg of beer at cost, and fired her after playing her a short segment of the recording concerning the beer. She and her lover sued under Title III and were awarded $40,000 in civil penalties against the store's owners, a judgment that was affirmed on appeal.

The employer argued that the employee had given implied consent to the recording because Mr. Spears had mentioned to her that he might start monitoring or restricting her use of the telephone if she didn't stop making so many personal calls. They also argued that she knew her telephone conversations might be monitored because she knew about the extension in his home. The court rejected these arguments. The court noted that the employer must have thought that the employee would not know her calls were being monitored, or they would not have thought she might admit her guilt. The employer's statement that he might monitor her calls was not definite enough to put her on notice of monitoring so that her consent might be implied from the circumstances. Finally, as to the extension, the employee testified that there was an audible click when it was picked up, whereas the recording device made no noise. The court also rejected the employer's business use/extension argument because the employer listened to everything that was recorded, whether it was business-related or not, and because the equipment used to record the conversations was purchased at Radio Shack and installed by the employer, not provided by the telephone company.

Continued on page 34

MAHA/MASON

continued from page 15

purpose other than that relevant to the proceeding regarding parentage, without a court order or the written permission of the individual."[21]

After destruction of the genetic material there is a requirement for the notification of the destruction of the samples using certified mail. In addition to the lost opportunities for problem investigation, this section poses a new problem: many of these certified letters will be returned as the population tested by the IV-D agency is highly mobile. Experience with certified mailing of reports to the tested individuals, even though these reports are mailed only a few weeks after testing, has shown the addresses have already changed (or were non-existent to begin with). Thus the use of certified mail is a waste of resources, needlessly expending tax money. A more rational approach is to require the laboratory to provide, upon request, a written comment on the destruction of the samples and records. Thus concerned citizens can monitor their samples.

Genetic privacy is a thorny issue, but legislatures should not rush in with broad regulations without thoroughly investigating the ramifications of their actions. Michigan furnishes a good example where hypothetical fears about genetic privacy resulted in unnecessary statutory language regarding paternity testing that is contrary to national standards and actually detrimental to its own citizens. Given the lack of diagnostic or prognostic indicators for health or employment, the genetic privacy issue in both paternity testing and forensic testing are hypothetical or unrealistic. Such hypothetical problems can be best addressed with simple statutes regulating the transfer of samples and keeping court records confidential.

FOOTNOTES

1. The opinions herein are solely those of the authors and do not necessarily reflect those of Laboratory Corporation of America Holdings.

2. By way of recent example, the cover story of *Newsweek*'s April 10, 2000 edition, opens its discussion of The Human Genome Project with the following analysis: "In the eyes of boosters, it promises to provide no less than the operating instructions for a human body, and will revolutionize the detection, prevention and treatment of conditions from cancer to depression to old age itself. In the eyes of critics, it threatens to undermine privacy and bring on 'genetic discrimination' in insurance and employment."

3. N.Y. Exec. Law § 995-f (October 18, 1999).

4. Lawrence O. Gostin & James G. Hodge, Jr., *Genetic Privacy and the Law: An End to Genetic Exceptionalism* 40 Jurimetrics 21 (1999).

5. These older tests were called "blood tests" however the blood actually refers to the sample used. The tests are genetic tests.

6. For a discussion of privacy of medical records, see the article by Joseph R. Slights, III and Nancy W. Law in this edition.

7. 42 U.S.C. § 666.

8. A completed valid voluntary paternity acknowledgment is to be considered the equivalent of a judicial determination of paternity 42 U.S.C. § 666 (a) (5) (D) (ii).

9. The authors' employer currently has a contract to provide genetic testing services to DCSE in IV-D cases whether ordered by DCSE or by Family Court.

10. The Family Law Section of the ABA recommended passage of the revised UPA at its meeting in April 2000. Although much has changed in the draft over the past year, a discussion of these revisions was *Delaware Lawyer's* cover story one year ago. (Vol. 17, No. 2, Summer 1999).

