

February 22, 2010

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex P2)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: **Privacy Roundtables - Comment, Project No. P095416**
The Need to Protect Commercial Data in B2B Exchanges

Dear Sir or Madam:

In connection with its privacy roundtables, the Federal Trade Commission (“FTC”) should consider the privacy of commercial data that is handled, stored and manipulated by electronic marketplaces or similar service providers operating in the business to business (“B2B”) sphere. This attention is warranted due to an emerging business model that creates the following risks to consumers:

- It subjects personal data of employees to heightened risk of unauthorized use or disclosure;
- It creates higher fees that will ultimately be borne by consumers; and
- It fosters unconscionable contract terms that are imposed on consumers of e-commerce services.

This business model operates as follows: a large purchaser of goods and services selects an e-commerce service provider (referred to commonly as an electronic “network”) through which all of its vendors must transmit or receive either commercial bids, orders and invoices, or discrete types of information, such as health, safety and environmental data. All of the vendors of that purchaser are then informed by the purchaser that, as a condition to do more business with the purchaser, the vendor must log onto the network’s website and receive or transmit data to and from the purchaser via that website. When the vendor visits the website, it is presented with Terms of Use that are not open for negotiation and amount to a contract of adhesion. There is no data confidentiality protection, the network may unilaterally amend the Terms of Use and the network disclaims all liability in relation to its website. The vendor is then left with the Hobson’s choice of accepting the Terms of Use or losing business with a large customer.

Tens of thousands of companies have accepted such poor Terms of Use. The networks have no incentive to modify or improve their Terms of Use and the vendors have little or no leverage to negotiate for better Terms of Use.

It is also common for the network to charge a fee to the vendor, even though the vendor did not freely select the network and the vendor would prefer to use another network. The vendor, unwillingly made into a purchaser of services from the network, has little or no leverage to negotiate these fees. That leverage will decline over time as more and more of the purchaser’s business processes migrate to use different aspects of the vendor’s technology. In common

parlance this phenomenon is referred to as the network having greater “stickiness” with the purchaser and thus greater leverage over its vendors. This emerging business model not only jeopardizes electronic data – the lifeblood of our new economy – but inhibits competition as vendors are unable to freely select or switch between competing networks. The inevitable result is higher fees.

The remainder of this letter explores in more detail typical provisions in such Terms of Use in order to highlight the need for guidance or protection from the FTC. While the quoted provisions of the Terms of Use are actual quotes, the names of the networks have been redacted to highlight that the focus of this letter is the general problem facing thousands of vendors and not any individual network.

Common and Sample Terms of Use

No Confidentiality Protection

A large, multinational network that receives and routes purchase orders and invoices, which contain pricing and similar trade secrets, has the following language in its Terms of Use:

If you submit Information to the Site . . . you grant XXXX an irrevocable, nonexclusive, worldwide, royalty-free license (sublicensable through multiple tiers) to (in any media now known or not currently known or invented) link to, utilize, use for any purpose, copy, exploit, and prepare derivative works of the submitted Information. No Information you submit shall be deemed onfidential (sic).

A network that collects financial, safety and other information from vendors so that purchasers may determine if they are pre-qualified to bid for contracts contains the following provision:

Please note that any information or material sent to XXXX will be deemed NOT to be confidential. By sending XXXX any information or material, you grant XXXX an unrestricted, irrevocable license to use, reproduce, display, perform, modify, transmit and distribute those materials or information, and you also agree that XXXX is free to use any ideas, concepts, know-how or techniques that you send us for any purpose.

A network that collects safety data and benchmarks vendors against their competitors so purchasers may compare them contains the following:

User Supplied Information

Our site gives users the ability to provide or enter information, including personal or confidential information, about the user, its employees and contractors. Examples may include contact information (such as name, email, or postal address), unique identifiers (such as username, password, identification number or social security number), demographic information (such as zip code), compliance information (such as safety manuals or accident reports) and other personal or confidential information. Such user supplied information is collected within XXXX to verify the user's identity, allow for database linkage, provide reporting capability (including aggregated data or benchmarking reports), allow for record keeping and tracking of data (such as internal training and injury and illness records), for use as account information in our system, and for other similar purposes appropriate to the operation of XXXX, including its review and verification services (and may also be used, from time to time, to enhance national security). This information is supplied at the user's discretion and will be used only as specified above.

