

WHEN THE CONSUMER BECOMES A LITIGANT

Consumers' privacy rights in the world of litigation.

23 January 2001

William E. Fason
Licensed Legal Investigator
SLN A-08111
1302 Waugh Dr #272
Houston, Texas 77019
713.529.4279; fax 713.529.9864
wfason@houston.rr.com

Conflicting visions of consumer privacy rights create a tension between a consumer-oriented model of “fair use” of personal information, and the administration of justice. The strict application of this “fair use” code to the world of investigating and litigating claims would undermine the rights and remedies of parties to legal disputes.¹ Policy-makers should exercise great care in implementing the Gramm-Leach-Bliley Act (G-L-B) and the Fair Credit Reporting Act (FCRA), and in crafting new legislation aimed at protecting consumer privacy and hindering identity fraud so that new rules and laws aimed at protecting consumers in the voluntary marketplace are not misapplied to the adversarial world of litigation.

Many privacy advocates (PA’s) endorse the “Code of Fair Information Practices,” a set of principles first issued by the US Department of Health, Education and Welfare in 1972.²

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

These principles form the public policy agenda of the PA’s, and color their view of issues involving access to public records as well as the distribution of personally identifiable information among private parties.³ The code makes no distinction between information demanded from citizens by the state, and information voluntarily provided to private parties in exchange for goods, services, or credit.⁴ The PA’s seek to codify these principles in laws regulating the business practices of financial services, medical, and legal sectors. Attempting to apply these principles to the world of adjusting and litigating

claims would produce strange results and unintended consequences, shield wrong-doers from accountability, and hamper the administration of justice. They would in fact harm the interests of innocent consumers and victims who seek relief through the courts.

The PA's define the right to information privacy as the right to control the flow of information about oneself. This point of view was succinctly stated by one privacy advocate, "if you want to know something about me, you need to ask me," or ask for permission of the subject to find out. In the field of claims and litigation, adjusters and attorneys do in fact ask subjects for information. Frequently subjects must answer the questions under oath. Nonetheless, claimants frequently make misstatements and outright perjurious statements. How shall a party to litigation check the accuracy of the claims made or the reliability of the person making the claims? Should a subject's "right to information privacy" prevent an attorney from hiring a licensed legal investigator to independently verify – i.e., to investigate – the claims made or the claimant's credibility? Should a "right to information privacy" prevent a legal investigator from conducting research in public records to find out whether a witness to a court proceeding has a prior criminal or civil litigation history that may bear on the reliability of the testimony? Should consumer privacy rights bar a licensed investigator from discreetly contacting private parties with relevant information for the purpose of identifying and locating subjects to litigation?

I find that my own business practices as an investigator, process server, and debt collector could be interpreted as regularly violating this so-called "fair" code. I work with personal information about other people, some of it quite sensitive; I never have the consent or foreknowledge of the subject to whom the information relates; I use information for my investigations which was originally provided for other purposes, and I keep the information long after the related legal case is concluded. Both the law and my contracts with data providers require that I keep the information available for a number of years for auditing purposes.

I locate people who do not want to be located, and contact people who do not wish to be contacted. On paper at least, I may appear to be one of the worst violators of privacy were it not for the fact that every case which my firm handles is in connection with or in anticipation of litigation. By the time a file lands on my desk, the transaction has left the realm of voluntary transactions in a free market and entered the arena of adversarial claims in search of adjudication.

The first rule forbids a “personal data record-keeping system whose very existence is secret.” The existence of my investigations company is a matter of public record, and licensing information is even available through the world wide web.⁵ While the existence of my investigations firm is not a secret, my “personal data record-keeping system,” i.e., my computer, my file cabinet and the files therein, is in fact confidential. While I am obligated to keep case files confidential, they are not privileged from discovery in the event that the Texas Commission on Private Security or some other agency or court issues a subpoena for them. In the event that my firm undertakes an investigation at the request of an attorney, then the ensuing report, file, notes, and related documents become attorney work-product, and are protected by attorney-client privilege. While such privileged documents are beyond ordinary discovery, there is a sufficient fraud-crime exception to allow accountability in the event that a court decides there are reasonable grounds to believe that an actual crime was perpetrated. In order for my firm to function properly, I must keep and I am in fact obligated to keep them confidential. An exception is that a licensed investigator must “divulge to any law enforcement officer or a district attorney, or his representative, any information he may acquire as to any criminal offense, but he shall not divulge to any other person except as he may be required by state law or court order so to do, any information acquired by him except at the direction of the employer or client for whom the information was obtained.”⁶

