Reflections on Cases

The journey from NCSA at the University of Illinois to Tahrir Square in Cairo is a long one. Since 1993 we have seen huge growth on the internet that has both widened access to information and education for users, created a wealth of new opportunities for business and presented a succession of challenges to governments. It is a journey scattered with examples of inherently disruptive innovations of a type that we might well now consider to be hallmarks of the internet, but one which is equally battle-scarred as a result of various efforts to legislate, regulate and restrict it. Today, the financial storm in the West rages on unabated, and the emergence of the next Twitter, Pinterest, or Airtime is just around the corner, no doubt to be greeted by the whoops and cheers of the technophile chorus. Though our seven case studies tell us much, for all our looking backwards and as we turn our attentions to the future, our view is little clearer. What the internet of our cases demonstrates, overwhelmingly, is that this inherently disruptive technology will continue to deliver the unexpected, and so it is that we leave any predictions about the future of the web for the snake oil salesmen. Nevertheless, the developments we have examined in this paper have identified a number of considerations that we should continue to be mindful of as the web moves forward.

In 1993, Mosaic unlocked the true potential of Berners-Lee’s world wide web and also captured the public imagination. It was the beginning of a steep growth curve that would accelerate through the ‘90’s and which continues to grow today, as our expectations of ‘anytime access’ bring connectivity to an ever greater number of devices. Mosaic did successfully bring together the key features from other competing browsers. Ultimately though, it succeeded for two key reasons that can be seen as heralds of significant tropes for the burgeoning internet: free and easy. In distributing the browser as free for non-commercial, personal-use and by rationalising the installation method so that it was accessible to non-technical users, NCSA gave Mosaic the best possible chance of being widely adopted, and simultaneously established an expectation among users and a model for businesses that would have far reaching implications for the web. The case of Mosaic also highlights a number of early issues around internet governance. The US government would have a defining influence over the web for many years, following their funding of ARPANET and then NSFNet — of which NCSA was part — even though WWW had originated with Berners-Lee at CERN, Switzerland. The rapid growth in numbers that Mosaic brought to the web shone a spotlight on the effective monopoly that had been granted to NSI by NSF, which would eventually lead to the foundation of ICANN, if only for similar questions of monopoly to remain. Mosaic was the catalyst for users, businesses and governments to begin exploring the possibilities and testing the boundaries of the new global networked environment. Their early interactions in this period highlighted the necessity for some formal structures of internet governance, as would eventually be defined by the World Summit on the Information Society (WSIS, 2005) as the “...development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet.“ The U.S. would hang onto effective control of the internet for a great many years and we are now, finally, seeing the internationalisation of internet governance in a meaningful way.

The online marketplace that we take for granted today sits atop a foundation of browser technologies from the mid-1990s, particularly SSL as developed by Mosaic creator Marc Andreessen. Thanks to this bedrock, Amazon and eBay have become trusted and established Internet brands that boast millions of users and billions of dollars in turnover, but their journey from startups to online behemoths involved the development and refinement of an online shopping model which successfully replicates the security and familiarity of the high-street experience, while leveraging the benefits of new internet technologies to offer both greater choice and convenience for the consumer. From secure payment systems to innovative methods of recommendation and referral, these companies led others in delivering choice across borders and vastly expanding the types of goods that could be purchased, and the destinations from where they could be sourced. They would also be in a position to collect more information about their customers than retailers had ever managed before.

