Vanderbilt Journal of Entertainment & Technology Law

Volume 7
Issue 1 *Issue 1 - Winter 2004*

Article 8

2004

A Traitor in Our Midst: Is it Your TiVo?

Teresa W. Chan

A Traitor in Our Midst:

Is it Your TiVo?

By Teresa W. Chan*

In the 21st century, the term "instant gratification" is no longer an idle pipe dream, but, an everyday reality. Technology allows us to indulge every entertainment whim we have. With the proliferation of digital video recorders (DVRs) such as TiVo, television viewing has been revolutionized. The viewer is no longer at the mercy of network companies and their programming schedules. To the contrary, the viewer controls what he watches and when he watches it. Thanks to DVRs, the television experience has been transformed into a smorgasbord of viewing delight. DVRs record television shows to a hard disk in digital format. This makes increasingly simple the recording of television shows to some storage medium so that it can be viewed at a time convenient to the consumer (traditionally a feature performed by a VCR). Further, DVRs also allow for trick modes such as pausing live TV, instantly replaying interesting scenes, and skipping advertisements. TiVo is currently the most popular mainstream DVR. In fact, TiVo is such a landmark of our technological times that culturally defining television sitcoms such as Friends[1] and Sex & the City have mentioned TiVo by name (and in once case, dedicated an entire episode to one character's "affair" with her TiVo)[2].

But is TiVo really the godsend most people seem to think it is? Is there something more to this friendly television service provider that is not immediately apparent? What if Scott Peterson, who currently stands trial on criminal murder charges, was subpoenaed for his TiVo records to show that he almost solely watched Law & Order, C.S.I., and other crime shows? Would the prosecutor be able to use this information to suggest that Peterson had been "studying up" on ways to commit a murder? What if the TiVo records of a political candidate came to light during elections and they reflected that this particular candidate frequently watched the Playboy channel? Would his opponents be able to use this information to cast aspersions on his character? Disturbingly, two cases, one of which is fairly recent, prove the possibility of these Orwellian scenarios, *Shibley v. Time Inc.*[3] and *DoubleClick Inc. Privacy Litigation*.[4] These two cases further highlight the need for legislative action to protect individual privacy from the dangers of consumer profiling that is ultimately expressive of consumers' personalities and habits.

> "What if the TiVo records of a political candidate came to light during elections and they reflected that this particular candidate frequently watched the Playboy channel?"

Whether embarrassing or downright damaging, what individuals do in their personal time in the privacy of their homes should remain private.

Just as most people would be uncomfortable with the thought that their employers know every website they visit, each keystroke they make, and how much time they spend on each webpage, many people are just as uncomfortable with the idea that others could have access to their television viewing habits.

TiVo is just one brand of a form of new media known as "Interactive Television" (ITV). ITV allows consumers to interact with their television, which then allows the service provider to focus the content of programming and advertising to suit individual preferences.[5] TiVo replaces the function of the video cassette recorder (VCR) and stores recorded programs on a computer hard drive rather than videotape.[6] The TiVo box plugs into the phone line and makes a quick daily phone call to TiVo headquarters, at no cost to the user to download the latest program guide data. It also gives the viewer listings up to twenty-one days in advance.[7] During those daily phone calls to TiVo headquarters, the TiVo box also surreptitiously sends back certain information about the viewer.

> "While TiVo uploads a viewer's daily information, it learns about his viewing habits, analyzes what the viewer has asked it to record, and suggests other programs that he may enjoy viewing."

Just what is TiVo doing with all of this information it collects about its viewers? There are two types of suspect behavior that raise privacy concerns: (1) the sale of aggregate data TiVo collects about its users, and (2) the level of scrutiny TiVo gives to TiVo users' viewing habits. First, as of June 2003, TiVo began to offer advertisers and broadcasters second-by-second information on the commercials and shows its users were watching—or skipping.[8] Secondly, while TiVo uploads a viewer's daily information, it learns about his viewing habits, analyzes what the viewer has asked it to record, and suggests other programs that he may enjoy viewing.[9] TiVo will then scan all available channels and choose similar programs that the viewer might like based on his past viewing habits and automatically records these suggestions.[10] The fact that TiVo has this capability leads to the inevitable conclusion that they are creating (and storing) a "viewer profile" of the TiVo user.

Part I of this Note provides a backdrop of the different aspects of privacy law, focusing on the federal statutory schemes that are applicable to the issue of information gathering and the different possible uses of that information as a violation of privacy rights that have appeared in similar technology cases up to this point in time. This section will also focus on the capabilities of TiVo in more depth.

Part II of the Note examines both of TiVo's questionable actions: first, whether gathering information to sell to advertisers and networks in the form of aggregate data violates privacy rights; and secondly, whether detailed information gathering that allows TiVo to create a "viewer profile," thereby allowing the service provider to customize its service, is a violation of privacy rights or contrary to public policy. This Note supports the position that selling aggregate data need not raise any privacy concerns, as the practices of TiVo, by-and-large, accord with both the law and sound public policy.[11] However, the question of whether TiVo violates privacy rights in tracking viewer habits to the point where TiVo is able to analyze a viewer's likes and dislikes, and then suggest other shows that the viewer might enjoy and tailor advertising towards that particular viewer, merits a second look.

Part III of this Note explains that, although TiVo has voluntarily chosen to impose the privacy framework initially built to protect regular cable television viewers, it is not enough to rely on TiVo's continued self-regulation of its behavior. This section suggests that federal privacy law should mirror the present state of California law, which extends the federal Cable Act to apply to "satellite systems" as well as other ITV providers who use mediums other

than simple cable or satellite. This type of legislation would provide TiVo users the protection they currently lack. Additionally, consumers should be allowed to file civil lawsuits against companies that violate the bill's privacy protections. As a final safeguard, users should be able to have an uncomplicated right of access to a viewer's "profile" that has been created by TiVo (in regards to their viewing habits) so viewers can correct any inaccurate or potentially embarrassing information at their discretion.

I. The Development of Privacy Rights in the Technological Arena

Privacy law has developed a great deal in recent years to meet the needs created by constantly evolving technology. Current law, however, affords a TiVo user no such guarantee of privacy.

A. Savoring the Solitude: Privacy Under the Common Law

It could be said that in 1890, Samuel Warren and Louis Brandeis "created" common law privacy rights in their oft-quoted article, "The Right to Privacy."[12] In their article, Warren and Brandeis describe privacy as the "right to be let alone."[13] They argue for the creation of a new privacy right in personal information as a defense against the overzealous and intrusive nature of the press.[14] Dean William Prosser then proceeded to develop the common law privacy right by classifying invasions of privacy into four distinct causes of action in tort law.[15] The four categories are: (1) intrusion upon one's seclusion or solitude, (2) publicly disclosing private facts of one's life, (3) placing another in a false light in the public eye, and (4) appropriation of name or likeness.[16] The Restatement (Second) of Torts later adopted these four classifications.[17]

The "intrusion upon seclusion"[18] cause of action is the most relevant to TiVo's practice of gathering information. The tort of intrusion occurs when one "intentionally intrudes physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns...if the intrusion would be highly offensive to a reasonable person."[19] This form of privacy invasion focuses on the manner in which the defendant obtains information and implicates the "use of the defendant's senses, with or without mechanical aids, to oversee or overhear the plaintiff's private affairs."[20] To be actionable, the tort does not require any actual disclosure of the information to a third party.[21]