11. Mich. Comp. Laws §§ 722.711, 722.716, 722.716(a) (March 15, 2000).

12. Mich. Comp. Laws § 722.711(1)(e) (March 15, 2000).

13. Mich. Comp. Laws § 722.711(1)(f) (March 15, 2000).

14. For example, in the American Association of Blood Banks, Standards for Parentage Testing Laboratories, 4th ed. (1999) Standard 6.515 requires the issuing of a report containing "Phenotype established for each person in each genetic system examined."

15. Mich. Comp. Laws § 722.711(1)(i) (March 15, 2000).

16. Using Michigan's term, a DNA Identification Profile

17. Mich. Comp. Laws § 722.716(4) (March 15, 2000).

18. Mich. Comp. Laws § 722.716a(2) (March 15, 2000). If an alleged father who is tested as part of an action under this act is found to be the child's father, the contracting laboratory shall retain the genetic testing material of the alleged father, mother, and child for no longer than the period of years prescribed by the national standards under which the laboratory is accredited. If a man is found not to be the child's father, the contracting laboratory shall destroy the man's genetic testing material after it is used in the paternity action, in compliance with section 13811 of the public health code, 1978 PA 368, MCL 333.13811, and in the presence of a witness. The witness may be an individual who is a party to the destruction of the genetic testing material. After the man's genetic testing material is destroyed, the contracting laboratory shall make and keep a written record of the destruction and have the individual who witnessed the destruction sign the record. The contracting laboratory shall also expunge the contracting laboratory's records regarding the genetic paternity testing performed on the genetic testing material in accordance with the national standards under which the laboratory is accredited. The contracting laboratory shall retain the genetic testing material of the mother and child for no longer than the period of years prescribed by the national standards under which the laboratory is accredited. After a contracting laboratory destroys an individual's genetic testing material as provided in this subsection, it shall notify the adult individual, or the parent or legal guardian of a minor individual, by certified mail that the genetic testing material was destroyed.

19. For example, in the American Association of Blood Banks, Standards for Parentage Testing Laboratories, 4th ed. (1999) Standard 6.300 Record Retention. The laboratory shall retain the following records for 5 years, or as required by applicable law: 6.310 Records related to each parentage case.

20. Note the author's laboratory and others are Delaware corporations, thus this type of genetic privacy hysteria may be important to Delaware Corporate lawyers.

21. From Section 504(c) Proposed revision of the Uniform Parentage Act, National Conference of Commissioners on Uniform State Laws, March 27, 2000 draft. Michigan used "A person shall not sell, transfer, or offer genetic testing material obtained under this act except as authorized by this act." Mich. Comp. Laws § 722.716(4) (March 15, 2000). ◆

CHEEK

continued from page 31

Employee Polygraph Protection Laws

The Federal Employee Polygraph Protection Act, 29 U.S.C. §§ 2001-2009, became effective on December 27, 1988. It significantly restricts a private employer's use of the polygraph test in the workplace, but federal, state, and local governments are exempt from the law. It includes various other exemptions, but as a practical matter, it has little effect on Delaware private employers, since they are in any event prohibited by Delaware law from requiring applicants or employees to take a polygraph test. 19 *Del. C.* § 704.

Credit Reports

Recent amendments to the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681, significantly increased the legal obligations of employers who use "consumer reports" and significantly greater protection to the privacy of employees and applicants who are the subjects of such reports. A "consumer report" is a summary of a person's personal and credit characteristics, general reputation, and lifestyle, which is prepared by a "consumer reporting agency" (CRA). Before an employer is permitted to get a consumer report for employment purposes, the employer must disclose to the applicant, in writing on a *separate* sheet of paper, that a report may be used. The employer also must obtain the applicant's written authorization to obtain the consumer report. A special disclosure is required "investigative consumer reports," which are reports containing information on a person's character, general reputation, personal characteristics, or mode of living based on personal interviews with a person's neighbors, associates, and friends. Employers who intend to obtain investigative consumer reports must tell the applicant or employee about the request within three days making it. The employer must also provide a summary of consumer rights under the FCRA, available on the Internet at ftc.gov/os/-statutes/2summary.htm. The employer must also tell the applicant or employee of his or her right to obtain a complete and accurate disclosure of the nature and scope of the investigation upon written request. The employer must respond to such a request within five days after it is received. If the employer decides to take adverse action based on a consumer report, FCRA imposes additional disclosure obligations.

