TiVo, Inc.

WHITE PAPER
SUBMITTED TO THE
FEDERAL TRADE COMMISSION

MAY 3, 2001

Matthew Zinn
Vice President,
General Counsel &
Chief Privacy Officer
TiVo, Inc.
2160 Gold Street
P.O. Box 2160
Alviso, CA 95002
(408) 519-9100

Of Counsel: ***Ronald L. Plesser***
Piper Marbury Rudnick & Wolfe LLP
1200 19th Street N.W.
Washington, D.C. 20036
(202) 861-3900

TABLE OF CONTENTS

I. Introduction

At the request of three Members of Congress, the Federal Trade Commission ("FTC") is inquiring into certain past and present practices of TiVo, Inc. ("TiVo"), a leader in the nascent personal video recording industry. The focus of this inquiry into TiVo's privacy practices, sparked by a Privacy Foundation report dated March 26, 2001 (http://www.privacyfoundation.org/privacywatch/report.asp?id=62&action=0), has centered on the following two issues: (1) whether TiVo's privacy policy adequately disclosed the system's collection of TV viewing information and whether this information is linked to personally identifiable information; and (2) whether information transmitted from a subscriber's home may have been personally identifiable at the point it left the TiVo "Receiver" (*i.e.*, the unit in the consumer's home) and whether it was received or stored as personally identifiable information at the TiVo Broadcast Center (*i.e.*, the server side), without the consent of the subscriber, in contravention of TiVo's privacy policy.

This White Paper is presented to inform the FTC, Congress, and the public at large about TiVo's commitment to privacy protection as attested to by the extensive measures it has undertaken in designing its system from the outset to protect the privacy of its subscribers' personally identifiable viewing information (what TiVo refers to in its privacy policy as "Personal Viewing Information").[1] TiVo welcomes this opportunity to contribute to an informed discussion of its privacy practices and policies, and TiVo will place this White Paper on its Web site to further this goal.

This Paper demonstrates that TiVo did not and does not receive or store personally identifiable viewing information without subscriber consent. TiVo has designed a system that ensures that any viewing data transmitted from the Receiver are anonymous on the Receiver and remain unidentifiable to a particular subscriber (what TiVo refers to herein and in its privacy policy as "Anonymous Viewing Information"), unless that subscriber consents to such identification before any viewing data leave the Receiver. Although account information, setup information, and information about the operation of the Receivers (what TiVo refers to herein

---

[1] *See* Appendix A for TiVo's privacy policy, which includes full definitions of the kinds of information TiVo collects.

and in its privacy policy as "Diagnostic Information") that is sometimes[2] transmitted to the TiVo Broadcast Center contain certain personally identifiable information, including the serial number of a subscriber's TiVo Receiver, the viewing data that are transmitted in a separate file within the same telephone transmission do not contain the Receiver's serial number or any other identifying information, except where there is explicit consumer consent. A few subscribers have affirmatively consented to TiVo's collection of personally identifiable viewing information for, for example, viewer surveys. Moreover, subscribers have the ability to opt out of the collection of even Anonymous Viewing Information by placing a toll free call to TiVo or by writing TiVo. For such subscribers, no viewing information is ever transmitted from the TiVo Receiver to the TiVo Broadcast Center. Any personally identifiable information TiVo needs about a subscriber in order to service the account is kept completely separate from any viewing information.[3] **As a result, unless subscribers specifically opt in to the collection of personally identifiable viewing information before the file containing such viewing information is transmitted from the Receiver to the distribution servers at TiVo Broadcast Center, TiVo has no way of matching particular viewing information with particular subscribers.**

The Privacy Foundation, in its report, focused its study exclusively upon the information being transmitted from the TiVo Receiver. It did not discuss the system that TiVo employs to ensure that personally identifiable viewing information remains anonymous, secure and separate from other information, except where a subscriber has opted in. Therefore, the Privacy Foundation's analysis reflected only one aspect of a larger process which, from the outset, has been designed to protect subscriber privacy. As part of this process, TiVo created the personal video recording industry's first privacy policy to describe the privacy protections it offers its subscribers. The policy (referenced on TiVo's Web site as its "Privacy Promise"), which is available on TiVo's Web site (http://www.tivo.com/flash.asp?page=support_privacy), and which is attached hereto as Appendix A, highlights the company's promise that, absent subscriber consent, TiVo will not collect personally identifiable viewing information.

---

[2] TiVo collects Diagnostic Information log files for a random sample of approximately 5,000 of the approximately 150,000 Receivers that have been sold.

[3] *See* IV. for a discussion of the kinds of information TiVo collects and how TiVo's servers collect and store information.

This Paper also demonstrates that, at all times, TiVo's privacy policy has been consistent with its information practices. As it indicated it would, TiVo has issued revised privacy policies both to account for updates of the software and to bring increased clarity to its information collection and use practices. Indeed, the current version of TiVo's privacy policy—in effect since September 2000—addresses many of the issues which the Privacy Foundation advisory brought up. These clarifications further reflect TiVo's commitment to privacy protection and to enabling consumers to make informed decisions concerning TiVo's information collection practices. Further, as discussed in TiVo's privacy policy, before providing a service that requires a substantial and material amendment to its privacy policy, TiVo will give subscribers notice of, and request consent to, any such change in TiVo's practices on collection, use and disclosure of information. TiVo's privacy policy also states that, in the event of an acquisition of TiVo, the acquiring company would assume the rights and obligations explained in the privacy policy regarding subscribers' information.