The relatively demanding criterion of the tort of intrusion prevents it from being brought indiscriminately by plaintiffs. Not only must the intrusion invade the zone of "private seclusion that the plaintiff has thrown about his person or affairs,"[22] but the intrusion must also be "highly offensive to a reasonable person."[23] The standard for "highly offensive" turns on whether the plaintiff has a reasonable expectation of privacy against that intrusion.[24]

The Indiana Court of Appeals found that "[i]t does not follow that a consumer gives up all expectations of privacy, and therefore, waives all [privacy] claims...when voluntarily revealing one's affairs to a third party."[25] Holdings in actions arising out of the Freedom of Information Act (FOIA) also substantiate the existence of a reasonable expectation of privacy against disclosure to the private sector.[26] The FOIA allows the public to request copies of records in the possession of federal agencies.[27] The requested records are released unless the record falls into one of the nine exemptions set forth under the Act (e.g., personal privacy, confidential business information, etc.).[28] In the context of the government's disclosure of

"Current law, however, affords a TiVo user no such guarantee of privacy."

personal information to the private sector, the federal courts have found a reasonable expectation of privacy in names and addresses,[29] in information concerning private activities, and in activities taking place in the home.[30]

The Supreme Court's interpretation of the Fourth Amendment's protection of the home has never been tied to the exact quantity or quality of information obtained.[31] In *Silverman v. United States*, for example, the Court made clear that any physical invasion of the structure of the home, "by even a fraction of an inch," was too much.[32] The Supreme Court's line of cases shows that *all* details within the home are intimate details, because the entire area is held safe from the prying eyes of the government.[33] For example, in *Kyllo v. United States*, police used a thermal-imaging device to discover an indoor marijuana growing operation from the street.[34] The court concluded that obtaining information about the interior of the home that could not otherwise have been obtained without physical intrusion into such a constitutionally protected area, constituted a search, at least where the general public did not use the technology.[35] Since thermal imaging technology was not in general public use, such surveillance was a search and was presumptively unreasonable without a warrant.[36] In addition, the physical size or impersonal nature of an object is largely irrelevant in determining whether a detail is intimate. In *United States v. Karo*, the only thing detected was a can of ether in the home.[37] In *Arizona v. Hicks*, the detection of the registration number of a phonograph turntable went beyond what lawfully present officers could observe in "plain view."[38] Despite the small and impersonal nature of both the can of ether and the registration number of the phonograph turntable, the Supreme Court found that they were intimate details because they were details of the home, as is information as to how warm a person keeps his house.[39]

B. In Order to Form a More *Private* Union: Privacy under the United States Constitution

The right to privacy is not explicitly granted in the United States Constitution. However, the United States Supreme Court, in *Griswold v. Connecticut*, held that there were "zones of privacy" created around "specific guarantees in the Bill of Rights."[40] The Constitution only provides protection from state actions that violate an individual's privacy.[41] As a result, no constitutional privacy right attaches when the intruding party is a private entity, such as TiVo.

The Supreme Court, however, has indicated that it may be willing to find constitutional protections of information privacy as it relates to computer profiling by governmental entities arising out of the Fourteenth Amendment and its guarantee of due process. In *California Bankers Association v. Shultz*, the Court, in dicta, expressed that an information gathering program that expands the scope of transaction data to include information "reveal[ing] much about a person's activities, associations, and beliefs" raises more difficult constitutional questions.[42] The Court seems to anticipate that future technological encroachments on privacy may be met with a more forcible constitutional challenge, including questions of violations of due process rights. In *Whalen v. Roe*, Justice Brennan expressed this view in his concurrence, stating, "The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will

> "The right to some degree of personal privacy deserves recognition as a basic principle of our constitutional system."

not demonstrate the necessity of some curb on such technology."[43]

Although the Constitution's privacy guarantees apply solely to invasions of personhood by the government and not by the private sector, the right to some degree of personal privacy deserves recognition as a basic principle of our constitutional system.[44] Case law further develops the link between the common law right of privacy and constitutional guarantees by attaching an "expectation of privacy" that arises out of the Fourth Amendment.[45] Because the rights enforced by the states under the Ninth and Tenth Amendments are rooted in basic constitutional protections, any strengthening or expansion of information privacy-related constitutional rights by the Supreme Court will likely produce a corresponding level of protection of information privacy by the states with regard to actions arising out of the private sector. If the Court hesitates to extend constitutional protection to information privacy, the lower courts likely mimic their behavior and will be unwilling to extend similar protections in their interpretations of the common law and the legislatures will hesitate to expand the statutory protection of information privacy.

"The precise boundaries and applications of the federal statutes, however, remain unclear since the federal legislation that touches on private entities' collection or use of information is drafted on an ad-hoc basis."

C. Laying Down the Law: Privacy Protected by Federal Statutory Schemes

Similar to the protection of privacy rights afforded by the Constitution, many federal statutes only regulate state actors, as opposed to private ones.[46] The precise boundaries and applications of the federal statutes, however, remain unclear since the federal legislation that touches on private entities' collection or use of information is drafted on an ad-hoc basis.[47] Thus, the legislation is reactive, rather than prophylactic, and addresses narrow, industry-specific privacy concerns.[48] Despite this uncertainty, the operations of TiVo seem to fall within the scope of the Cable Communications Policy Act of 1984 ("Cable Act") at first glance.[49] However, because TiVo is not a cable operator, TiVo's operations are exempt from the limitations of the Cable Act.

The Cable Act establishes a comprehensive framework for cable regulation and sets forth strong protections for subscriber privacy by restricting the collection, maintenance, and dissemination of subscriber data—also called "personally identifiable information" (PII).[50] The Cable Act defines the term "personally identifiable information" as precluding "any record of aggregate data which does not identify particular persons."[51] Under the subscriber privacy provisions of the Cable Act, cable operators must inform their subscribers when they initially enter into a contractual arrangement, and annually thereafter, of the nature of the personally identifiable information they collect about subscribers,[52] their data disclosure practices,[53] and subscriber rights to inspect and correct errors in such data.[54] The Act bars cable operators from monitoring the viewing habits of cable subscribers.[55] Without subscriber consent, cable operators are prohibited from using the cable system to collect PII about their subscribers, except that which is necessary to render cable service.[56]

Additionally, without written or electronic consent, current laws generally bar cable operators from disclosure of such data to third parties.[57] Further, cable operators may disclose their mailing lists to third parties only if they have given their subscribers an opportunity to limit such disclosure, and the disclosure does not reveal the viewing habits or other transactions of the subscriber.[58] However,

the transmission of ITV will occur through various media sources, including satellite links and telephone lines, arguably evading the protection of the Cable Act.[59]

Another federal statute aimed at addressing informational privacy issues is the Video Privacy Protection Act of 1988 ("Video Act").[60] The Video Act "limit[s] the dissemination of information relating to video cassette rentals and sales."[61] This law and similar state laws "arose out of disclosures relating to the possible use of video rental information in the confirmation hearings for Supreme Court Justice-designate Robert Bork, and apparently reflect[ed] perceptions that information on video viewing habits are particularly private and personal."[62]

> "California is at the forefront of the movement to regulate new technologies such as ITV."

