Before the
Department of Commerce
Washington, DC 20230

In the Matter of	)	
	)	Docket No. 101214614–0614–01
Information Privacy and Innovation in the Internet Economy	)	RIN 0660–XA22
	)	
	)	
	)	
	)	
	)	

To: Department of Commerce

National Telecommunications and Information Administration

International Trade Administration

National Institute of Standards and Technology

COMMENTS OF KINDSIGHT

Mike Gassewitz
President & Chief Executive Officer
KINDSIGHT
555 Leggett Drive
Ottawa, Ontario, Canada
K2K 2X3
(631) 745-0287

January 28, 2011

TABLE OF CONTENTS

Before the
Department of Commerce
Washington, DC 20230

In the Matter of	)	
	)	Docket No. 101214614–0614–01
Information Privacy and Innovation in the Internet Economy	)	RIN 0660–XA22
	)	
	)	
	)	
	)	
	)	

To: Department of Commerce

National Telecommunications and Information Administration

International Trade Administration

National Institute of Standards and Technology

COMMENTS OF KINDSIGHT

I. INTRODUCTION

Kindsight values this opportunity to provide its views in response to the Department of Commerce (Commerce) green paper, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* (Green Paper). The Green Paper has identified many important points for businesses and policymakers to consider when evaluating practices and possible standards for commercial activity relating to consumer privacy. Kindsight offers the following comments based on its experience in developing a service that allows consumers to better protect themselves against online threats based on a business model that allows consumers to choose whether to pay a fee for that service or receive it at no cost through the collection and use of their online browsing information for advertising purposes. In particular, Kindsight supports the following:

- Kindsight believes that current laws, such as the Federal Trade Commission (FTC) Act, combined with self-regulation provide consumers sufficient privacy protections. Kindsight also believes that a voluntary privacy program that provides consumers more transparency could be developed through a self-regulatory process as described in the Green Paper as long as it preempts state privacy laws and prohibits private rights of action. Without such protections, the privacy policies and notices that firms provide online will have to focus less on educating consumers about the firm's activity and more

on protecting the firm from potential liability arising from a patchwork of state laws and from private actions. Self-regulatory programs can be effective but simply adding another program on top of existing requirements will add to, rather than reduce, complexity for consumers. Thus, Kindsight supports the creation of a voluntary federal Internet data privacy program that requires transparency about data collection, use, and disclosure as long as such a program includes preemption of state laws and prohibits private rights of action.

- Any federal privacy program should focus on the type and amount of consumer information collected and how it is used, not the technology used to collect such information.
- Transparency is the most important principle for consumer privacy. A system with a multitude of differing or inconsistent privacy laws can work against transparency, however, by requiring entities to create privacy policies to satisfy all these laws. A statutory safe harbor combined with a new federal transparency requirement that preempts state privacy laws and promotes plain language explanations of what information is collected and how it is used and disclosed may reduce or even eliminate the need for additional regulatory activities. Furthermore, although plain language explanations are crucial, a one-time explanation to a consumer is not always sufficient. A voluntary federal transparency safe harbor should incorporate the concept of continuing disclosure and consent so that users know and remember what is happening on an ongoing basis.
- Transparency should also be the touchstone for simplified choice, rather than any particular technology or format.
- Kindsight supports higher protections for sensitive information, particularly precise location information, which should be defined to cover the vicinity of an individual.

After a brief description of its service and business model, Kindsight will discuss these points in greater detail.

II. KINDSIGHT

Kindsight, headquartered in Mountain View, California, partners with Internet service providers (ISPs) to provide consumers with an additional layer of protection against online threats that might lead to identity theft or other harms.[1]

One can think of the Kindsight service as an online burglar alarm. Homeowners typically protect their residences with strong locks, bars on windows, and other physical security tools. For an added level of security, homeowners frequently use an alarm service. Kindsight enables ISPs, by adding security equipment to their network, to make available to their subscribers the online equivalent of a burglar alarm. If the Kindsight service detects the presence of an online threat (i.e. a break-in) that was missed by an ISP subscriber's security software (i.e. a burglar picked the lock on the door), it will send subscribers an alert (i.e. sound the alarm) to prompt them to

[1] Kindsight was started as a concept within Alcatel-Lucent and transitioned into an independent corporation in 2007.

secure their computer and protect their personal information. In the event of an alert, a subscriber is given step-by-step instructions on how to fix the problem on his computer.

