Glynx will change the way you use the internet and telecommunications

Privacy matters. From making a phone call to browsing the internet, to updating or viewing a social networking site, social communication today exposes the fundamental weakness of the current online world: it is mediated and monitored. And this continual violation of privacy increasingly inhibits activity or productive activity online.

Glynx is the first product to provide real-world-like private search, sharing and communications online. It uses patented technologies to provide privacy that complements today's online world.

Glynx is bringing about a mind shift in social communications, and will affect all online interactions where privacy matters.

At present, social communication services are supplied from the 'centre' and consumed from the 'edge'. It's all about web-sites and browsers; e-mail services and clients; centrally switched telephony and personal devices; and central directories of all flavours – search engines, social networking sites, web shop fronts; auction sites; services listings etc. Even advertising is targeted and supplied from the centre to consumer devices or software. However, these services are not passive; they actively restrict, record, correlate and document user interactions in order to satisfy a variety of business models.

And so, compared to the real world where relationships and communications range from public to private, from unmediated to chaperoned, from anonymous to monitored; current internet practices are non-private, they are mediated and monitored.

That's naive, dangerous and ultimately a losing proposition for businesses today. Unless today's online businesses can mimic real-world-like direct private interactions consumers and software companies will move their activities to providers that do.

It is increasingly naive to assume that consumers of social communication services will continue to accept arbitrary restrictions, constant observation and interference and then pay.

- Consumers are expected to pay for access to information others would readily supply for free. For example, telephony businesses do not disclose the in-call or off-network state of subscribers prior to connecting calls. This maximises the chance that all calls incur a flag-fall charge – irrespective of success. Thus, callers find themselves paying for connections to voicemail services even if, say, an email or hanging-up would be preferred at that point.

- Consumer information held on service sites is considered a business asset to be exploited. Consider the recent Facebook 'Beacon' or Google's 'Google Reader/Shared Lists' features. This information may be provided to third parties at their convenience and to the detriment of users. To paraphrase Tim Berners-Lee's concern: "If I search for information about some form of cancer, will my insurance premium go up because they've figured out what I'm looking at?" And these companies have a strong incentive to find ways to monetize this information as they regard it as a core business asset.

- Even humble e-mail is interfered with by service providers, companies, government organisations, SPAM houses and hacker nets to support advertising, censorship, unsolicited communication, and computer viruses. In fact, all of this interference has almost shifted e-mail from being a nifty communications tool to being a necessary evil.

Consumers are increasingly suspicious of a dangerous paradigm that is vulnerable to abuse. They are disenfranchised by services that don't live up to assurances that they will hold user profile, content and history information securely. Substantial violations are reported almost daily, and frequently by the best known, most trusted brands online. Their terms of use, by and large, absolve them of responsibility for misuse. The centralised paradigm is vulnerable to mass inadvertent disclosure, employee abuse, identity breaches and theft.

Ultimately it is a customer losing proposition. By forcing all online interactions into 'one-size-fits-all' non-private, mediated and monitored paradigm, current services are not satisfying customer needs. There are large demographics that cannot and do not use existing services due to privacy or confidentiality concerns. And there are increasing numbers of customers who are tuning in to the issues, and turning off by not accepting arbitrary constraints, and dropping out from the 'my life as public content' world. This is a growing potential customer base which has recognised the gap between real-world experience and pale, online imitations. Centralisation imposes costs that many are not willing to pay.

Everything that you do online today has the potential to be restricted, observed, recorded, exploited, leaked or stolen.

Glynx addresses these fundamental weaknesses.

Glynx gives people the ability to search, locate, connect, share and communicate directly with others - without mediation, observation or interference.

Glynx is a new platform for social communication. It changes the way the internet and telecommunications are used.

Glynx is new

Glynx stands out from the noise and bustle of all the 'next big things' on the net. It represents the future of social communication. Glynx was developed after five years of research and development creating the software and infrastructure to implement these ideas – and a portfolio of patents in private communications and online directories.

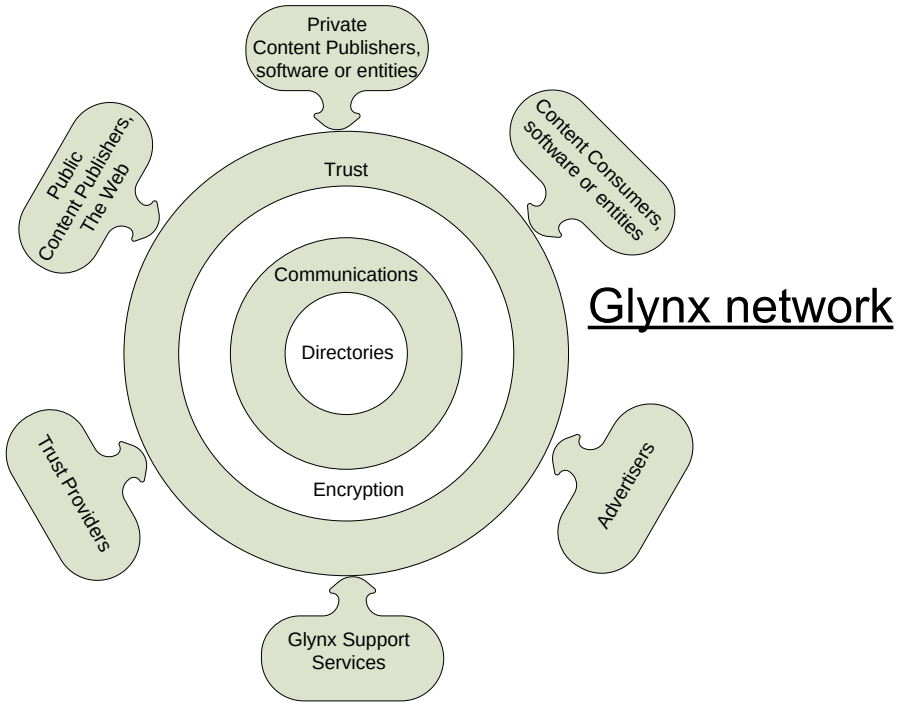
Glynx is not just another search engine, social networking concept or interoperability standard. It is a new internet framework for social communication and telecommunication based on the power of consumer devices.