D. Caring for the Citizens: Privacy Protected by State Statutory Schemes

Some states have filled the gaps in federal law by passing statutes in an attempt to guard citizens' informational privacy rights from invasions by the private sector. California is at the forefront of the movement to regulate new technologies such as ITV.[63] On March 27, 2002, California State Senate Bill 1090 ("S.B. 1090"), which became law on October 11, 2001, took effect despite stringent opposition from several groups, including Microsoft Corporation, America Online, Inc., and California Cable Television Association.[64] S.B. 1090 extends the federal Cable Act to "satellite system[s]," which include a broader array of media used to transmit ITV.[65] The bill also expands California's cable privacy laws to prevent satellite companies from disclosing any personal information or television viewing habits to anyone but the individual customer, unless the customer "opts in" and allows such information to be collected and sold.[66] Companies that violate the bill's privacy guidelines are subject to a misdemeanor penalty and up to a $3,000 fine.[67] The bill also allows individuals to file civil lawsuits against companies that violate the bill's privacy protections.[68] S.B. 1090 directly addresses the privacy concerns surrounding ITV, mandating stringent regulations on the collection and use of personal information by California ITV providers who use satellite or cable mediums.[69]

E. No Thanks, I'm Watching My Privacy: Getting the Skinny On Cookies

Internet users have also confronted informational privacy issues for some time. Computer files called "cookies" can expose the identity of Internet users.[70] World Wide Web servers generate cookie files and store them on a user's computer for future Web server access.[71] Cookies allow Web servers to recognize the user's browser, provide the user with customized content, and store information about the user.[72] Often, users do not notice this storage and access of personal information because Web servers automatically access cookies whenever the user connects to the Web server.[73]

Without overt disclosure on the user's part, cookies generally do not reveal a user's specific identity, and they cannot be used to determine other sites the user has visited.[74] There are, however, two potential ways in which a cookie can be used to discover a user's identity. First, cookies can recall authentication or login information (e.g., name, address, password, etc.) which could suggest the user's identity.[75] The user, however, must first disclose the identifying information on the website for a cookie to include this type of identifying information. Secondly, an organization can cross-reference the information in a cookie with names, addresses, and consumer histories that exist in

separate marketing databases.[76] The Internet advertising firm DoubleClick, which acquired a massive marketing database through its purchase of Abacus Direct, proposed such a method of user identification.[77]

In a sense, Internet cookies are similar to TiVo and their "customized" viewing suggestions. Both technologies create a "memory" of the consumer's preferences that, if ever compiled with additional collected information from another sort of service, might provide an unnervingly complete profile of an individual. Despite the similarity to Internet cookies, it is not certain how much weight this resemblance will carry. While there is some case law addressing Internet cookies, as of yet, no legislation controls their use.

F. A Profile of the Problem With Consumer Profiling

To increase the efficiency of communication and commerce, computer databases and network standards are making the identification of individuals easier than ever.[78] Databases and the sale of database information have introduced significant potential for large scale and detailed monitoring that has never been possible.[79] These technological developments pose a serious threat to an individual's anonymity and personal privacy by allowing companies to create profiles of their consumers.[80]

Consumer profiling is a growing trend.[81] Several converging technological and theoretical changes have led to this business trend.[82] First, transaction data is no longer being looked at simply as random bits of information, but rather as a commodity in and of itself. [83] Secondly, the data warehouse is enabling the processing and storage of data in ways previously thought impossible.[84] Finally, there is an emerging unified market for the exchange and sale of transaction data profiles.[85]

Due to the fact that intimate details of a person's activities, associations, and beliefs can be revealed, profiling is extremely intrusive.[86] Profiling, therefore, could easily intrude into the zone of seclusion where a person conducts his private affairs.[87] Since the reasonable expectation of privacy is often defined with reference to general social norms,[88] the high incidence of consumer discomfort with profiling further demonstrates the strength of the reasonable expectation of privacy in consumer information. According to a *Business Week/Harris* poll, 82% of those surveyed expressed substantial discomfort with "user profiling," a practice in which companies track and record users' online movements while tied to a profile of the user consisting of personal information such as name, income, driver's license, credit data, and so forth.[89]

Looking at the kind of information collected and how it is used reveals the nature of the threat to privacy. However, certain legal scholars find that there is no immediate danger since, "without the context of the consumer culture, much of this information is unexpressive, and the collection of it should not cause alarm."[90] On the other hand, privacy is threatened when companies compile data into profiles that reveal the individual's consumer and, consequently, personal identity.

The introduction of consumer databases has created a world in which consumption is no longer a way of expressing one's identity; rather, consumption patterns, as revealed by consumer records, are tied to individuals' identities.[91] On one level, they reveal a person's response to the various meanings that are embodied in products and brands.[92] However, consumption patterns can also reveal a person's socioeconomic status as well as their "cultural and social inclinations."[93]

"The introduction of consumer databases has created a world in which consumption is no longer a way of expressing one's identity; rather, consumption patterns, as revealed by consumer records, are tied to individuals' identities."

One legal scholar makes the analogy, "while scattered bits of a puzzle are unintelligible, when they are put together, a picture does emerge."[94] Accordingly, legislative limits must be placed on the compilation of records in third party databases.[95] Illustrative of this analogy is the difference between the cases *Shibley v. Time, Inc.*[96] and *In re DoubleClick Inc. Privacy Litigation*.[97] A differentiation of the two practices, however, is flawed, since both practices pave the way for the same questionable use of information gathered by the companies.

> "Danger exists when any sort of information is compiled and put into a database, since there is a potential avenue for someone to eventually put the pieces of the puzzle together."

In *Shibley*, the Ohio Court of Appeals held that the disclosure of magazine subscription information did not constitute a violation of the right to privacy.[98] Similarly, in *DoubleClick*, a New York court determined that the defendant's use of cookies to collect potentially personally-identifiable information to build demographic profiles of Internet users is permissible under federal law.[99] Application of the model of privacy proposed in this Note will demonstrate that the practices involved in both *Shibley* and *DoubleClick* are questionable due to the possibility of aggregating information into comprehensive profiles that convey consumers' personalities and habits.

Shibley involved a magazine subscriber who sued Time Inc., a subsidiary of Time Warner Inc. and the preeminent magazine publisher in the world,[100] for selling lists of subscribers of certain magazines to third parties.[101] The plaintiff claimed that this practice constituted an invasion of privacy because it amounted to a sale of individual "personality profiles."[102] The plaintiff, Shibley, argued that "the buyers of these lists are able to draw certain conclusions about the financial position, social habits, and general personality of the persons on the lists by virtue of the fact that they subscribe to certain publications."[103] The court held that even if subscription information amounted to "personality profiles," the sale of such information does not rise to the level of a privacy violation.[104] *DoubleClick*, the most prominent case in the emerging field of privacy regarding Internet cookies, involved a much more expansive effort to collect and use information.[105] DoubleClick, the largest provider of Internet advertising products and services in the world, utilized cookies to allow collection of information about users' online activities.[106] DoubleClick used proprietary technologies and techniques to collect, compile and analyze information about Internet users.[107] It would then use that analyzed information to target online advertising.[108] In June 1999, DoubleClick purchased Abacus Direct Corp., a direct-marketing company that maintained an extensive database, containing names, addresses, telephone numbers, retail purchasing habits and other personal information about approximately ninety percent of American households.[109] The plaintiffs claimed that DoubleClick intended to merge the two databases of online and offline profiles to create extremely detailed profiles of Internet users' consumer behaviors.[110] The court dismissed the plaintiffs' federal claims, holding that DoubleClick's activities fell within the statutory exceptions.[111] Because the defendants affiliated web sites were "users" of Internet access under the Electronic Communications Privacy Act (ECPA), and the submissions containing "personal" data made by users to defendants affiliated web sites were all "intended" for those web sites, the web sites' authorization was sufficient to except defendants access under 18 U.S.C.S. §2701 (c)(2).[112]

Some legal scholars argue that the danger is the scope of the violation of privacy, not the type of violation. Therefore, some agree with the *Shibley* decision but not with *DoubleClick*.[113] However, their

theory fails to acknowledge that danger exists when any sort of information is compiled and put into a database, since there is a potential avenue for someone to eventually put the pieces of the puzzle together. DoubleClick's actions are more blatantly egregious because the defendant made a deliberate attempt to compile and sell comprehensive profiles that embodied Internet users' consumer identities. However, *Shibley* makes a move in the same direction by making it possible for third parties to create a similar comprehensive profile as was discussed in *DoubleClick*.

