

Internet Intelligence

The Internet hosts the biggest conversation in the world.
With over 35,000 billion pages; are you only hearing a whisper?



Harness the power of the Internet



“Knowledge is power.”

Francis Bacon

More than 40 years have passed since the birth of the Internet, with a whole generation now having grown up not knowing a world without it. As a medium it is frequently described as the ‘biggest conversation in the world’; and with 2 billion users worldwide and an ‘always on’ reputation, that should come as no surprise.

The Internet transcends both our professional and personal lives and is used for communication, information, education, advertising, sales and many aspects of day-to-day life. It does, however, have a dark side and is exploited by those with criminal, malicious and predatory intent. It can also offer anonymity and/or false identity. It therefore requires diligence and vigilance in use and awareness of content.

On pages separated by only a few clicks, large companies showcase their wares whilst customers comment on the quality of the service; banks advertise their offerings whilst customers access their bank accounts and luxury goods are advertised alongside counterfeits. The Internet is unregulated, unpoliced and opinionated; but with our help not ignored. In the majority of occasions it can even be an asset if managed correctly.

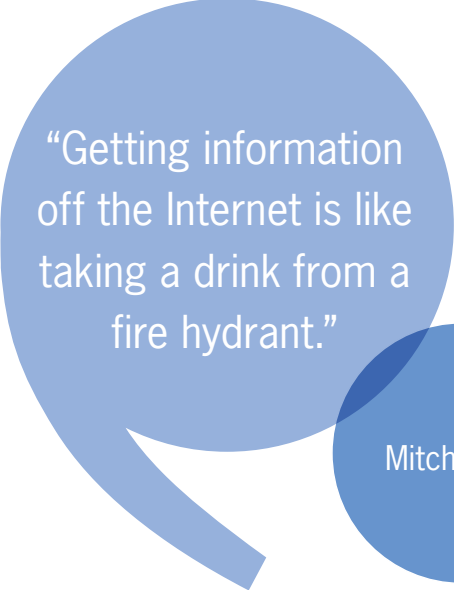
Where we add value

Given the aggressive growth of the Internet and its diversity of content, Internet Intelligence is used to address or complement a whole variety of issues including:

- Reputational due diligence
- Market intelligence
- Brand protection
- Counterfeiting
- Corporate fraud
- Asset tracing
- Trademark infringement
- Compliance issues

Decision makers need to have access to all available information before committing to a decision or course of action. Additional value is derived by complimenting traditional open source data with opinion and commentary available on the Internet which can validate or discredit original source information.

Grant Thornton's Internet Intelligence professionals are recognised experts and have proprietary tools and methodologies to locate, categorise and analyse intelligence often unavailable through conventional processes.

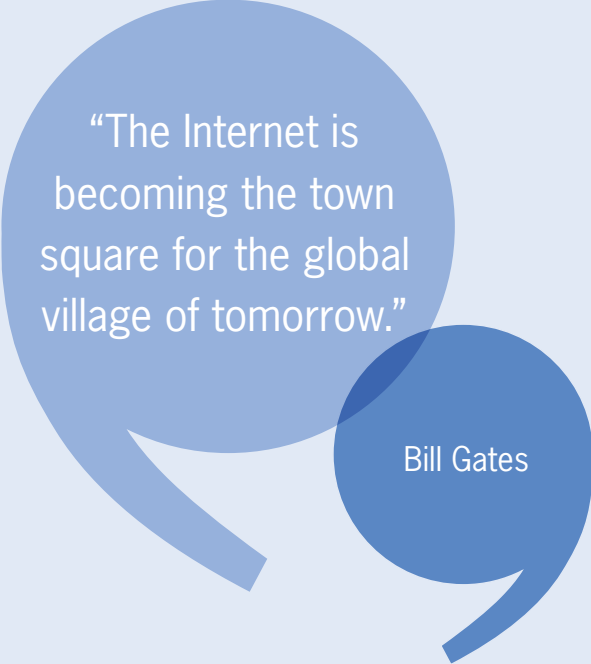


“Getting information off the Internet is like taking a drink from a fire hydrant.”



Mitch Kapor

Understanding social 'chatter'



“The Internet is becoming the town square for the global village of tomorrow.”

Bill Gates

The impact of social networking over the last few years has been tremendous with an estimated one in three surfers all over the globe joining any one of the many networking sites on offer. In 2003 nobody was talking about Internet based social networks, now over 1.5 billion people are chatting online. This kind of propagation is previously unheard of.

Some key areas for somebody diving into the social media space for the first time, or wanting advice on revising their strategy, could be:

- Is anyone online having conversations about my brand?
- What are they discussing?
- Who is conversing?
- Are they complaining or complementing?
- Are they employees or competitors?
- Where are they congregating?
- Finally, is there an agenda?

Case Studies

Personal reputational due diligence

A company was in the process of employing a new executive and, as part of their screening process; the individual's details were checked. Nothing untoward was identified. The company decided to extend the checks to include the Internet where any reputation issues might be highlighted.

