

A conceptual analysis on the taxation system for highly virtual enterprises

Guozhen George Huang
The Open Polytechnic of New Zealand
George.huang@openpolytechnic.ac.nz

ABSTRACT

Highly virtual enterprise (HVE) as a new form of business has existed in the cloud for a long time, but its taxation system is far from establishment. This paper analysed the characteristics of a HVE in the cloud environment, suggested the criteria for its tax residency determination, and recommended the framework for accounting, auditing and legislation in New Zealand. It further proposed the network system for monitoring HVE activities and accounting for their website transactions. It also provided deliverables for cloud technology to develop in the future.

Keywords

Taxation, highly virtual enterprise, cloud technology, legal regulation, network system

1. THE SCENARIO

Mr. Smart is a web programmer who resides in China. He registered a domain name www.forbiddendownloadables.biz and an IP address with an ICANN¹ accredited registrar in New Zealand, selling downloadables around the world. He uses a web server hosted by an ISP in India. He has made a large amount of sales to many countries. All the payments were made through an online payment intermediary (OPI) in the U.S. to his bank in China. Two years after the launch of the website, he closed the New Zealand website, and started a new domain name with a new IP address in Australia, and had his business continued...Mr. Smart has neither filed or paid any GST or income tax, nor has been caught by any tax authority.

2. ENTITY IDENTIFICATION

For taxation, Mr. Smart's business entity must be clearly identified. Current definitions of a virtual enterprise (VE), such as "The virtual enterprise is based on the ability to create temporary co-operations and to realize the value of a short business opportunity..." (Katzy & Schuh, 1999) are too broad because

they cannot match the case of Mr. Smart. Based on the degree of virtualisation, we classify a VE into three kinds: lowly virtual enterprise, moderately virtual enterprise, and highly virtual enterprise, as shown in Table 1.

	Lowly virtual enterprise (LVE)	Moderately virtual enterprise (MVE)	Highly virtual enterprise (HVE)
Input	Digital and/or physical material	Digital and/or physical material	Digital material
Process	Physical and virtual worksites with people's physical contact	Physical and virtual worksites with people's physical contact	Virtual worksite without people's physical contact
Output	Physical product	Digital product	Digital product
Physical establishment	Permanent	Permanent or temporary	Temporary
Web server ownership	Self owned	Self owned or be hosted	Be hosted
Typical situation	Online collaborative alliance, online joint venture for production of cars, phones, etc	Online marketing and selling of e-books, e-music, e-videos, etc	Online production, marketing and selling of e-books, e-music, e-videos, etc

Table 1 Classification of Virtual Enterprises

Mr. Smart's business entity is a HVE because it uses digital material, operates in virtual worksite which temporarily registered with the registrar and hosted by an ISP, needs no physical people contact, and produces downloadables.

3. BUSINESS LIFE

Although a HVE exists in the virtual world, it has attachments that are Internet service organisations in the physical world. There are five kinds of attachments: Mr. Smart (*the business initiator*); the registrar (*the domain name and IP address controller*); the ISP who hosts the server (*the business executor*); the OPI (*the payment transferor*); and the bank (*the money keeper*). Although Mr. Smart's business is in cyberspace and can trade

¹ ICANN is the abbreviation of Internet Corporation for Assigned Names and Numbers.

anywhere, each of the attachments must be somewhere in the physical world, and this is the point where we should consider for taxation.

4. TAX RESIDENCY

A HVE's tax residency is the first issue that needs to be determined for taxation. Current determination criteria including "centre of management", "control of the company", and "permanent establishment" (IRD, 2009) stated by IRD² for both physical world entities and e-commerce entities are neither pertinent nor practicable to a HVE. To determine the tax residency, each of the aforesaid attachment locations can be used as the basis. The physical address is considered because current tax rules emphasises the citizenship and permanent place of abode (Income Tax Act 2007, s YD1(2)); the location of the server or web hosting ISP is considered because it can be treated as the place of "the fixed automated equipment...for the core functions of the enterprise" (Ho et al, 2001); the location of the registrar is considered because it can be argued that the intention of choosing New Zealand as the market domain is to "create legal relations" and to retain the "legality" (Bassett, 2007) in New Zealand; the place where the bank sits is considered because it is where the real money exits from the virtual world, a separate jurisdiction from any countries of the physical world. Among them, the location of registrar is most appropriate, because unlike the others, it is relatively fixed and culpable. It is something that Mr. Smart cannot change easily, and once it is changed, the business life underpinned by the domain name and website will end, and in terms of common law, the "offeror" or the "offeree" attached (Ho et al, 2001) would not exist anymore. It is also a choice which complied with the Taxation Framework Conditions for Electronic Commerce (OECD, 1998), especially the principle of "effectiveness and fairness".