The second rule holds that “there must be a way for a person to find out what information about the person is in a record and how it is used.” This principle has shaped recent reforms of and Federal Trade Commission (FTC) interpretations of the Fair Credit Reporting Act (FCRA).⁷ If a consumer is denied credit, employment, or some other

benefit on the basis of a report generated by a consumer reporting agency, then the law states that the subject has the right to obtain a copy of the report. In the past, employers, creditors and others could make decisions affecting the consumer on the basis of secret information, denying the consumer the opportunity to challenge the accuracy of the information. Bewildered innocent consumers who were mistaken for convicted criminals found themselves caught up in a Kafkaesque nightmare, denied employment or credit by a faceless machine that had no obligation to divulge or verify credit reporting data.⁸ The incorporation of this second principle into the FCRA is for the most part beneficial and just. While most employers and creditors have had little trouble adapting to the rule, some employers, such as public safety agencies, do not want to have to provide a copy of the background report to the applicant. They want their third party investigators to be able to assure all witnesses that their comments about the applicant will be held in strict confidence.

Observers spotted an unintended consequence of the 1996 amendments to the FCRA. The FTC has interpreted the amendments to the FCRA as requiring the permission of a suspect before any third party investigation can be conducted in the workplace, and as mandating that any report prepared by any third-party investigator be provided in unedited form to the suspect employee if any adverse action is taken against the employee.⁹ That information could include a list of witnesses who first identified the suspect employee. This dictum, if upheld by the courts, would seriously hinder investigations of internal theft, fraud, illegal drug use and sales in the workplace, sexual and racial harassment, and workplace violence. Prior notice would tip off the suspect, allowing him to destroy evidence, pressure witnesses, or otherwise sabotage the investigation.

The FTC recognizes the unintended negative consequences of the application of the FCRA to workplace investigations. Chairman Robert Pitofsky stated that the FTC “agrees that legislation to relieve an employer of those enumerated requirements is warranted.”¹⁰ Attempts to rectify this problematic interpretation of FCRA were stymied during the 106th Congress when H.R. 3408 died in committee.

The second rule of the “fair code” also animated Senate Bill 2328, the “Identity Theft Prevention Act of 2000” introduced 30 March 2000 by Senator Dianne Feinstein. There is no question that the panoply of crimes under the category “identity theft” is a serious matter of national importance which must be addressed.¹¹ In our economy built around instant credit, it is a relatively easy form of white collar crime to commit, the chances of successful investigation and prosecution are slim, and the punishments meted out to perpetrators have been lenient. The true damage to consumers comes when defrauded creditors make false, derogatory reports to credit reporting agencies, damaging the reputations of innocent consumers. Surprisingly, there is no study which documents the true incidence of identity fraud, but it appears to be on the increase. Since the misappropriation of personal information is critical to the commission of such crimes, it is no surprise that Congress should address the matter by considering the enactment of legislation to regulate more strongly the transmission of personal information.

Section 6 of Senate Bill 2328 would have required all consumer reporting agencies once per year and free of charge to provide a copy of all information relating to the consumer - with the exception of credit risk scores. The requirement that these reports be provided for free only means that the cost of providing them is to be borne by the consumer reporting agencies.

Section 8 defined “individual reference services provider” (IRSP) and would have imposed onerous requirements on them. An “individual reference service provider” was defined as any person who for a fee regularly engages in the practice of “creating, assembling, evaluating, or providing, either directly or as a supplier to others, with respect to any person regarding any 2 or more items of information described” below:

- (A) Social Security Number or other social security information;
- (B) mother's maiden name;
- (C) prior address;
- (D) birth date;

- (E) criminal history;
- (F) history of civil actions;
- (G) driving records;
- (H) vehicle information;
- (I) past employment history;
- (J) income level;
- (K) tax records;
- (L) history of voter registration; and
- (M) other similar information, as determined by the Federal Trade Commission.