G. Rating the Nielsen

Nielsen Media Research is the leading provider of information on television-viewing habits. The national ratings service uses an electronic measurement system called the Nielsen People Meter.[114] These meters are placed in a sample of 5,100 households in the U.S., randomly selected and recruited by Nielsen Media Research.[115] The meter is placed on each TV set in the sample household and measures two things—what program or channel is being watched, and who is watching.[116] Nielsen Media Research collects audience estimates for broadcast and cable networks, nationally distributed syndicated programs and satellite distributors.[117]

The identity of the TV source (broadcast, cable, etc.) in the sample homes is continually recorded by one part of the meter, which has been calibrated to identify which station, network or satellite each channel in the home carries.[118] The meter also electronically monitors channel changes.[119] Nielsen Media Research gathers and maintains a database of information about the source and time of telecast for TV programs. When this information is combined with source tuning data from the sample homes, Nelson Media Research can then credit an identifiable audience to specific TV programs.[120]

An electronic "box" at each TV set in the home and accompanying remote control units measure the identity of the viewer.[121] Each family member in the sample household correlates to a personal viewing button on the People Meter.[122] Furthermore, the Nielsen Media Research representative who recruits the household links the assigned button to the age and sex of each person in the household.[123] Whenever someone turns on the television set, a red light flashes on the meter, reminding viewers to press their assigned button to indicate when they are watching television.[124] Additional buttons on the meter solicit viewers in a sample home to report when they watch TV by entering their age and sex and pushing a visitor button.[125]

H. Play it Again, TiVo

The appeal of TiVo is its ability to facilitate entertainment for today's busy consumer. Once TiVo records a program selected by the viewer, it enables a viewer to watch the program at *any* time. It therefore frees the viewer from the need to be in front of the television at a certain time to watch his favorite shows.

While this does not sound much different than the VCR, TiVo users prefer TiVo to VCRs for several reasons. The first of these factors is the ease in programming TiVo. To record a favorite show, the user can browse by time, browse by channel, search by title or search by genre.[126] If the user consistently cannot watch the show "live," the user can opt to, "Get a Season Pass," which instructs TiVo to record more than one episode of the show.[127] Additionally, the user can tell TiVo to only record new episodes, ensuring that no re-runs are recorded.[128] The user can also do "Wishlist" recordings by title, subject, director or actor.[129] For instance, a TiVo user who is a football fan can set his TiVo to automatically record every football game with the words "UCLA" in the description, regardless of what time, channel, or day it is broadcast. The user can set it to record every movie that features Russell Crowe, or every documentary about beta fish or the ocean. The user can also start watching a show on TiVo as it is still being recorded or watch one show while TiVo records another.

While the perks and the convenience of TiVo are plentiful and varied, the use of TiVo is not without disquieting concerns. Every time the viewer chooses to record a show, the TiVo box automatically marks the show as if the viewer has given it a "thumbs up," regardless of whether recording the show was a regular occurrence, a one-time incident for a friend, or a mistake.[130] Based on the "thumbs up" report, TiVo begins to create something akin to a user profile and suggests similar shows that the viewer might also like.[131] TiVo can even go so far as to tape every show on which a particular person appears—whether it is a regularly-aired show, a talk show, or a guest appearance on another sitcom.[132] A viewer can

rate each program with one to three thumbs up or thumbs down, depending on how much he likes it. TiVo compares what a viewer likes with preferences of other TiVo users like in order to find additional new shows that the viewer might like.[133] For instance, if a viewer gives three thumbs up to "The O.C.," TiVo may notice that most O.C. aficionados also like "North Shore," and will record that as a suggestion. The ability to analyze a TiVo user's viewing habits in such detail seems dangerously close to the ability that the court feared in *DoubleClick*—that is, the ability to create an invasive profile of users by putting isolated pieces of information together.

As mentioned earlier, TiVo operates through a user's telephone line.[134] While this phone line is used primarily to download television schedules to the box, it can also upload information back to TiVo.[135] In particular, the following types of information are sent back to TiVo: the customer's ID number for the TiVo service, times and dates when the TiVo box is in use, and information as to which television programs viewers watched.[136] While that type of information may not seem out of the ordinary, appearing similar to the Nielsen box and fairly innocuous, researchers for the Privacy Foundation intercepted a series of calls made from a TiVo unit through the use of a connected laptop computer for the purposes of determining exactly what information TiVo was uploading during those daily phone calls.[137] The researchers discovered that the unit was logging any change in volume and channel.[138] This information seems highly unusual for a digital television recorder provider to monitor.

I. The Difference Between Nielsen and TiVo

Since Nielsen Media Research is specifically a data collection company, the viewers must be especially proactive about "giving" their television viewing data by pressing buttons to allow the "box" to register who is watching the television. Additionally Nielsen monetarily compensates participating families. TiVo, on the other hand, conducts its data collecting much more surreptitiously since viewers do nothing more proactive than turn on the television before TiVo begins to collect information on them.

In fact, TiVo recently signed a deal to provide data to Nielsen Media Research.[139] Under the agreement, TiVo supplies Nielsen with anonymous data regarding the habits of subscribers who agree to hand over their information.[140] One Nielsen spokesman said that the next deal Nielsen reaches with TiVo, or any other DVR supplier, will involve more valuable demographic information about viewers, such as age or sex.[141] Lee Tien, lead staff attorney with the Electronic Frontier Foundation, said that TiVo's deal with Nielsen "pushes the envelope" when it comes to guarding its customers' personal data because it threatens to remove the anonymity from the data collected.[142]

II. The Terror that Lurks in the Living Room

Consumers value the benefits that they reap from advances in technology. However, many of them also value their privacy. The question now is whether the two are mutually exclusive, or whether they can coexist.

"The ability to analyze a TiVo user's viewing habits in such detail seems dangerously close to the ability that the court feared in *DoubleClick*—that is, the ability to create an invasive profile of users by putting isolated pieces of information together."

A. Going Once, Going Twice, Sold!: The Practice of Selling Aggregate Data

Beyond selling airtime, television providers are now in the business of selling data and the use of

data. Matthew Zinn, Vice President, general counsel, and chief privacy officer of TiVo, Inc., submitted a report to the Federal Trade Commission on May 3, 2001. In that report, TiVo disclosed that it sold "aggregated Account Information and aggregated Anonymous Viewing Information and any reports or analyses derived therefrom, to third parties including advertisers, broadcasters, consumer and market research organizations, movie producers, and other entertainment producers."[143]

Given that there are privacy advocates who quake at the thought of someone obtaining and selling any sort of personal information, it is worth examining the kinds of data being recorded, what is being done with it, and what exactly is being sold. There are several different ways in which aggregate data can be gathered, held, and sold.