The value Kindsight provides to consumers is twofold. First, it recognizes that today's computer security has limitations and provides an additional layer of protection that cannot be disabled, does not require the consumer to install anything, and is always on and up-to-date. Kindsight partners with some of the security industry's most respected brands and is also an active member of several security industry organizations, including Messaging Anti-Abuse Working Group (MAAWG), Anti-Phishing Working Group (APWG), Online Trust Alliance (OTA), and others. Second, it recognizes consumers' resistance to spending on Internet security and ISPs' resulting hesitance to invest in network resources to that end. While the Kindsight service is available for a subscription fee, like many Internet applications, consumers have the option to use the service at no cost in exchange for the consumers' consent to be served relevant advertising.

Kindsight has developed this alternative economic model where the Kindsight security service can be offered by ISPs to their subscribers free of charge in exchange for the opportunity for ISPs to serve them advertisements relevant to their online behavior using a traditional ad network model. Consumers receive a needed and effective Internet security service at no monetary charge, and ISPs are able to offer that service to them by offsetting the costs through advertising revenue. And, as noted above, the Kindsight security service is also offered for a monthly fee for subscribers who do not wish to receive such advertising. Most importantly, a consumer is never assumed to have opted-in to the Kindsight service. Consumers must first express their interest in the service and then make a choice to either pay for the service or to receive the service at no cost through relevant advertising.

The Kindsight service uses advanced threat detection technologies, including what may be considered deep packet inspection (DPI)–the analysis of layer 7 information–to analyze consumer Internet traffic for attacks and other malicious activity that could place the subscriber's personal information or computer at risk. This is the case for all subscribers to the Kindsight service, whether they choose the fee-based or the advertising-supported subscription option.

For subscribers that opt-in to the advertising-supported option, the subscriber's ISP, while analyzing the subscriber's Internet traffic for threats, will continually score the online activity related to a household Internet protocol (IP) address. Scoring is the process of analyzing, but not storing, web sites visited and searches conducted to assign a numeric value to various interest categories.

The Kindsight service does not read or analyze the content of emails or instant messages for advertising purposes. The Kindsight service also does not analyze for advertising purposes any traffic related to sites that Kindsight classifies as sensitive, including sites related to pornography, sexuality, health, politics, hate, violence, drugs, and criminal behavior. We also do not target any specific age demographic and sites categorized as being for kids are not scored or used for targeting.

When a subscriber visits websites or performs other online activities, the Kindsight service is designed to not interrupt, affect, or inject anything in the communication between the

consumer's computer and any Internet content. This means that no traffic management (throttling or blocking) is done.

Kindsight understands the increasing privacy sensitivities regarding behavioral advertising. Our approach, which offers ISP subscribers a reliable, effective, and needed home network security service funded through relevant advertising, recognizes that transparency and consumer privacy are paramount to the fair exchange for consumers.

As a consequence, Kindsight contractually obligates its ISP customers to use clear, transparent notice and to obtain affirmative express consent (see attached Kindsight recommended notice and opt-in consent screen capture and privacy policy). This level of notice and consent comports with the FTC's existing self-regulatory principles for online behavioral advertising by third parties by providing a prominent, plain language, free-standing opt-in disclosure that is not buried in a privacy policy.[2] Kindsight also requires ISPs to include in monthly bills and in monthly emails to subscribers a reminder of the service and to provide links to additional information, including how to change subscription types and opt out of the service.

Kindsight contemplated the consumer impact of its use of DPI technology to provide a network-based security service, as well as to also provide a no-cost advertising supported option to consumers. Ultimately, Kindsight concluded that the use of DPI itself was not the crucial issue for consumer privacy. Instead, the challenge for Kindsight with respect to privacy protections is the same as the challenge associated with behavioral advertising generally: ensuring that consumers have sufficient information about an entities' data handling practices and the ability to exercise informed choice before sharing their data. Thus, as we explored our business model and corporate strategies, we have been very mindful of the continuing string of privacy "incidents" and the response of consumers, the media, and policymakers to each.[3]

Kindsight has carefully developed a valuable service, which can be offered to consumers at no cost through relevant advertising, offered with transparent notice and consent, as well as options for consumers who do not wish to share such data. Kindsight also conducted consumer testing

---

[2] *See* FTC Staff, Proposed Self-regulatory Principles for Online Behavioral Advertising, (Feb. 2009), available at *http*://www.ftc.gov/os/2009/02/P085400behavadreport.pdf. Although Kindsight's service shares some of the attributes of first-party advertising in that consumer data is not actually shared with ad networks and consumers know they can complain to their ISP if they have concerns, Kindsight still requires clear disclosure and opt-in consent to ensure that consumer expectations regarding an ISP's collection and use of their online browsing information for marketing purposes are met.