In this instance, it is clear the network collects, stores and transmits sensitive personal information of employees but does not protect that information. The list of permitted uses is so broad (and not coupled with any obligation of confidentiality) as to provide practically no limit on the use the network may make of the employee data.

Right to Make Commercial Use of Aggregated Data.

Even in instances where the network imposes limitations on its permitted use of Data, the network will typically retain the right to sell aggregated data, even when it is composed of information that competitors normally regard as trade secrets, i.e. prices:

XXXX may use the bidding information submitted by Suppliers in the course of XXXX Sourcing Services projects to determine general price trends in various supply industries, to create predictive analyses useful for estimating likely market prices, and to evaluate suppliers appropriate for inclusion in future spend management projects in similar markets. XXXX may also use such bidding information in the publication of "high level" sourcing project results, provided that such publication (i) does not directly or indirectly identify Supplier or Buyer by name or provide a third party with sufficient information to allow a third party to identify Supplier or Buyer, (ii) is aggregated with data from at least four (4) comparable suppliers from a single project, (iii) does not specifically identify Supplier's products or services, or the prices

of those products or services, and (iv) does not identify Supplier as a participant of any specific project.

Other examples include:

XXXXI also retains the right to analyze, aggregate and report statistically sound summaries of the transactions flowing through the Marketplace.

XXXX will use anonymized information gleaned from registrations and from auctions conducted on our web site to provide better service to our customers. XXXX may also analyze the information including performing a trend analysis to better serve its customers.

In addition, XXXX maintains the right to disseminate Data you send to XXXX, so long as such Data is in an anonymous, aggregated form so as not to identify you.

There are two primary concerns with provisions such as these. First, not a single provision contains a time limitation on the data that may be aggregated released, meaning that “live” data could be released. In that regard, the protections do not comport with the safe harbor enunciated by the FTC in its 1996 *Statement of Antitrust Enforcement Policy in Health Care*, which required a three month delay in releases of aggregated data. While some of the provisions quoted above protect the identify and prices of an individual supplier, none of them close the door on the mischief that can result when a third party determines which rivals can instantly view prices or quotes of their competitors – especially in industries with few transactions and limited sellers and buyers.

Second, there is no other medium through which commercial data could be transmitted in which only “caveat emptor” determines the limits of the service provider’s use of the *content* of the data being transmitted. The United States postal service cannot open mailed bids and sell access to aggregated data to select customers. Nor can telecommunications providers listen to conversations and publish price trends based on those conversations. The content of the information being transmitted is owned by the recipient and the sender – and neither should be compelled to forfeit that ownership under contracts of adhesion.

This issue was addressed by the FTC in 2000 in its report entitled “*Entering the 21st Century: Competition Policy in the World of Electronic Marketplaces*” (the “B2B Report”). That analysis contemplated electronic market places entered into voluntarily by buyers and sellers looking for a market for their goods and services. In that scenario, it was predicted that abusive or unfair use of commercial aggregated data would be “self correcting” once participants in the marketplace learned of the practices. See B2B Report at Footnote 110. Others expressed doubt and urged “comprehensive public standards regarding the control of competitive information within B2Bs.” *Id.* at Footnote 111. This letter addresses a phenomenon not anticipated in the B2B Report. This letter does not address electronic market places that are

freely joined or abandoned by buyers and vendors, much as a farmer may choose to choose to sell his produce in one town's open air market or another. The emerging business model addressed by this letter is not a marketplace where buyers and sellers meet, but instead an outsourcing of certain processes, where sellers and buyers have already met and now all sellers are instructed to employ a specified means of communicating with the buyer. That mandatory method of sending transaction information to the buyer is controlled by a third party who claims for itself the right to view and profit from the "river of data" passing through its network system, as well as the right to determine who has access to that data. In that scenario, there is little hope for any "self correction" and the call for comprehensive public standards is even more compelling than when it was made in 2000.