Section 8 defined IRSP so broadly as to encompass not only the operators of specialized databases, but also licensed private investigations firms, title companies, debt collection agencies, law firms, newspapers, magazines, and other news reporting outfits. It might also have included the Mormon Church for its massive genealogical files, or the TV show “America’s Most Wanted.” AMW collects, assembles and provides commercially information about the criminal history, date of birth, and other identifiable information of suspects and fugitives. The full reach and scope of this bill would have been difficult to predict as the very troublesome Section 8(M) delegated authority to non-elected executive branch bureaucrats to "fill in the blanks" later on. The bill would have forced anyone defined as an IRSP to make available all information in his files regarding a consumer to the consumer to whom the information relates within ten days of a demand by a consumer.

There are a number of serious problems with this bill. First, there is no evidence that the specialized, commercial individual reference services which Section 8 seeks to regulate play any substantial role in the commission of identity fraud.¹² This may come as a surprise to those who have heard the steady drumbeat in the media concerning allegations that the wave of identity fraud is supposedly caused by access to personally identifiable information on the Internet. There is already a law which criminalizes the provision of personal identifiers, such as Social Security Numbers, for the purpose of committing fraud.¹³ The major individual reference services already screen their clientele to prevent

access by criminals and conduct audits of their customers to ensure that the information provided is used for certain authorized purposes in accordance with the terms of service.¹⁴ Individual reference services cooperate with inquiries from law enforcement agencies in order to determine whether information was wrongfully obtained through their dial-up computer systems.¹⁵ Secretive organized crime rings which wrongfully obtain and misuse information about consumers will of course not be affected by Section 8's requirements on legitimate, above-ground businesses. While this bill employed the language of fraud prevention, there is no reason to think that the passage of Section 8 would have any discernible effect on the very real problems of identity fraud.

Second, Section 8 disregards the property rights of people who work with information. The files in my office are the property of my firm, even if they contain information that somehow pertain to other people. Absent a contractual relationship with the consumer to whom it relates, I do not hold the information in my files "in trust" for the subject.¹⁶ If someone wants to see my files, then he needs to ask me. If he has grounds to believe that information about him in my custody has somehow been misused, then he should access the legal system. In the name of consumer privacy, the bill would violate the rights of private parties to be secure in their houses, papers, and effects, against unreasonable searches.

Third, if the information and reports collected, assembled, or provided by my firm are used to make decisions regarding the consumer's ability to obtain employment, credit, housing, or other benefits, then they fall under the purview of the Fair Credit Reporting Act (FCRA). There are already mechanisms in FCRA that address the concern that erroneous information might be provided to an employer, creditor or other decision-maker, resulting in possible adverse action. Suppose that my firm performs a pre-employment background check which uncovers a criminal record or other derogatory information regarding a consumer who is applying for a job. If the employer rejects the candidate on the basis of my report, then the consumer may demand a copy of the report or record which my firm obtained or generated. This gives the person against whom adverse action was taken an opportunity to review the information, and correct it. It is

possible in the above example that the criminal record actually pertains to someone with the same or similar name. Allowing a consumer a chance to review the derogatory information builds a measure of accountability into the credit reporting system, and works to prevent abuses and unfair decisions. While such a principle may be fair within the context of a consumer seeking fair play in the marketplace, it is unrealistic to apply this FCRA-style model to non-credit situations, particularly investigation in anticipation of litigation.

Fourth, this investigator is frequently retained to create, assemble, evaluate, and provide to others information about people for the non-FCRA purpose of investigating or litigating claims, or otherwise resolving disputes through the legal system. If and when my client – usually an attorney or insurance adjuster - believes that the time is appropriate, he may introduce the report, information, or attached exhibits into evidence before a court or tribunal in order to persuade a decision-maker, i.e., a judge or jury, to take a particular course of action. At that time, the rules of court already allow the subject to whom it relates to challenge it, or explain it, or otherwise refute it. Converting a “consumer right to privacy” into carte blanche subpoena power against the attorneys and investigators of adverse litigants would undermine due process and the rule of law. Litigation is a form of information warfare fought according to its own rules, not according to rules handed down originally for the purpose of granting the privilege of credit, or deciding qualification for receiving welfare benefits. Requiring a licensed investigator to turn over his file, notes, and related documents upon demand by any consumer who comes knocking would compromise legitimate investigations. For example, it could allow a wrongdoer to flee the jurisdiction before the service of legal process, to fraudulently transfer assets, to destroy evidence, or otherwise to engage in bad conduct.