Along the way, Amazon's ambitions have expanded considerably, and they have taken no prisoners in pursuing them. Today it holds a significant and growing share in markets that, until recently, were dominated by publishers, booksellers, records stores, electronics and clothing retailers, and other bricks and mortar stores. It sits at the top table of the internet, alongside giants such as Google, Facebook and Apple. Among the many to whom its growth has caused alarm are the major print publishers, who have been prompted to take, what appears to be, extreme action in order to protect their businesses. Hachette Livre, HarperCollins, Simon & Schuster, and Penguin (Pearson) are among those that now stand accused, along with Apple, of collusion with respect to the price fixing of ebooks. Amazon's dominance in the the emerging ebook market casts a heavy shadow over the entire episode. Not content with the huge success of Kindle for e-books, Amazon has diversified the Kindle brand with the Kindle Fire, now placing itself in direct competition with Apple, Samsung and others for a slice of the tablet market. With Amazon Prime Instant Streaming, the recent acquisition of U.K. DVD and online TV and movie rental service, LoveFilm, and the announcement that it will commission original TV content through Amazon Studios, it is clear that the company is also making moves to see off the likes of Netflix and Hulu, and make a serious challenge to Apple's bid to own the living room. One thing is clear: at the same time it makes its customers feel secure in their shopping, Amazon makes its competitors exceedingly nervous. The traditional high-volume, bricks and mortar U.S. retailer, Wal-Mart, has faced relentless criticism and a litany of controversies over its business practices, and raised many a concerned voice over its impact on the 'main streets' of the U.S. By comparison, Amazon is a company that operates truly globally, only planting their feet where absolutely necessary — and, of course, wherever is most tax efficient — and which shows no signs of slowing in either growth or its efforts to diversify. The only reasonable expectation should be criticism and controversies of an order of magnitude that dwarf those faced by Walmart and kin thus far.

While e-commerce grows ever larger we are simultaneously seeing further support for smaller and smaller value transactions, for both physical and digital goods. This rise in micropayments has the potential to further disrupt traditional markets. Services such as Flattr, crowdsourced funding platforms like Kickstarter, or micro-loans agents like Kiva stand to revolutionise, not only the way we shop, but also the way we ascribe value to content on the internet and more generally. The extent to which consumers' browsing and shopping habits are monitored now means that vendors know more about us than ever before, and there are significant questions regarding what happens to this information. For instance, user data can be sold to third parties, retained and analysed to build up ever more detailed user profiles, or can be targeted by hackers, stolen and used to commit fraud — as in the recent case that affected 2.2m users of Sony's Playstation network, during which hackers exposed users credit card details. Just what redress internet shoppers have when things go wrong with their personal details is also open to question. Sony PSN customers, for example, couldn't move to Xbox Live without abandoning their existing investment in the Sony platform and incurring some considerable costs. Many were trapped in a walled garden that they no longer trusted as being secure or safe.

Buying into walled gardens in a limited way as a consumer, as above, is one thing. To exist in a walled garden of information is quite another, about which there has been growing concern in recent years and with one particular company as its focus. In fifteen years, Google has grown from garage to gargantuan. It provides answers to some 90% of all search queries and is arguably now the single most important company on the web. But for all its successes, for all the innovative services it has bestowed upon the web and made available to users, businesses and governments, Google has proved one thing above all: the web works because of advertising. It was with extraordinary prescience, that Ken McCarthy predicted, in 1994, our current malaise, having allowed marketers and advertisers to accede to a powerful position of influence over the internet. And so it is, that for all the money at its disposal, and for all the incredible talented minds among its ranks, Google is seemingly unable to carve a significant revenue stream outside of AdWords. This has huge implications for users, businesses and governments on the web, and has given rise to what now seems to be a cat-and-mouse game of user privacy breaches by the internet's giants, followed by punitive measures from governments and regulators that only serve to conjure up images of pea shooters and heavy armour. How do we unshackle the web from the yoke of advertising? This is where we need our brightest and best to focus their attention: harvesting user data for advertisers and marketers should be just one of multiple ways — and, ideally, no longer most lucrative or attractive — for businesses to provide profitable, sustainable, innovative web services. We need a new generation of start-ups that are prepared to meet this challenge, who want to create businesses that do more than cultivate marketing fodder for advertisers, and who are prepared to respect the rights of users as a first principle and aim higher than just an IPO or lucrative takeover.