Mr. Smart is a tax resident of New Zealand since the registrar who controls his business life is in New Zealand.

5. ACCOUNTING FRAMEWORK AND AUDITING PARADIGM

Current accounting framework is underpinned by the assumption of "Going concern" (FRSB NZ Framework, 2004). This assumption should be replaced by "Present concern" because it would be groundless to assume that

a HVE has any intention or needs to keep a website ongoing to "a foreseeable future" (FRSB NZ Framework, 2004). In fact, "Present concern" is a "natural representation of economic reality" (Baker, 2006) for HVEs. It needs only to concern the period from when a website appears to when it disappears, and not to worry about "permanent establishment" (IRD, 2009).

Given the dynamic and evasive nature of a HVE's transaction evidence, a continuous audit which defined as "a methodology that enables independent auditors to provide written assurance on a subject matter using a series of auditors' reports issued simultaneously with, or a short period of time after, the occurrence of events underlying the subject matter" (Shields, 1998) is required.

6. LEGAL REGULATION

With recognition of the great and fast growing power of Internet, many countries have implemented different regulations or laws to regulate economic activities on the web (ISOC, 2009), but fewer have taken actual steps on taxation of HVEs. Although New Zealand, followed other countries such as U.S. and Australia has formulated its tax rules for e-commerce, without a well-established legal system these rules would rather be a paper statement than something workable. For example, it sets a scenario where a non-resident like Mr. Smart who operates a business through a website in New Zealand is to be taxed in New Zealand (IRD, 2009), without the registrar's reporting the existence of such a website, how would IRD be able to discover it and verify that it is not at other countries but in New Zealand?

Under the capabilities of current cloud technology, the legal system for taxing HVEs will be complicated, but its framework must be built on some basic rules. These rules can be:

Privacy violation exemption of IRD

IRD should be exempt from privacy violation to any attachments including OPIs, registrars, ISPs and their clients in requesting and getting access to "all account information" (PayPal UK, 2009) about any New Zealand website in order to conduct a tax investigation. This seems to be an obvious pre-condition, but it is not favoured by the organisations. For commercial interest, privacy is often administrated in favour of their clients rather than the government. This would result in an invitation to those who intend to evade tax.

² IRD is the abbreviation for Inland Revenue Department of New Zealand.

Registrars to verify registrants' addresses

Registrars must have had each registrant's address verified physically in a regular manner to facilitate IRD in catching a tax evader. Although ICANN requires each of its registrars to abide by the "reasonable and commercially practical...verification at the time of registration ...or periodic re-verification" (Sec 3.7.8 of RAA ICANN, 2009), because of that an "electronic form" of a registered name holder and registration data will suffice (Sec 3.4 of RAA ICANN, 2009), there is in effect no physical address verification. This makes the taxation enforceability questionable.

OPIs and ISPs to impose transaction limits to those whose addresses unverified

It is necessary for OPIs and ISPs to impose limits on money transfer to those who haven't got their addresses verified. In EU countries, a PayPal account holder cannot receive more than £1,700 if his or her address is not verified (PayPal UK, 2009), which in New Zealand, the withdraw limit is \$770 per month (PayPal NZ, 2009). Because such verification usually involves checking whether a credit card provided by an account holder is working or not, rather than a direct contacting, its effect is unguaranteed. An ISP may be even more lenient than an OPI, for example, Trademe does not impose such limit for those whose addresses unverified (Trademe, 2009). Without the imposition, a HVE will trade more freely.

Registrars, ISPs and OPIs to collect and store clients' transaction data for tax purpose

Currently most OPIs, registrars and ISPs collect and store their clients' transaction data for commercial purposes such as to understand their customers better and to improve their services continuously. The data they collected may not be relevant or adequate for tax accounts. Also there is a confliction between these attachments and IRD in how long a record should be kept. For example, IRD requires to keep a tax payer's record for at least 7 years (IRD, 2009), while a registrar may only require to retain a client's data for 3 years (Sec 3.4 RAA ICANN, 2009). This situation may make tax accounting and auditing impossible.