Service providers such as TiVo may wish to do business with consumer data companies, offering to upgrade either their anonymous data or PII with analysis of click stream data (raw viewing data).[144] In this case, both TiVo and the third party purchaser of the data benefit from their arrangement.

If the service provider does not want to sell viewer data to third parties, it might instead use the data for "merge and purge" campaigns. The provider will combine the collected data with data that other companies have to offer for the sole purpose of a mass mailing or a targeted television ad campaign.[145] After such an effort, companies destroy the combined data.[146] This allows them to say, "We do not give information to third parties," while effectively handing them anything they want.[147]

Set top boxes use artificial intelligence algorithms.[148] A box can start with the input of several factors when viewers sign up for service.[149] For example, it can make public a user's age, household size, marital status and number of children. Software then records and analyzes each viewer's click stream.[150] This software can compare what the individual users do with what people in the general public are doing.[151] The artificial intelligence software attacks raw data from many users to find patterns in the lifestyles and viewing habits of subscribers.[152] This is the same type of software at work on Amazon.com that suggests books other Amazon.com users who read the book that the consumer is contemplating enjoyed.[153]

Since increased ratings mean more money from advertisers, television networks who wish to increase their ratings by offering more desirable programming are interested in TiVo's data. Advertisers are also willing to pay substantial sums to discover what click stream data has to reveal—down to the second-by-second information of how long viewers are watching certain commercials, what programs they are watching, and so on.[154] This information makes it possible for advertisers to target viewers through changing the way they market the product, along with strategically placing advertising for certain items in a way that a group shown more likely to purchase that item becomes the targeted audience.[155] This information can also be valuable for calculated product placement advertising within television shows and movies.[156]

“TiVo's sale of aggregate data is something that seems to fall just outside the jurisdiction of any prohibitions under the areas of law discussed above.”

TiVo's sale of aggregate data is something that seems to fall just outside the jurisdiction of any prohibitions under the areas of law discussed above. Sale of aggregate data does not qualify as an "intrusion upon seclusion" cause of action under common law tort. The common law tort defines "intrusion upon seclusion" as an intrusion that is highly offensive to a reasonable person.[157] The standard for "highly offensive" turns on whether the plaintiff has a reasonable expectation of privacy against that intrusion.[158] Since TiVo's sales of aggregate data do not disclose

a person's identity tied to their viewing habits, only the viewing habits of a group of people generally, even though an intrusion has occurred, it does not seem that this would be found to be "highly offensive."

However, it seems that the mere *collection* of the data could be found to fall under the protection of state tort law. It has been found in cases involving illegal wiretaps or surveillance in searches not authorized by a warrant based upon probable cause violate the Fourth Amendment.[159] While the lack of a governmental actor may not make it a constitutional violation, a person whose phone conversations were intercepted or recorded by a private party would still be able to bring a cause of action against that party.[160] Although interceptions of phone conversations seem more invasive than tracking television viewing habits, there is nevertheless something intrusive about how closely TiVo can monitor users' television viewing actions. It is arguable, however, that the collection of data used in sales of aggregate data is no different than when telephone companies keep phone records which the telephone company can review or the government can subpoena at any time. The distinction that can be raised between the two practices is that even if the government subpoenas a person's phone records, the content of his conversation is still private. However, in the case of television, the mere act of revealing what a person watches is telling in itself and necessarily not content neutral.

"It is arguable, however, that the collection of data used in sales of aggregate data is no different than when telephone companies keep phone records which the telephone company can review or the government can subpoena at any time."

There is no recourse under federal statutes since the sale of aggregate data is specifically excluded from regulation under the Cable Act.[161] The general sentiment seems to be that as long as consumers' names are not tied to their personal information, the infringement upon their private sphere has not been egregious. TiVo executives are quick to reassure consumers that they gather information only in the aggregate, such as by ZIP code, and that the habits of individual users will remain anonymous.[162] TiVo also notes in their privacy policy that the default privacy preferences allow TiVo to "collect, use, and disclose Anonymous Viewing Information."[163] However, a subscriber may change his privacy preferences either by calling TiVo's toll-free number or by writing to TiVo.[164] This default, opt-out rule places the entire burden on the *consumer* to notify TiVo that he does not wish to participate in the data collection campaign.

During the 2004 Super Bowl half-time show, Justin Timberlake tore Janet Jackson's leather outfit at the finale of their performance, baring her breast for a split second. TiVo reported that this particular half-time stunt was the most replayed moment not only of the Super Bowl, but of all TV moments that the company had ever measured.[165] TiVo used its technology to measure audience behavior among 20,000 users during the Super Bowl revealing a 180 percent spike in viewership at the time of the skin-baring incident.[166] TiVo's release of this information sparked headlines that "dramatically publicized the power of the company's longstanding data-gathering practices."[167] While there were TiVo subscribers who were apprehensive upon learning about TiVo's capabilities, TiVo spokespeople were quick to respond that the company operated well within established privacy standards.[168] However, they were forced to admit that, "TiVo could conceivably investigate an individual's viewing habits."[169]

B. Tracking the Television: Profiling the Customer

TiVo's ability to create detailed consumer profiles is wholly different from its collection and analysis of aggregate data. TiVo has the ability to

acquire PII from its subscribers. PII is information that any subscriber of TiVo releases while first subscribing to the service. It can be anything from a name, to addresses, to credit card numbers. There are several things that can be done with PII.

Log information and PII can be sent back to a central computer at TiVo headquarters.[170] The user's viewing data may or may not be separated from PII.[171] Each individual TiVo machine can use downloaded algorithms to build profiles of users.[172] Content for all profiles is sent out over broadband connection.[173] The TiVo box then knows which programs to record based on the profiles it contains.[174] Software running at the server end can also create the profile instead of software on the individual TiVo box.[175] The implications of this are that either the viewer's profile stays with the viewer on the viewing end of the television, or at the service provider end. It may be comforting for consumers to know that at the moment, TiVo's practices leave consumer profiles on the consumer's end. Section two of TiVo's privacy policy explains, "in order for your Receiver to provide you with Personal TV, it will gather Personal Viewing Information when you use it. Personal Viewing Information is stored on your Receiver. ... All Personal Viewing Information stays on the Receiver and does not get transmitted to TiVo without your consent."[176]

The head office may have access to software that can be installed on the TiVo box, or the server end, which attaches tags to households and users.[177] Marketing departments attach similar corresponding tags to TV programs, parts of programs, and commercials.[178] From there, advertising executives can play the software as they would a video game—instructing the system to show certain tailored commercials in an attempt to target certain families or family members.[179]

Some companies are purchasing third party data from consumer research companies instead of selling it.[180] SpotOn, for instance, is researching the residents of Aurora, Colorado, trying to answer such questions as "when will this person's auto lease run out?"[181] When that data is collected in one database, SpotOn will use it to send different commercials to each household, tailored to their needs.[182]

> "TiVo has made it clear that its business model has very little to do with selling boxes when it started to license its technology to other manufacturers in order to boost revenues."

TiVo substantiates its collection of personal viewing information with claims that it is used to, "tune, schedule, record, and recommend programs for you. The Receiver may also use this Personal Viewing Information to select advertisements or other promotions for you that you may be interested in."[183] The company also has an opt-in rule which assumes that a consumer does not wish to participate in data collection of his personal viewing information absent express written consent.[184]

Of concern however, is that TiVo has made it clear that its business model has very little to do with selling boxes when it started to license its technology to other manufacturers in order to boost revenues.[185] Given that the type and sophistication of data that the boxes can collect is possibly far more valuable in real dollars than the monthly fee that TiVo charges, indicates that it has another revenue stream – selling data on its subscribers' viewing habits.