As users, we have to more effectively realise our agency as citizens of the web. What started with Mosaic, which runs through the Napster episode to BitTorrent and Pirate Bay, and to Google and the myriad services they supply — that is the establishment of free as first preference for the web — arguably has to stop, at least in its current guise. Contracts, and make no mistake this is what those T&Cs are, are drafted at great expense and designed to be legally bulletproof, not to protect the end user, but to protect the interests of the issuing company. While this is nothing new, what has changed is the frequency with which we now encounter and enter into legally binding contracts. It would once have been the case that in the course of one's life signing contracts was reserved for, if not milestone events, then at least for those of some significance: on commencing employment for certain, for a bank loan perhaps, or to acquire a credit card, on the occasion of marriage, or buying a house. By virtue of their infrequency we treated contracts respectfully, fearfully even, and, for most of us at least, we would give each its due consideration before signing and agreeing to the terms they held. By increasing the frequency with which we are presented with T&Cs, the internet has debased the seriousness of contractual obligations between parties, at least in context of the internet itself. For the most part, we feel sufficiently removed from the implications of these contracts that they simply do not exist for us. We are flies in honey and, having gorged ourselves on the wealth of apparently free services, it may now be that we are stuck. We have collectively failed to grasp the implications of what are very simple mechanisms of exchange: providers — about whom we often know very little — give us access to services in exchange for a limited transfer of rights over our personal data. How limited is anyone's guess. What they can do with it, where it may end up, and to what end? Ditto. We have little understanding about what we are actually signing over, and even less about what the implications of that might be, though we may be slowly waking up to it.

Certainly, businesses are satisfied with arrangements as they are, and can be expected to keep pushing services to users, eager to sign-up for whatever is this week's new Evernote/Instagram/Pinterest/Tumblr. There is perhaps hope though, in that business remains a fairly singular beast and predictable, to a degree, as a result. Someone will respond to meet a given demand, whether it is established businesses or newcomers. What EMI or Fox couldn't work out, Spotify and Netflix eventually did. It is perhaps then incumbent upon us to demonstrate that we want another web and, perhaps, that we are prepared to pay for it. This is a considerable challenge, akin to the proverbial turning of the tanker. The idea of paying for intangible products and services — and by this we mean those that can be delivered in bits and bytes over the web — runs contra to the behavioural norms that have established themselves since the advent of Napster. In the eyes of some observers, the nearly decade long spree of free has devalued cultural output irreparably by creating a generation of users who refuse to pay for digital music or movies. How to reconcile our new expectations when buying online cultural products will be a crucial feature of the web's development in its third decade.

What the Napster story demonstrates most clearly is the inability of both the established entertainment industry and governments to understand technology. P2P and BitTorrent protocols made the sharing of content — intellectual property — across borders so simple that it almost immediately rendered the concept of copyright irrelevant. What was previously difficult to rip, replicate or remix suddenly became easy and free, leading the recorded music industry to spend millions of dollars in the US suing its own customers — ironically enough, the very people who, time and time again, would be shown to be among their very best customers (Doctorow, 2011). They have spent similar amounts, with similarly little effect, in lobbying governments to protect their old business models. The net effect in both instances has been the same, and technology continues to reliably outpace copyright law and there is no reason to think this should change. Despite the global success of Apple's iTunes, Amazon's mp3 store or Netflix, there has been a fundamental failure to address the complete irrelevance of regional markets in the internet age, and we are sadly no closer to doing away with regional release dates or technical protection measures that restrict content to regions. There are no technical reasons why a global marketplace for goods is not possible, only legislative or political ones. Internet users instinctively understand this; repressive governments and giant companies who got rich off of divide and conquer tactics instinctively shy away from it. This, when combined with the often laughable claims produced by the entertainment industry and their advocates on the effects of piracy, appears to have reduced the legitimacy of these companies in the eyes of consumers who, in many cases, simply want to purchase content they are told they cannot have.

