

**A PRIMER ON
'REGULATION OF CYBER SPACE
AND RIGHT TO INTERNET'**

Executive Note:

It is our absolute pleasure to welcome you all to the Committee for Control and Regulation of Cyber Space at VIT Technical United Conference 2016. It is our distinct privilege to serve you all as the Executive Board of the Committee.

Having said that, this primer should be the first step towards your research but it must be kept in mind that this is not all exhaustive research on this agenda and hence we are expecting you to research further on the given agenda and its sub topics using this primer as your guide. We have identified the major topics under this agenda in this guide but research on the same is expected from your side. The Executive Board has not seen it fit to list the Questions that a Resolution must answer since that will be entirely dependent on the manner in which the committee probes and explores an agenda. Only Reuter's reports will be accepted by the Executive Board as proof of the fact that the United Nations Organization recognizes something to be fact. Delegates may use reports by official government sources/agencies only against that particular government/agency.

We believe that the agenda is not that complex in nature and is something that has seen a lot of debate on in recent times in the Indian context and thus we expect participation from all the delegates in the councils, first time delegates and veterans alike. We will be holding a feedback session on the effectiveness of this study guide on Day 1 of the council and are looking forward to your comments on the same.

We want to especially emphasize on the need for solutions that you propose in councils to be viable and practical in terms of their implementation and should be having reasonable prospects of working out because being a delegate in an international legislative body, the practicality of everything mechanism you propose is extremely important and is something we will be giving a lot of importance.

Delegates are especially requested to be well versed with basic principles of international law, their foreign policy and display diplomatic courtesy befitting that of a representative in an international body. Regardless, whether this is your first time or one of many conferences, we look forward to impassioned and rigorous debates in the days to come. Feel free to contact the Executive Board in case of any doubts/query.

Wishing you the best of luck with your preparations.

Regards,

Srijesh Sudarsanan
Chairperson

Shreyansh Banthia
Vice Chairperson

CONTENTS

ROADMAP TLDR)

I. A DISCUSSION ON RIGHTS, NATURE OF

- Defining characteristics of rights
- The Right to Internet, evolution of nature of rights

II. GUARANTORS OF RIGHT TO INTERNET

- Case studies of censorship heavy regimes
- Handling dissent, disapproval and angst

III. A DISCUSSION ON REGULABILITY OF THE INTERNET

- A review of ideological stances
- Challenges impeding regulability:

Ability Constraints

- Regulation of the dark web
- Regulation of disruptive agents and service providers
- Bit Coins and E Currency