When Supreme Court Justice-designate Robert Bork's video rental habits became public during his confirmation hearings, Congress passed a law explicitly protecting the privacy of such records.[186] The Video Act is the reason for programs such as "Blockbuster Rewards" in which you are implicitly "opting in" to release your data in exchange for "free" gifts.[187] In Blockbuster's privacy policy, it states that, "Blockbuster collects PII from Users when voluntarily submitted by a User, for example when a User participates in a sweepstakes or contest, purchases products online, or registers on blockbuster.com for an e-newsletter or other individualized services."[188] Included in the "individualized services" mentioned is the "Blockbuster Rewards" program discussed above.

If such a high premium is placed on the private nature of one's video rentals (i.e. the Video Act), it is unclear why television viewing habits should not merit the same elevated protections.

Increasingly, book purchase records are being subpoenaed.[189] Prosecutors can use book purchase records in various ways:[190] to establish a particular suspect's intent or motivation to commit a crime;[191] to establish that a crime has been committed in the first place, distinguishing an apparent accident from an intentional crime or providing evidence of a longstanding conspiracy;[192] to show that the suspect bought a "how to" manual for illegal activity, and then meticulously followed it;[193] or to bolster the credibility of a witness planning to testify against a defendant.[194] For example, Independent Counsel Kenneth Starr attempted to subpoena Monica Lewinsky's book purchase records from the Washington, D.C. bookstore Kramerbooks, to show that she had bought a novel about phone sex, hoping to corroborate Lewinsky's claim that she had had phone sex with the President.[195] The use of credit or debit cards in daily purchasing leaves a paper trail that makes data collection and tracing easily obtainable. While not everyone is investigated on a national scale, a person never knows when his data trail may come under scrutiny.

Due to First Amendment concerns, courts currently require prosecutors to show a "compelling need," and a close nexus between the subpoena and the contemplated prosecution before they will enforce a subpoena for bookstore purchase records.[196] The "close nexus" standard is similar to the requirement of "narrowly tailored" which is applied in many constitutional law cases. This requirement assesses whether the connection between the case and the subpoena is direct and obvious, or vague and unconvincing.

However, the danger lies in the possibility that data trails may be subpoenaed in court proceedings that are more germane to our everyday lives. What we watch on television may be of interest to an ex-spouse in a divorce proceeding or custody battle. For example, is there a record of late night Cinemax being watched on the TiVo? Is someone in the household spending a lot of time in front of the television, period? From there it might be inferred who was at fault or who was not a good parent. Even those who do not plan on running for office or entering a custody battle should be aware of how their personal preferences are collected and the ways in which they can be used against them.

The mere fact that TiVo does not hold on to consumer profiles at TiVo headquarters does nothing to alleviate the fear that it has the *ability* to access these profiles (the profile of customer's viewing habits that is stored on the customer's end of the television along with name, address, and credit card number, or whatever other PII the customer released to TiVo when first signing up for service) and to release that information if the need ever arises (due to a subpoena) or if their privacy policy ever changes.

III. Turning the Tide: Making TiVo Terrific

While TiVo's privacy policy at this time purports to keep under wraps any sort of detailed viewer profiles that are created in order to deliver customized viewing for its consumers, there are too many loopholes for the consumer public to rest easy when it comes to its privacy. TiVo's privacy policy also includes a standard clause that states that before making a "substantial and material amendment" to the privacy policy, consumers will be given notice of and asked to consent to any of these changes in their subscriber information collection, use, and disclosure practices.[197] However, without defining what a "substantial and material amendment" is, it is difficult to decipher whether a decision to disclose or even allow headquarters to begin *accessing* personally identifiable viewing information will be reported to consumers in a conspicuous manner.

The Video Programming Consumer Privacy Protection Act of 2003, a bill presently sitting in congressional committee, seeks to prohibit the collection and disclosure of PII by a commercial entity to an un-affiliated third party without proper notice and opportunity to opt-out.[198] Although this behavior is already employed at TiVo, it would be unwise to rely on presently existing and future ITV providers to continue to impose the appropriate restrictions upon themselves without being mandated to do so. Alternatively, TiVo could potentially be purchased by another company that is more unscrupulous and aggressive in its data use.

The second loophole that has been left open for TiVo is that its current privacy policies are not regulated because its technology does not fit exactly under the parameters of the Cable Act and its protection of cable subscribers. Presently, there is

a bill pending in Congress that proposes to extend the Cable Act's privacy protections to satellite service carriers and distributors.[199] Since it covers both cable and satellite operators, two of the leading mediums in the ITV industry, this bill would protect TiVo subscribers as well as other ITV users. The Satellite Home Viewer Extension and Reauthorization Act of 2004 also places enforcement duties in the hands of the FTC.[200] As of now, the Satellite Home Viewer Extension and Reauthorization Act of 2004 has not yet been enacted.

> "Proposed privacy legislation should implement broader language that will serve to include the entire range of ITV providers."

While an extremely ground-breaking piece of legislation, the Satellite Home Viewer Extension and Reauthorization Act of 2004 still leaves some gaps with regard to ITV providers who use neither satellite nor cable (for example, master antenna television and multipoint distribution service). Proposed privacy legislation should implement broader language that will serve to include the entire range of ITV providers.

While these significant pieces of legislation have so far been left in committee, and while past Congressional attempts to pass similar pieces of legislation have been thwarted by burying these bills in committee, technology continues to advance and so does the threat to our privacy. The pieces are all available; it would simply take an ITV provider finally putting the available pieces together to finally obliterate what small amount remains of our privacy. If anything, the events of the 2004 Super Bowl half-time show fiasco and the resulting media frenzy covering TiVo's capabilities should be enough to make TiVo owners take notice and to urge their representatives to revisit their efforts on these two bills. It is imperative that these pieces of legislation are passed. Additionally, consumers must remain vigilant as the advancement of technology marches on and continues to imperil our privacy, as well as our security in knowing that, to some extent, we can lead our lives as we see fit, away from the prying eyes of unknown third parties.

To provide an additional safeguard, consumers should have the option to file civil lawsuits against companies that violate these bills' privacy protections. This is currently being done with most Do-Not-Call registries where violations of the law are enforced by civil suits brought about by the injured party, the Public Safety Commission, or the attorney general's office. Penalties are not specified but may include civil fines and injunctions. Similarly, in order to give companies an incentive to honor users' privacy rights, a similar right to file a civil lawsuit should be available to DVR users.

As a final defense, an uncomplicated right of access to a viewer's "profile" that has been created by TiVo (in regards to their viewing habits) should be created so that users of TiVo can look at their profile and correct any inaccurate or potentially embarrassing information.

The threat to our privacy increases as technology continues to press forward. While most of us will acknowledge that we are willing to trade in certain personal privacies in return for the luxury of convenience, it is still within our power and our rights to protect, to the best of our abilities, as much as our personal privacy as we can. However, it is at our discretion to enable such vigilance. We must be mindful that once we allow the threat to our privacy to pass unchecked for too long, it may become too late to reclaim what has been lost.