[3] *See, e.g.*, Miguel Helft, *Critics Say Google Invades Privacy with New Service*, N.Y. Times, (Feb. 12, 2010), http://www.nytimes.com/2010/02/13/technology/internet/13google.html; Saul Hansell, *Nebuad Observes "Useful, but Innocuous" Web Browsing*, N.Y. Times, (Apr. 7, 2008), http://bits.blogs.nytimes.com/2008/04/07/nebuad-observes-useful-but-innocuous-web-browsing/; Brad Stone, *Facebook Executive Discusses Beacon Brouhaha*, N.Y. Times, (Nov. 29, 2007), http://bits.blogs.nytimes.com/2007/11/29/facebook-responds-to-beacon-brouhaha.

of its privacy messaging and consent features to ensure that consumers understood the exchange and can provide informed consent.

III. A VOLUNTARY FEDERAL INTERNET DATA PRIVACY PROGRAM WITH STATE LAW PREEMPTION AND A SAFE HARBOR AGAINST PRIVATE RIGHTS OF ACTION WILL BENEFIT CONSUMERS; ANY PROGRAM SHOULD BE TECHNOLOGY NEUTRAL.

The Green Paper calls for the adoption of a baseline commercial data privacy framework based on an expanded set of fair information practice principles focused on transparency, purpose specification, use limitation, and auditing. It further asks whether such a framework could be enhanced by using voluntary, enforceable industry codes of conduct that would be approved by the FTC.

Kindsight believes that existing laws, such as the FTC Act, combined with self-regulation provide consumers sufficient privacy protections. As privacy becomes an increasingly important issue and individual states enact new laws to protect online privacy interests, however, affected service and application providers will continue to be subjected to a patchwork of inconsistent state obligations. As a consequence, the privacy policies and notices that firms provide online focus less on educating consumers about the firm's activity and more on protecting the firm from potential liability arising from a patchwork of state laws and from private actions. This could fatally undermine Commerce's efforts to promote transparency in the area of consumer privacy.

The Green Paper recommends the development of voluntary codes of conduct enforceable by the FTC that may be accompanied by legislation to create a safe harbor for companies that adhere to such codes. Kindsight agrees that voluntary self-regulation, accompanied by a statutory safe harbor from state privacy laws and private rights of action, could benefit consumers by providing greater transparency. As the Green Paper notes, self-regulation has played an important role in Internet privacy protection in the past, such as the hybrid, public-private system to regulate online privacy practices that developed in the 1990s. Existing law supplemented by self-regulation has allowed innovation to flourish while building consumers' confidence in online commerce.

A new self-regulatory program focused on improved transparency could benefit consumers but not if it simply added a self-regulatory program on top of existing requirements. Otherwise it would add to, rather than reduce, complexity for consumers. This is because companies will still have to include language to comply with a multitude of privacy requirements rather than simply focusing on providing consumers transparency about their data handling practices.

Furthermore, any federal Internet data privacy program should focus on the type and amount of consumer information collected and how it is used, not on the technology used to collect such information. Online applications and service providers can use many different technologies to collect consumer information, from cookies tracking web sites visited across an extensive network of Internet properties, to collecting and using searches conducted, to analysis of online activities using DPI. Disparate treatment of entities engaged in behavior with similar privacy impacts based solely on the technology they employ would undercut the privacy protection and clarity for consumers that any privacy regime should otherwise seek to promote. Further,

technology-specific regulation fails to recognize that technology changes rapidly, and it may become quickly out of date or even hurt privacy-enhancing innovation.

Kindsight therefore supports a statutory safe harbor for companies that adhere to a voluntary federal Internet data privacy program that requires transparency about data collection, use, and disclosure. Such a program should preempt the patchwork of state privacy laws, provide a safe harbor from private rights of action, and be technology neutral. Such a program would prompt business to provide clearer and less complex privacy notices, facilitate informed choice by consumers, and improve the administerability of privacy protections overall.[4]

How such a program should use transparency as a touchstone is discussed further below.

IV. TRANSPARENCY OF COMMERCIAL DATA PRACTICES IS THE KEY PRINCIPLE FOR PRIVACY REGULATION.

The behavioral advertising market is not new. Online search firms, advertising networks, and publishers have been engaged in some form of behavioral advertising for years. It is also the case that much of the online collection, use, and disclosure of information is not particularly transparent and many online firms do not provide a transparent and meaningful privacy notice. As a result, public understanding and acceptance of behavioral advertising is generally tenuous.