Finally, this Paper responds to other issues raised by the Privacy Foundation report, such as the statement that no encryption was used to secure the communication between the Receiver and the TiVo Broadcast Center. In fact, the authentication process used to secure the communication between the Receiver and the TiVo Broadcast Center has always been based on public key cryptography protocols, and the current version of the software now uses public key-private key 128-bit encryption when transmitting files containing viewing information between the Receiver and the TiVo Broadcast Center.

II. TiVo's Privacy Policies and Practices Address the Major Concerns of the Privacy Foundation's Report

The following discussion of TiVo's collection and use of information, and of its statements regarding those practices, addresses the major objections of the Privacy Foundation's report. In addition, TiVo also has already addressed these objections both in a response and a set of questions and answers, which it posted on its Web site (http://www.tivo.com/flash.asp?page=support_privacy). Many of the Privacy Foundation's objections can be traced to the Privacy Foundation having conducted its analysis on an older version of the software, without the benefit of complete information about the server side of transmissions, and with an outdated manual.

A. Consistency of Disclosures of Policies on Web site and In Manuals

The Privacy Foundation used the manual included with an older version of the software for its analysis. By the time the Privacy Foundation conducted its analysis, this version of TiVo's privacy policy had been updated and the current 2.0 software was being released. In subsequent versions of the manual, TiVo updated and expanded its discussion of its privacy practices, to reflect the launch of version 2.0 of its software and to provide its subscribers with a fuller understanding of its privacy policies. Outdated manuals are an inescapable byproduct of retail distribution of a new technology that is undergoing revisions to improve the service. Even the (outdated) privacy policy in the user manual the Privacy Foundation used for its analysis was consistent with the updated version of the privacy policy on TiVo's Web site. Indeed, TiVo's privacy policy has consistently stated that the privacy policy is subject to amendment, and TiVo took steps to inform consumers of expansions of and clarifications to its privacy policy.[4] At all times, TiVo's descriptions of its information practices have been consistent with its practices, which have remained the same since initial rollout.

B. Adequacy and Form of Disclosures and Consent

TiVo has created the personal video recording industry's first privacy policy, which describes in detail the kinds of information TiVo collects and how that information is used. TiVo makes this policy available to subscribers in its user manual, on its Web site, on request in response to a toll-free call, and alerts subscribers through occasional messages.[5] TiVo therefore disputes the Privacy Foundation's suggestion that users without Web access have no practical means of obtaining its privacy policy. TiVo also gives subscribers ample choice about what information is collected and allows subscribers to change these choices at any time by calling TiVo's toll-free number or by sending a signed, written request to TiVo.

The Privacy Foundation conducted its study with limited knowledge of the extraordinary measures TiVo takes once information is received by the Broadcast Center distribution servers to ensure that viewing information is automatically received and stored separately from any

[4] *See* V.

[5] *See* V.B.3. for information on how TiVo sends messages to its subscribers.

information that could be used to match it to individual Receivers or to subscribers. Consequently, the Privacy Foundation's conclusions are not supported. For example, the Privacy Foundation criticized TiVo for its statement in its user manual that "[none] of TiVo's computer systems will have access to [your personal information] without your prior consent," because TiVo Broadcast Center receives viewing information and subscriber identity information during the same telephone transmission. As shown herein, TiVo designed its system so that viewing information is anonymous before being transmitted to TiVo Broadcast Center, unless the subscriber consents, and is kept anonymous once it is received. Therefore, it is inaccurate to consider files of Anonymous Viewing Information as "personal information," as the Privacy Foundation implies, since these files do not contain personally identifiable viewing information and since TiVo designed its system to break any possible linking between viewing information and personally identifiable information received during the same telephone transmission.[6] At the same time, TiVo has exhibited a flexibility and willingness to revise and expand its explanation of its privacy policies as its technology changes and in response to questions and concerns, such as those posed by the Privacy Foundation's report.

C. Encryption

Focusing upon the transmission of viewing data, the Privacy Foundation's report concluded that no encryption methods are used to secure the communication of viewing or diagnostic information from the Receiver to the TiVo Broadcast Center. In fact, the key needed for authentication has always been encrypted. As part of a long-range security plan, TiVo began using public key-private key 128-bit encryption in conjunction with the release of its version 2.0 software to ensure that the files containing viewing information are transmitted securely.[7]

D. Potential Use of Information

The Privacy Foundation report paints an incomplete picture and then speculates as to what TiVo could do with viewing information, not what it actually does. The report examines

---

[6] *See* IV.B.3. for an explanation of the procedures TiVo uses to ensure that viewing information remains anonymous, except where a subscriber has previously opted in.