Before taking the adverse action, the employer must provide a "pre-adverse action disclosure" that includes a copy of the individual's consumer report and a copy of the consumer rights under the FCRA discussed above. The purpose of this requirement is to give the employee or applicant a chance to respond to the report before the adverse action is taken. After the action is taken, notice that the action has been taken must be provided and it must include (1) the name, address, and telephone number of the CRA that supplied the report; (2) a statement that the CRA which supplied the report did not make the decision to take the adverse action and cannot give the specific reasons for it; and (3) a notice of the individual's right to dispute the accuracy or completeness of any information the CRA furnished, and his or her right to request an additional free consumer report from the agency upon request within 60 days.

Commentators on privacy rights generally agree that they are in danger of disappearing altogether, and that employers are generally free to intrude on employees' privacy as much as they like. Nevertheless, employers should be advised to proceed with reasonable caution in the area of workplace privacy, not only for legal reasons, but also to preserve employee morale and to avoid costly litigation. ◆

BOOK REVIEW

continued from page 36

adultery under District of Columbia law, and, thanks to a statutory repeal in 1994, was not itself a sexual felony. Clinton did, however, in Posner's estimation, almost certainly obstruct justice in violation of federal criminal law in several respects: he perjured himself in his deposition in the Paula Jones case, before the grand jury, and in response to questions put to him by the House Judiciary Committee; he tampered with a witness by encouraging Lewinsky to file a false affidavit and then to secrete gifts that were subject to a subpoena; he suborned perjury by Lewinsky. Applying the Federal Sentencing Guidelines, Posner estimates that a first-time offender convicted of these crimes would receive a prison sentence of thirty to thirty-seven months.

In Chapter 2, Posner absolves Ken Starr of most of the charges leveled against him and refutes the principal arguments made in Clinton's defense. Posner thinks little of the accusation that Starr leaked grand jury testimony and he thinks even less of what he calls "the White House's slander machine." Contrary to the suggestion that only Starr would have pursued the sex-related claims against Clinton, Posner argues that a hypothetical ordinary prosecutor would have grounds for prosecuting a hypothetical high-status defendant who had done what Clinton did. Posner writes: "Such a lengthy string of crimes would invite prosecution, especially if the criminal was a prominent person already under investigation, by the same prosecutor, for other possible criminal activity." To Posner, the most compelling criticism of Starr is that the Starr Report gratuitously invaded the President's privacy, but as we shall later see, some of the most salacious details are not without relevance. The fact that Starr uncovered so much detail is largely attributable to Clinton's decision to deny what he had done and to the enactment of the independent counsel statute.

In Chapter 3, Posner debunks the argument that impeachable offenses must be crimes, reasoning that "high Crimes and Misdemeanors" had no such settled definition, the colonial practice was to the contrary, and that such a limitation would be inconsistent with the constitutional structure, which specifies that impeachment is the only means to remove a President from office. And since a President can commit horrific acts in private, it would be unsound to limit impeachable offenses to conduct taken in an official capacity.

All of this is a prelude to the questions of how bad Clinton's conduct was and whether it justified impeachment and removal from office. Posner uses as his standard "the nation's current moral code," which, according to Posner, means that Clinton could not appropriately be punished for having oral sex with a subordinate who is not his wife, or for misleading family, friends, associates and the public—the only wrongs for which Clinton apologized. Posner observes that Clinton's lies and obstructions of justice, however serious they

may be deemed by lawyers and judges, were not seen as disqualifying in the eyes of most Americans, who had little sympathy for Paula Jones or the politically-minded lawyers who financed her case against the President.