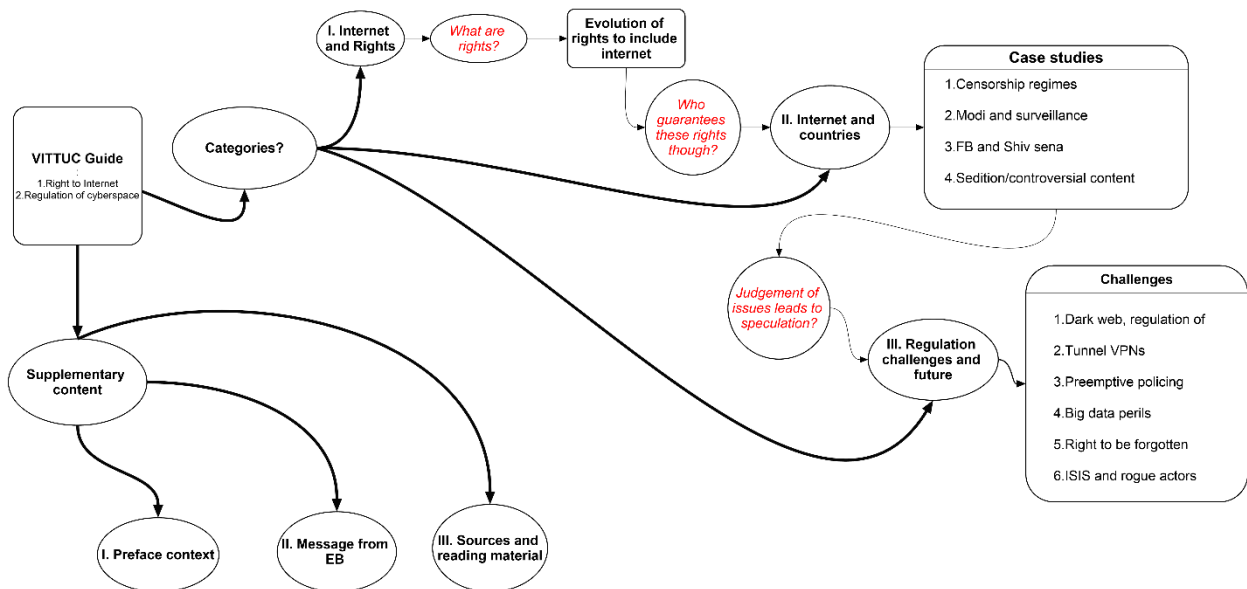
Ideological Challenges

- Big Data mining, the dilemma that is privacy
- The Right to be Forgotten

III. BIBLIOGRAPHY

ROADMAP (TLDR)

Roadmap



A DISCUSSION ON RIGHTS, NATURE OF

What are human rights?

Human rights are rights inherent to all human beings, whatever our nationality, place of residence, sex, national or ethnic origin, colour, religion, language, or any other status. We are all equally entitled to our human rights without discrimination. These rights are all interrelated, interdependent and indivisible. Universal human rights are often expressed and guaranteed by law, in the forms of treaties, customary international law, general principles and other sources of international law. International human rights law lays down obligations of Governments to act in certain ways or to refrain from certain acts, in order to promote and protect human rights and fundamental freedoms of individuals or groups.

Defining Characteristics of Rights

Universal and inalienable

The principle of universality of human rights is the cornerstone of international human rights law. This principle, as first emphasized in the Universal Declaration on Human Rights in 1948, has been reiterated in numerous international human rights conventions, declarations, and resolutions. The 1993 Vienna World Conference on Human Rights, for example, noted that it is the duty of States to promote and protect all human rights and fundamental freedoms, regardless of their political, economic and cultural systems.

All States have ratified at least one, and 80% of States have ratified four or more, of the core human rights treaties, reflecting consent of States which creates legal obligations for them and giving concrete expression to universality. Some fundamental human rights norms enjoy universal protection by customary international law across all boundaries and civilizations.

Human rights are inalienable. They should not be taken away, except in specific situations and according to due process. For example, the right to liberty may be restricted if a person is found guilty of a crime by a court of law.

Interdependent and indivisible

All human rights are indivisible, whether they are civil and political rights, such as the right to life, equality before the law and freedom of expression; economic, social and cultural rights, such as the rights to work, social security and education, or collective rights, such as the rights to development and self-determination, are indivisible, interrelated and interdependent. The improvement of one right facilitates advancement of the others. Likewise, the deprivation of one right adversely affects the others.

Equal and non-discriminatory

Non-discrimination is a cross-cutting principle in international human rights law. The principle is present in all the major human rights treaties and provides the central theme of some of international human rights conventions such as the International Convention on the Elimination of All Forms of Racial Discrimination and the Convention on the Elimination of All Forms of Discrimination against Women. The principle applies to everyone in relation to all human rights and freedoms and it prohibits discrimination on the basis of a list of non-exhaustive categories such as sex, race, colour and so on. The principle of non-discrimination is complemented by the principle of equality, as stated in Article 1 of the Universal Declaration of Human Rights: "All human beings are born free and equal in dignity and rights."

The Right to Internet, evolution of nature of rights

The 'normal' way of classifying these rights is into 'first, second and third generation' rights, so we shall follow this for the time being but, as we shall see, such a classification has limited use and can even be misleading at times.

First generation rights (civil and political rights)

It had begun to be recognized that there were certain things that the all-powerful state should not be able to do and that people should have some influence over the policies that affected them.

- Civil rights for example, the rights to equality and liberty, freedom to practise religion or to express one's opinion, and the rights not to be tortured or killed.
- Legal rights for example protection against arbitrary arrest and detention, the right to be presumed innocent until found guilty in a court of law and the right to appeal.
- Political rights for example, the right to vote, to join political parties, to assemble freely and attend meetings, to express one's opinion and to have access to information.

