

Intellione® Technologies Corporation
Privacy Protection Statement
Version 2.7 - October 2009



Intellione embraces a technical, legal and operational approach to protecting consumer privacy in the measurement of roadway speeds from mobile network signaling information and provisioning of its location services.

Privacy Defined

Privacy protection, as described in this comprehensive statement, has been engineered into Intellione's solutions. Individuals may interact with one or more Intellione systems as follows:

- As an anonymous contributor of device location information for the purpose of measuring road traffic ("**Traffic**") conditions;
- As a user of the Company's Intellione, ioVector or other Web sites ("**Online**"); and,
- As a user of an Intellione mobile device application ("**Mobile**").

Privacy protection varies for each interaction type. In a general information technology context, however, there are three aspects to privacy:

1. Personal
2. Territorial
3. Informational

Personal privacy is about *content filtering* and other mechanisms to ensure end users are not exposed to whatever violates their moral senses.

Territorial privacy is about *protecting users' property* – e.g. the user equipment – from being invaded by undesired content such as SMS or email/SPAM messages.

Informational privacy is about *data protection*, and the users' rights to determine how, when and to what extent information about them is communicated to other parties, and the execution of this right may be based upon their knowledge about what the other party's intention is.

In general terms, consumer information, or Identifiable Information that must be protected includes:

> Information associated with a user

- Name
- Address
- Telephone number
- Social Security Number
- Credit card number
- Network data that could uniquely locate a user
- Any other personally identifiable information
-

> Information about use

- Biographical data
- Calling habits
- Preferences
- Disposition to be contacted

> Information when combined with other information that could infer the user's identity

- IP address
- User Agent profile

Traffic Systems

For the purpose of calculating roadway speeds from mobile network signaling data, only **Informational** privacy need be addressed because there is no interaction with the subscriber.

- Technical approach – network signaling information is created by mobile stations (“MS” or “handsets”) communicating with base stations to ensure prompt and reliable phone service via mobile networks. Intellione’s mobile positioning system (“MPS”) converts ordinary network signal information into handset locations which in turn, is used to calculate speed and flow of vehicles moving along all roadways with mobile phone coverage. The Intellione MPS may be deployed in two ways: 1) Integrated within a wireless carrier’s network switching center (“in-network”); and, 2) Centrally located in a secure data center (“off-network”).

In-network MPS servers connect to the carriers’ networks via probes configured to: a) monitor the streaming signaling data; b) scramble each report containing personally identifiable information; and, c) pass the identity-stripped records to the Intellione MPS. The MPS provides further protection by assigning randomly generated codes to the scrambled reports and deleting the originals prior to forwarding for processing by Intellione’s Traffic Determination Engine (“TDE”).

Off-network MPS servers receive signaling data directly from the mobile phones of subscribers authorizing and granting permission to Intellione to locate and monitor the phone movement in exchange for a predetermined value. The off-network MPS assigns randomly generated codes to the signaling data and deletes the original, identifiable information before forwarding for TDE processing.

- Legal approach – In November 2001, Intellione retained Perkins Coie LLP to file comments before the Federal Communications Commission regarding the use of Customer Proprietary Network Information (CPNI) and Other Customer Information (CC Docket No. 96-115). The conclusion: “The creation and use of aggregate information from CPNI has enormous potential. Similarly, there may be incentives for wireless carriers to seek customer consent to permit disclosure of CPNI to facilitate certain public safety applications. The Commission should ensure that important public safety goals are met consistent with protection of privacy and free speech.” A copy of the Comment may be found by entering “Intellione” in the “Filed on Behalf of” search field on the FCC Web site: http://gullfoss2.fcc.gov/prod/ecfs/comsrch_v2.cgi.
- Operational approach – There is no commercial or other value in storing or maintaining mass quantities of unidentifiable mobile phone locations. Once Intellione MPS servers pass the volumes of bulk, anonymous location data to TDE servers, the records are permanently erased. Further, upon completion of speed calculations by the TDE for each monitored phone – generally within a 10-20 minute timeframe, the location records are also permanently erased.

Online Systems

Intellione’s opt-in services use subscribers’ locations to deliver turn-by-turn driving directions, provide information about their surrounding environment, and reach their destinations more quickly around traffic. Subscribers mainly interact with Intellione services through their handheld device and web sites. This privacy policy applies to the following Intellione U.S. web sites: www.intellione.com and www.iovector.com for both individual consumers and certain business and government organizations that use these Web sites.

All three privacy needs – **Personal, Territorial & Informational** – for On-line systems are addressed.