The primary goal of Kindsight is to offer consumers products and services that provide significant value and to create an alternative business model funded through advertising that makes these products widely available. Like other providers of online content, applications, and services, Kindsight believes that an advertising-supported model can create sufficient value to provide consumers a useful security product in exchange for analyzing their online activities to serve them relevant advertisements. Informed consumers can determine for themselves the types of economic relationships they may enter into to obtain content, applications, and services of interest to them.

What follows are specific recommendations for developing meaningful transparency practices in the context of a voluntary federal Internet data privacy program, backed up by preemption of state law and protection from private rights of action.

1. TRANSPARENT NOTICE: CLEAR, PLAIN LANGUAGE EXPLANATIONS OF WHAT INFORMATION IS COLLECTED, USED, AND DISCLOSED ARE NEEDED; NOTICE SHOULD BE ONGOING IN CERTAIN CONTEXTS

For consumers to make informed decisions about whether to allow the collection and use of their data in exchange for receiving content, applications, or services they must have meaningful and transparent information about what data the provider will collect and how it will use or share that information. In particular, a notice requirement should obligate firms collecting, using, and

[4] A voluntary federal data privacy program should apply to consumer information not already covered by sector-specific laws, such as the Health Insurance Portability and Accountability Act (HIPAA).

disclosing consumer data to explain, clearly and precisely, the information collected, how it is used, whether it is disclosed, and to whom. Any online firm should know exactly what information it collects, how it uses such information, and with whom it shares such information. Thus, there is no adequate reason for an online firm to be unable to comply with such a simple and useful requirement.

Transparency should also incorporate the concept of continuing disclosure and consent in certain contexts so that users know and remember what is happening on an ongoing basis. Checking off a box at the beginning of a relationship may provide insufficient transparency if ongoing information collection is not apparent to consumers. Kindsight therefore requires ISPs to include in monthly bills and in monthly emails to subscribers a reminder of the service and to provide links to additional information, including how to change subscription types and opt out of the service.

2. A FEDERAL TRANSPARENCY REQUIREMENT THAT PREEMPTS STATE LAWS ELIMINATES THE NEED FOR MICROMANAGEMENT OF NOTICE FORMATS AND TERMINOLOGY

The Green Paper asks about the feasibility of standardizing the format and terminology for describing data practices through mechanisms such as privacy impact assessments. Instead of micromanaging formats or terminology in notices, policymakers should focus on transparency, which will give companies flexibility to best inform consumers. A standardized approach is not feasible without a federal law that preempts state laws, however, because adding another layer of federal requirements on top of state-level requirements will just create more complexity that will undermine transparency and meaningful notice. Imposing a transparency requirement that mandates a clear description of a firm's actual behavior, relieving firms of the burden of trying to comply with possibly fifty different state-level interpretations of privacy requirements, and protecting them from threats of private litigation will free firms to focus on explaining their own practices clearly and tailoring their notices to fit the context appropriately.

3. CONSUMERS SHOULD HAVE ACCESS TO EXISTING PROFILES BUT THERE SHOULD NOT BE A REQUIREMENT TO CREATE PERSONAL PROFILES

Kindsight supports a requirement that affords consumers access to a profile maintained by firms that collect, use, and disclose their behavioral information. Allowing consumers to view their profiles could help consumers engage more actively in their own privacy protection. Kindsight advocates that such access be simple to use and displayed in a manner that is easily understood by the consumer.

Recent innovations have allowed Kindsight to create a profile mechanism that offers consumers an increased level of privacy protection. The Kindsight technology does not involve a permanent association of a particular profile with an individual, a web browser, or a computer, as is typically found in today's behavioral advertising solutions. Instead, a profile is temporarily associated with an individual's browsing patterns at the specific point in time that the person is accessing the Internet through his home network. Every time an individual goes online, however, he may be associated with a different profile corresponding to his activity during that online

session. Kindsight plans to enable individuals to view the profile that is associated with their activity at the time they are using the Internet.

It is important that a federal privacy framework not inhibit the development of new technologies or more privacy-sensitive business practices, however. In particular, access requirements should not encourage linking profiles to individuals when such practices are not otherwise contemplated or necessary for a given business model. A hard and fast access requirement may inadvertently require firms to build profile databases that would not otherwise be necessary. Consumer access to existing profiles, and the rules governing them, must take care not to inadvertently mandate less privacy-sensitive technologies and business practices.