IRD to enforce all websites PICS tax labelled

PICS³ is a technique to label Internet content. Although "It was originally designed to help

parents and teachers control what children access on the Internet, it also facilitates other uses for labels, including code signing, privacy, and intellectual property rights management" (W3C, 2009). The current version of PICS has been stable since March 1996, and many software vendors are getting their products compatible to it. PICS if labelled with tax code will be an important tool for IRD to retrieve a website by industry, product or type of transaction.

Registrars to report about registrants and their primary ISPs to IRD

Since a registrar is an administrative organisation who holds the first-hand data of HVEs and maintains the database including their registered date, renewed date, expiry date, primary ISP(s), and other information, it is an ideal reporter to IRD. Without the registrar regularly reporting, IRD would not be able to know the existence of a HVE and all such entities in the country.

ISPs to decrypt information for IRD

As a common practice, an ISP usually encrypts transaction data in transmission for its clients. Without the encryption keys, IRD as an external user would have no way of decrypting and interpreting the data within a short period of time. It should be the ISP's duty to provide encryption keys as required by IRD.

7. CLOUD TECHNOLOGY FOR HVEs MONITORING AND ACCOUNTING

There is a dilemma in HVE taxation that IRD could not get any evidence without technical support of the attachments, and at the same time an attachment would not provide any support without IRD getting some evidence first. The dilemma is caused by both the lack of legal regulation and the non-existence of an automated system to monitor and account for activities of HVEs' websites, and this is where cloud technology should contribute to.

The automated system should consist of three parts: *distributed network platform* to collaborate the work between attachments and IRD, *website monitoring and accounting software* to automate the monitoring, recording, analysing and reporting about HVEs' websites, and *middleware* to integrate different software.

Distributed network platform

Since the virtual world has no boundaries of any country, monitoring HVEs is a universal task. New Zealand as a country should set up and maintain a national network to collaborate

³ PICS is the abbreviation for Platform for Internet Content Selection, a technological application issued by the World Wide Web Consortium (W3C).

the operations of those attachments who are involved in the businesses of HVEs. Unfortunately we cannot find such a network in the world, however there are techniques if adapted can be used for the purpose. The related techniques could be from the areas of Internet content control (ISOC, 2009), and cyberspace forensic engineering (Kahai et al, 2006), where our thoughts on the network platform got sparked off. The main components of the platform are as follows:

The main server

The main server situates at IRD, monitoring business activities of target HVEs, logging their transactions, and interacting with proxy servers that deployed in different regions of the country. It maintains a database of HVE profiles. Each profile is being updated daily either automatically by alerts sent from proxy servers, or manually by staff at IRD. The database is built upon the reports of registrars.

Proxy servers

A proxy server stays with one of the network tax agents at different regions. It acts as an intermediary between a subnet of HVEs and the main server, providing the services of transaction data close monitoring, collecting and analysing, and alert sending. It also provides a cache, and keeps a separate database of HVE profiles.

Network tax agents

A network tax agent is a registrar, an ISP, an OPI who has contract with IRD to maintain a proxy server and fulfil the monitoring and reporting task at a specific region. Such an agent is chosen based on not only its technical capability but also its locality.

Alert and probe

An alert is triggered by website monitoring software when a certain number of downloads or online payments occurs. It is sent from a proxy server to the main server on daily basis. A probe is a request sent from the main server to a proxy server or several proxy servers when IRD suspects that a HVE website is under-monitored, or believes a collaboration of several network tax agents is necessary.

Website monitoring and accounting software

Although there is currently no website monitoring and accounting software, there are network tools if adapted could fulfil the task. These tools can be from different network applications, in particular network forensics, Internet content control, and website statistics.

They can help fulfil the following specific jobs:

A HVE's identification and trace-out

This would enable IRD to find out or verify the tax residency of a suspect HVE. There are reconnaissance tools such as nslookup, Whois, and dig (Kloth.net, 2005) that can trace out a HVE's physical address and IP address. The software owned by authoritative organisations such as APNIC⁴ could also be used to identify a HVE in the cloud.