[7] Version 2.0 software was shipped with DIRECTV/TiVo combo Receivers in September 2000. Version 2.0 software (in the form of a version 2.0.1 release) began to be distributed to stand-alone TiVo Receivers in late March 2001.

only what happens at the Receiver end, and acknowledges that the "server-side practices are beyond the scope of the advisory." TiVo has gone to great lengths to design its server system to ensure that the viewing information received by the TiVo Broadcast Center distribution servers is and remains anonymous, except where a subscriber has consented to the collection of personally identifiable viewing information. **As a result, unless subscribers specifically opt in to the collection of personally identifiable viewing information before the file containing such viewing information is transmitted from the Receiver to the distribution servers at the TiVo Broadcast Center, TiVo has no way of matching particular viewing information with particular subscribers.** TiVo could have designed its system a number of ways, but it specifically designed its service to protect subscribers' privacy, including giving subscribers the choice to opt out of the collection or use of Anonymous Viewing Information. That is TiVo's past, present, and future promise to its subscribers.

III. Background

TiVo is a pioneer in the personal television industry. Formed in 1997, TiVo offers a subscription-based service (the "TiVo Service") that works in conjunction with a personal video recorder (the "Receiver"). In addition to the Receiver's ability to pause, rewind, and play back live or recorded television broadcasts, the TiVo Service enables consumers to easily find, record, and manage their favorite TV programs. In addition, TiVo subscribers may select programs with their favorite actors and directors, or relating to certain content for which they have indicated a preference. For example, a subscriber could program the Receiver to record all programming relating to CBS's "Survivor," including the program itself, news broadcasts with interviews of the contestants, and entertainment shows featuring the contestants, or all programming about dogs, including regular programming devoted to dogs on the Animal Planet network, rerun episodes of "Lassie" and movies on premium movie channels featuring dogs, such as "Best in Show."

All of this can be done without setting a timer or using videotape. In particular, the TiVo Service provides subscribers with numerous features including: Season Pass—the ability to automatically record every episode of the subscriber's favorite show—even if the show changes time slots; Now Playing—an on-screen listing of shows the subscriber recorded in which each show is instantly available with the touch of a button on the TiVo remote; Network Showcases—current listings of the highest rated shows the TV networks have to offer; TiVo Suggestions—the

ability to find and record programs that match a subscriber's interest based on the subscriber's rating of programs using the "Thumbs Up" and "Thumbs Down" buttons on the TiVo remote; and an interactive program guide—which allows the subscriber to quickly and easily search scheduled programs up to two weeks in advance. The result is a richer and more enjoyable viewing experience that allows subscribers to watch what they want when they want.

There are currently approximately 150,000 TiVo subscribers. The Receiver, which is manufactured by separate companies licensed by TiVo, including Sony, Philips, and Thomson, retails for approximately $400.00, and there are monthly ($9.95), yearly ($99.00) and product lifetime ($249.00) subscriptions available, which are chosen as part of subscriber "setup" directly with the TiVo Service. As with many new technologies, TiVo's software has been upgraded since the launch of version 1.0 in March 1999.[8]

TiVo purposefully designed the system so that information about specific programming watched or skipped by the individual subscriber is anonymous when leaving the Receiver, and is kept automatically and permanently anonymous, unless the subscriber consents before the information is transmitted. From the outset, TiVo envisioned, and has implemented, a plan to:

- Automatically ensure that any information TiVo collects about a subscriber's particular viewing choices is and remains anonymous, unless subscribers consent to collection of personally identifiable viewing information before any viewing data leave the Receiver.

- Continually increase the security of the transmission of information between subscribers' Receivers and TiVo Broadcast Center; and

- Ensure that subscribers are informed about TiVo's information practices and have choices about how their information is used.

Consistent with the system's design, and in furtherance of this plan, TiVo created the personal video recorder industry's first privacy policy and hired a Chief Privacy Officer to

[8] There have been several software upgrades in the ensuing years. TiVo began shipping the current version of its software, version 2.0.1, in March 2001.

ensure that subscribers' information is protected and that subscribers are informed and given choices about TiVo's collection and use of information.

IV. What Information Does TiVo Collect and How Is it Collected?

A. Kinds of Information and Subscriber Choices

TiVo's privacy policy governing subscribers' use of the TiVo Service describes the kinds of Subscriber Information[9] TiVo collects and the choices that subscribers have about the collection of that information. This policy is made available on TiVo's Web site (http://www.tivo.com/flash.asp?page=support_privacy) and in its user manual, and is attached hereto as Appendix A. In addition, the TiVo Web site makes available separate privacy policies for Web site users and for subscribers who receive their video signals through DIRECTV (as opposed to cable or broadcast).[10] The current version of the policy, posted on TiVo's Web site since September 2000, defines the following categories of information.[11]

1. *Account Information* is information about a subscriber's account, including Contact Information (defined below) and other information linked to a subscriber's Contact Information, such as the model and serial number of the Receiver, software version used, the subscriber's zip code, TV programming source (cable, satellite or an antenna), the type of cable hook-up (digital or analog) and level of service (basic or premium), the subscriber's privacy preferences, and the cable or satellite box model used. This minimum service identity information must be exchanged on an ongoing basis for TiVo's servers to ensure the Receivers are entitled to service and for TiVo to provide the TiVo Service to the Receivers. Account Information includes information TiVo collects from subscriber communications or other personally identifiable

---

[9] TiVo uses the term "Subscriber Information" in its privacy policy and herein to refer to all of the various types of information about subscribers. Subscriber Information, therefore, is Account Information, Contact Information, Diagnostic Information, personally identifiable viewing information (defined as "Personal Viewing Information" in TiVo's privacy policy), and Anonymous Viewing Information. *See* Appendix A.