Imagine a court case against a stalker or sex-harasser in which a legal investigator’s entire work file would *have* to be revealed to the defendant upon his request. Who would ever give a statement to an investigator knowing that all remarks would have to be turned over at the whim of the subject?

Fifth, in 99 percent of the cases handled by my investigations firm, the client is in fact an attorney, and therefore the reports which my firm generates become confidential attorney-work product, privileged from ordinary discovery. S. 2328 would have foisted upon legal investigators a duty of disclosure to the consumer/adversarial party which would be at odds with the attorney-client privilege. How shall such conflicts of duty be resolved? The bill does not contemplate these unintended consequences, much less address them. Even if licensed investigators are exempted from Section 8's definition of IRSP, the bill still has serious conflicts with the First and Fourth Amendments to the Constitution.

A consumer, whether the victim of fraud or of misinformation from a creditor or credit bureau, already has remedies under the FCRA, and can file a criminal and/or a civil complaint for damages. A consumer who seeks certain privacy practices is free to negotiate such arrangements with his vendors and creditors. I know of one consumer who operates in the credit economy without having to provide his social security number (SSN). I know of another who does not care who has his SSN, but has arranged his affairs so that his home address does not appear in any public or credit records. A consumer who has been libeled by a creditor in the case of identity fraud can now file a criminal complaint against the perpetrator of fraud, as well as file suit against the creditor for the ensuing damage to his reputation.¹⁷ A consumer who thinks he has been harmed by a licensed investigator can file a complaint with the state licensing board, which can easily subpoena the investigator and his file. Or the consumer can file a suit or even criminal complaint directly against the investigator alleging any number of specific violations of privacy. Suppose that an investigator prepares a report containing erroneous information for an attorney which results in adverse action in the form of an innocent consumer's bank account being temporarily frozen until the mistake is uncovered. In such a case, the innocent consumer may have a cause of action for wrongful execution against the investigator. A consumer could file a claim against the investigator's insurance or bond. Consumers already have rights and remedies under legislation and at common-law for real violations of their privacy.

The third rule is that information about a person that was obtained for one purpose should not be used for other purposes without the person's consent. This would prevent "secondary uses" of information. The argument is that an address given to the state driver license bureau should be used only for driving-related purposes, and an address given out to obtain credit should be used only for the purpose of granting credit to the consumer. PA's argue that neither address should be used for the service of legal process unless the consumer at the time he gave out the address checked off a box explicitly stating, "I authorize this information to be used for the purpose of locating me for service of legal process." In the case of credit data, the facts are that consumers who apply for credit frequently sign a release authorizing the re-disclosure of information for certain lawful purposes.

The general application of this third rule to our legal system is particularly impractical. Who in his right mind gives out information for the purpose of allowing others to prove up a legal cause of action? Successful fraud investigations depend upon the ability to compare statements made for one purpose with statements made by the same subject for another purpose. For example, a con artist will lie to a bank about his assets in order to obtain credit, and then may lie in a different direction years later in a bankruptcy proceeding. It is the calling card of dishonest people that they tell completely different stories at different times in order to exact advantage. As there are no truly reliable and accurate nationwide databanks available to the private sector for conducting criminal or civil litigation background checks, legal investigators use information derived from credit headers to establish or verify a subject's address history in order to conduct public record research in those jurisdictions. A ban on the secondary use of information would critically undercut successful investigations of fraud.

We consider now the third rule's application to post-judgment asset investigations. When two people get into a legal dispute, the person who gets to court first becomes the plaintiff, the other the defendant. When one party wins the court case and is awarded damages, in reality that person does not win money, but rather a judgment for money. The winner of the lawsuit become the judgment creditor; the loser the judgment debtor.