Online **Personal** privacy is protected via:

- Technical approach - Privacy protection begins during the enrollment process as each subscriber sets a password during registration. The Intellione technical staff uses commercially reasonable efforts to maintain safe and secure systems, including physical, administrative, and technical security procedures to safeguard Personal Information.
- Legal approach – Intellione will use legal means available to aggressively pursue individuals, companies or other entities breaching personal privacy regarding Online content as it pertains to its Web sites and Web service applications.
- Operational approach – Intellione takes commercially reasonable steps to give visitors to our Web sites clear notice of: when information is requested; the types of information requested; the general purposes for which that information will be used. Users' unique information will not be disclosed to third parties.

Online Privacy Policy

NOTICE

The Information We Collect From and About You

This Online Privacy Policy applies to all information we receive online from you and about you in connection with an online transaction or request. The information, if any, which we collect from or about you while you, are accessing and using our Web sites covered by this privacy policy depends on what you do while you are on our Web sites.

If you **register** or fill out any forms at an Intellione web site, including iovecor.com, iovector.mobi or request to download ioVector, then we do collect *information* from you or about you online. However, in these situations we only collect certain information from you and about you to process your request.

How We Use the Information We Collect

Once you download ioVector, we use the information when you request io-vector to provide you with 1) services; 2) support; and 3) information about io-vector and 4) to provide advertisements relevant to your profile and location.

CHOICE

If you choose to stop using io-vector and the services provided within, delete it from your device according to your device manufacturer instructions. You may also email us at customersupport@iovector.com provide us with your cell phone number and we will delete your phone's MIN from our files. Following this, you will need to reenroll in io-vector to use the service.

SECURITY AND CONFIDENTIALITY

Intellione recognizes the importance of secure online transactions, and we maintain physical, administrative, and technical safeguards to protect your information. We safeguard the privacy of information you provide us through online forms. For online requests and io-vector product downloads, we use programs that encrypt the information you provide on the form before transmission to Intellione. Information you provide to us online is transmitted to us through a secured socket layer (SSL) transmission. The information is decrypted only upon receipt by Intellione.

We restrict access to *information* that is collected about you to only those who have a need to know that information in connection with the purposes for which it is collected and used.

Additionally, we have security protocols and measures in place to protect the information we maintain about you from unauthorized access or alteration. These measures include internal and external firewalls, physical security and technological security measures, and encryption of certain data.

You also have a role in protecting the security of information about you. For example, you should guard your Login ID and password to www.iovector.com and not permit unauthorized use of your account. Additionally, you should close your browser when you have finished viewing your information on the ioVector Web site to protect the privacy of your individual or business organization information.

ACCOUNTABILITY

"Accountability" is generally recognized as an important component of "Fair Information Practices" and refers to the process that a company has in place to be sure it adheres to its privacy policy. It also means that a redress process exists to address privacy policy compliance questions.

If you have questions or comments about Intellione's Online privacy policy and fair information practices, please contact us by:

- E-mail at PrivacyMatters@intellione.com
- Mail in writing to Chief Privacy Officer, Intellione Technologies Corp., 1100 Circle 75 Parkway SE, Suite 900, Atlanta, GA 30339; or
- Phone using our toll-free Privacy Matters Hotline number: (866) 817-6685.

USE OF COOKIES TECHNOLOGY

What is a Cookie?

A cookie is a piece of text information that a Web server may transfer to the hard drive of your computer through your Web browser when you visit a Web site. Cookies are commonly used on Web sites to improve your experience and to enable systems to recognize your browser. Some cookies last only through a single visit (session cookie); others may have an expiration date; still others may remain on your computer until you delete them (persistent cookie). Only the information that you provide, or the choices you make while visiting a Web site can be stored in a cookie. For example, the Web site cannot determine your e-mail address unless you choose to type it.

How We Use Cookies

We use session and persistent cookie technology for several purposes. For example, cookies:

- Allow us to gather aggregated statistical data about the use of our Web site for research purposes;
- Help us improve your navigation of our Web site(s);
- Enable us to store your preferences for certain kinds of information and marketing offers;
- Help us to provide features such as personalized greetings;
- Allow us to store your user name and encrypted customer identification number so that we recognize you when you return to our Web site(s);
- Help us combat identity theft and fraud with more reliable identity verification and authentication data.

Our cookies only collect information during your online activity at our Web sites to which this privacy policy applies, and not during any of your other Internet activity. Cookies set by us or our agents are not interpreted or shared with any other third party. We may sometimes use outside technology companies to set cookies on our Web site and collect cookie information for us. We use the cookie information collected by these companies in the same manner as stated above in this section. Those companies may not use these cookies for their own internal purposes or share the information collected with any party other than Intellione.

How You Can Accept or Reject Cookies

You can decide if and how your computer will accept a cookie by establishing your preferences in your Web browser. Please understand that, if you choose to reject cookies, you may not be able to use certain of our online services or web site features. Internet Explorer is set up to allow the creation of cookies; however, you can specify that you be prompted before a Web site puts a cookie on your hard disk, so you can choose to allow or disallow the cookie; or you can prevent Internet Explorer from accepting any cookies. You can specify different settings for different security zones. For example, you might want to allow Web sites to create cookies if they are in your Trusted sites or Local intranet zone, prompt you before creating cookies if they are in your Internet zone and never allow cookies if they are in your Restricted sites zone.