[10] Some TiVo subscribers are DIRECTV subscribers, while most receive their video signals from cable or over the air. TiVo's privacy policy for DIRECTV subscribers and those whose video source is cable or broadcast are substantively the same. The privacy policies are different to account for the different methods of receiving video signals. For ease of discussion, any references herein to the TiVo privacy policy are to the policy applicable to subscribers receiving their video signals from cable or broadcast, except as noted otherwise.

[11] *See* Appendix A for complete definitions.

information and does not include any personally identifiable viewing information. Account Information is kept separate from viewing information, unless a subscriber opts in.

2. *Contact Information* is information that allows someone to identify or contact the subscriber, including, for example, name, address, telephone number, credit card information, e-mail address. Contact Information is a subset of Account Information, and, therefore, is linked to the Receiver's serial number. Contact Information is kept separate from viewing information, unless a subscriber opts in.

3. *Diagnostic Information* is information about the operation of the subscriber's Receiver. For a small number of randomly sampled subscribers, Diagnostic Information log files are transmitted to the TiVo Broadcast Center. Diagnostic Information must include the serial number (so that TiVo can troubleshoot any errors) and, therefore, is linked to a subscriber's Account Information, but it does not include any personally identifiable viewing information. Diagnostic Information log files contain information about the system status reports, such as memory consumption, user interface response time, disk space, enclosure temperature and enclosure fan speed. Subscribers may opt out of the collection of Diagnostic Information log files.

4. *Personal Viewing Information* is information about the viewing choices made by subscribers while using the Receiver, if that information is linked to or associated with Contact Information. For the sake of clarity, this information is referred to herein as "personally identifiable viewing information." Viewing information is stored on a subscriber's Receiver so that an algorithm in the Receiver can recommend viewing choices if there is available space on the hard disk drive.[12] Subscribers must consent (*i.e.*, opt in) by sending TiVo a signed, written request or calling TiVo directly in order for viewing information to be treated as personally identifiable viewing information (*i.e.*, linked to a particular subscriber) when it is collected by the TiVo Broadcast Center distribution servers.

---

[12] *See* IV.B.3. for information on the algorithm used to recommend program choices.

5. Anonymous Viewing Information is information about viewing choices that subscribers make while using the Receiver, but it is not associated with or linked to any Contact Information whatsoever. This information allows TiVo to know that a subscriber from a particular zip code watched certain programming between calls to the distribution servers in the TiVo Broadcast Center, but TiVo is unable to associate those viewing choices with a particular subscriber after it is collected by the distribution servers in the TiVo Broadcast Center. Subscribers may opt out of the collection of Anonymous Viewing Information by calling TiVo's toll-free number or by writing TiVo.

Subscribers may change their choices about TiVo's collection of information at any time, and TiVo will immediately adhere to the change. For example, if a new subscriber opts in to the collection of personally identifiable viewing information during the first 12 months as a TiVo subscriber, and then elects to opt out during the second 12 months, TiVo will not collect personally identifiable viewing information from that point forward, unless the subscriber subsequently opts back in.

B. What Information is Received by the TiVo Broadcast Center Distribution Servers and How is it Stored?

TiVo collects the following categories of information from subscribers:

- Account Information, defined above.
- Information necessary to activate a subscriber's account.
- Diagnostic Information, defined above.
- Security information necessary for the TiVo Broadcast Center to validate that the TiVo Receiver is authorized to receive the TiVo Service and that the TiVo Receiver is receiving the actual TiVo Service, and not an imposter.
- Anonymous Viewing Information, defined above.
- Personally identifiable viewing information, defined above, which is only collected when the subscriber opts in.

Except where the subscriber opts in, viewing information is kept separate from, and TiVo cannot link it to, these other categories of information.

Information is transmitted to and from the Receiver and the distribution servers at the TiVo Broadcast Center at the activation stage, and once a day thereafter, or when the subscriber chooses.

1. Activation: Setup and Account Information

When a new TiVo subscriber takes a Receiver out of the box and connects it to a television for the first time, the Receiver dials the TiVo Broadcast Center to authorize the Receiver to obtain the TiVo Service, in much the same way as cell phone users must activate their phones when used for the first time. The TiVo subscriber is led through a "Guided Setup" process, during which the TiVo Broadcast Center receives the serial number of the Receiver, the zip code of the subscriber, the signal source (*e.g.*, cable, broadcast, or satellite), and other non-personally identifiable information. The subscriber furnishes Contact Information (such as name, address, telephone number, credit card information, and e-mail address) either by a toll-free phone call to TiVo or by sending e-mail through TiVo's Web site. At this point, and at any time thereafter, a subscriber may opt out of the collection of any viewing information, including Anonymous Viewing Information, and/or Diagnostic Information log files by contacting TiVo by phone or by writing TiVo. The Receiver's serial number will, of course, remain linked to a subscriber's Account Information, Contact Information, Diagnostic Information log files, public key-private key encryption information and, where the subscriber has opted in to the collection of personally identifiable viewing information, information about the subscriber's viewing.