The implications of this situation could be far-reaching. If the big entertainment companies have their way there will be greater restrictions on the use and re-use of digital content by the artists and creators of tomorrow, and legislative overreach that could threaten services such as YouTube, Facebook or Reddit today, and also stifle the emergence of their future successors. Less likely, though still of some concern, is that poorly-drafted copyright legislation might lead to fundamental changes in the Internet's architecture in order to restrict access to certain websites, something that will undoubtedly contribute to an awkward standoff in terms of technologies to facilitate and evade detection online. At a time when a talented teenager can circumvent any of the technical roadblocks put in place by governments, the wisdom of continuing to drive potential consumers underground to a world of torrent sites, cyberlockers and freenets must be questioned. Alternatively, it could turn out that copyright is really this generation's prohibition, and the post-Napster period will ultimately lead to a rejection of an outdated concept and a new wave of innovation, new social norms on creation and sharing, and far less influence for giant entertainment corporations. However, if this is to happen then copyright frameworks are going to be have to be redrawn to reflect the global nature of the Internet — and the appetite among policy makers for doing this is not yet evident. The emergence of a two-tier Internet — one for those who know how to use all of the potential the technology has to offer, and one for those in the slow, legally constricted slow lane, is a real possibility.

When considering that two-lane Internet however, let us not forget that for many of the world's Internet users, it's already here. Our paper has mainly concentrated on the influence that the U.S. and major U.S. companies have had on the internet's development, but the case of China's Great Firewall draws our attention to the information inequality that exists in large swathes of the rest of the world as a result of governments censoring websites or monitoring Internet use. While avoiding detection to download the latest Lady Gaga single is difficult to paint as heroic, avoiding detection to post details of an illegal protest is a far braver deed — although in the world's most repressive internet regimes the consequences for doing so can far outweigh what the RIAA or MPAA can possibly impose.

The rise of Internet censorship and surveillance detailed in our case study is unlikely to come as a surprise to future students of history. Nation states have always shown a tendency to monitor their populations, and the internet is merely another tool to help them hoover up vast amounts of information. The net effect of increased surveillance is, in nearly all states that remain at least partly open to the wider world, likely to be either passive citizen resentment, or active resistance that takes advantage of all that online technologies offer. What makes the situation a heady mix in the 21st century however, is the extent to which private companies are providing technologies to facilitate surveillance, or collecting information on their users that governments may find useful to access at a later date. This intermingling of the private sector with the public, with the aim of uncovering private information, has seen the Iranian government use Nokia's technology to monitor their own citizens in the Green Revolution, or the Egyptian Government forcing Vodafone to send its subscribers anti-revolution messages during the Arab Spring. The vast amounts of information now being collected in the digital age, whether it is volunteered publicly on social networking sites, or stored privately in the cloud by third parties, is of tremendous interest to all governments whether they are in pursuit of terrorists, revolutionaries or common-or-garden criminals. How to get at this information is the trick they are desperate to pull, and every year sees more purported anti-terror legislation that tries to open up back doors to social networks or VOIP services.

At the heart of this is the issue of control — can anyone ever win this battle in the face of the disruptive technology now at the disposal of over two billion people on the planet? Maybe not, but that won't stop the world's giant institutions trying. 'Civilising' the Internet, a la Nicolas Sarkozy, means subjecting its users to the same degree of regulation that exists offline. For Russia and China, making the Internet civilised means having control of what information can and cannot be seen and spread by users, and choking off the types of online discourse that could create trouble for the country's rulers. The US dominance of the Internet's backbone institutions, such as ICANN, is viewed warily from those outside of the west, and any opportunity, such as the World Conference on International Telecommunications (WCIT) in December 2012, will be taken to try to grab back some sort of control of what is, after all, a most dangerous medium for non-democratic regimes. On the other hand, it is very much open to question just how much the Internet can really be controlled, and user awareness of the extent to which governments can monitor is rising, with tools such as TOR or anonymising VPNs becoming more commonplace. The transparency movement, whether led by Wikileaks or the hackers of Anonymous, also continues to grow, and no less a person than Tim Berners-Lee has urged users to take back control of their personal data from Google and Facebook. Expect the continuation of a high-stakes arms race in the near future, and even the prospect of 'Internets', as famously mis-spoken by George W.Bush - governments shutting themselves off from the wider Internet, in an effort to 'do a China', or even increasing amounts of 'cyber warfare' to defend one's turf or exploit another's. For every advance that diverts the flows of bits and bytes