4. CONSUMERS SHOULD RECEIVE NOTICE OF MATERIAL CHANGES TO DATA-HANDLING PRACTICES

Kindsight favors a policy whereby any material change regarding how data will be used or disclosed after it has been collected should require clear notice to consumers before their data is used or shared in a way they did not expect. The FTC has typically defined express claims as material.[5] Kindsight believes that express claims limiting the use or sharing of consumer data (i.e., we will not share your data with third parties) should be considered material and any changes to a firm's practices with respect to these activities should require notification to consumers and the opportunity for consumers to object to the change, such as by stopping usage of an application or service or by prohibiting the new usage of the information. Changes in data use or disclosure practices that are not likely to affect a reasonable consumer's choice or conduct regarding a product or service should not be considered material. This may include changes regarding how data will be stored if the security of the data is not affected or changes that increase privacy protections. As we have learned with privacy policies, it is important not to overwhelm consumers with details that would not be of concern to most reasonable consumers lest consumers begin to disregard all such notices.

V. SIMPLIFIED CHOICE

As is the case with transparency in general, policymakers should likewise focus on improving consumer understanding of data handling practices, not on a particular technology, format, or wording, for simplifying consumer choice in this area. Rather than focusing on the relative effectiveness of opt-in versus opt-out consent, the touchstone should be ensuring that consumers are able to understand what information they will provide and how it will be used before they decide to accept the service or access the content or application. Such disclosures should be concise and in plain language to avoid becoming an impediment, rather than an aid, to consumer understanding.

---

[5] See FTC Policy Statement on Deception, *appended to* Cliffdale Assocs., 103 F.T.C. 110, 174 (1984) ("A 'material' misrepresentation or practice is one which is likely to affect a consumer's choice of or conduct regarding a product. In other words, it is information that is important to consumers. . . . [T]he Commission presumes that express claims are material.") (citations omitted).

Accordingly, firms should be free to determine the exact mechanism they use to obtain such consent, whether opt-in or opt-out, to ensure it is effective for a particular context. Over time, technology and software advances may render a pre-determined mechanism less effective or appropriate. Accordingly, Kindsight supports allowing companies to use different methods of notice and consent for different contexts, as long as the notice is sufficiently clear so that the consumer can make an informed decision.

What follows are some specific recommendations regarding a simplified choice model.

1. CHOICE SHOULD BE OFFERED WHERE AND WHEN CONSUMERS ARE MAKING A DECISION ABOUT THEIR INFORMATION

Kindsight believes that choice should be offered clearly and prominently when consumers are making a decision about whether to share their information and, as discussed above, choice should be offered on a continuing basis for ongoing information collection. Thus, as described more fully above, Kindsight obligates its ISP customers to use clear, transparent notice and obtain affirmative express consent when the customer chooses to subscribe to the advertising-supported Kindsight security service. This notice is a prominent, plain language, free-standing opt-in disclosure that is not buried in a privacy policy. Customers receive monthly reminders about their service and are free to switch at will from the advertising-supported security service (which uses online browsing information for targeted advertising) to the fee-based model (which does not use information for advertising), and also may decline the security service completely.

2. ADDITIONAL PROTECTIONS ARE APPROPRIATE FOR THE USE OF SENSITIVE DATA FOR ADVERTSING, INCLUDING DATA ON THE VICINITY OF AN INDIVIDUAL

Kindsight believes that additional protections are appropriate for the collection, use, and sharing of sensitive data for advertising purposes. The proposed BEST PRACTICES Act from the 111th Congress offered a generally appropriate definition of sensitive information: "Information associated with covered information that relates to that person's medical records or treatment, race or ethnicity, religious beliefs, sexual orientation, financial records and account information except that provided by the individual for an authorized transaction, precise geolocation information, unique biometric data, or social security number."[6] This definition should be modified, however, to include a clearer definition of geolocation information. Kindsight believes that location information is highly personal and that the proposed definition lacks sufficient clarity to ensure consumer privacy. Kindsight advocates defining the term "precise geolocation information" to include the vicinity of an individual. The definition should not be solely associated with cellular or wireless technology but should also be defined to include information that is related to GPS location data, "zip+4", cellular location information, and/or Wi-Fi-related triangulation.

