CYFY
THE INDIA CONFERENCE ON CYBER SECURITY AND INTERNET GOVERNANCE

ORF CYBER MONITOR

CYFY 2015 14th to 16th October

VOLUME III | ISSUE 8 | AUGUST 2015 | http://cyfy.org

COMMENTARY

US to Rewrite Controversial Cyber Export Rule

Deepak Maheshwari

Earlier this year the US Department of Commerce published a rule which would impose new export regulations on cybersecurity services and products. Why is it now being reconsidered?

Making Digital India Successful

Srinath Sridharan

Indian PM Narendra Modi launched Digital India Week on July 1, highlighting various schemes intended to integrate government departments and make services available to citizens using the internet.

Internet for All

Vignan Velivela

The internet has become a truly global communication system connecting people across the world. Its growth has been fuelled by various factors, but why aren't more people on the internet?

Bringing Down the Digital Berlin Wall

Shubh Soni

The creation of a digital single market is the natural next step in European integration, designed to boost Europe's share of the online economy. But it will be no easy feat to bring down the Digital Berlin Wall.

Immoral Hacktivism

Anahita Mathai and Bedavyasa Mohanty

The hacking of the Ashley Madison website raises several questions not only about the nature of hacktivism but also about anonymity, privacy and when users should entrust their personal data to websites.

The Observer Research Foundation's monthly round-up of the biggest stories making international headlines in cyberspace.

ESSENTIAL READINGS

STATEMENTS

Turn to Page # 16

EDITORIAL

Associate Editors: Anahita Mathai, Bedavyasa Mohanty

US to Rewrite Controversial Export Rule on Cybersecurity

Deepak Maheshwari

The Issue

In May 2015, the United States Department of Commerce published a controversial new export control rule, titled *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*. This rule would impose far-reaching new export regulations on cybersecurity services and products and have detrimental effects on the cybersecurity industry and the security of the Internet.

By way of background, the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (hereinafter referred to as 'Wassenaar') is a multilateral export control regime amongst its 41 participating countries that, in turn, decide whether and how to control export of any particular item. India is not currently a member. However, during his visit to India in November 2010, U.S.President Barack Obama supported India's bid to join Wassenaar.

Wassenaar is not a treaty, and therefore is non-binding. The decision to transfer or deny transfer of any export item is the sole responsibility of each participating country that implements the rules at their own discretion and through their respective national legislation and policies.

The Implication

Should the U.S adopt the rule as proposed, intrusion and surveillance systems software, and technology would be added to the Commerce Control List (CCL) under the Department of Commerce Export Administration Regulations (EAR).This would necessitate specific export licenses for these items. Such requests would lead to large numbers of licenses per company, in some cases even running into thousands every year.

In a world where malware and zero-day vulnerabilities are causing widespread damage, compliance with such regulations would not only make the process needlessly cumbersome, it would result in significant delays in development, distribution and deployment of critical solutions. Considering the number of R&D facilities of U.S. companies in India that would be impacted by this rule, the burden of export licensing paperwork would likely bring the licensing system to a halt; and India is just one export destination.

The Purported Objectives & The Unintended Consequences

While the rule was intended to protect national security interests and preserve human rights, it is predicated on the faulty presumption that software and systems designed or modified for the generation, operation, or delivery of, or communication with, "intrusion software" are "hacking" tools that are *all* used for nefarious purposes.

This is simply not the case. In fact, Symantec – and virtually every other legitimate organization engaged in cyber security – uses such tools to ensure the security of their own networks and products.

The unintended consequences of the proposed rule on the cyber security ecosystem would be severe, including:

- Restricting access to legitimate cybersecurity technologies and testing tools across borders – *even among security professionals who work for the same company*.

- Curtailing research into cybersecurity vulnerabilities and their associated exploits, as researchers would be hindered from testing networks and sharing the results and technical information across borders.

- Limiting cybersecurity threat information sharing and collaboration on cybersecurity risks both within cybersecurity companies and with customers and industry partners, as information would be deemed "exported" if it is shared with *any* non-U.S. persons, even if they are physically located in the U.S and employed by a U.S. company.