Today the Glynx platform has four main segments:

- A peer-to-peer-based directory lookup service which enables, online connection and exchange of information without observation or interference;
- A mechanism of peer-to-peer unmediated communications and presence, which enables true consumer device-to-device control of communications;
- An encryption layer which ensures all interactions in the Glynx network are private and all content and directory entries are fully encrypted before sharing; and
- A trust framework whereby participants can be confident of the identities of those with whom they communicate;

This will be supported by a portfolio of applications which leverage these components to provide truly private and unmediated content search, social discovery, advertising and communications.

Elements of the Glynx network



The patented Glynx lookup service is unique. It is a directory – and it is private. It enables you to find others and connect – but it cannot be harvested for SPAM. It allows you to express yourself with multiple identities and personas and associate whatever information you want with those personas. It allows visibility on the net to be as public or private as you wish. And, no-one can observe or overhear you looking for others, searching for information, introducing themselves, forming relationships, or exchanging information.

It is just like the real world.

And as with the real world, trust between Glynx participants is not assumed or enforced from a single authority. With Glynx, strangers can form a weak relationship and grow to trust each other as their interactions deepen. Or they can start off from some higher level of trust – for example when one or both parties exhibit credentials. Credentials may be formal, e.g. a certified business or government document, or informal, e.g. a recommendation from a mutual acquaintance.

Similarly, Glynx does not aspire to be the provider of credentials. While Glynx performs this function today, the Glynx trust framework provides for the bulk of this work to be handled by others. The government is best-placed to verify your social security number; your ISP can verify your e-mail address; likewise your telephone company can verify your cell-phone number; and, perhaps most importantly, you are best placed to endorse your relationships with others. In fact, some Glynx users may wish to forgo formally verified credentials, relying solely on the endorsement of other Glynx users.

With Glynx, these authorities simply electronically sign the credentials. They need take no part in future interactions between Glynx subscribers. With Glynx no central server mediates the exchange of credentials. So interactions remain private.

Finally, Glynx has identified about twenty distinct application domains which leverage these facilities. Even though we are building applications to fill these spaces, we do not aspire to be the source of all Glynx-based applications. To this end, the Glynx APIs will enable any complying end-user software and any user to participate directly in unmediated relationships.

Glynx is freedom in social communication.

Glynx is software that enables online freedom: freedom to publish and search, and freedom to associate and communicate – all without observation or interference by third parties. Glynx facilitates these freedoms. Glynx represents an ideal bigger than the business or its artefacts.

Glynx provides freedom to search and discover others online; freedom to associate with others based on user controlled trust; freedom from unsolicited online communication and freedom to exchange information with others – all without observation or interference by third parties.

It provides the freedom to post information and absolutely determine who views it based on user controlled trust levels; and it provides the freedom to search for information that may be stored on user devices or the web – again without observation or interference by third parties.

Glynx enables people to control their online identities and really take advantage of the power of personal consumer devices to optimise their social communication.

Glynx will change the way the internet and telecommunications will be used

By giving online users the ability to locate and connect directly to each other without mediation, Glynx provides new opportunities for end-user software businesses. Prior to Glynx there was no method for self discovery and self-organisation of end-user software and no protocol for users to establish an unmediated relationship. As examples:

- Contact management software is improved when contact details can be exchanged and updated automatically without fear of observation or interference by mediating third party contact synchronization services,
- Telephony is improved when devices negotiate directly with each other before establishing the call, to check presence, availability and the most mutually convenient service to use, whether that be VoIP, GSM, email or voicemail, perhaps in that order,
- Financial software is improved when other instances of similar software are automatically discovered and invoices, payment, remittances, etc., are shared directly, without third party mediation or observation, and
- Social networking can start to replicate the spectrum of real-world interactions by providing services from the very public "… guy looking for girl…" to the most private "…how about we meet tonight…"

The view of social communication through the lens of privacy is profound.

In the same way that Microsoft changed the definition of computing to mean "a computer on every desk and in every home" or Skype propagated the meme "voice communications should just work and be free on the internet", Glynx will bring about a shift of perspective towards "the internet should be private when you want it to be" or "you should be in control of every aspect of your social communication".