— whether they be carrying music, movies or leaked documents that could bring down a regime — in new, unexpected directions, there will be a counter-measure in the form of legislation, subterfuge, or even plain old repression that comes with a knock on the door in the middle of the night. The struggle for control will continue and while those who understand the technology of anonymity may be able to watch from the sidelines, a substantial portion of the world's Internet users may well end up being 'civilised' in ways they may eventually find uncomfortable.

On the flipside, anyone that doubts that, given certain circumstances, users have the power to influence and change the web need only look at the volte face that wiped millions off the value of, first Friendster, and then MySpace. Herd-like sudden migrations were the ruin of both companies and their rise and falls stand as testament to the volatility of any social business venture on the web. Facebook may currently reign supreme but regardless of how permanent a feature it may appear to be today, it will itself eventually fall victim to some as yet unknown plucky newcomer if, that is, it doesn't first fall victim to what seems to have been a gross misvaluation in its recent IPO. Despite its brief moment at the top, the fiercely enthusiastic youth membership that formed around MySpace changed social networks from niche pastimes into common sites of exchange and communication which, for many, have now replaced email as their primary means of electronic communication. As a result, previous distinctions between the public and private spheres have been completely and irrevocably reconfigured. Collectively, we've thrown ourselves into social networking with the same kind of enthusiasm a cash-strapped student might muster for a paid psychological experiment, and without having first found out what the test is, how long it might last, what the risks might be, or how much we might get paid for it. The present is produced, published and preserved for posterity in the same moment. We have numerous services to satisfy our whims as consumers and our aspirations as authors, yet we remain unable to publicly fund a true digital library; a comprehensive common holding of recognised knowledge. No Library of Utopia# for us, not just yet.

We are instead, facing considerable philosophical questions that require an informed public discussion, with the broadest participation possible, to debate the information that is collected about us, by whom, and to decide what can and should be done with it. Businesses would love to be able to build up whole-life profiles of users — see Google's recent UK advertising campaign as brazen evidence of this — to be able to hone their predictions of user behaviours and anticipate habits before they have formed. Similarly governments — more febrile than ever post-9/11 — also need little encouragement that more data is inherently good, for them who govern at least. However, it is arguably of equal import to the development and evolution of both ourselves and our societies that we forget. The ever falling costs of data storage threaten a tyranny of abundance: we can, so why not? There are things we should remember and those we should forget, some to be preserved and those best discarded, and the value is, perhaps, as much in the choosing as anything. We may none of us live forever, but our personal data — our thoughts, feelings, likes and dislikes — just might and, we could have very little say in the matter.

The EU's pursuit of a 'Right to Privacy' roused a number of voices recently, many of whom were quick to decry it as impractical and unworkable. Whatever transpires with regards to that, there is still room for another solution. Privacy, as Cory Doctorow has recently pointed out,# is a business opportunity and it is entirely possible that DuckDuckGo may be the first in a coming wave of alternative providers, offering familiar services but differentiating themselves on the basis of their privacy and data preservation policies. 24hr tweets? A finite Facebook? It may not be our existing providers that venture there and, perhaps, even if it were there would be certain brand contamination issues that would have to be surmounted, but it will happen. It may not prove popular with governments, it may not entice marketers or advertisers in the same way

Google or Facebook do, but it will appeal to users who, having seen a generation above them inadvertently submit themselves to a lifetime of ‘managing their online brand’, will wish to redefine their relationship with their online selves and reclaim a little of their souls in the process.