The Department of Commerce has also stated in the rule that there would be a presumption of denial of licenses for items that have or support rootkit or zero-day exploit capabilities. These items are among the most important for cybersecurity professionals to share and work with to find fixes. Because of their great importance, the proposed rule would make it almost impossible to make progress in dealing with these most dangerous of threats.

Indeed, the scope of the rule is very broad. As written, it would cripple cyber security organizations' ability to share cyber threat and vulnerability information around the world. No cybersecurity company or its customers can afford to wait months for a license before addressing a vulnerability, or deploying testing tools. What's more, drawing restrictions broader than is absolutely necessary simply in an attempt to catch all potentially malicious tools will not limit, to any effective degree, the transfer of those nefarious hacking tools. It would only bolster cybercriminals and rogue regimes and hamstring legitimate researchers working to detect and provide protections against malicious activity.

The Comments

More than 260 comments were received by the Department of Commerce – including from technology companies, their customers, trade associations, and even Members of Congress. From India, NASSCOM and DSCI also sent in a joint response. The industry and end users alike all urged the Department of Commerce to reconsider the proposed rule, explaining the adverse impacts it would have on cybersecurity in the U.S. and around the world.

The Way Forward

On 29 July 2015, the Department of Commerce announced that they will develop a substantially revised rule. The intent is to take into consideration the comments provided by industry and other interested parties; then draft a revised rule that will not undermine the use and development of security technologies.

While this reconsideration does offer a respite, Symantec believes the best approach is for the U.S. to return to Wassenaar in 2016 and reopen the original agreement. This would allow for a thorough review that takes into account the serious negative impacts it currently has on global cybersecurity.

The Broader Lesson

While policymaking remains the prerogative of governments, it is of utmost importance to include the private sector and civil society early on in the process and stay the course throughout the engagement and technical negotiations. Equally, the private sector also needs to engage early to help governments see the wider implications of the policies that they are considering. Public-private partnerships are a critical avenue to ensuring that necessary exchanges take place to develop sound public policy, and to avoid unintended consequences that may harm global industries or security in the future.

The author is Head of Government Affairs, India Region, Symantec.

Making Digital India Successful

Srinath Sridharan

Prime Minister Narendra Modi kicked-off the Digital India Week on July 1 to create awareness about e-governance and encourage greater public involvement. As part of the programme the PM has launched various products and schemes intended to integrate government departments and services and making them available to citizens using the internet. These include a digital locker to minimize the use of physical documents, the mygov.in platform to engage with citizens and disseminate information and government services and, an e-sign framework allowing for online document authentication using Aadhar number. On the infrastructure side the government also plans to build the architecture to connect the country using optical fiber.

Governments around the world are moving services online to meet citizen demand and capture benefits of digitization. For example, in Estonia, residents can use electronic identification cards to vote, pay taxes and access more than 160 services online, from unemployment benefits to property registration. The United Kingdom's gov.uk site serves as a one-stop information hub for all government departments. Such online services provide greater access for rural populations, improve quality of life for those with physical disabilities and offer options for those whose work demands don't allow access to services during typical daytime office hours. In the developed world, the focus of the digital policy has shifted from development and implementation of building blocks of information infrastructure to digital interaction of the government with business and citizens.

A successful e-governance platform will take into consideration 4 factors:

1. **User Centricity**, which looks at online availability and usability. Online availability assesses the existence of an electronic channel for public services either through a portal or standalone. Online usability looks at the overall user experience by assessing ease and speed of use.

2. **Transparency** examines the extent to which governments are transparent about their own responsibilities and performance, the service delivery process and any personal data involved.

3. **Cross Border Mobility** involves giving businesses and citizens seamless access to online public services when they are away from their country.

4. **Key Enablers** measures the availability of five technical elements which are essential for public services: Electronic Identification (eID), Electronic documents (eDocuments), Authentic Sources, Electronic Safe (eSafe) and Single Sign On (SSO).