Second generation rights (social, economic and cultural rights)

These rights concern how people live and work together and the basic necessities of life.

- Social rights for example, the rights to recreation, health care and privacy and freedom from discrimination.
- Economic rights for example, a lack of meaningful employment or housing can be psychologically demeaning.
- Cultural Rights for example, the right to non-discrimination and equal protection of the laws.

Third generation rights (collective rights)

The list of internationally recognized human rights has not remained constant. Although none of the rights listed in the UDHR has been brought into question in the 50 or so years of its existence, new treaties and documents have clarified and further developed some of the basic concepts that were laid down in that original document. These additions have been a result of a number of factors: they have partly come about as a response to changing ideas about human dignity, partly as a result of technological changes and often as a result of new threats emerging.

The Right to Internet, the proposition

The Internet has revolutionized how people interact, allowing individual citizens to speak out freely in ways that were impossible. The Internet has made it much easier for people to access basic rights – **freedom of expression, freedom of association and assembly – and other civil rights**. For this reason, internet access for all – with a minimum standard of service – should be a public goal. Some tenets worth maintaining are:

The Internet should be available to all – regardless of age, place of residence or income.

Governments should recognize this as a right, both in law and in practice, and lay down universal service requirements that service providers must comply with, drawing on United Nations standards.

Web access should be affordable and secure, subject only to legitimate restrictions laid down by law, and

Data traffic should be treated without discrimination on a basis of strict “net neutrality”.
And so on.

Criticism is nevertheless voiced about regarding Internet access as a human right. One of the most cogent reviews has been presented by Vint Cerf, who is often presented as one of the creators of Internet. Cerf stated in a New York Times opinion that *“Technology is an enabler of rights, not a right itself”*. Cerf noted that Internet is an important means to an end, creating new possibilities for people to exercise their human rights. However, according to Cerf, acknowledging access to Internet as a universal service comes close to regarding access as a civic right. As a response to Cerf’s opinion, Amnesty International USA has noted that *Cerf’s view of human rights is particularly narrow and tantamount to contesting physical access to a town square as a human right without understanding that*

such access is inseparable from the right of association and expression.

Cerf points out that the *Internet is a specific technology that may come and be replaced. Thus, when we talk about fundamental rights, we should use language that is independent of any particular technology* so that our discourse on rights may stand the test of time.

As the power of the Internet and Web increases, the desire of governments and corporations to try to control, limit, or take over the Internet becomes stronger.

Recently this matter has come to a head, and people have started to ask whether the ability to participate in this empowered, connected society should be considered a right worthy of protection. We can perhaps consider access to the Internet as a human right, and conclude that urgent action is needed in promotion and defense of the Internet and the Web.

GUARANTORS OF RI

Several countries have acknowledged that access to Internet has become a focal tool for exercising freedom of speech and opinion and thus requires protection as a fundamental human right. As of 2011, national policies for promoting broadband access had been adopted in more than 100 countries worldwide. Also, agencies such as the Broadband Commission for Digital Development, joint project of the ITU and the United Nations Educational, Scientific and Cultural Organization (UNESCO), promote broadband policy making.

The European Union has recognized access to Internet as a universal service in Universal Service Directive (2002/22/EC) on universal service and user's rights relating to electronic communications networks and services. The directive obliges member States to ensure that requests for connection at a fixed location to the public telephone network are fulfilled. According to Article 4.2, "The connection provided shall be capable of allowing end-users to make and receive local, national and international telephone calls, facsimile communications and data communications, at data rates that are sufficient to permit functional Internet access, taking into account prevailing technologies used by the majority of subscribers and technological feasibility" [emphasis added].

National courts have also started to consider Internet access as a crucial commodity for daily life. The German Federal Court of Justice (Bundesgerichtshof) came to this conclusion in its recent decision (III ZR 98/12) on 24 January 2013, as it granted compensation to a plaintiff who was disconnected from accessing Internet between December 2008 and February 2009 due to the service provider's failure to provide connectivity. The court ruled that access to Internet had already become of central importance for individuals as it: offers access to a wide-range of information globally – replacing traditional media such as television and print media and enables communication between users.