Searches of the Internet highlighted a number of individuals with the same name. By drilling deeper, fragments of the correct individual's past started to emerge; one such fragment was a photograph of the person involved in a car crash on a racetrack with 'his' high performance Italian sports car.

This raised some suspicions, especially as the vehicle was valued at £1m, substantially more than his mortgaged house and not something that would generally be the possession of an individual on a £100k salary.

Further enquiries, widened to include traditional intelligence methods, identified three other Italian supercars in an extended garage behind his house. It emerged that he had been defrauding his previous employer to the tune of over £3m and converting these gains into his passion.

Social network monitoring

A large financial institution in the USA was alerted to a forum on the web where an individual was posting complaints about their company. Examination of the forum identified a clearly disgruntled individual criticising senior staff and the overall ethics of the company. The postings were anonymous.

During the following four weeks the poster attracted 20-30 further online followers, all who purported to have had similar bad experiences with the company. The poster's language was now more aggressive and content had propagated to other forums and chat rooms. In the posts threats were being made against the company and named senior management so measures were put in place to try to identify the poster's identity and location.

Over the following weeks an electronic profile of the suspect was constructed. From this information, it was possible to tell when the poster would be online, for how long and the physical location. A report was created and law enforcement involved. The individual was identified and arrested. His computer was confiscated and forensically imaged; the result of which confirmed that he was planning a series of disruptions to company activity, particularly forthcoming investor meetings.

Corporate reputational due diligence

An acquisition was being planned of a medium-sized company specialising in the manufacture of personal electronic devices; MP3 players, organisers etc.

The traditional financial due diligence process was well advanced and a price was close to agreement. It was decided to extend the due diligence process to include the Internet, primarily to ensure that any commentary on the web supported the provisional valuation. A thorough review unearthed numerous discussions criticising the company's recent product reliability, customer support and overall corporate reputation. It seemed that although the past sales figures were respectable, the future of the company looked in doubt.

As a result of the Internet review, it was agreed that the sale should still proceed but with a revised price that included a figure for reversing brand damage, starting with a major product recall, and improving quality and business controls.

Brand protection – Rebranding

A company commissioned an 'Internet Brand Landscape', which involved a one month intensive period of monitoring the web followed by analysis of the findings and compilation of a comprehensive report. The report identified information relevant to legal counsel, marketing, security, intellectual property and customer services.

Amongst the highlighted findings was possible customer confusion over the company logo; there were two variations in existence on the web with no obvious explanation. It transpired that the company changed their logo twelve months earlier. Using proprietary image tracking software, all occurrences of the old logo on the web were identified; the locations were then reviewed for legitimacy and, where necessary, a new logo was supplied. Similar solutions were devised to address the other issues identified.

Brand protection – Counterfeits

A global pharmaceutical company raised concerns at the increase in presence of online pharmacies; their main areas of concern were counterfeiting, grey market trading and reputation.

Using proprietary software capable of advanced image and text monitoring, numerous online pharmacies were identified advertising/selling in multiple languages. Further intelligence was gathered on the key players and a strategy defined with the client. Trial purchases were made and the authenticity of the product checked. In some cases larger orders were made and whole shipments monitored enabling the counterfeit product to be tracked back to its source.

Introduction to Paul Mewett and Michael Stannard

Grant Thornton's Internet Intelligence specialists bring a unique blend of skills acquired throughout their long and varied careers to date, ranging from traditional multinational investigations to complex Internet based investigations involving the identification of illegal covert groups for foreign governments.

Paul's early career started in the military where he was involved in the areas of intelligence and electronics. He subsequently spent the following 20 years working with state-of-the-art search and data mining technologies with a strong focus on the Internet. It is his knowledge and experience in these areas that allows Grant Thornton to now lead the way in this field.

Michael has more than 30 years of experience in the fields of intelligence and investigations. During his career, Michael has spent much of his time consulting to FTSE 100 and Fortune 500 companies on counter-fraud measures, anti-counterfeiting strategies, and asset recoveries. Prior to his career in the private sector, Michael worked for the UK Custom's Investigation Service.



Paul Mewett

Head of Internet Intelligence (Technical)

T +44 (0)20 7865 2158

M +44 (0)7974 083682

E paul.mewett@uk.gt.com



Michael Stannard

Head of Internet Intelligence (Operations)

T +44 (0)20 7865 2141

M +44 (0)7976 504230

E michael.j.stannard@uk.gt.com



© 2010 Grant Thornton UK LLP. All rights reserved.

'Grant Thornton' means Grant Thornton UK LLP, a limited liability partnership.

Grant Thornton UK LLP is a member firm within Grant Thornton International Ltd ('Grant Thornton International'). Grant Thornton International and the member firms are not a worldwide partnership. Services are delivered by the member firms independently.

This publication has been prepared only as a guide. No responsibility can be accepted by us for loss occasioned to any person acting or refraining from acting as a result of any material in this publication.

www.grant-thornton.co.uk

B1619021