The government of Netherlands has been at the forefront of the digitization process, *redesigning all government service processes*. In 2011, the Netherlands released i-NUP(National Implementation Program for E-Government Services), its overarching government implementation agenda for e-government services to prioritize user-centered design by boosting convenience and trimming red tape. The implementation rules state, "We do not pose superfluous questions. Data included in one of the basic registrations will not be asked for again." As per the implementation, municipalities serve as "citizens' desks" and act as the first line of contact for citizens. They are supported by a website, customer-contact center, and central phone number. All of the municipalities have been connected to a single access

number. The plan required an overhaul of the country's government-to-business services. To make that happen, the Dutch launched a comprehensive digital-infrastructure project led by the national digital-governance agency, Logius which created a government-wide dashboard to highlight project status, risks and used conferences and social media to disseminate and refine key lessons with public-sector IT managers around the country.

The architecture of the program set up a system of base registries consisting of 13 base registries with common information services and standards. The base registries are databases comprising data which are needed for a broad range of government services. The data is stored under the principle of multiple reuse, interoperability and common information services and standards. This enabled all government departments to access the data without requiring the citizens to provide information for use of public services. As a result of these initiatives, physical visits to municipalities and government offices have decreased significantly and service levels have increased.

Compared to the developed world, India has a long way to go, but Digital India week can become that launch-platform that will take digital government services to the people and cut down bureaucracy that has constantly kept India in the bottom of global competitiveness rankings. For Digital India to be a success, access to, affordable and user friendly digital platforms are a prerequisite. As of 2011, the literacy rate in India stands at 74% and only about 10% of the population, i.e. 120mn people speak English and the rest vernacular. Even though India boasts the third largest online population in the world, internet penetration stands at only ~19%. Internet access has been increasing in India with rural areas reaching 101 million users in October 2014, whereas urban India had 177 million subscribers in October 2014. This however belies that fact that for most of rural India's internet usage is extremely low and they are only just discovering the uses of the internet. This is the reality on the demand side of the digital revolution.

The supply side, in terms of government services does present a dismal picture. For example, India currently has 32 million court cases pending and it can take 10-15 years to get cases resolved. To take justice to the masses, this process has to be expedited by computerizing court records, police and prisons. All financial institutions, including banks and insurance companies offer their range of services online, but the uptick of these even amongst the educated urban class has been poor largely due to lack of awareness or security concerns with regard to payments. All banks provide banking services via net-banking including payments, transfers, loans, credit cards, saving products and insurance for rural India too. While the use of POS machines and business correspondents has helped financial inclusion, the use of digital by customer to transact has not yet taken place. Rural India has been excluded from this digital revolution that is occurring in the cities. As of 2014, only 0.3% of adults used mobile money, compared to 76% in Kenya, 48% in Tanzania, 43% in Uganda, and 22% in Bangladesh. This is due to many reasons, but lethargic and outdated regulation has been the major cause. More importantly, the Reserve Bank of India allows non-banks to participate in payment services in two ways; they can build and manage an agent network on behalf of a bank; or they can issue a "semi-closed" wallet which allows customers to cash-in, buy airtime and other services, but not cash-out. Experience in Africa has shown that m-pesa and other mobile money services took-off only when cashing out was allowed. This regulatory framework has ensured that India's banks control not only the market for savings and credit, but also payments. Banks on their part have struggled to innovate and move away from branch based approaches (again due to RBI regulations on branches and distance restrictions on BCs) and legacy technologies to establish digital payment connections in poor and rural communities. With such a scenario, it's unsurprising that only 0.3% of Indian adults use mobile money.

Technology has so far not been able to level the playing field for the rural population. The digital revolution is not about the urban, the elites or Bollywood. It is for everyone. India should take a leaf out of its bigger neighbor's book and promote more vernacular content and provide government content in regional languages. China through protection of its internet economy has allowed local behemoths to appear and grow like Alibaba, Weibo and others. All content is available in Mandarin and therefore more inclusive, something India needs to learn and implement. While lack of knowledge and awareness is certainly a major deterrent

to digitization in rural India, another reason is that of language. Currently, almost all of the services and information available online are in English. Social media sites, news sites and even search engines are available in many languages but, for most people who do not read English, services like online shopping, banking and even government services remain inaccessible via the internet. The purpose of accessing internet in rural India, as per an i-cube survey, is primarily for entertainment, communication and social networking. If the digitization process continues in the country as is, more than 70% of the population will be able excluded from internet based services mostly because this population is unaware of the possible value addition digital can bring to their lives.