Before those in the 'developed' countries think they can rest easy in the assumption that nominally democratic countries will preserve their rights, note that the **SOPA and PIPA**

acts in the USA, the DEA in the UK, the Hadopi in France and so on show that governments are, as quietly as possible, giving themselves the legal right to cut off the Internet access of people, households and companies; to spy on Internet traffic; and to have web sites blocked on suspicion of criminal activity without a trial. In the US and France, it is the companies themselves that want to play judge and jury, without any oversight or democratic governance. We have a responsibility to protest when rights are surreptitiously removed.

In the US, the unprecedented online protest sparked by activists and the Internet blackout against SOPA and PIPA occurred not only inside the USA, but because the effects of filtering DNS (Domain Name System) are international, these laws provoked truly international outrage. Yet at the same time, many governments quietly signed the ACTA agreement which commits signatories to passing similar laws without public discussion. Violations of net neutrality contravene the right to Internet access. At the birth of the Internet, there was a largely informal guarantee of net neutrality, so that the data sent across the Internet would not be discriminated against based on their origin or receiver. In the United States and Europe, companies are currently pushing to end net neutrality over wireless Internet connections and provide a 'two-tier' model where pay-as-you-go services become faster than free services. It's hard to determine whether this violates the right to freedom of expression, but it definitely violates a popular expectation for the right to access content on the Internet without discrimination. As these kinds of abuses are new, they are not covered by the right to freedom of opinion and expression by itself.

10 Most Censored Countries

The 2015 list of 10 Most Censored Countries is part of CPJ's annual publication, *Attacks on the Press*. These repressive nations threaten jail terms and restrict Internet access to silence press

1. Eritrea

Fearing the spread of Arab Spring uprisings, Eritrea scrapped plans in 2011 to provide mobile Internet for its citizens, limiting the possibility of access to independent information. Although Internet is available, it is through slow dial-up connections, and fewer than 1 percent of the population goes online, according to U.N. International Telecommunication Union figures.

2. North Korea

In place of the global Internet, to which only a select few powerful individuals have access, some schools and other institutions have access to a tightly controlled intranet.

3. Saudi Arabia

Saudi Arabia, where the ruling monarchy, not satisfied with silencing domestic dissent, teamed up with other governments in the Gulf Cooperation Council to ensure that criticism of leadership in any member state is dealt with severely

4. Ethiopia

The threat of imprisonment has contributed to a steep increase in the number of journalist exiles. Amid a broad crackdown on bloggers and independent publications in 2014, more

than 30 journalists were forced to flee.

5. Azerbaijan

There is little independent traditional media, criminal defamation laws have been extended to social media and carry a six-month prison sentence.

6. Vietnam

Vietnam (sixth most censored) uses a vague law against "abusing democratic freedom" to jail bloggers,

7. Iran

Iran, the seventh most censored country, has one of the toughest Internet censorship regimes worldwide, with millions of websites blocked; it is also the second worst jailer of journalists, with 30 behind bars. Authorities there are suspected of setting up fake versions of popular sites and search engines as part of surveillance techniques.

8. China

Document 9 made it clear that the role of the media is to support the party's unilateral rule. The paper reasserted the necessity for China's technological and human censors to be ever more vigilant when keeping watch over the country's 642 million Internet users—about 22 percent of the world's online population.

9. Myanmar

The Printers and Publishers Registration Law, enacted in March 2014, bans news that could be considered insulting to religion, disturbing to the rule of law, or harmful to ethnic unity. Publications must be registered under the law, and those found in violation of its vague provisions risk de-registration.

10. Cuba

Although the Internet has opened up some space for critical reporting, service providers are ordered to block objectionable content. Independent journalists and bloggers who work online use websites that are hosted overseas and must go to foreign embassies or hotels to upload content and get an unfiltered connection to the Internet. These critical blogs and online news platforms are largely inaccessible to the average Cuban, who still has not benefited from a high-speed Internet connection.