2. Daily Call from the Receiver to the TiVo Broadcast Center's Distribution Servers

Once each day,[13] the Receiver "calls" the distribution servers at the TiVo Broadcast Center through the subscriber's phone line (the "Daily Call"). The Receiver communicates with the distribution servers at the TiVo Broadcast Center for only a few minutes each day during the

[13] This call will not take place daily if the subscriber's Receiver is not connected to the phone line every day. The TiVo Service will still function if the call is less than once per day, although the subscriber will not receive the most up-to-date programming information.

Daily Call. No television programming is received through this phone call; television program content is delivered by cable, broadcast, or direct broadcast satellite.

The initial stage of the Daily Call is authentication. To combat fraud, authentication is designed to ensure that the TiVo Receiver is authorized to receive the TiVo Service from the Broadcast Center distribution servers. This authentication stage is based on industry-standard public key cryptography protocols. The public key protocol is based on the ElGamal algorithm using an 894-bit key length, which provides extremely strong encryption. The use of this protocol ensures both that the Receiver is valid and should receive service and that the Receiver is communicating with the actual TiVo Service (as opposed to an imposter service). During this process, a randomly chosen encryption key is securely passed between the Receiver and the TiVo Service.

Once authentication is complete, and using the zip code and programming source information furnished by the subscriber, the Broadcast Center distribution servers send program guides and other elements necessary to receive the TiVo Service, such as codes for operating the remote control, to the Receiver. These updated program guides enable the Receiver to record the subscriber's favorite shows, and give the subscriber updated programming information.

The Receiver compiles information on the Receiver's viewing actions (*i.e.*, what is watched in the subscriber's home). **These viewing files are not linked to the Receiver's serial number,** or any other form of personally identifiable information, unless the subscriber opts in to the collection of personally identifiable viewing information. When the Receiver calls the Broadcast Center for updated program guide information, the Receiver sends this viewing information to the Broadcast Center distribution servers for storage as Anonymous Viewing Information. For the handful of subscribers who have affirmatively opted in, the TiVo Service links the viewing data with identifying information at the Receiver, thereby enabling it to be personally identifiable in TiVo's servers. For a small number of randomly sampled TiVo subscribers (currently about 5,000 of the over 150,000 TiVo subscribers), the Receiver also sends Diagnostic Information log files, which enable TiVo to evaluate and fix technical problems in the Receivers. The longer the TiVo Service is in the marketplace, the less need TiVo has to collect Diagnostic Information log files to address technical problems. Subscribers may also opt out of the transmission of Diagnostic Information log files.

Adding increasing levels of security to the communications between the Receiver and the TiVo Broadcast Center has always been a part of TiVo's business plan. In earlier versions of the TiVo software, only the key needed for authentication was encrypted. As previously discussed, since the release of its version 2.0 software, the TiVo Broadcast Center now uses public key-private key 128-bit encryption using the industry standard Blowfish encryption algorithm to ensure that the files containing viewing data are transmitted securely.

3. TiVo Broadcast Center: Processing and Storing of Anonymous Viewing Information and Personally Identifiable Viewing Information

Once the encrypted data files with viewing information are received by the distribution servers in the TiVo Broadcast Center, TiVo takes extraordinary measures to ensure that any information that could possibly associate or link viewing choices with a specific Receiver are removed, except for the handful of subscribers who have consented to TiVo linking their viewing patterns to their personally identifiable information. These procedures on the server side—which automatically remove any potentially identifying information and then store that Anonymous Viewing Information—ensure that TiVo is unable to associate viewing information with particular subscribers, unless those subscribers have told TiVo before their viewing information is received that they consent. These steps are represented in the diagram attached hereto as Appendix B.

To account for its growing subscriber base, TiVo's Broadcast Center uses numerous servers to receive and process the kinds of information described herein. TiVo designed its servers to automatically and permanently keep information about subscriber viewing separate from the other streams of information (*e.g.*, Account Information and Contact Information) TiVo must collect in order to activate the subscriber's service and to service the customer's account, unless the subscriber consents. Of course, the serial numbers of Receivers remain linked to Account Information, Contact Information, Diagnostic Information log files and public key-private key encryption information so that TiVo can service the subscriber's account, provide the TiVo Service to authorized Receivers, and troubleshoot problems with Receivers. In addition, where the subscriber has opted in to the collection of personally identifiable viewing information, the Receiver serial number is linked to the subscriber's viewing information.