To gain the maximum benefits out of the digitization process, the government should redesign the service delivery processes rather than simply re-engineer them for online access. The redesign process should imply a "**digital by default**" approach, in which citizens gain the right to interact with government in a digital way. The general principle for the interaction should be 'digital where possible and personal where needed'. Offline access should be maintained for citizens who for any reason cannot access them online. But, they should be one stop shops for all services and not a separate platform for every government department, service and office. The government is a single body and not an amalgamation of departments and a digitization must reflect this whole.

All this said, Digital India cannot be restricted to only broad band internet users. Even as the PM plans to connect the length and breadth of the country through optic fibres, this is no easy task. Broadband internet penetration in India is only 19%but mobile penetration, especially smart phones, and DTH have greater and far flung reach. Disruptive technological innovations are the need of the hour to make available not just government services but any kind of service through other mediums of digital. This would necessarily mean reengineering our processes and not merely redesigning them. The definition of digital must include simplification of processes. A cumbersome digital process is no better than a cumbersome offline process. Digital India will be a success only if it is inclusive; if not, it will only create two more castes – the digital caste and the digital outcaste.

The author is a member of the Group Management Council – Rajesh Wadhawan Group; member of the Board of Directors – DHFL Pramerica Life Insurance Ltd; and Visiting Fellow at ORF.

Internet for All

Vignan Velivela

Since its birth in the labs of ARPANET half a century back, the internet has risen to create a truly global communication system connecting people across the world. The last two decades have seen users rising from forty million to over 3 billion, with one billion added in the last four-five years alone. This exponential growth is fueled primarily by three factors: a robust and resilient global network, the growth of cheaper and powerful computing driven by the Kurzweil curve and an ecosystem of relevant services created by new companies powered by network effects.

Why aren't more people on the Internet?

Internet users today are predominantly urban since the vast majority of investments by the telecom industry went into solving the problem of capacity and complexity while not investing enough in accessibility. Case in point, the United States. Over 17% of its population has no access and around half of rural Americans lack quality internet access. The problem is not merely economic (lower rural revenue, higher capex) as often argued, but also because of technological limitations. In a developing country such as India, this problem is compounded by the lack of reliable support infrastructure (like grid power).

To solve the last mile connectivity problem, we must design a network with the end user in mind. Smartphones today provide the lowest point of entry ($ 30-35 Android) to the internet and over a billion of them are being produced annually. To bring the next four billion people on to the internet in the next few years, wireless (3G/LTE/WiFi) should act as the primary access network.

Governments and internet majors have been pursuing multiple approaches to solve this problem. Among private companies, two of the leading internet companies are pursuing interesting methods to provide connectivity. Google with its Project Loon is creating a worldwide network of high-altitude balloons which would connect directly to a user's smartphone through 3G and LTE. Each of their balloons has a coverage area of 5000 sq km, meaning around 600 of them would be needed to cover the whole of India. These balloons can now communicate among themselves for as long as 80 km and in chains, meaning not a lot of investment in telecom backhaul and ground stations is needed. Although these balloons are difficult to navigate since they rely only on stratospheric winds, it is a fun problem to solve. As Google is perfecting WiFi to cellular handoffs with Project Fi, its new role as an MVNO (virtual network), balloons and drones (Titan) may play a crucial role in its roaming success. Facebook through their Connectivity lab is developing stratospheric drones which would use a mix of laser and radio links to connect to ground receivers and also create an aerial drone-based backhaul network. Facebook's drones are still in the prototyping stage and details of their delivery model are not yet available in the public domain.

The Case for Satellite Internet

A promising new approach to connectivity is by the proposed small satellite constellations of SpaceX, OneWeb, LeoSat and Yaliny. These satellites would be in low earth orbit altitudes (around 1000-1200 km) meaning the latency of their connection would be similar to fibre (<30ms). Current satellite internet services have high latencies (>300ms) due to the distant location of their satellites (geostationary - 35786km). Although not all internet applications need low latencies, it is crucial for communication services like Voice over Internet Protocol, messaging and transactional services like banking. Also, satellites would need far fewer hops to connect to international content delivery networks compared to fibre-based networks, meaning countries in Africa where most fibre connections still have very high latency can now be serviced with faster connections.