The money judgment is actually a hunting license giving the creditor the right to use legal process to discover and attach the debtor's assets. Under the FCRA, at this point the judgment creditor (or his agent) may legally obtain a consumer credit report about the judgment debtor for the purpose of enforcing the money judgment. Consumer credit reports provides information about a subject's financial life, and are regulated by the FTC under the FCRA. A person may not obtain a consumer credit report without a legally-defined "permissible purpose." The distribution of credit reports is also controlled by the contracts of the credit bureaus themselves. By virtue of the fact that the winner of the lawsuit becomes a creditor of the consumer-turned-judgment debtor, he may legally obtain a consumer credit report about the debtor without having to obtain his permission or even to first notify him. Why? What about the privacy rights of the debtor? The law recognizes that the prerogatives of justice supercede the normal privacy rights of the debtor. The "right to information privacy" is not an all-purpose trump card to be played by wrong-doers to obstruct the enforcement of laws and legal judgments. And yet, some PA's are working to prevent anyone, including judgment creditors and custodial parents owed child support, from obtaining a consumer credit report without first obtaining the permission of the subject. The US Public Interest Research Group (PIRG) is on record as endorsing legislation that would bar the release of consumer credit reports without the express consent of the consumer to whom it relates.¹⁸ Although such provisions are couched in terms of preventing crime and invasions of privacy, the unintended consequences would allow for perpetrators to escape justice.

This third commandment drives the opposition to the use of credit header data for purposes other than the extension of credit. When applying for credit, a person fills out an application with personal information. When the applicant's credit report is obtained by the creditor, the credit file is updated to reflect the new information regarding the name and address of the subject. In 1994 the FTC ruled that such information relating solely to the identity and location of the subject can be parceled out from the body of the credit report and sold separately. The bureaus began selling this information, called "credit header information," to specialized database providers for use by lawyers and licensed investigators in identifying and locating people. (A credit header typically

contains the consumer's name(s), most recently reported addresses, month and year of birth, and whatever SSN(s) the consumer is using in the credit economy. It contains neither the subject's mother's maiden name, nor any financial information such as the consumer's creditors, purchases or bill-paying history.) Ed Mierzwinski, director of USPIRG, no doubt articulated the perception of many privacy advocates when he stated in *The National Journal* that the sale of credit header data is "probably the most unfair secondary use of personal information."¹⁹

Should a licensed investigator attempting to locate a defendant in a lawsuit be allowed to access credit header data? Rephrased, may someone authorized by law to locate other people for a fee be allowed to contact the creditors of the subject (either directly or through a credit bureau) and discreetly inquire as to the subject's location for the purpose of service of legal process? May a creditor provide a current address to such a person without fear of incurring liability for "invasion of privacy"? If you answered no, then the next question becomes, may a licensed legal investigator contact neighbors, friends, relatives, associates, enemies or anyone else in order to obtain the location of the defendant *absent the express permission of the consumer*? Perhaps a former neighbor of the subject heard in casual conversation that he planned on moving to Alaska. Should that person be allowed to reveal this fact to the investigator? A strict application of the third commandment would indicate a negative answer. After all, that neighbor did not get explicit permission from the subject to reveal this fact to an investigator. The third rule is predicated on the idea that a person "owns" the facts about oneself. Maintaining privacy in one's address is inevitably claimed as necessary to prevent stalking, harassment and fraud. In this sense, the privacy issue is in reality a proxy for crime prevention issues, but its application in the context above is inappropriate.

My argument is that as a licensed legal investigator, I am authorized by the laws of the State of Texas to locate individuals for a fee. In nearly every missing-person case I work, I have been retained by an officer of the court to locate a subject for the purpose of serving that person with legal process – either a summons, subpoena, warrant, or some other judicial writ. Some of these are witnesses whose testimony is critical in criminal

defense cases. Others are parties entitled by law to certain legal notices. Examples include missing or unknown heirs, owners of abandoned property, and absent spouses or presumed biological parents. The right to notice of legal actions is codified in the Fifth Amendment to the US Constitution. In the event that a missing spouse cannot be located, the court orders service by publication, and the divorce citation is published in a newspaper. What can start as a quiet, obscure event at the courthouse can thus spill into the pages of the daily newspaper between the obituaries and the cartoons, with all the negative implications for the privacy of the parties.