Africa and the Internet

While blatant attempts to censor the Internet like the Zambian example are rare, concerns are growing that African governments will exert their control over content and access to the Internet by maintaining and extending their monopolies on telecommunications services.

In many African countries, these services are obstructed by inefficient state-owned post and telecommunications companies (PTCs). Despite their failure for years to provide adequate telephone services, these companies have moved into the Internet market with remarkable speed. Twenty-six African PTCs have brought full Internet services to their

countries in the last few years.

In all but three of those countries, the PTC has assumed a monopoly in the provision of Internet services, although few have officially defined themselves as the only provider. Many African governments would like to maintain sole access to revenue from the new technology, and some also view it as a way to control access to and information on the Internet. Either way, government monopoly of telecommunications is a threat to freedom of expression online.

Article 19 of the International Covenant on Civil and Political Rights states that it may be limited as far as is necessary in a democratic society to protect national security, public order, health and safety, public morals, and the rights and freedoms of others.

Reports that the Internet may be facilitating a proliferation of extremist 'hate' groups are posing difficult legal and ethical questions. A report by a special investigator to the United Nations Human Rights Commission in March 1997 stated that racism is increasing worldwide and that the Internet 'has already conquered the imagination of the people with a message where those who incite the hatred, the racists and the anti-Semites, all participate.' In Africa, there is evidence that extremist groups are coming online. The Broederbond - South Africa's most powerful secret society, made up of men who managed the design and implementation of apartheid, has set up a website.

Although all references to race and gender have been removed from its constitution, the Broederbond has as its objectives: 'Activities with individual Afrikaans speakers, associations, organizations, or groups of the Afrikaans community to protect their rights and interests, including economic, social, educational, cultural and religious.'

A Web notice-board about Kenya contains information about a fictitious Kenyan rebel movement and some calls that 'Asians must go'. Chat rooms provide little or no trace of users and are prime forums for those intent on peddling pornography and fomenting racial and religious hatred.

The balance between protecting free expression online and ensuring that the rights and dignity of others are protected is an extremely delicate one and must be applied carefully.

ON THE REGULABILITY OF THE INTERNET

A review of ideological stances

Lawrence Lessig's 4 modes of regulation (**Digital realists**):

Norms / Education

In order to function and be accepted in a society, a person will live by its norms. You believe in the role of educating people so that new norms may develop as new technology is used.

As an example of the change of attitudes that result from education programs you might look back on smoking ads that once portrayed cigarette smokers as beautiful, sophisticated, sexy people with the ads of today, where a blackened sponge is wrung out to show the impact of smoking on the lungs.

Law

You believe in parliament's capacity to make laws to regulate the behavior of its citizens. Where parliaments are silent, the courts will make precedents. People who break the law suffer sanctions - these can be civil penalties of loss of money when an infringing party is ordered to pay damages to another. There is also criminal law through which you believe society establishes what constitutes acceptable and unacceptable behavior.

Architecture

You believe in the power of human to design systems that regulate behavior. To control speeding in a back street you would design and build speed humps. In a digital world you believe in the power of software code to be able to create a form of regulation. For example, you might design a technological protection measure in your software that prevents a program with a license of ten users from allowing an eleventh user to open it over a network. You find education / norms too slow to bring about change. You find law too expensive. You can design the world you want and have people regulate their

behaviour because such restrictions in behavior are inherent in what you have created.

Market Forces

You are convinced that market forces regulate behavior. If a manufacturer creates an unsafe product this will become known to the market and consumers will not purchase these products. If a software designer wants to copyright and license his or her work, then the market will determine if the software is worth buying as compared with that of competitors. Markets will determine what survives and what doesn't in the market place.