At the receiver end, OneWeb and SpaceX are developing low-cost (USD 100-300), solar-powered transceivers which would provide 3G, LTE and WiFi connectivity to local communities. OneWeb has a constellation size of 648 satellites with a combined throughput of 10Tbps and each transceiver can provide services at upto 50Mbps. SpaceX has a more ambitious plan of launching around 4000 satellites from 2019 until 2030, predominantly to serve the international backhaul market which today operates on a network of undersea cables carrying over 95% of international traffic. Yaliny is developing a handheld satellite transceiver which would connect to the user and provide unlimited data at $10 per month. LeoSat is primarily targeting enterprise customers such as Telecom backhaul, Defence, Oil & Gas and would deliver bandwidth as high as 1.2 Gbps.

Two important issues that crop up on the regulatory front are spectrum allocation and landing rights. OneWeb has been granted the global license to operate in the non-geo Ku-band by the International Telecommunication Union if they become operational by 2019. But it isn't clear how new satellite constellations would be allotted such spectrum while operating relatively free of interference. SpaceX's application for permission from the US Federal Communications Commission to test two of its satellites has already drawn objections from Intelsat. On the issue of landing rights, OneWeb would be partnering with domestic telecom operators using their ground stations and gateways to beam internet, therefore they may not confront many domestic regulatory road blocks. It is not clear at this point how SpaceX would be delivering their services to the end user. Yaliny is perhaps most prone to governmental scrutiny since they would be operating based on a network of international ground stations.

India

In India, the second largest telecom market, internet penetration is still estimated to be around 20% although rural and urban teledensity stand at 45% and 148% respectively. Over 90% of Indian internet users connect to wireless networks and 65% of the traffic flows through them. These numbers are no different compared to sub-Saharan Africa because telecom networks in developing nations today are predominantly built for voice (2G) and not data communications. Although average revenue per user (ARPU) in rural ($1.5) and urban ($2-2.5) areas does vary, the lack of connectivity can be attributed majorly to the high CapEx (costly backhaul) and OpEx (off-grid diesel power) of existing technologies.

The Government of India is developing BharatNet as part of the Digitial India program, a revamped and larger version of the National Optical Fibre Network (NOFN) which plans on providing fibre optic connectivity to most of the 2.5 lac Gram Panchayats (GPs, moderate size villages). The projected cost of the project stands at $12 Billion with around 75% cost going into laying the optical fibre to connect 2.26 lac GPs. Of the rest, 20 thousand GPs would be connected wirelessly and 3000 through satellite internet. At the village level, community WiFi would be provided to local institutions such as schools, post offices and health centres along with cable internet provided to households.

The Indian government can take proactive steps to augment the capacity and reach of BharatNet by following open standards in integrating them with private internet ventures to ensure interoperability. ISRO, India's national space agency, can launch more geostationary satellites (like the INSAT) to increase the throughput over its territory. This would allow traffic to be diverted from low altitude systems for applications such as video, news and less interactive content which wouldn't need low latency connections. These geostationary satellites can also be used to empower community-defined broadcasting services like Outernet. Other models such as building small satellite platforms in highly elliptical orbits (like Molniya) can be explored to improve performance over specific regions.

Possibilities

The internet is the most important invention of the 20th Century. It has changed the way people communicate, cooperate, learn and trade globally. Four key areas which would experience the direct and positive effects of ubiquitous internet coverage are healthcare, education, agriculture and governance. Innovations in

technology are rapidly miniaturizing and reducing costs of diagnostic devices and new drone-based delivery networks (Matternet) are making medicines more accessible, meaning early detection and fast remedial actions can now be made universal. Education will face a similar disruption when the best educators in the world can reach a virtual classroom of hundreds of thousands of students while also personalizing their learning experience. Small satellites (like those of Planet Labs and Skybox) are democratising satellite imagery meaning agricultural production and the environment among others can now be monitored in near real time and smart tools can be built for farmers across the world to improve their productivity and incomes.