At times, I am called upon to locate bad actors who are intentionally attempting to escape detection. Examples include participants in accidents, including hit-and-run cases, suspected con-artists, thieves, rapists, and others who must be brought into court. I frequently use credit header data in my investigative work to correctly identify or locate a subject. Privacy advocates consider this to be an unfair use. "It's an intrusion," they claim. It might be an intrusion, albeit a slight one, but so is being named a defendant in a lawsuit, as a private dispute becomes a matter of public record. It is also an intrusion to appear uninvited at someone's home, knock on his door and hand him a summons. Yet, such intrusions are necessary for the administration of justice. The world does not and must not revolve around the "right to privacy" of a consumer who becomes a party to a suit.

If you need to know something and you do not have the subject's permission, then go get a subpoena or court order, argue PA's. So a third party needs government permission in order to exercise First Amendment rights? Besides, the "go get a subpoena" argument fails in the above-described case. A licensed PI or process server seeking a defendant *already* has legal process issued with the subject's name on it, a demonstration of the legitimacy of the request, even if it is not legal process directed at any particular custodian of records or the subject's ex-neighbor. Why should it be necessary to have even *more* legal process issued each and every time a new witness is encountered who might have information about the location of the subject? Getting legal process issued and served is not cheap. Requiring a plethora of subpoenas would needlessly complicate

the issue and drive up the price of simple legal-investigative services, while not providing any appreciable layer of “protection” to the consumer-defendant. At this point, some PA’s adopt a stance of “that’s not our problem, that’s the courts’ problem.” In truth, it is the problem of any consumer or victim who seeks redress through the courts. A common complaint about our legal system is that justice is only for those who can afford it.

In the context of litigation, it would be a mistake to apply such “pro-privacy” rules as notice, consent, opt-out, and other so-called fair information provisions hailed by the privacy rights movement. The world of litigation is not a marketplace; it is an adversarial arena in which an information war is fought according to its own rules. The type of notice that is given is the kind that comes knocking on the door unexpected, hand-delivered by a deputy or process server. It comes with or without the consent of the subject, and there is no right to opt-out. Unfurling the flag of consumer privacy to prevent the detection of the subject for the purpose of service of legal process is the equivalent of giving every defendant the right to say, “King’s X, you can’t catch me, because I opt-out.”

Guided by the principles of choice, notice, and opt-out, Congress passed the Gramm-Leach-Bliley Act of 2000, setting forth more regulation of the use of consumer data in the financial services market. The FTC has interpreted these rules in ways that will produce bizarre implications for debt collection, particularly post-judgment. There is a market for unpaid money judgments as judgment creditors decide they would rather sell their uncollected judgments. The buyers of these judgments typically have backgrounds in law, investigations, and collections, and are willing to risk their own time, skill and money to locate the debtor, use legal process to attach his assets, or otherwise negotiate a pay-out arrangement. The professional judgment collector steps into the shoes of the original judgment creditor in terms of using the legal process to discover and attach the debtor’s assets.

The FTC considers judgment collectors to be collection agencies, thus falling under the definition of “financial institutions” with all attendant responsibilities under the G-L-B

Act.²⁰ “After careful consideration of the comments and purposes of the Act, the Commission retains its view that if a business purchases a defaulted account for collection,” it then establishes a “customer relationship” with the account debtor as soon as it locates the individual and tries to obtain payment on the debt.²¹ At this point, the judgment collector is obligated to comply with G-L-B in the same way as, say, a bank must comply regarding one of its customer’s account. The collector must provide to the debtor an initial notice as well as annual notices thereafter regarding the debt collector’s privacy policies and practices regarding the redistribution of nonpublic information about the debtor. The collector must not disclose nonpublic personal information about a debtor to nonaffiliated third parties unless the collector satisfies various disclosures and opt-out requirements, and the debtor has not elected to opt-out of the disclosure.²²

The FTC’s interpretation of G-L-B to the field of debt collection is perplexing. The G-L-B Act was passed to provide rules for protecting consumers of financial services within the context of a marketplace. It is a mistake to attempt to superimpose a consumer-rights model to the adversarial and litigious world of debt collection, particularly post-judgment collection. Judgment debtors are not “customers” of the judgment collector in any meaningful sense of the word. They are in fact defendants entangled in the legal system, not consumers shopping for a mortgage. Judgment collectors are not “servicing a consumer’s account,” they are investigating the debtor and enforcing a money judgment through lien and levy. Judgment debtors do not “consume financial services,” they tend to try to hide their assets and dodge process servers.