CHILDREN'S PRIVACY

We strictly comply with the Children's Online Privacy Protection Act and do not knowingly solicit or collect information from children.

NON-APPLICABILITY OF PRIVACY POLICY TO COMMERCIAL USE

This Online privacy policy applies to individuals using the Intellione and io-vector Web sites identified at the beginning of this privacy policy to request the services and products provided through these Web sites for personal, family or household purposes and to business organizations that obtain io-vector products and for their own business organization.

KEEPING UP-TO-DATE ON OUR PRIVACY POLICY CHANGES

We want you to be fully informed about how we protect your privacy. We may change our privacy policy in the future, but we will not change our practices until they have been posted at this Web site. If changes occur, we will also show the date of revision. By using our Web sites to which this privacy policy applies you agree to changes in our privacy policy through this Web site.

HOW TO CONTACT US WITH QUESTIONS OR COMMENTS

If you have questions or comments about Intellione Online privacy policy and fair information practices, please contact us by:

- E-mail at PrivacyMatters@intellione.com
- Mail in writing to Chief Privacy Officer, Intellione Technologies Corp., 1100 Circle 75 Parkway, Suite 900, Atlanta, GA 30339; or
- Phone using our toll-free Privacy Matters Hotline number: (866) 817-6685.

Handset Systems

In addition to delivering traffic navigation and other location services to subscribers via Web sites, Intellione offers enhanced features and functionality through small applications downloaded over-the-air (OTA) to subscribers' mobile phones and devices (Handsets). Subscribers must grant Intellione permission to locate and monitor their handsets as a condition of downloading and using the handset application(s). All three privacy needs – **Personal, Territorial & Informational** – for Handset systems are addressed.

Handset **Personal** privacy is protected as follows:

- Technical approach - Intellione's Handset applications do not permit content downloads external to the io-vector servers, blocking potentially offensive images, text, video or other content from reaching subscribers.
- Legal approach – Intellione will use legal means available to aggressively pursue individuals, companies or other entities breaching personal privacy regarding mobile content as it pertains to its Handset applications.
- Operational approach – Subscribers receiving offensive content on their handsets via the io-vector are encouraged to immediately report the privacy breach to Intellione staff via its toll-free Privacy Matters™ Hotline at (866) 817-6685 or via email: PrivacyMatters@intellione.com. Intellione's Privacy Manager will respond to submissions of privacy breach within five (5) business days.

Handset **Territorial** privacy is protected as follows:

- Technical approach - Intellione's Handset applications do not transmit unsolicited content (content not specifically requested by subscribers or agreed to as a ioVector user) via SMS (text message), WAP push or traditional voice calls to subscribers, nor do they permit third-party providers to transmit unwanted or unsolicited content via io-vector. Advertisements tailored to your profile and location will be delivered through ioVector. Text messages and emails will not be generated from these advertisements without your expressed request for such information.
- Legal approach – Intellione will use legal means available to aggressively pursue individuals, companies or other entities breaching personal privacy regarding mobile content as it pertains to its Handset applications.
- Operational approach – Subscribers receiving unsolicited content on their handsets via the Traffic System are encouraged to immediately report the privacy breach to Intellione staff via its toll-free Privacy Matters™ Hotline at (866) 817-6685 or via email: PrivacyMatters@Intellione.com. Intellione's Privacy Manager will respond to submissions of privacy breach within five (5) business days.

Handset **Informational** privacy is protected as follows:

- Technical approach - Intellione's io-vector Handset application requires that the subscriber location be calculated and monitored – at the subscriber's request – in order to provide the location-based services. Both Handset and server applications automatically purge subscriber location information derived from interaction with a subscriber's Handset every seven (7) days.
- Legal approach – Intellione will use legal means available to aggressively pursue individuals, companies or other entities breaching personal privacy regarding subscriber location or other personally identifiable information as it pertains to its Handset applications.

- Operational approach – Prior to download of Intellione’s io-vector handset application from the Web site, consumers are provided **Notice** and **Choice** options as follows:

Notice –

io-vector and other Intellione applications also contain an easily accessible Privacy option linking to the URL for viewing within the application.

Intellione may publish a *Supplemental Privacy Statement* to address privacy protection matters unique to specific applications.

Choice –

If you choose to stop using io-vector and the services provided within, delete it from your device using your device manufacturer’s instructions. You may also email us at customersupport@ivector.net, provide us with your cell phone number and we will delete your phone’s MIN from our files. Following this, you will need to reenroll in io-vector to use the service.