Peter Diamandis opens his book *Abundance* with a story on aluminium. When the King of Siam visited Napoleon III's court, Napoleon was himself served in gold utensils while the honoured guest was served in aluminium utensils. Although it is the third most abundant element on Earth, aluminium was the costliest metal until the 19th century. With the invention of electrolysis, we were able to make aluminium one of the cheapest and most accessible metals today. The conflict over net neutrality arose primarily because bandwidth has been perceived as a scarce resource. Exponential innovation can create abundance through a combination of cheap smartphones and global connectivity allowing us to avert such conflict.

Never before in human history could we expand our circle of empathy and develop a collective consciousness encompassing the whole of humanity. This could be our first chance!

The author is a Research Intern at ORF.

Bringing Down the Digital Berlin Wall

Shubh Soni

The European single market was established in 1992 with the aim of removing internal physical barriers and thereby enabling free movement of goods, services, persons, and capital, across European borders. The next step in this European integration naturally then is the creation of a single digital economy, which has been rolled out this year. Currently, a number of barriers, which are not prevalent in the physical space, exist in digital economy, hampering economic growth in the continent. The Digital Single Market (DSM) is an ambitious proposal that looks to bring down the regulatory walls and boost Europe's share of the online economy- it is expected that initiative will add €415 million to the European GDP by creating opportunities for new start-ups while allowing existing companies to further expand their market base.

The DSM strategy is based on three pillars- the first looks to provide **better access to online goods and services across Europe** by (i) devising a unified, simple, and modern framework to foster enterprise; (ii) tackling delivery issues by improving price transparency and regulatory over sight of parcel delivery; (iii) ending unjustified geo-blocking; and (iv) simplifying VAT payment procedures.

The second pillar aims at **creating the right conditions for digital networks and services** by (i) creating a harmonised framework within which individual Member States can implement policy regarding management of spectrum; and (ii) by launching a comprehensive assessment of the role of platforms, including in the sharing economy, and of online intermediaries, which will cover issues such as transparency; how platforms use the information that they get; relations between platforms and suppliers; difficulties faced by businesses and individuals to move from one platform to another; and the best ways to fight illegal content on the internet.

The third focuses on **maximising the growth potential of the European digital economy.** This will be done (i) by way of the 'Free flow of data' initiative which will focus on issues of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data; (ii) by upgrading the "European Interoperability Framework" to ensure better connectivity along supply chains or between industry and services sector; and (iii) through a pilot project titled 'Once-Only' principle (where public administrators reuse information about the citizen or companies that is already in their possession) which looks to empower businesses to expand online operations across borders within a month of establishment.

While the EU is optimistic about the growth potential of the strategy, there exist some very serious concerns. The first is the fear amongst industry, particularly U.S. companies, that the strategy is a protectionist tool being adopted by a region which has fallen behind in digital innovation and is trying to play catch-up. The Information Technology Industry Council (ITI), the global voice of the leading tech companies, has accused the EU of trying to create a digital "Fortress Europe" which will fracture the open internet market and sour relationships between the U.S. and Europe.

It is not just the U.S. which is concerned with these developments- within Europe too there are a number of dissenting voices. For instance, policy-makers in Europe have highlighted the lack of clarity on how the DSM plans to push its reform agenda by pointing towards a contradiction between the stance of the DSM and individual Member States on Big Data. The DSM strategy highlights how the generation, collection, and aggregation of large sets of information creates new value and potential for consumers, firms, and public authorities. Member States however have on more than

one occasion expressed their displeasure at companies generating and using big data for profiteering, benefits of which are not always passed on to the country where such data is generated.

There is also the fear of loss of market should "unification" take place. For instance, some of Europe's top film directors have argued that the new rules would decimate the European film industry. From their point of view, a unified market across Europe would handicap producers as they would no longer be able to finance films by selling them to individual countries across Europe. Further they argue that by providing access across borders the initiative will aid dominant market players (read: large American networks such as Netflix) and adversely affect local language cinema.