Endnotes

* J.D. Candidate, Vanderbilt University Law School, 2005; B.A., University of California, Los Angeles, 2002. The author would like to express her sincere appreciation to Professor Steven Hetcher for his advice. The author would also like to extend her thanks to Darby Green, who helped to shape this note initially; to Rob Leclerc, Katherine Todd, and Joe Christian who were always willing to let her change "just one more thing;" to Tracey Boyd, Rachana Desai and Rashmi Puri for their valuable input and attention to detail; and to her friends for their patience, wisdom, insight and the many ways they have touched her life. Finally and most importantly, the author would like to thank her family for their unconditional love and

support.

[1] *Friends: The One With the Stripper* (NBC television broadcast, Nov. 15, 2001).

[2] *Sex & the City: Great Sexpectations* (HBO television broadcast, June 29, 2003).

[3] 341 N.E.2d 337 (Ohio Ct. App. 1975).

[4] 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[5] David Katz, Note, *Privacy in the Private Sector: Use of the Automotive Industry's 'Event Data Recorder' and Cable Industry's 'Interactive Television' in Collecting Personal Data*, 29 RUTGERS COMPUTER & TECH. L.J. 163 (2003).

[6] *What is TiVo?*, TiVoPortal, *at* http://www.tivoportal.co.uk/ (last visited Sept. 12, 2004).

[7] *Id.*

[8] May Wong, *TiVo To Sell Customer Viewing Data*, CHI. TRIB., *at* http://www.chicagotribune.com/technology/local/chi-030602tivo,0,2009746.story (June 2, 2003).

[9] *See* TiVoPortal, *supra* note 6.

[10] *Id.*

[11] Katz, *supra* note 5, at 164.

[12] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

[13] *Id.* at 195.

[14] *Id.* at 196.

[15] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[16] *Id.*

[17] RESTATEMENT (SECOND) OF TORTS § 652A(2) (1977) (stating, "the right of privacy is invaded by (a) unreasonable intrusion upon the seclusion of another ... or (b) appropriation of the other's name or likeness ... or (c) unreasonable publicity given to the other's private life ... or (d) publicity that unreasonably places the other in a false light before the public").

[18] *See id.* § 652B.

[19] *Id.*

[20] *Id.* at cmt. b (discussing how the invasion may be by physical intrusion into a place in which the plaintiff has secluded himself).

[21] *See id.* at cmt. a.

[22] *Id.* at cmt. c.

[23] *Id.*

[24] *See* White v. White, 781 A.2d 85, 91-92 (N.J. Super. Ct. Ch. Div. 2001) (stating that what is highly offensive to a reasonable person turns on one's reasonable expectation of privacy, which is measured objectively).

[25] Pohle v. Cheatham, 724 N.E.2d 655, 660 (Ind. Ct. App. 2000).

[26] 5 U.S.C. § 552 (2000).

[27] *Id.*

[28] *Id.*

[29] HMG Mktg. Assoc. v. Freeman, 523 F. Supp. 11, 14-15 (S.D.N.Y. 1980).

[30] Wine Hobby USA, Inc. v. United States, 502 F.2d 133, 137 (3d Cir. 1974).

[31] Kyllo v. United States, 533 U.S. 27, 37 (2001).

[32] 365 U.S. 505, 512 (1961).

[33] *Kyllo*, 533 U.S. at 37.

[34] *Id.* at 29.

[35] *Id.* at 40.

[36] *Id.*

[37] 468 U.S. 705, 709 (1984).

[38] 480 U.S. 321, 325 (1987).

[39] *Kyllo*, 533 U.S. at 38.

[40] 381 U.S. 479, 484 (1965) (discussing the First, Third, Fourth, Fifth, and Ninth Amendments in reference to the guarantee of the Bill of Rights that creates privacy rights; in this case, the right of married couples to use contraceptives).

[41] *Id.* at 484-85 n.*.

[42] 416 U.S. 21, 78-79 (1974) (Powell, J., concurring).

[43] 429 U.S. 589, 607 (1977) (Brennan, J., concurring).

[44] Rosenblatt v. Baer, 383 U.S. 75, 92 (1966) ("The protection of private personality, like the protection of life itself, is left primarily to the individual States under the Ninth and Tenth Amendments").

[45] *See* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 773 (N.Y. 1970) (comparing the protections of the Fourth Amendment to common law privacy torts).

[46] Suzanne M. Thompson, *The Digital Explosion Comes With a Cost: The Loss of Privacy*, 4 J. TECH. L. & POL'Y 3, para. 35 (1999). (explaining that, "This targeted approach results in uneven, inconsistent, and often less than adequate protection for personal data." With the technological advances of the Internet, targeted standards are problematic. In this case, "[t]he use of computers allows personal information to be disseminated across sectors thus defying the aim of context-specific regulations and practices.").

[47] *Id.* at para. 31.

[48] *Id.* at para. 33-37.

[49] 47 U.S.C. § 521-613 (2000).

[50] *Id.*

[51] *Id.* § 551(a)(2)(A).

[52] *Id.* § 551(a)(1)(A).

[53] *Id.* § 551(a)(1)(B).

[54] *Id.* § 551(a)(1)(D).

[55] *Id.* § 551(b)(1).

[56] *Id.* § 551(b).

[57] *Id.* § 551(c)(1); *see* Denver Area Educ. Telecomms. Consortium v. FCC, 518 U.S. 727, 834 (1996).

[58] 47 U.S.C. § 551(c)(2)(C).

[59] *See* Center for Digital Democracy, TV That Watches You: The Prying Eyes of Interactive Television (June 2001), at 3, *available at* http://www.democraticmedia.org/privacyreport.pdf.

[60] 18 U.S.C. § 2710-2711 (2000).

[61] Joseph A. Post, *A Lawyer's Ramble Down the Information Superhighway: Privacy and Communications Networks*, 64 FORDHAM L. REV. 770, 778 (1995).

[62] *Id.*

[63] *See* S.B. 1090, 2001-2002 Reg. Sess. (Cal. 2001) (amending Cal. Penal Code 637.5 (Deering 2000)).

[64] *See* S.B. 1090, 2001-2002 Reg. Sess. (Cal. 2001) (amending Cal. Penal Code 637.5 (Deering 2000)); S.B. 1090 Senate Bill-Bill Analysis *available at* http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1051-1100/sb_1090_cfa_20010418_115050_sen_comm.html (last visited Sept. 12, 2004).

[65] *See* S.B. 1090, 2001-2002 Reg. Sess. (Cal. 2001) (amending Cal. Penal Code 637.5 (Deering 2000)).

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] *See* Steven A. Hetcher, *Norm Proselytizers Create a Privacy Entitlement in Cyberspace*, 16 BERK. TECH. L. J. 877, 889 (2001).

[71] For a more extended explanation of cookie technology, *see* Eamonn Sullivan, *Are Web-based Cookies a Treat or a Recipe for Trouble?* PC WEEK, June 24, 1996, at 75.

[72] *See id.* (Cookies are used to store settings for customized search engines like MyYahoo! and to keep track of a shopping list at online stores like Amazon.com).

[73] *See* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERK. TECH. L. J. 1085, 1104 (2002).

[74] *See* Sullivan, *supra* note 71.

[75] *See id.*

[76] John Buskin, *Our Data, Ourselves*, WALL ST. J., Apr. 17, 2000, at R34.

[77] *Id.*

[78] Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 290 (2001).

[79] *Id.*

[80] *Id.*

[81] *See* Acxiom, *Consumer Recognition Solutions*, *at* http://www.acxiom.com (last visited Sept. 12, 2004) (describing how the company's customer recognition solutions enable companies to distinguish customers accurately and consistently, providing complete and instant access to relevant customer data across all channels of communication); *see also* Janet D. Gertz, Comment, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 950 (2002) ("[c]onsumer profiling is a growing trend in the financial services industry").