Digital libertarians' / anarchists

Barlow's 'Cyberspace Declaration of Independence' (1996):

Regulation will fail; Internet cannot be regulated. Nations have *no right* to regulate 'new realm of mind'

Trotter Hardy - The 'proper regime' (1994)

Decentralized regulation is efficient. Decentralized power is the '*proper* regime'

Filters on Internet content

As stressed in the Danish debate on B46, and also in both judgments on CDA and COPA, *filters are also over broad in scope; they restrict more than intended by the inherent moral norms*. Recalling the European Court's principle of non-discrimination, we can therefore argue that should authorities by legitimate means restrict individuals' right to receive information, then this restriction should be applied in a nondiscriminatory fashion. The non-discriminatory principle is also part of the UNESCO Universal Service Principle outlined in chapter four, whereby Internet shall be accessible by all individuals, on a non-discriminatory basis regardless of geographic location. I would argue that **applying filters to Internet access in public libraries is discriminatory in two senses**.

- Firstly, it discriminates against those citizens who have no other means of Internet access, thereby undermining the equalizing aspect of providing Internet in public libraries as stressed in the Danish IT-policy. Citizens with no access to the public sphere of Internet are currently restricted in their information access and have no other means but the physical public space to seek information and express their opinions. They are excluded from the radically stronger means of appearance on Internet, hence referred to the physical public sphere and its inherent limitations. Providing Internet in public libraries is a means for ensuring cyber-access for all. When the library restricts Internet access by the use of mandatory filters, they discriminate the citizens who access Internet through their public library by allowing them to access only a limited part of the cyber conversations.
- Secondly, applying filters on Internet in public libraries also provides for discriminatory information access, since information is being excluded on normative grounds (defined by private parties) that are neither visible nor transparent to the individual seeking information in the public sphere of Internet. As stressed in the Danish debate on B46, in the CDA judgment and in the lawsuit on CHIPA, filter software with built-in norms (model 1) is overbroad in scope thus restricting more content than intended by the norms⁸⁶. But even if filters functioned perfect, we could still argue, that it is disproportionate to restrict

individuals' right to receive information by technical means, that determine which legal information should be accessible for adults and which should not.

The issue of cyber assemblies exemplified by Jubii and AOL touches the very core of cyberspace being a public, private and commercial sphere, but managed by private parties. The question points to the dilemma of whether to perceive cyber assemblies as public sphere - where communication is protected under the right to freedom of expression -, or whether to perceive them as privatized meeting forums, thus subject to privatized restrictions. Currently, they are services provided for in the commercial sphere of cyberspace connected to commercial content providers. Since they are privately managed, it implies a legitimate right to subject the services to restrictions; for instance by **automatically altering expressions** such as "dick" or "whore" in order to **secure a "clean" environment**. AOL and Jubii are commercial parties, and they have a legitimate right to regulate according to the codes of their system. Or do they? It all depends on whether we apply a system or lifeworld perspective.

Challenges impeding regulability

The dark web

Recent years have seen a dramatic growth in the sale of a variety of illicit substances on Dark Net drug markets, with on line sales projected to increase exponentially due to expanding internet availability, evolving technologies and the profusion of social media.

This new form of retail market poses a major challenge to not only law enforcement agencies but also the UN international drug control system and related legal structures within which these agencies operate.

For vendors and purchasers who use the sophisticated, user friendly and increasingly secure Dark Net sites, hidden markets present a safer environment for drug transactions and they reduce the multiple risks (coercion, violence, arrest, exposure to other drugs) associated with 'street' sales.

The 2016 **UN General Assembly Session (UNGASS)** on the World Drug Problem is a timely opportunity to discuss reform of the UN drug control treaty system to better deal with the challenges of the increasingly complex illicit drug market in the twenty-first century.

Outlining the challenge this type of transnational, remotely operated web based criminal network posed to traditional law enforcement, the head of e-crime at SOCA set out that ShadowCrew was distinct from the 'old-style "top down" organized crime groups

(Tor) 'a technology that bounces internet users' and websites' traffic through "relays" run by thousands of volunteers around the world, making it extremely hard for anyone to identify the source of the information or the location of the user'.

Breach of Privacy and Confidentiality (Hacker groups and disruptive agents)

It means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected. Generally for protecting secrecy of such information, parties while sharing information forms an agreement about the procedure of handling

of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monetary gains and causes breach of contract of confidentiality. Special techniques such as Social Engineering are commonly used to obtain confidential information.