Posner's most provocative argument is that the case for impeachment and conviction could have been pitched most powerfully "on the ground of disrespect for his office and for decency in the conduct of government." Posner pulls no punches:

> Talking on the phone to members of Congress while being fellated was not even a minor crime; but it displayed a deep disrespect for the Presidency. It has been said that President Reagan always put on a necktie before entering the Oval Office, as a sign of respect for the sanctum sanctorum of the Presidency, the chapel of our civic religion ... Clinton's disrespect for the decorum of the Presidency, especially when combined with the disrespect for law that he showed in repeatedly flouting it with his barefaced public lies, constitutes a powerful affront to fundamental and deeply cherished symbols and usages of American government, an affront perhaps unprecedented in the history of the Presidency. Imagine a President who urinated on the front porch of the White House or burned the American flag; these acts could be thought metaphors for what Clinton did.

Posner notes that neither Starr nor the Republicans on the House Judiciary Committee sought impeachment on these grounds. Posner thinks this "may be a symptom of a change in expectations concerning political leadership that Max Weber's concepts of charisma and rationality can help us see." Under this theory, our current period of peace and prosperity means that Americans are not looking for an authority figure in the White House. We only want a competent professional politician and we are reluctant to risk the destabilizing effects of removing a President whose policies are generally sound. This, at least, appears to be Posner's own view. Without taking a firm stand on whether Clinton should have been impeached or convicted, he closes his book with the thought that "Americans have reached a level of political sophistication at which they can take in stride the knowledge that the nation's political leaders are their peers, and not their paragons."

I cannot help but wonder if we should be especially thankful that the Framers of the Constitution did not entrust any aspect of impeachment proceedings to the federal judiciary.

A year of hindsight in which the Republican presidential candidates each appealed to voters by promising to restore honor and dignity to the White House suggests a different thesis. Perhaps the House Republicans blundered by not pressing for impeachment on the grounds suggested by Posner, and instead trying to prove perjury and obstruction of justice without discussing Clinton's underlying conduct. After all, Clinton lied for a reason. He feared the truth would be politically devastating. His greatest moment of political jeopardy was the weekend before he forcefully denied having sexual relations with Miss Lewinsky. Even at the time the Starr Report was sent under seal to the House of Representatives, politicians on both sides of the aisle were uncertain where the American public stood. Whether out of weakness, fecklessness or a misplaced sense of decorum, the Republicans made the fateful decisions to disseminate the Starr Report on the Internet, televise the President's grand jury testimony, and let the salacious facts speak for themselves.

In a chapter titled "The *Kulturkampf*," Posner attempts to explain why the debate over Clinton's impeachment became so passionate and caused so many intellectuals to overlook the President's lies and crimes. Brushing aside the fact that it was the President's defenders who pressed the argument that the entire scandal was "just about sex," Posner argues that because the Right chose to turn the Clinton affair into a debate about the values of the 1960s, the Left united behind Clinton and forced *the public to take sides.*

It would be more accurate to say that the unmasking of Clinton's affair unavoidably became a high-stakes battle in the continuing *Kulturkampf* over the status of inherited prohibitions in our laws and in our society. Because of the centrality of the culture war in American society, winning the battle subordinated all other concerns. In the aftermath of the fight, one thing has become clear. Whether the Clinton affair represents an unprecedented cultural low or a new level of political sophistication, our politicians and our judges now have a better understanding of where the majority of the American public stands. ◆