[82] Gertz, *supra* note 81, at 950.

[83] *Id.*

[84] *Id.*

[85] *Id.* at 951.

[86] *Id.* at 993.

[87] RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977) (this may be analogized to the Supreme Court's protection of a zone of privacy in intimate associations from state intrusion under the

Fourteenth Amendment); *see supra* notes 40-42 and accompanying text.

[88] *See, e.g.*, State v. Hempele, 576 A.2d 793, 802 (N.J. 1990).

[89] *See generally Business Week/Harris Poll: A Growing Threat*, BUS. WK., Mar. 20, 2000, at 96, *available at* http://www.businessweek.com/2000/00_12/b3673010.htm.

[90] *See* Stan Karas, *Privacy, Identity, Databases*. 52 AM. U. L. REV. 393, 442 (2002).

[91] *Id.* at 439.

[92] *Id.*

[93] *Id.*

[94] *Id.* at 444.

[95] *Id.* at 444-45.

[96] 341 N.E.2d 337 (Ohio Ct. App. 1975).

[97] 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

[98] *Shibley*, 341 N.E.2d at 339 (relying in part on a statute enacted by the Ohio legislature that permitted the violations of any of the three federal statutes under which they brought the suit).

[99] *DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d at 519-26 (finding that plaintiffs failed to plead violations of any of the three federal statutes under which they sued).

[100] Time Inc., at *http://www.timewarner.com/corp/businesses/detail/time_inc/index.html.*

[101] *Shibley*, 341 N.E.2d at 338.

[102] *Id.* at 339.

[103] *Id.*

[104] *Id.* at 339-40.

[105] *See DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497.

[106] *See id.* at 500, 503.

[107] *Id.* at 500.

[108] *Id.*

[109] *Id.* at 505.

[110] *Id.*

[111] *Id.* at 514, 526.

[112] *Id.* at 509-511; 18 USCS § 2701 (Lexis 2004) (making it an offense to access intentionally without authorization a facility through which an electronic communication service is provided or to intentionally exceed an authorization to access that facility and thereby obtain, alter or prevent authorized access to wire or electronic communication while it is in electronic storage in such system).

[113] Karas, *supra* note 90, at 441.

[114] *See* Nielsen Media Research, *About Us*, *at* http://www.nielsenmedia.com/ (last visited Sept. 12, 2004).

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.*

[120] *Id.*

[121] *Id.*

[122] *Id.*

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] TiVoPortal, *supra* note 6.

[127] *Id.*

[128] *Id.*

[129] *Id.*

[130] TivoPortal, *How do TiVo suggestions work?*, *at* http://www.garysargent.co.uk/tivo/faq/faqentry.php?faqid=29 (last visited Sept. 12, 2004).

[131] *Id.*

[132] TiVoPortal, *supra* note 6.

[133] *Id.*

[134] *Id.*

[135] *An Examination of Existing Federal Statutes Addressing Information Privacy: Hearing Before the House Subcomm. on Commerce, Trade, and Consumer Prot.* 107th Cong. 26 (2001) (Statement of Richard Smith, Chief Technology Officer, Privacy Foundation).

[136] *Id.*

[137] Epinions.com, *Television That Watches YOU!*, *at* http://www.epinions.com/content_1617797252 (June 4, 2001).

[138] *Id.*

[139] Ben Charny, *TiVo watchers uneasy after post-Super Bowl reports*, CNET News.com (Feb. 5, 2004) *at* http://msn-cnet.com.com/2100-1041_3-5154219.html?part=msn-cnet&subj=ns_5154219&tag=tg_home.

[140] *Id.*

[141] *Id.*

[142] *Id.*

[143] Matthew Zinn, *White Paper Submitted to the Federal Trade Commission* (TiVo, Inc. May 3, 2001), *available at* http://www.tivo.com/pdfs/ftc_letter.pdf.

[144] David Burke, *Guide to Interactive TV*, *at* http://www.whitedot.org/issue/iss_story.asp?slug=shortspytv2 (last visited Sept. 12, 2004).

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *See* White v. White, 781 A.2d 85, 91-92 (N.J. Super. Ct. Ch. Div. 2001).

[158] *See id.* (stating that what is highly offensive to a reasonable person turns on one's reasonable expectation of privacy, a concept that is measured objectively).

[159] United States v. Taketa, 923 F.2d 665, 675-78 (9th Cir. 1991).

[160] *See, e.g.*, Spetalieri v. Kavanaugh, 36 F. Supp. 2d 92, 111 (N.D.N.Y. 1998) (acknowledging the existence of a defamation cause of action against a private party).

[161] 47 U.S.C. § 551(a)(2)(A) (2003).

[162] Wong, *supra* note 8.

[163] Zinn, *supra* note 143.

[164] *Id.*

[165] *TiVo: Jackson stunt most replayed moment ever*, CNN.com, *at* http://www.cnn.com/2004/TECH/ptech/02/03/television.tivo.reut/index.html (Feb. 3, 2004).

[166] *Id.*

[167] Charny, *supra* note 139.

[168] *Id.*

[169] *Id.*

[170] *See* Burke, *supra* note 144.

[171] *Id.*

[172] *Id.*

[173] *Id.*

[174] *Id.*

[175] *Id.*

[176] Zinn, *supra* note 143, at 18 (quoting Section Two of TiVo's "Privacy Policy").

[177] Burke, *supra* note 144.

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] *Id.*

[182] *Id.*

[183] Zinn, *supra* note 143, at 18.

[184] *Id.* at 2.

[185] Joris Evers, *TiVo Compiles, Sells Users' Viewing Data*, PCWorld, *available at*, http://www.pcworld.com/news/article/0%2Caid%2C111015%2C00.asp (June 3, 2003).

[186] 18 U.S.C. § 2710-2711 (1994).

[187] *See* Blockbuster, *Privacy Policy: When Does Blockbuster Collect Personal Information? available at* http://www.blockbuster.com/corporate/displayPrivacyPolicy.action (last visited Sept. 12, 2004).

[188] Blockbuster Incentives, *Privacy Policy, available at* http://www.bbincentives.com/privacy_policy.php?src=sellcomm (last visited Sept. 12, 2004).

[189] Julie Hilden, *FindLaw Forum: Should bookstore purchase subpoenas be enforced?* (Feb. 21, 2002), *at* http://us.cnn.com/2002/LAW/02/columns/fl.hilden.bookstore/.

[190] *Id.*

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] *Id.*

[195] *Id.*

[196] Tattered Cover v. City of Thornton, 44 P.3d 1044, 1058 (Colo. 2002).

[197] Zinn, *supra* note 143, at 3.

[198] Video Programming Consumer Privacy Protection Act, H.R. 3511, 108th Cong. § 715 (2003).

[199] Satellite Home Viewer Extension Act, S. 2013, 108th Cong. (2004).

[200] *Id.*

vanderbilt journal of entertainment law & practice

A one-year subscription to the Vanderbilt Journal of Entertainment Law & Practice may be purchased for thirty dollars. Please remit checks or money orders payable to "JELP Subscriptions," along with the completed form below to:

JELP Subscriptions
Vanderbilt Law School
131 21st Avenue South
Nashville, Tennessee 37203

Name: _____
Firm/Company: _____
Address: _____
Phone: _____
Email: _____
Occupation/Title: _____