Initially, files of anonymous viewing information that have not been "tagged" as belonging to subscribers who have opted in to collection of personally identifiable viewing

information are assigned separate, random names by the distribution servers and stored in a directory separate from any identifying information. The file transfer logging is turned off so that there is no log file to refer to later for correlation. This begins the process of ensuring that this viewing information remains anonymous, which is why TiVo refers to files without these "tags" (the vast majority of viewing files) as Anonymous Viewing Information files. In other words, the distribution servers in the Broadcast Center store the Anonymous Viewing Information files without making any record of the identity of the Receiver that transmitted the files. Every 30 minutes, Anonymous Viewing Information files are then automatically and randomly transferred into one of 10 directories.[14] This process essentially scatters the files of Anonymous Viewing Information, so that TiVo cannot link them to Receiver serial numbers or other personally identifiable information. Subsequently, every three hours, the distribution servers automatically erase all time stamp information associated with each file, thus eliminating any possible correlation between the time of reception and when a particular Receiver called. During this same three-hour interval, the distribution servers combine the anonymous viewing data in each file within a directory into a single file, which is transferred to restricted access backhaul servers.[15] After the daily backup of the restricted access backhaul servers, the original files on the distribution servers are deleted. This entire process is designed to ensure that, unless the subscriber has opted in, TiVo cannot attach viewing information to Receiver serial numbers or any other information identifying specific subscribers, either in the servers containing the Diagnostic Information or the servers storing subscriber Account or Contact Information. Nor can TiVo reattach such information after it has been received by TiVo's servers.

Files with viewing information that have been "tagged" for subscribers consenting to association of their viewing with their personal information (what TiVo, in its privacy policy, calls "Personal Viewing Information" and what is referenced herein as personally identifiable viewing information) are received and stored in a separate and secure database to which very few TiVo staff members have access. This access is limited to the analysis of personally identifiable viewing information only for specific, limited purposes, such as audience measurement.

---

[14] The same random assignment into one of 10 directories is used for log files of Diagnostic Information. TiVo scatters the Diagnostic Information file logs across 10 directories for security purposes. However, this process does not remove Receiver serial numbers, as the diagnostic information would be essentially useless without it.

[15] This process also occurs for Diagnostic Information log files separately.

Because of its importance, this process of ensuring that viewing data remain anonymous—except where a subscriber has indicated otherwise—merits elaboration. Analogizing to "marbles" of information, the Receiver begins with a marble of viewing information. The marble itself does not identify the Receiver serial number. The marble is securely sent to TiVo via an encrypted communication. Unless the marble's owner has indicated that it should be "tagged" with the owner's name, TiVo receives and stores the marble without making any record of where the marble came from (*i.e.*, no "how did this arrive?" information is gathered). The system that stores the marble randomly tosses the marble into one of a collection of boxes and shakes the boxes, so that TiVo is unable to tell the source of, or the time when, a specific marble was received. Even if TiVo received a subpoena from a law enforcement agency to reattach a "marble" of viewing information to a particular subscriber, TiVo would not be able to do so. Unless a subscriber had previously opted in, TiVo would have no way of obtaining information about that subscriber's personal viewing habits.

To use another analogy, viewing information is placed inside a blank, sealed (*i.e.*, encrypted) envelope at the Receiver. The envelope is then sent to a separate mailbox (*i.e.*, server) in TiVo Broadcast Center. Unless the sender (*i.e.*, subscriber) has written the address on the envelope, there is no mechanism to tell who sent the letter. TiVo then automatically places the envelope in one of 10 random bags of similar envelopes, and shakes the bag. In addition, TiVo turns off the log that would indicate when the envelope was received and erases the stamp indicating the time and date. The envelope's contents are then opened, combined with the contents of other anonymous envelopes, and sent to a separate, secure mailbox.

By contrast to the elaborate server-side processes for disassociating viewing with individual subscribers in the home, each TiVo Receiver stores information about the specific programming watched in that particular household. The individual viewing information stored on the TiVo Receivers is what makes the TiVo Service attractive for many of its subscribers. Subscribers can indicate their preferences for shows with particular actors, directors, or programs of a particular genre, and the TiVo Receiver will recommend and automatically record programs for the subscriber based on those preferences. In addition, subscribers indicate whether they like particular programs by using the "Thumbs Up" and "Thumbs Down" buttons on their remote controls; this information is stored on the Receiver and factored into the algorithm used to recommend and record shows where there is excess capacity on the hard drive. At any time, the subscriber can clear the preferences on the Receiver, or turn off the program that automatically

fills up the excess capacity on the hard drive with suggested programming. **Again, for the sake of clarity, personally identifiable viewing data do not leave the Receiver unless the subscriber opts in.**

C. What Does TiVo Do With Information It Collects?

As described in its privacy policy, TiVo staff members use *Anonymous Viewing Information* to analyze what programs, advertisements, and types of programming subscribers watch, skip, or time-shift for later viewing. For example, TiVo uses Anonymous Viewing Information to develop inferences that people who watch show X are likely to watch show Y. TiVo shares certain "top line" Anonymous Viewing Information with advertisers, cable networks, and other third parties. This information is not identified with any particular subscriber. TiVo has no other plans for future uses of Anonymous Viewing Information. Whatever such future uses may be, they will comport with TiVo's core promise: viewing information will remain anonymous unless subscribers consent before such information has left the Receiver.

TiVo uses *Diagnostic Information* to assess technical problems both with the hardware on individual Receivers and with the software, which may affect large numbers of Receivers. This detailed information is not shared with third parties, except that the overall results may be shared with manufacturers to determine the source of and corrective action needed for specific hardware and/or software problems. Diagnostic Information log files must include the Receiver serial numbers in order for TiVo to identify and correct faulty Receivers.