As for whether express affirmative consent is necessary for the collection and use of sensitive information for advertising, Kindsight generally agrees this additional protection is appropriate

[6] BEST PRACTICES Act, H.R. 5777, introduced July 19, 2010.

for sensitive information. Although Kindsight obtains express affirmative consent to collect online browsing information from consumers, it does not collect financial account numbers or information about visits to sensitive sites, such as those involving pornography, sexuality, health, politics, hate, violence, drugs, and criminal behavior. We also do not target any specific age demographic and sites categorized as being for kids are not used for targeting.

VI. CONCLUSION

Kindsight appreciates the opportunity to comment on Commerce's proposed privacy framework. For the foregoing reasons, Commerce should pursue a statutory safe harbor for companies that adhere to a voluntary federal Internet data privacy program that requires transparency about data collection, use, and disclosure. Such a program should include preemption of state laws, prohibit a private right of action, and be technology-neutral.

Respectfully submitted,

KINDSIGHT

By: /s/ Mike Gassewitz
Mike Gassewitz
President & Chief Executive Officer
KINDSIGHT
555 Leggett Drive
Ottawa, Ontario, Canada
K2K 2X3
(631) 745-0287

January 28, 2011

Kindsight Statement of Privacy Principles

Last modified: Oct 27, 2010

At Kindsight, we respect and recognize the importance of privacy. That is why we continually strive to operate our business alongside our Internet Service Provider (ISP) partners with the goal of providing unparalleled transparency and consumer choice.

This Statement of Privacy Principles describes our technology and the assurances we seek to obtain from our ISP partners that they will deploy the Kindsight service in a manner that respects subscriber privacy. We believe our technology sets a new standard in the online domain and that these Principles meet or surpass the guidance set forth by agencies and other bodies that regulate or address privacy and online advertising issues, such as the Federal Trade Commission (FTC), the Interactive Advertising Bureau (IAB), and the Network Advertising Initiative (NAI).

This Statement of Privacy Principles applies to the products and services licensed by Kindsight to our ISP partners. These services may be branded as “Kindsight” or as an ISP-branded service, and we refer to them collectively herein as the “Kindsight service." We seek assurances from our ISP partners that they will possess all authorizations necessary to deploy the Kindsight service pursuant to this Statement of Privacy Principles. We also expect our ISP partners to keep their subscribers informed of the steps they take to protect their privacy; so, to the extent an ISP uses the Kindsight service, we expect its usage to be disclosed, in a manner consistent with these principles, in the ISP’s privacy policy.

Questions about an ISP’s privacy policy should be directed to the ISP. If you have questions about this Statement of Privacy Principles, please feel free to email us at privacy@kindsight.net or write to us at:

Privacy Department
c/o Kindsight, Inc.
755 Ravendale Drive
Mountain View, CA 94043
USA

Consumer Choice

The Kindsight service is opt-in.

Kindsight believes in setting the highest standard for transparency and consumer choice. As a result, we expect our ISP partners to obtain the subscriber’s consent before activating the Kindsight service for the subscriber’s household. This means we assume the subscriber’s household to be “opted out” of the Kindsight service unless and until the subscriber opts-in to the Kindsight service.

As with other changes the subscriber makes to his/her broadband service, only the account owner or someone acting on his/her behalf may opt-in to the service for the household. To communicate this opt-in has occurred, the subscriber will receive: a service activation notice via email; a notice with the subscriber’s monthly Internet service invoice (either by mail and/or online); as well as a monthly email that shows their security status, and, if they selected the no-cost option, a reminder of this consent and links to how to disable the service or change their subscription type.

This reinforcement is consistent with our goal of securing clear and informed consent from the subscriber.

The Kindsight service has multiple subscription types.

The Kindsight service will be offered by our ISP partners for a fee or, like many other Internet applications, at no cost through relevant advertising. Subscribers will select one of these subscription types when they sign-up for the service.

The subscriber can switch between these subscription types at any time by going to the Kindsight service portal for his/her ISP and following the instructions posted there.

The subscriber can discontinue the Kindsight service at any time.

The subscriber can discontinue (i.e., opt-out of) the service at any time by going to the Kindsight service portal for his/her ISP and following the instructions posted there. Instructions for opting-out also will be included as part of the service activation notice.

Information Collection and Use

The subscriber's Internet traffic is analyzed for threats.

The Kindsight service uses advanced threat detection technologies to analyze consumer Internet traffic for attacks and other malicious activities that could place the subscriber's personal information or computer at risk. When the Kindsight service detects a threat, an alert is communicated to the subscriber via the ISP's security portal and/or email and/or text message.