Active ISPs trace-out

An active ISP in New Zealand could play a very important role in helping IRD collecting evidence and monitoring a HVE's website. Network scanning techniques such as ping sweeps, network mapping, port detecting and sniffers can be used to find out all active ISPs and applications in relation to a HVE's website. Many forensic software such as Sam Spade, Ping, IP block, Whois, Traceroute, CyberKit (Sam Spade; Ping; IP Block; Whois; Traceroute; CyberKit, 2009) could also be used to do the job.

Website download and payment monitoring

The number of downloads and online payments with a website is useful to derive the total sales and how much has been paid. Acquiring it will require to discern not only a transaction packet but also its content, where techniques in network sniffing, content filtering and digital decryption⁵ can help. It can be done by software such as CAPSA (CAPSA; DNAttrade, 2009) and Green Dam (Wolchok et al, 2009).

Website transactions statistics

For taxation, financial transactions need to be measured, recorded, analysed, reported and stored. The techniques for network management and traffic analysis such as NAPA, Scrutinizer, and NetFlow Analyzer (NAPA, Scrutinizer, NetFlow Analyzer, 2009) can be useful in this area.

Middleware for system integration

Given the fact that none of software mentioned above can provide precise and comprehensive measurement about what they are meant to do, either detecting an attack, or filtering out a forbidden content, or reporting a 100%

⁴ APNIC is the abbreviation for the Asia Pacific Network Information Centre.

⁵ Digital decryption is the technique used to reflect and interpret the meaning of a digitalised message which hid by a sender and/or receiver.

accurate statistics, there must be middleware to integrate different software for consolidation or verification of a HVE's tax account.

Based on the characteristics of HVEs, current Internet protocols and our tax accounting needs, we suggest the deliverables for the integrated website monitoring and accounting system, as shown in Table 2.

Needs	Deliverables
Essential	<ul style="list-style-type: none"> • A website domain name, business name, and its registered IP address • Physical and IP address of the registrar • Physical and IP address of primary ISP • Physical address and stable IP address of the website • Time the website is registered • Which primary ISP(s) the website has used • Time the website expires • What downloadable and price it sells • Each sale transaction: which product, how many downloads, from which country, to which country, at what price, and when • Each payment transaction: which currency, amount, name of payer, name of payee, from which country, to which country and which bank, through which OPI, pay for what, and when • Which network tax agent(s) or region(s) a sale transaction occurs • How many downloads were made for each and every month • How much money were transferred for each and every month
Desirable	<ul style="list-style-type: none"> • Name of the entrepreneur, postal and email address, and telephone number • The entrepreneur taxation number and passport number • Physical address and time the entrepreneur is usually and/or recently logged onto the website • Physical and IP address of the OPI the website has used • Physical and IP address of the bank the website has used

Table 2 Deliverables of Integrated Website Monitoring and Accounting System

8. GOING FORWARD

To comply with the five guiding taxation principles (Ho et al, 2001) and to ensure the practicability for taxing HVEs, there are many issues to be resolved.

For the time being New Zealand government implement the taxpayer-to-file system (IRD, 2009), that it is the duty of each individual to file their own tax returns. If a tax payer is at overseas or somewhere unknown, how would he or she be bound to pay tax on time?

Under "Present concern" accounting, a real-time collection is suitable because once a website is gone, there may not be any way to collect tax. This raises a question what taxes should be imposed to a HVE. Is GST which levied on each Internet sale, the same way as VAT to EU countries (Noronha & Vinten, 2003) or Internet sales tax to US (Cardinali, 2001) suitable and practicable? If GST is automatically collected through a network programme depriving part of each online payment, an approach "if we cannot get you, we will get your money", will it encourage a HVE to claim taxable expenses therefore to file a voluntary income tax return? Or if this is still not so attractive to those who net a profit after deduction of taxable expenses, will a shutdown of website by the registrar be the only choice?

There are challenges for cloud technology. Since a data transmission between a HVE website and a buyer can be routed differently, it may not be caught by a network tax agent. Will there be a technique for other agents to catch it? A file can be dissembled to parts which are then transmitted through different routes, will there be a technique for a network tax agent to identify the parts and assemble them back? If any of such parts is gone through a server at a neighbouring country, will there be a technical protocol incorporated in the DTA⁶ which enables an international collaboration? All of these wait to be answered in the near future.