Unilateral Right to Amend the Terms of Use

Even if a vendor received protection of its data in the Terms of Use, it would feel little comfort as the Terms of Use typically grant the network a unilateral right to amend its Terms of Use. The vendor is left to inspect the Terms of Use upon each use of the Website to determine if they have changed, which, as the networks well know, is neither practical nor realistic. Common terms are as follows:

You agree to review this Agreement prior to any Site Use, and each Site Use by you shall constitute and be deemed your unconditional acceptance of this Agreement. This Agreement may be prospectively modified by XXXX, by posting a revised Agreement on this Site.

XXXX reserves the right at its discretion to add to, modify, change or withdraw portions of its Privacy Policy without notice.

XXXX may make changes and corrections to information on this Web site and/or changes in the products, services and/or the programs described in these documents at any time without notice.

Disclaimer of All Liability

If a user were to negotiate protection from the prior two categories, the user may still have only a pyrrhic victory, as the Terms of Use typically seek to disclaim all liabilities of the network. Typical language includes the following:

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES WILL XXXX OR OTHERS BE LIABLE OR RESPONSIBLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL (INCLUDING DAMAGES FROM LOSS OF BUSINESS, LOST PROFITS, LITIGATION, OR THE LIKE), SPECIAL, EXEMPLARY, PUNITIVE OR OTHER DAMAGES, UNDER ANY LEGAL THEORY, ARISING OUT OF OR IN ANY WAY

RELATING TO THE SITE, YOUR SITE USE, OR THE CONTENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOUR SOLE REMEDY FOR DISSATISFACTION WITH THE SITE AND/OR CONTENT IS TO CEASE ALL OF YOUR SITE USE.

In no event will XXXX be liable to any party for any direct, indirect, special or other consequential damages for any use of this web site, or on any other hyper linked web site, including, without limitation, any lost profits, business interruption, loss of programs or other data on your information handling system or otherwise, even if we are expressly advised of the possibility of such damages.

In no event will XXXX be liable for any damages, including, without limitation, indirect, incidental or punitive damages, whether under a contract, tort or any other theory of liability, arising in connection with any party's use of the website or in connection with any failure of performance, error, omission, interruption, defect, delay in operation or transmission, computer virus, line system failure, loss of data, or loss of use related to this website or any website operated by any third party or any contents of this website or any other website, even if XXXX is aware of the possibility of such damages.

As the liability limits disclaim direct damages as well as the normal litany of consequential and similar special damages, the user is left with no recourse, rendering the contract nugatory. The user, meanwhile, is not entitled to any limitation on its liability.

Fees

Just as networks may change their Terms of Use, so they may change their fees. Terms such as the following are common:

You may inquire as to our most recent fee schedule by contacting us. We change our fees for our services from time to time. We may in our sole discretion change some or all of our services at any time. No refunds or credits will be extended at any time.

The users of the network's services, who did not select the network, must accept the stated fees or forfeit their business relationship with the large customer.

Summary

As more companies incorporate the internet "cloud" into their business processes (whether bidding, procurement or HS&E compliance) similar Terms of Use will govern ever

greater amounts of commercial and employee data. We are, however, witnessing a “race to the bottom” in Terms of Use as no network has incentive to improve them and no individual user has the leverage to modify them. In 2001, the National Association of Wholesaler-Distributors proposed voluntary standards for Terms of Use for e-marketplaces, which are attached. Those voluntary standards have not worked. The FTC should provide guidance regarding the minimum protections that should be afforded to commercial data and users of e-marketplaces, especially when the user is required to use the e-marketplace as a condition to doing business with a pre-existing customer.

These comments are submitted by the following individuals:

Phillip Schmandt*
Chair, Technology Practice Group

Jon M. Garon
Professor of Law

Lisa R. Lifshitz†
Partner, Business Law Group and Member, Technology Industry Group

Jose A. Santos, Jr.
Jose A. Santos, Jr., P.A.

Susan H. Stephan
Attorney and Shareholder