The process of judgment collection involves filing writs and liens, instruments which by necessity contain personal and nonpublic information about the debtor: his identity, location, property, and the existence of the debt. A correctly prepared abstract of judgment should contain the debtor’s full name, maiden name or aliases, date of birth, driver license number, home address, and (if it can be determined) the debtor’s Social Security Number. It requires specificity so that an innocent Robert Smith is not confused with a debtor of the same name. An abstract of judgment is publicly filed in the deed records in the county where the debtor lives, conducts business or owns property, in order

to create a judgment lien which attaches to real estate owned by the debtor, and to put his creditors on notice. It is reported by the specialized court newspapers and invariably ends up reported to the credit bureaus, ultimately included in the debtor's credit report. It is as public as public can be, and yet the FTC's own rules forbid the re-disclosure of personal information of the "consumer" to a non-affiliate if the "consumer" has objected. The judicial system says otherwise; the public notice of the abstract of judgment is intentionally posted for all to see.

Future regulation of credit header data should at the very least recognize a "judicial permissible purpose" for pre-litigation situations in which justice demands that the consent of the subject not be obtained. Such a permissible use has precedent under current law. Reacting to concerns about stalking, in 1993 the United Post Office stopped giving out change of address information or boxholder information to anyone who walked in and paid a nominal fee. While now such information is not releasable to the general public, it is still available to attorneys, process servers, and legal investigators in order to locate subjects for service of legal process.²³ The applicant must fill out and sign a form under penalty of perjury, and provide proper identification evidencing his role as a legitimate requester.

"There are other ways to locate people besides using credit headers," goes one argument. Yes, it is possible to locate people without credit header data. One can work the phones contacting the subject's neighbors, friends, relatives, creditors, debtors, and business associates in order to locate the subject. Shall I explain to each and every one of them that an investigator is out looking for the subject?²⁴ That he has been named as a defendant in a court case? People would talk, and would embellish the story as it made the rounds. As anyone who ever played the game "Telephone" in elementary school knows, eventually the story would be, "Did you hear that Bobby Lee is wanted? Yep, the law was out looking for him. I wonder what he's guilty of..." What impact would that have on the subject's privacy? All things considered, discreetly using credit header data to locate a subject is actually one of the *least* invasive methods of skip-tracing.

If consumers are allowed by law to opt-out of “their” credit header data being used for judicial purposes, why stop there? Why not allow them to opt-out of getting served with a lawsuit entirely? “I don’t accept service, take these papers back,” more than one defendant has pleaded with me. Since getting caught up in legal action is necessarily intrusive, why not just allow consumers to opt-out of being enmeshed in litigation as well? After all, you don’t really want some process server to track you down and serve you with a lawsuit, do you?

The fourth rule holds that “there must be a way for a person to correct or amend a record of identifiable information about the person.” As I have pointed out, the introduction of information about a person into evidence before a court or tribunal gives the subject about whom the information relates ample opportunity to challenge the accuracy of the information.

The fifth rule concerns the responsibility of data-handlers to assure the reliability of information and take steps against its misuse. This rule will meet no argument from licensed investigators whose professional reputation depends upon providing accurate information and guarding against the misuse of information.

As the 107th Congress convenes to take up the issue of privacy, policy-makers should not promulgate rules in the name of consumer privacy which undermine property rights, victims’ rights, freedom of expression, freedom of contract, or the rights of litigants to pursue justice through the courts. Creating *ex novo* a new “right to privacy” divorced from property rights but instead based on the five commandants of the Code of Fair Information Practices would undermine our existing rights and freedoms. Applying the consumer privacy rights model to the legal system would undoubtedly drive up the fees for routine services, ultimately increasing costs to the consumers of legal services and preventing the administration of justice. The “right to privacy” should not become the right to escape the jurisdiction of our nation’s courts while continuing to enjoy the benefits of the credit economy. The “right to privacy” must not become a license to walk away from one’s legal or financial responsibilities, knowing that an aggrieved party will

not have the capability or resources to catch up. Simply put, a “right to privacy” must not be perverted into a shield for scoundrels. When Congress examines legislation to regulate credit header information and public records, it should recognize that the administration of justice requires access to personally identifiable information in order to allow informed decisions about a correctly identified, discrete individual.