While the U.S. and European stakeholders have voiced concern and sought clarification on how the DSM will impact their digital industry, their Indian counter-parts are looking for synergies between the Indian Government's "Digital India" initiative and the DSM. As the Ambassador of the European Union to India, Dr João Cravinho, pointed out at #Digilogue2015 (on 27th April, 2015), these synergies "could be implemented by closer cooperation on important topics such as standardisation in information and Communication technologies (ICT) as well as ICT research and innovation". However there still exists a lack of clarity as to whether any synergies even exist between the two initiatives, and what will be the potential impact of DSM on Indian industry and thereby the India-EU digital relationship.

The author is a Research Assistant at ORF.

Bringing Down the Digital Berlin Wall

Shubh Soni

Last week, Avid Life Media, the Canadian firm which owns cheating website AshleyMadison.com (slogan: 'Life is Short. Have an Affair') was hacked. Personal information, credit card details, sexual fantasies and potentially explicit chat logs of almost 40 million users have reportedly been compromised.

The website confirmed the hack, saying it was likely perpetrated by an insider. But this was not just another hack leaking random financial information. These hackers (or hacker), calling themselves 'The Impact Team' were on a mission to get Ashley Madison and its sister website, Established Men, shut down.

Why Ashley Madison? The nature of the website has led to assumptions that this was a hack by digital do-gooders, outing and punishing the unfaithful. There was a certain lack of remorse for the victims in the message left by the hackers: "Too bad for [these] men, they're cheating dirtbags...", but the main reason for targeting Ashley Madison seems to be the way the website handles former users' data.

The website had a controversial 'full delete' feature, which required a payment for all personal and purchase details to be erased. In fact, the hackers claim that the company retains this information even after deletion – and that's what's allegedly been stolen.

What Anonymity?

Many of Ashley Madison's users may only have dared to dabble in infidelity because of the discretion the website claimed to provide. Inhibitions tend to be reduced when you are behind a computer screen, whether you're posting comments on YouTube or chatting up a potential date. The availability of services and features provided by the internet combined with the potential for anonymity makes for a heady cocktail. The mistake that many users seem to be making is assuming that the secrecy provided by websites like Ashley Madison is equivalent to privacy – in the real world or online.

So, what does the Ashley Madison hack mean for online privacy? The hack stands out among other privacy leaks of the recent past in its apparent lack of malice. It is different from other invasive hacks like doxing where people's personal information is dumped on the internet with the intent of harming the person. It seems to be aimed at rectifying the company's practice of wrongfully retaining users' personal information.

But that does not detract from the equally damaging effect of this attack. In fact, the damage is more pronounced because The Impact Team is allegedly a group of 'privacy hacktivists' threatening a massive privacy breach – a breach that will not only affect Ashley Madison users personally but will breach the associational privacy of their spouses and have financial consequences.

Earlier, privacy was erroneously conflated with a complete lack of access to one's personal information. This has proved increasingly difficult to reconcile in a world where data is currency and entire economies are sustained on the cloud. Privacy debates have moved away from that conception. Now, informational privacy is increasingly seen as retaining control over data about oneself. This is what the hackers seem to be addressing: That the website does not allow users control over permanently deleting data that they created.

Perceived Dangers

However, informational privacy also includes the right to determine how information about oneself is used and appropriated. The fact that these hacktivists have resorted to misusing other peoples' information to drive home a point only strengthens the increasing

paranoia about an open internet and sets the privacy discourse back by years.

In fact, it is the unreliability of traditional cyber systems that drives people towards the darker corners of the internet like the deep web. The deep web has long served as an online hub for some of humanity's darkest indulgences – from drugs to child pornography. It only seems natural that, with time, clandestine activities like online adultery will move towards these dark corners. But even that is only a temporary relief.

The deep web is not absolutely secure. The advent of newer technologies like quantum computing will render privacy safeguards redundant in the next decade or so. It is only a matter of time before another hack like this threatens to destroy companies and ruin their customers' lives and we see a rerun of this tale of two victims.

The authors are Junior Fellows at ORF.