Jurisdiction and sovereignty

Issues of jurisdiction and sovereignty have quickly come to the fore in the era of the Internet. The Internet does not tend to make geographical and jurisdictional boundaries clear, but Internet users remain in physical jurisdictions and are subject to laws independent of their presence on the Internet.

As such, a single transaction may involve the laws of at least three jurisdictions:

1. The laws of the state/nation in which the user resides,
2. The laws of the state/nation that apply where the server hosting the transaction is located, and
3. The laws of the state/nation which apply to the person or business with whom the transaction takes place. So a user in one of the United States conducting a transaction with another user in Britain through a server in Canada could theoretically be subject to the laws of all three countries as they relate to the transaction at hand.

Bit Coins and E currency

Bitcoin first appeared in January 2009, the creation of a computer programmer using the pseudonym Satoshi Nakamoto. His invention is an open source (its controlling computer code is open to public view), peer to peer (transactions *do not require a third party intermediary such as PayPal or Visa*) digital currency (being electronic with no physical manifestation).

The Bitcoin system is private, with *no traditional financial institutions involved* in transactions. Unlike earlier digital currencies that had some central controlling person or entity, the Bitcoin network is *completely decentralized*, with all parts of transactions performed by the users of the system. Their identities are encrypted and no personal information is transferred from one to the other. However, unlike a fully anonymous transaction, there is a transaction record. *A full transaction record of every Bitcoin and every Bitcoin user's encrypted identity is maintained on the public ledger*. For this reason, Bitcoin transactions are thought to be pseudonymous, not anonymous. Although the scale of Bitcoin use has increased substantially, it still remains small in comparison to traditional electronic payments systems, such as credit cards, and the use of dollars as a circulating currency. **Congress is interested in Bitcoin because of concerns about its use in illegal money transfers, concerns about its effect on the ability of the Federal Reserve to meet its objectives (of stable prices, maximum employment, and financial**

stability), and concerns about the protection of consumers and investors who might use Bitcoin.

Bitcoin offers users the advantages of

- Lower transaction costs and freedom from failing banking sectors.
- Increased privacy
- Long-term protection of loss of purchasing power from inflation.

However, it also has a **number of disadvantages** that could hinder wider use. These include

- Sizable volatility of the price of Bitcoins,
- Uncertain security from theft and fraud,
- Long term deflationary bias that encourages the hoarding of Bitcoins.
- In addition, Bitcoin raises a number of legal and regulatory concerns including its potential for facilitating money laundering, its treatment under federal securities law, and its status in the regulation of foreign exchange trading.

Aspersions about security, a brief review

- In January 2015, Bitstamp, a large European Bitcoin exchange, suspended services after a security breach involving the loss of 19,000 Bitcoin, valued at about \$5 million.
- Hackers mounted a massive series of distributed denial-of-service attacks against the most popular Bitcoin exchange, Mt. Gox, in 2013. About 850,000 Bitcoin valued at over \$400 million were stolen. Mt. Gox subsequently declared bankruptcy.
- In late August 2012, an operation titled Bitcoin Savings and Trust was shut down by the owner, allegedly leaving around \$5.6 million in bit coin-based debts
- In September 2012, Bitfloor, a Bitcoin exchange, reported being hacked, with 24,000 Bitcoins (roughly equivalent to \$250,000) stolen. As a result, Bitfloor temporarily suspended operations.
- On April 3, 2013, Instawallet, a web-based wallet provider, was hacked, resulting in the theft of over 35,000 Bitcoins. With a price of \$129.90 per Bitcoin at the time, or nearly \$4.6 million in total, Instawallet suspended operations.
- On August 11 2013, the Bitcoin Foundation announced that a bug in the software within the Android operating system had been exploited to steal from users' wallets.
- October 23 and 26, 2013, a Bitcoin bank operated from Australia but stored on servers in the United States was hacked, with a loss of 4,100 Bitcoins, or over 1

million Australian dollars.

Has Bitcoin failed to achieve lift off?

It's pretty simple, really. For any medium of exchange to displace another as a means for buying stuff, users need come out ahead. And this isn't happening with bitcoin.