Personally identifiable viewing information resides in the Receiver. Without a subscriber's prior consent, no "tag" is added to viewing files transmitted from Receivers to TiVo Broadcast Center's servers that would enable TiVo to identify the Receiver from which it came. For those subscribers who have opted in to the collection of personally identifiable viewing information, TiVo may use this information for surveys of particular subscribers and audience measurement. TiVo has committed to notify subscribers who have opted in if TiVo plans to change the current uses of personally identifiable viewing information, and will give subscribers an opportunity to opt in to any such new uses.

Account Information is disclosed to the appropriate service provider (*e.g.*, DIRECTV), where operationally necessary to facilitate the provision of service. TiVo also uses contractors

and third-party service providers (*e.g.*, billing agents), who may have temporary access to Account Information and other Subscriber Information for specific purposes. TiVo's contracts bind these contractors and third-party service providers (*e.g.*, DIRECTV) to TiVo's privacy policies; specifically, contractors and third parties may collect and use Account Information only for the specific and limited purposes designated in those contracts (*e.g.*, bill collection).

The TiVo employee handbook states that misuse of personally identifiable viewing information or Anonymous Viewing Information by TiVo employees constitutes grounds for immediate termination.

V. What Does TiVo Do to Inform Its Subscribers About Collection and Use of Information?

TiVo takes far-reaching measures to inform its subscribers about its practices on collection and use of Subscriber Information. As discussed in greater detail below, this notice is primarily accomplished through its privacy policy (what TiVo calls its "Privacy Promise"), which is posted at its Web site and available in its user manuals. TiVo further gives subscribers choice to opt out of the collection of information that is not necessary for TiVo to activate and service the subscriber's account.[16] At all times, TiVo's privacy policy has been consistent with its information practices. However, as TiVo indicated it would, TiVo has issued revised privacy policies both to account for updates of the software and to bring increased clarity to its information collection and use practices. Key provisions of TiVo's privacy policy, the methods TiVo uses to communicate with its subscribers, and the chronology of revisions to the privacy policy are outlined below.

A. Privacy Policy

TiVo's privacy policy sets out the different types of information TiVo collects, how it uses this information, the categories of information it discloses to third parties, and how subscribers can exercise choice with respect to TiVo's collection, use and disclosure of Subscriber Information. Key provisions include:

---

[16] *See* IV.A. and Appendix A for a description of the kinds of Subscriber Information.

1. Collection

TiVo's privacy policy sets out the different types of information that TiVo collects in two ways. First, the policy begins with a definitions section (Section 1) in which it defines the universe of information collected as Subscriber Information. It then goes on to delineate the three different kinds of information that comprise Subscriber Information: (1) Account Information, which includes Contact Information and Diagnostic Information; (2) Personal Viewing Information (referred to herein as "personally identifiable viewing information"), and (3) Anonymous Viewing Information.

After defining these terms, TiVo's policy discusses collection of Subscriber Information (Section 2). In describing TiVo's collection practices for Personal Viewing Information, the policy states:

> 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. We have worked very hard to ensure that no Personal Viewing Information is sent to TiVo without your consent. All Personal Viewing Information stays on the Receiver and does not get transmitted to TiVo without your consent. Not even our TiVo staff has access to your Personal Viewing Information unless you choose to disclose it to us or other parties.

The privacy policy's description of TiVo's collection practices goes on to state that "[y]our Receiver sends Anonymous Viewing Information to TiVo on an ongoing basis."

2. *Uses*

TiVo's privacy policy then proceeds to inform subscribers of the uses that TiVo makes of Subscriber Information (Section 3). In describing the uses of Personal Viewing Information, the policy states:

> Your Receiver uses your Personal Viewing Information 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. TiVo does not collect your Personal Viewing Information without your consent; your Receiver accomplishes this personalization without sending any Personal Viewing Information to TiVo. All the "smarts" are in the Receiver in your home.

With respect to uses of Anonymous Information, the policy states:

> We use Anonymous Viewing Information to develop reports and analyses about what programs, advertisements, and types of programming our subscribers (as a whole or in subgroups) watch or skip, or for other programming or advertising research.

3. Disclosures

Section 4 of the policy discusses TiVo's disclosure practices, describing what types of Subscriber Information are disclosed and to whom. For example, the policy states that:

> We disclose 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.

Section 4 of the policy informs subscribers that TiVo may disclose personally identifiable viewing information (*i.e.*, where the subscriber has affirmatively consented to its collection) to its hardware manufacturing partners, such as Sony, Philips and Thomson. Section 4 also explains that TiVo's hardware manufacturing partners are bound to adhere to the privacy policy.

4. Choices

In Section 5 of the policy, TiVo outlines subscribers' choices with respect to limiting TiVo's collection, use and disclosure of their information. In describing subscribers' choices, the policy states:

> The default privacy preferences, to which you hereby consent if you do not request a change to your settings, do not allow TiVo to collect Personal Viewing Information, but do allow TiVo to collect, use, and disclose Anonymous Viewing Information, and Diagnostic Information in manners consistent with this Privacy Policy.