BOOK REVIEW

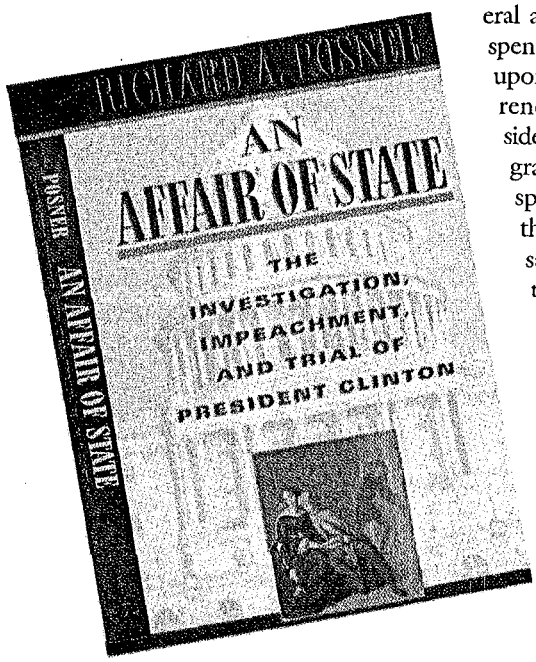
THE CLINTON AFFAIR AS DRAMATIC COMEDY

Joel Friedlander

AN AFFAIR OF STATE: THE INVESTIGATION, IMPEACHMENT, AND TRIAL OF PRESIDENT CLINTON

Richard A. Posner

(Harvard University Press, 276 pp.)



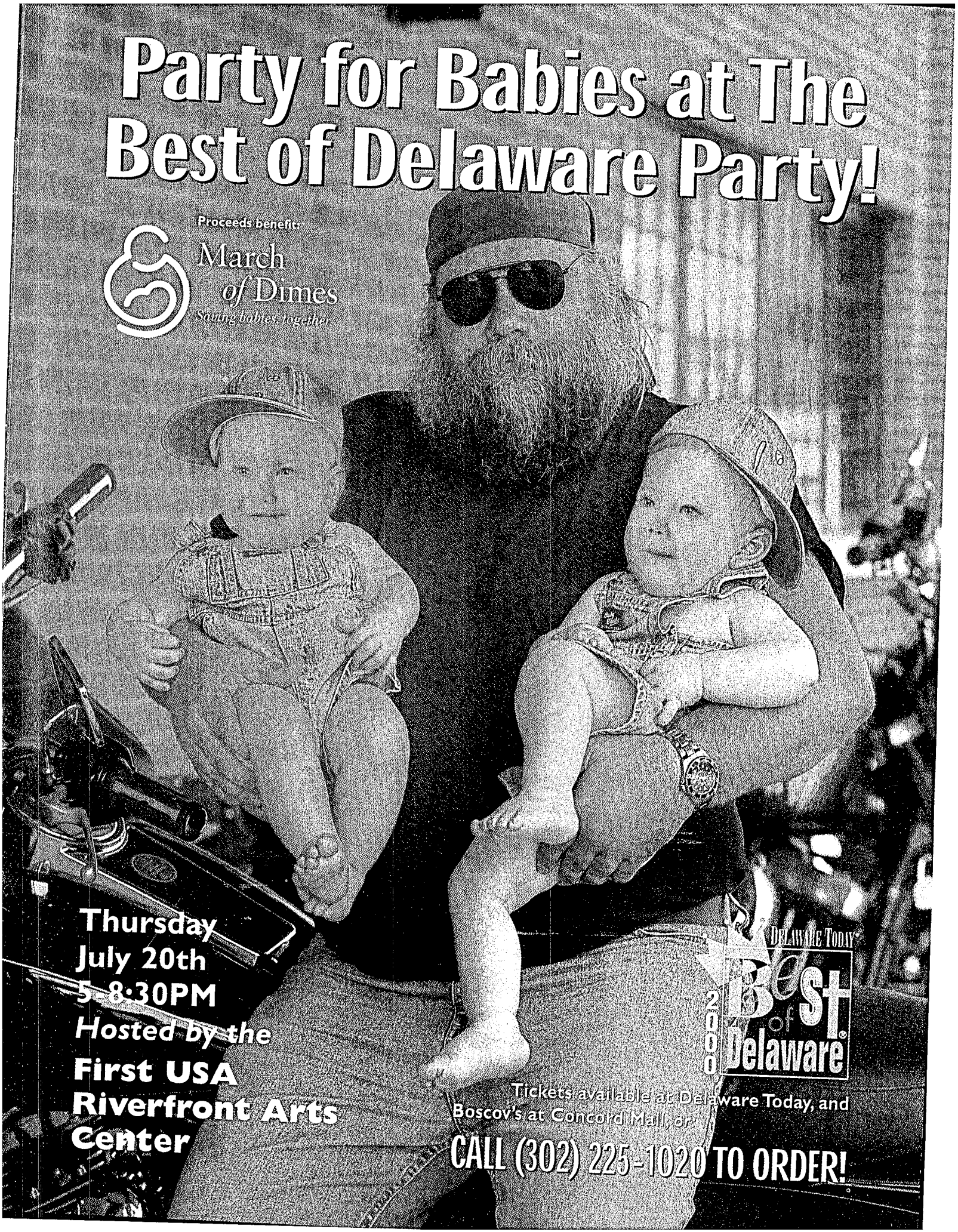
By writing *An Affair of State*, Judge Richard Posner has performed at least one important public service. He has brought to bear upon the controverted legal questions surrounding the investigation and impeachment of President Clinton the immense talents that have won him acclaim as a federal appellate judge. Anyone who spent portions of 1998 reflecting upon the punditry and advocacy rendered on behalf of the President and his opponents can be grateful that Posner decided to spend his evenings appraising the Starr Report and its thousands of pages of supplementary materials.