Several of our case studies indicate a growing relationship with the web and ancillary technologies that may not be entirely healthy. Are we now technophile magpies building nests of shiny things, lining the walls with reviews of shiny things, and adorning them with leaked pictures of shiny things that may or may not eventually come to pass. Whether it’s a new iPhone, Google Goggles, or some mythical Facebook app — the app to end all apps — there is now a vast archive of techno-consumerism masquerading as journalism. While many of these publications are home to some invaluable commentary on many of the meta-level issues around internet governance and user privacy developments, they do have to pay the bills and for many of them it’s a question of footfall and ad-clicks and, in the technology pages at least, what once would have been referred to as ‘info-tainment’ and rigorous journalism now live side-by-side. Traditional news media also has to make ends meet and, following year after year of falling ad revenues for their print publications, many are looking at ways of monetising their online offerings, whether it’s the Guardian’s iPad app or the Wall Street Journal’s paywall, all are moving into the online space in an effort to stem falling revenues. One wonders about the coincidence of this fall in revenue and, for instance, the sharp uptick in Twitter headlines over a similar period. As newspaper proprietors migrate to the online environment, we should perhaps be concerned about the extent to which search engine optimisation (SEO) considerations could impact the veracity of our journalism.

It is perhaps not quite such a controversial suggestion when considered against the backdrop of the so-called Twitter revolutions of 2009 and the Arab Spring that later defined 2011. Together, these represented an outbreak of popular protest on a scale unseen since the wave of revolutions that followed the collapse of the Soviet Union in 1989, and the western news media were quick to characterise the role of social media as critical catalyst in the uprisings. Would readers have been as interested without the Twitter headlines? Sadly, perhaps not. This episode can be seen as yet another expression of the increasingly fevered and insufficiently critical enthusiasm for technology that now permeates much of western culture and its news media. The true complexity of what actually occurred is only now beginning to emerge, but it is clear that it was not quite so simple as tweets overturning governments. Through this episode we got a glimpse of the shifting relationship between traditional news media, social media and the rise of ‘citizen journalism.’ It also served as some indication of the damage wrought by the tyranny of the efficiency dogma: news outlets with with ever falling revenues, at a loss over how to replace lost TV and print advertising revenues, scale back on international correspondents, lean more heavily on citizen journalism and overplay — irrespective of whether or not this was consciously done — the instrumentality of a western technology, such as Twitter. It is perhaps also not entirely a coincidence that this should occur as the West is reeling from the huge financial shocks of 2008, and is having to come to terms with a dramatic shift in economic influence towards the east.

All of the issues raised in this paper must now be considered against the increasing number of people on the planet who now access the Internet primarily via a mobile device. There are now 1.1 billion 3G subscribers worldwide and this number is growing at 37% per year (Meeker, 2012). Many of the internet’s next billion users will be entirely free from a fixed-line connection and who may well view our desktop browsers as something of an anachronism. The implications of this are stunning: our mobile phone operators are the new ISPs; iOS, Android and Microsoft themselves — although somewhat late to the party — are all vying to be the

Windows of the new mobile space. Because of the legacy of the platform — the mobile phone's roots as a simple, single-purpose device — our expectations are very different from those of the personal computer, and we have so far been accepting of new levels of control over what applications we get to use, what we get to buy, and who is able to see where we are and what we are up to. The glare from our mobile's screens may make the future seem bright, but the reality may end up being somewhat different. As we migrate to a new mobile web, we may find that new technologies once again raise many of the same questions we have considered here. We can only hope that the questions raised by our case studies continue to be asked of the coming mobile web.