This service can be offered at no cost through advertising.

Our ISP partners may provide their subscribers with a free trial of the Kindsight service, after which subscribers will be provided with an option of continuing the Kindsight service for a fee or, like many Internet application, at no cost through relevant advertising. If the subscriber selects the no-cost option, then in addition to analyzing the subscriber's Internet traffic for online threats, our technology will also analyze the subscriber's Internet traffic to display relevant ads on the ISP's and selected partner web sites. The subscriber will NOT see more ads or pop-ups as a result of this service.

While analyzing a subscriber's Internet traffic for threats at no cost, our ISP partners will continually score the online activity related to your household Internet protocol (IP) address. Scoring is the process of analyzing, but not storing, web sites visited and searches conducted to assign a numeric value to various interest categories. Using your household IP address, relevant ads may be shown on the pages you visit if the scoring suggests an interest in a pre-existing category. These scores are not shared with advertisers or publishers. It will not store web sites or searches against a person, computer or household.

Our technology uses an innovative, privacy-centric approach to infer interests. Instead of using cookies to track an individual, our technology creates "characters". A "character" is a summary of scores in various interest categories based upon online activities. An individual's online activity will most likely generate several characters and individuals with similar browsing patterns will typically be inferred to the same character within the household. When our technology estimates a match between browsing patterns and a previously created character, then the online activity is scored and these scores are added to that "character". If no match is found, then a new "character" is created. When a "character" visits the ISP's or partner web sites, then the ads the character sees at these sites may be more relevant. In the future, browsing patterns may match a totally different character or cause a new character to be created. At no point is the subscriber's online activity stored against a character nor can any character be attributed to any actual person, computer, or browser. At no point are these characters given to or shared with partner web sites, publishers or advertisers.

Let's look at an example: if our technology recognizes a browsing pattern and that online activity includes a number of searches for hotels in a certain city or visits to a few travel sites looking for an inexpensive flight to that destination, our technology will create a character and assign this character a high score for the travel category. The Kindsight service will NOT store which web sites the individual in the subscriber's household visited, which searches they conducted or any other online activities against any individuals, any characters, or the subscriber's household. The next time our technology infers this character from the browsing patterns of the subscriber's household and the character visits a partner web site, our technology may show an ad about travel instead of a potentially irrelevant ad.

Subscribers who have opted-in to the no-cost option may view their inferred interest categories at a certain point in time by visiting the Interests page on the Kindsight service portal for their ISP from a computer in their home network.

As previously noted, the Kindsight service analyzes Internet traffic for advertising purposes only for subscribers that have expressly opted-in to the no-cost identity theft protection service option. If the subscriber selects the paid subscription option, then the subscriber's ISP will analyze the Internet traffic only for attacks and other malicious activities that could place the subscriber's personal information or computer at risk (*i.e.,* the subscriber's Internet traffic will not be analyzed or used for purposes of relevant advertising).

No Personally Identifiable Information (PII) collected.

Unlike other popular Internet-based applications, the Kindsight service does NOT collect or process personally identifiable information such as names and addresses. As explained below, information recognized by our service as personal or sensitive in nature is immediately removed and never stored.

No inspection of email or instant messages for advertising purposes.

Other than looking for attacks and malicious activities, our service does NOT read or analyze the content of emails or instant messages for advertising purposes.

No encrypted Internet traffic is analyzed.

Internet traffic that is encrypted (*e.g.*, https) is not analyzed for any purpose.

All sensitive sites are immediately filtered.

The Kindsight service does NOT analyze, for advertising purposes, any traffic related to sites that Kindsight classifies as sensitive, including sites related to pornography, sexuality, health, politics, hate, violence, drugs, and criminal behavior. Such traffic is, however, analyzed in connection with the detection of attacks and other malicious activities, provided the subscriber has opted-in to that aspect of the service.

No altering of Internet traffic and no performance impact.

When you visit websites or perform other online activities, the Kindsight service is designed to not interrupt, affect, or inject anything in the communication between the consumer's computer and any Internet content. The Kindsight service does not slow down the consumer's computer or his/her Internet connection.

No additional ads or pop-ups

With the no cost option of the Kindsight service, the subscriber will not see any additional ads or pop-ups. Kindsight and our ISP partners will acquire ad space on partner websites and display ads that may be more relevant in these acquired spaces.