This article originally appeared in The Quint, July 25, 2015,

ESSENTIAL READINGS

COMMENTARIES

Chris Stewart, "It's time to take cyberattacks seriously and install a deterrence plan",*The Washington Post*, July 23, 2015

Benjamin Wittes, "Thoughts on Encryption and Going Dark Part II: The Debate on the Merits",*Lawfare*, July 12, 2015

P.W. Singer and August Cole, "The Reality of Cyberwar: World War III would be unlike any other conflict",*Politico Magazine*, July 9, 2015

Joe Davidson, "Lack of digital talent adds to cybersecurity problems",*The Washington Post*, July 19, 2015

Gautam Bhatia, "Sorry, Mr. Attorney-General, We Do Actually Have a Constitutional Right to Privacy", *The Wire*, July 28, 2015

JOURNAL ARTICLES

Martin GiljeJaatun, "Security in Critical Information Infrastructures", *Department of Electrical Engineering and Computer Science, University of Stavanger*, Dissertation, July, 2015

Michael L. Rustad&SannaKulevska, "Reconceptualising the Right to Be Forgotten to Enable Transatlantic Data Flow", *Harvard Journal of Law & Technology*, Volume 28, Number 2, July 2015

Scott Shackelford,"On Climate Change and Cyber Attacks: Leveraging Polycentric Governance to Mitigate Global Collective Action Problems" Social Science Research Network, July 13, 2015

REPORTS

Eric Jardine, Global Cyberspace Is Safer Than You Think: Real Trends In Cybercrime, Global Commission on Internet GovernanceJuly 2015

KadriKaska and Lorena Trinberg, Regulating Cross-Border Dependencies of Critical Information Infrastructure, NATO Cooperative Cyberdefence Centre of Excellence, July, 2015

TCS Global Trend Study, Internet of Things: The Complete Reimaginative Force, Tata Consultancy Services, July, 2015

Juan C. Zarate,The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response, Foundation ForDefense of Democracies, July, 2015

BOOKS

Gideon Samid, *Tethered Money: Managing Digital Currency Transactions*, Academic Press, July 28, 2015

Robert Ratcliffe, *Daemon*,CreateSpace Independent Publishing Platform, July 3, 2015

Jean-Loup Richet,*Cybersecurity Policies and Strategies for Cyberwarfare Prevention*, IGI Global, July 17, 2015

Bryan Seely,*Cyber Fraud: The Web of Lies*, Amazon,July 15, 2015

Ross Blankenship, *Cyber Nation: How Venture Capital & Startups Are Protecting America from Cyber Criminals, Threats and Cyber Attacks*, CreateSpace Independent Publishing Platform July 9, 2015

Opening of Digital India Week

Highlights of the Address by Narendra Modi, Prime Minister of India

New Delhi, India – July 1, 2015

I dream of a Digital India where High-speed Digital Highways unite the Nation.

I dream of a Digital India where 1.2 billion Connected Indians drive Innovation.

I dream of a Digital India where Knowledge is strength – and empowers the People.

I dream of a Digital India where Access to Information knows no barriers.

I dream of a Digital India where Government is Open - and Governance Transparent.

I dream of a Digital India where Technology ensures the Citizen-Government Interface is Incorruptible.

I dream of a Digital India where Government Services are easily and efficiently available to citizens on Mobile devices.

I dream of a Digital India where Government proactively engages with the people through Social Media.

I dream of a Digital India where Quality Education reaches the most inaccessible corners driven by Digital Learning.

I dream of a Digital India where Quality Healthcare percolates right up to the remotest regions powered by e-Healthcare.

I dream of a Digital India where Farmers are empowered with Real-time Information to be connected with Global Markets.

I dream of a Digital India where Mobile enabled Emergency Services ensure Personal Security.

I dream of a Digital India where Cyber Security becomes an integral part of our National Security.

I dream of a Digital India where Mobile and e-Banking ensures Financial Inclusion.

I dream of a Digital India where e-Commerce drives Entrepreneurship.

I dream of a Digital India where the World looks to India for the next Big Idea.

I dream of a Digital India where the Netizen is an Empowered Citizen.

Read the full speech here (in Hindi).