Section 5 discusses how subscribers may change their privacy preferences. A subscriber may change his privacy preferences (*i.e.*, opt in to the collection of personally identifiable viewing information or opt out of the collection of Anonymous Viewing Information and Diagnostic Information log files) by calling TiVo's toll-free number or by writing TiVo.

5. Changes

Section 9 discusses amendments to the policy. Specifically, Section 9.1 provides:

> Before we provide you a service that requires a substantial and material amendment to this Privacy Promise, we will provide you with notice of, and request your consent to, any such change in our Subscriber Information collection, use and disclosure practices. . . . For example, in the future, we may develop a new program or feature in which we propose to collect, use or disclose [personally identifiable viewing information.] In that situation, TiVo will inform you about how we plan to use and disclose the [personally identifiable viewing information] and will request your express permission to do so.

B. How Does TiVo Inform Its Subscribers of Its Privacy Practices?

TiVo notifies its subscribers about its privacy practices through several mechanisms: through its Web site, in its user manuals, through e-mail, and in messages it sends to subscribers through the TiVo Service.

1. Web Site

TiVo's Web site contains a complete description of its separate privacy policies for the TiVo service offered through cable and broadcast video sources and the service offered to DIRECTV subscribers. TiVo's privacy policy for subscribers who receive video signals from cable and broadcast is attached hereto as Appendix A. These policies are modified to account for the technical differences in the video sources, but contain the same promises on collection and use of information. TiVo's Web site also has a separate privacy notice applicable to the information collected from TiVo's subscribers over the Web site. In response to the Privacy Foundation's report, on March 26, 2001, TiVo posted a statement on its Web site and a page of questions and answers on the issues raised by the report.

2. Manual

Each TiVo Receiver now sold contains a manual, which includes the same privacy policy as is currently posted on TiVo's Web site, and which contains a response to a "Frequently Asked Question" concerning protection of subscriber privacy. However, because TiVo Receivers are sold through the slower-than-cyberspace retail distribution method, it is unavoidable that some users will receive manuals that do not contain the most recent version of the privacy policy. This inevitable byproduct of retail distribution resulted in the Privacy Foundation receiving a user manual with an outdated privacy policy. To address this contingency, TiVo can also communicate with subscribers through a messaging system.

3. Messages

TiVo can send a message to subscribers through the TiVo Service that subscribers can't ignore (known as a "pre-TiVo Central message," or "PTCM"). As described below, TiVo sent a PTCM message to subscribers informing them of the September 2000 update to its privacy policy. To avoid annoying its subscribers, TiVo sends these messages only on rare occasions. Each TiVo Receiver also has a message area (similar to an e-mail inbox) where TiVo can send messages, which subscribers can review at the time of their choosing. The message informing subscribers of the September 2000 privacy policy update also appeared in this area.

4. E-Mail

A large percentage of TiVo subscribers voluntarily have provided TiVo with their e-mail addresses, and TiVo regularly uses e-mail to communicate with its subscribers. In September 2000, TiVo sent an e-mail message to subscribers informing them of the September 2000 revisions to its privacy policy.

C. Chronology and Amendments

TiVo's privacy policy states that TiVo reserves the right to amend its privacy policy. In a new industry, with a new company employing a technology that is constantly being upgraded, amendments are inevitable. Accordingly, TiVo has revised and expanded its privacy policy to make its information collection and use practices clearer. At their core, however, TiVo's practices with regard to subscriber viewing data have not changed; TiVo does not collect personally identifiable viewing information without prior consent.

The chronology of TiVo's revisions to its statements about subscriber privacy on its Web site and in its user manuals is as follows. TiVo adopted a privacy policy around the time that the first Receivers were shipped, on March 31, 1999. This policy was contained in the manual accompanying the Receiver, and was posted on TiVo's Web site, which also included a response on privacy to a "Frequently Asked Question." In March 2000, TiVo revised the responses to certain frequently asked questions to clarify the kinds of information TiVo collects and how that information is used. Other than minor revisions, the privacy policy did not change. In September 2000, TiVo made further expansions and clarifications to the privacy policy in its user manual and on its Web site in anticipation of its expansion into Europe and to inform

subscribers that the policy protected Subscriber Information provided to third parties, affiliates, or as the result of an acquisition of the company. This September 2000 update to the privacy policy did not change TiVo's privacy practices but was intended to give subscribers a fuller understanding of what information TiVo collects and how it is used.

TiVo sent an e-mail as well as a PTCM message to alert subscribers to the September 2000 revisions to the privacy policy and the availability of the updated policy on the Web site, in September 2000. For subscribers without Web access, TiVo provided a toll-free number for subscribers to request a paper copy of the policy. This version of the policy remains on TiVo's Web site and is included in current manuals. TiVo plans to send a message to subscribers after the release of the FTC's response and periodically thereafter to ensure that new subscribers are aware of the updated privacy policy (in the event that they receive an outdated manual).

VI. Conclusion

TiVo is proud of taking the lead on privacy in the nascent personal video recording industry. Consumer trust is essential to the growth of TiVo's revolutionary product. TiVo therefore welcomes an informed discussion of its privacy practices and policies.

APPENDIX A:

TiVo Personal Video Recorder Privacy Policy

APPENDIX B:

Diagram of the Transmission of
Diagnostic Information and Anonymous Viewing Information