Other uses

Our ISP partners may store fully anonymized and aggregated data regarding sites visited and searches conducted for opted-in subscribers for the purpose of continually improving the Kindsight service. None of this anonymized and aggregated data can be attributed to any individual or subscriber's household. Our ISP partners also may audit or analyze the effectiveness of the Kindsight service, to ensure its proper functioning and to improve Kindsight offerings.

Cookies

Kindsight service does NOT use cookies to track your interests.

A cookie is a small text file that is stored on a user's computer for record-keeping purposes. A persistent cookie remains on your hard drive for an extended period of time. Session cookies expire when you close your browser.

The Kindsight service offered through our ISP partners does NOT use 3rd party or persistent cookies to create characters and score your online activity (i.e. web sites visited and searches conducted) or to handle opt-in/opt-out of the Kindsight service.

Third-party cookies may be used on the Kindsight service website to more efficiently acquire advertising space, from publisher websites, where relevant ads may be displayed to users that have opted-in to the no-cost option.

Session cookies are used on the Kindsight service website to make it easier for you to navigate that site. This session cookie expires when you close your browser. Communications

Registering for the Kindsight service.

When a subscriber signs up for the Kindsight service, the Kindsight service asks for the subscriber's preferred email address and/or text message address in order to send service activation notices, monthly reports, and/or alerts to the subscriber when a threat is detected on one of the computers in the subscriber's home network.

The Kindsight service uses the subscriber's email address and/or text message address for the purpose of sending alerts and will, either through Kindsight or its partner ISP, communicate with the subscriber according to the preferences the subscriber sets. At no point will the Kindsight service sell or share these email addresses and/or text message addresses with other third parties.

Service-related announcements.

The Kindsight service may send the subscriber a welcome email to verify the subscriber's username and password and also may send the subscriber monthly reports and service-related announcements when it is necessary to do so.

The Kindsight service will communicate with the subscriber in response to subscriber inquiries, to provide the services requested, and to manage the subscriber's account.

Information Sharing

The subscriber's information is NOT shared with third parties.

The Kindsight service treats the subscriber's information with strong privacy in mind, and does NOT share or sell the subscriber's information to third parties such as advertisers.

As with most websites, our ISP partners may be passed an IP address, referring URL or other ad selection parameters during the ad serving process. This is a standard practice and done to assist in content and ad selection as well as to prevent "click fraud."

Technology Integrity

Technology within the Kindsight service processes information only for the purposes set forth in this Statement of Privacy Principles. We review our technology's data collection, storage and processing practices to ensure that it collects, stores and processes only the minimal amount of information necessary to provide or improve the Kindsight service. Our technology provides appropriate security measures to protect against unauthorized access to or unauthorized alteration, disclosure or destruction of data. Although no data security system is 100 percent secure, we take reasonable steps to ensure that subscriber data is protected and that our technology performs as outlined in these Privacy Principles.

Changes to this Statement of Privacy Principles.

Please note that this Statement of Privacy Principles may change from time to time, so please review it frequently. We will not reduce the subscriber's rights in this Statement of Privacy Principles without the subscriber's consent.

If we decide to change these Privacy Principles, we will post those changes to this privacy web page and other places we deem appropriate so that you are aware of the changes.

Contact Us

If you have any additional questions or concerns about these Privacy Principles, please feel free to contact us any time through email at privacy@kindsight.net or at:

Privacy Department
c/o Kindsight Inc.
755 Ravendale Drive
Mountain View, CA 94043
USA

Kindsight

Subscribe to the Kindsight Service at No Cost

Like many other Internet applications, we can offer the identity theft protection service at no cost through relevant advertising. **When you agree to the no-cost option, your Internet traffic is analyzed for threats and it will also be analyzed to display relevant ads** on our own and selected partner web sites. You will not see more ads or pop-ups because of this service.

To offer this service at no-cost, **our technology will continually score the online activity** related to your household Internet protocol (IP) address. Scoring is the process of analyzing, but not storing, web sites visited and searches conducted to assign a numeric value to various interest categories. Using your household IP address, relevant ads may be shown on the pages you visit if the scoring suggests an interest in a pre-existing category. **These scores are not shared with advertisers or publishers.**

Your privacy is important to us. Our technology **will not store or use personal information** such as your name, address, or financial data. It will not store web sites or searches against a person, computer or household. Our technology does not install software on any computers nor does it read e-mail or instant messages.

You may cancel this service at any time. For more details, CLICK HERE.

I agree to the terms of the no-cost option.

Protect Me at No Cost | $3.95 per month | No Thanks