Fason is an investigator, debt collector, and process server.

¹ My use of the term “claims” is not limited strictly to insurance cases, but applies to any legal dispute in which adversarial parties make conflicting claims which may require litigation before a court or tribunal.

² The Code of Fair Information Practices, http://www.epic.org/privacy/consumer/code_fair_info.html

³ By privacy rights community, I refer to Electronic Privacy Information Center (EPIC), Center for Democracy and Technology (CDT), Privacy Rights Clearinghouse (PRC), Privacy Journal, Privacy Times, and the American Civil Liberties Union (ACLU).

⁴ I include here the incessant demands by the state for a citizen’s Social Security Number as a condition of his receiving a license to drive, travel, hunt, fish, marry, divorce, or keep and bear arms; to own property; or to receive education.

⁵ <http://www.tcps.state.tx.us/>

⁶ Vernon’s Civil Statutes, Art. 4413(29bb), Private Security Act, Section 28(a).

⁷ The FCRA can be viewed at <http://www.ftc.gov/os/statutes/fcrajump.htm>.

⁸ Such problems persist in the cases of identity fraud.

⁹ See FTC Chairman Robert Pitofsky’s letter to Representative Pete Sessions dated 31 March 2000.

<http://www.ftc.gov/os/2000/03/sessionletterrehr3408.htm>. This requirement also applies to law firms.

¹⁰ Ibid.

¹¹ I prefer the more conceptually accurate term “identity fraud” over “identity theft.”

¹² See my article, “SSNs and Credit Headers: Tools of Fraud or Internet Urban legend?” The Texas Investigator, November/December 2000.

¹³ In fact, identity fraud is prosecutable under a variety of statutes. Most recently, on 28 January 1998 President Clinton signed into law the “Identity Theft and Assumption Deterrence Act of 1998,” which makes it a crime to knowingly transfer or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law...”

Also, see Title 42, Chapter 7, Section 408 of the Social Security Number which outlaws the misuse of Social Security numbers, a common element of identity fraud. The Social Security Act of 1935 states that “whoever, (1) for the purpose of obtaining anything of value from any person, or for any other purpose, with intent to deceive, falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person, or (2) discloses, uses, or compels the disclosure of the social security number of any person in violation of the laws of the United States; shall be guilty of a felony and upon conviction thereof shall be fined under title 18 or imprisoned for not more than five years, or both.”

Title 18, Chapter 47, Section 1029 defines access device fraud to include the use of any “account number” to obtain money, goods, or services. The offense is punishable by a \$10,000 fine and up to 10 years in prison.

The commission of identity fraud typically involves the commission of several felonies such as larceny, theft of mail, mail fraud, bank fraud, wire fraud, conspiracy, manufacturing false identity documents, and other crimes.

¹⁴ I refer to such companies at Lexis-Nexis, Westlaw, Database Technologies and other major companies in this field.

¹⁵ Statement by Jim Milford, Vice-President of Database Technologies, Inc., 21 October 2000, Galveston, Texas.

¹⁶ Or a purpose governed by the FCRA, explained below.

¹⁷ It is generally understood that most police agencies are ill-equipped to deal with such crime, while those that are – e.g., the Secret Service – refrain from handling such cases unless they involve rather large sums of (federally-insured) money.

¹⁸ PIRG Identity Theft II: Section III PIRG’S Platform, Additional Amendments Needed to Protect Identity Theft Victims. <http://www.pirg.org/reports/consumer/xfiles/page7.htm>.

¹⁹ The National Journal, “The Privacy In Social Security Regulation,” 6 November 2000.

²⁰ Federal Trade Commission “Privacy of Consumer Financial Information,” Rules implementing G-L-B issued April 2000, p.115.

²¹ Ibid, p. 30.

²² Ibid, p. 1.

²³ 39 C.F.R Section 265.6(d) (1989)

²⁴ Or an investigator could use a pretext, with all the incumbent risks. The Gramm-Leach-Bliley Act made illegal the use of pretexts for financial information. The FTC has interpreted “financial information” in certain situations to include mere identity and location.