Author Biography

Guozhen G. Huang is the lecturer of accounting information systems at The Open Polytechnic of New Zealand. He served as a systems accountant at Bax Global NZ Ltd before he took the lecturer position. He is interested in issues in virtual enterprise accounting, enterprise information systems, and accountants' role in application of computer technologies.



⁶ DTA is the abbreviation for a double taxation agreement.

REFERENCES

- Baker, R. (2006), Epistemological objectivity in financial reporting: Does internet accounting require a new accounting model? *Accounting, Auditing & Accountability Journal*, Vol. 19 No. 5
- Bassett, I. (2007), *Contract Law in New Zealand: Lawyers' Handbook*, retrieved Nov 1, 2009 from <http://www.contract-law.co.nz>, ISBN 978-0-473-12265-2
- CAPSA, retrieved Nov 1, 2009 from <http://www.capsa.org>
- Cardinali, R. (2001), Taxing the Internet: levelling the playing field or milking the cash cow? *European Business Review (UK)*, Vol. 13, No 6
- Cyber Kit, retrieved Nov 1, 2009 from <http://www.cyberkit.net>
- FRSB of NZICA, (2004), *New Zealand Framework*
- Ho, D., Mak, A. & Wong, B. (2001), Assurance of functionality of tax in the e-business world: the Hong Kong experience, *Managerial Auditing Journal* 16/6 pp. 339-346, MCB UP Ltd
- Income Tax Act 2007 of New Zealand
- Inland Revenue Department of New Zealand, ecommerce tax and record keeping, retrieved Nov 1, 2009 from <http://www.ird.govt.nz>
- IP Blocks, retrieved Nov 1, 2009 from <http://www.countryipblocks.net>
- ISOC, retrieved Nov 1, 2009 from http://www.isoc.org/inet97/proceedings/B1/B1_3.HTM
- Kahai, P., Namuduri, K. & Pendse, R. (2006), *Digital crime and forensic science in cyberspace: tracing cyber crimes with a privacy-enabled forensic profiling system*, Idea Group Publishing
- Katzy, B. & Schuh, G. (1999), *The Virtual Enterprise*, University of St. Gallen, Erasmus University Rotterdam, retrieved on Nov 1, 2009 from <http://portal.cetim.org>
- ICANN (2009), *Registrar Accreditation Agreement*, retrieved on Nov. 1, 2009 from <http://www.icann.org>
- Kloth.net, retrieved Nov 1, 2009 from <http://www.kloth.net>
- NAPA, retrieved Nov 1, 2009 from <http://www.intel.com/cd/software/products>
- NetFlow Analyser, retrieved Nov 1, 2009 from <http://www.networkinstruments.com/products>
- Noronha, C. & Vinten, G. (2003), Taxation of e-commerce in Hong Kong: applying UK and US experience, *Managerial Auditing Journal*, 18/9, pp702-709, MCB UP Ltd
- OECD (1998), *Electronic Commerce: Taxation Framework Conditions*, Committee on Fiscal Affairs, Paris
- PayPal New Zealand, retrieved Nov 1, 2009 from <https://www.paypal.com/nz>
- PayPal U.K. retrieved Nov 1, 2009 from <http://www.cms.paypal.com/uk>
- Ping, retrieved Nov 1, 2009 from <http://network-tools.com>
- Sam Spade, retrieved Nov 1, 2009 from <http://samspade.org>
- Scrutinizer, retrieved Nov 1, 2009 from <http://www.scrutinizer.com.au>
- Shields, G. (1998), Non-stop auditing, *CA Magazine*, Vol. 131 No.7, pp. 39-40
- The W3C, Fact Sheet, retrieved Nov 1, 2009 from <http://www.w3.org>
- Traceroute, retrieved Nov 1, 2009 from <http://www.traceroute.org>
- Trademe, retrieved Nov 1, 2009 from <http://www.trademe.co.nz>
- Whois, homepage, Retrieved Nov 1, 2009 from <http://www.whois.net>
- Wolchok, S., Yao, R. & Halderman, J. (2009), *Analysis of the Green Dam Censorware System*, The University of Michigan, retrieved Nov 1, 2009 from <http://www.cse.umich.edu>