But that legal analysis accounts for only half of Posner's book. The remaining chapters are devoted to analyzing the moral, political and cultural dimensions of what Posner describes with detached bemusement as "an edifying political drama" and "the ultimate Washington novel." These chapters have their virtues, but given Posner's ultimate assessment that the Clinton affair had no obvious negative effects on the country and two salutary effects—"the shattering of the Presidential mystique" and "the encouragement of franker public discussion of sex"—I cannot help but wonder if we should be especially thankful that the Framers of the Constitution did not entrust any aspect of impeachment proceedings to the federal judiciary.

Chapter 1 begins with a remarkable fifteen-page exposition of "The Facts." Posner's style is concise and authoritative, and he does not shy from drawing inferences from the public record, creating the perception that a familiar tale is being dissected for the first time. These pages would make an ideal teaching tool for how to write a Statement of Facts.

Posner then considers what crimes the President committed. Posner argues that Clinton's sexual relationship with Lewinsky did not constitute sexual harassment, may not have constituted

Continued on page 34


Party for Babies at The Best of Delaware Party!
Proceeds benefit:
March of Dimes
Saving babies together
Thursday
July 20th
5-8:30PM
Hosted by the
First USA
Riverfront Arts
Center
Delaware Today
2006 Best of Delaware
Tickets available at Delaware Today, and
Boscov's at Concord Mall, or
CALL (302) 225-1020 TO ORDER!

YOUR PROTECTION IS OUR PROFESSION

Wilmington, Delaware
302.658.8000

London, England
171.962.2003

BUSINESS

Disability

LIFE/

Professional Liability

Malpractice

PERSONAL

unusual Risks

Health

We know all about protecting the things you value. Since 1940 Zutz has specialized in creating innovative insurance solutions for professionals. We are well known for covering unusual risks faced by firms of all sizes and descriptions.

Zutz professionals tailor complete insurance coverages to meet very specific needs, including comprehensive life and health coverage for you and your employees and personal insurance for your home and valuables.

Over the years, we have earned the endorsement of many professional organizations, including state bar associations, medical and dental societies. For quality insurance protection, contact Zutz, *the last word in insurance.*

www.zutz-pli.com

PLI
Professional Liability Insurance, Inc.

Sponsored administrators for professional liability insurance by the Delaware State Bar Association since 1979. Lawyers who value quality value Zutz.

ZUTZ
INSURANCE