We can break any exchange medium's user base into *consumers* and *sellers*. Now we know that sellers love bitcoin—they've been adopting it at a blistering pace, from Amazon to Microsoft to CVS. No wonder when we consider the cost savings they enjoy. A merchant is required to pay around 1.5-2.0% for each credit card transaction. Bitcoin payment processors like Coinbase, Bitnet, and Bitpay charge just 0.5% while simultaneously absorbing all of merchant's forex risk. A retailer with \$1 million in sales that converts all of its shoppers from Visa/MasterCard payments to bitcoin has just earned themselves \$10,000.

While sellers are jubilant, consumers aren't. Tim Swanson shows that bitcoin payments haven't budged in over a year with bitcoin processor Bitpay's transactions volume amounting to a piddling \$57.5 million or so in 2014 (not including precious metals and mining). Bitpay controls at least a third of the payments market. That's what failure looks like.

This aborted takeoff can be blamed on the fact that the dominant consumer payments medium, the credit card, leaves the consumer with significantly more resources after each payment than bitcoin does. Consider the fact that consumers are always paid in U.S. dollars (or whatever their respective national currency happens to be). At the same time, sellers price their wares in dollars and accept payment in that unit, the dollar being both the dominant unit of account and medium of exchange. This is highly convenient to consumers. If someone wants to buy an annotated hard cover edition of *War & Peace* for \$100, they never have to leave the dollar ecosystem.

The **top 10 countries for BTC merchants' adoption** to date that make up Bitcoin Country are as follow: *Italy, United States, United Kingdom, Finland, Australia, Singapore, Netherlands, Canada, Slovenia, and the most accommodating location of Bitcoin Country is Isle of Man.*

Bitcoin has been the de facto currency of the Dark Web – the 'hidden' Internet accessible only by Tor – since the pioneering marketplace Silk Road, the 'eBay of drugs', arrived in 2011.

Refer: <http://www.coindesk.com/bitcoin-on-the-dark-web-the-facts/>

Ideological challenges

Data Mining

A few relevant applications are as follows:

- Sentiment analysis of twitter messages
- Analyze web-site visitors; what makes a customer leave your web page?

- What type of news articles do you like?
- Personalized suggestions
- Find influential persons in a community of bloggers
- Targets for viral marketing
- Which customers are likely to “churn”
- What kind of customers like a specific offer?
- Which promotions to offer to a customer?
- Which promotions to offer to a customer?

Data mining in policing

- Predict crimes: type, location, time, time of the year.
- Learn characteristics of people that wear concealed weapons.
- Find patterns in crimes; eg. Sudden increase in burglaries in one particular area.

Perils and ideological issues

Potential dangers include interpretation of results

- Implication is not causality
- Simpson’s Paradox
- Privacy issues
- False discoveries
- Discriminating models
- Combining different sources may lead to privacy issues

An illustration of why mining data and usage of conclusions is pernicious

If lenders think that race is a reliable proxy for factors they cannot easily observe that affect credit risk they may have an economic incentive to discriminate against minorities

Thus, denying mortgage credit to a minority applicant on the basis of minorities on

average-but not for the individual in question- may be economically rational. But it is still discrimination, and it is illegal.

Right to be forgotten

In 2010 a Spanish citizen lodged a complaint against a Spanish newspaper with the national Data Protection Agency and against Google Spain and Google Inc. The citizen complained that an auction notice of his repossessed home on Google's search results infringed his privacy rights because the proceedings concerning him had been fully resolved for a number of years and hence the reference to these was entirely irrelevant. He requested, first, that the newspaper be required either to remove or alter the pages in question so that the personal data relating to him no longer appeared; and second, that Google Spain or Google Inc. be required to remove the personal data relating to him, so that it no longer appeared in the search results.

The Spanish court referred the case to the Court of Justice of the European Union asking:

- (a) whether the EU's 1995 Data Protection Directive applied to search engines such as Google;
- (b) whether EU law (the Directive) applied to Google Spain, given that the company's data processing server was in the United States;
- (c) whether an individual has the right to request that his or her personal data be removed from accessibility via a search engine (the 'right to be forgotten').

In its ruling of 13 May 2014¹ the EU Court said:

- a) On the territoriality of EU rules : Even if the physical server of a company processing data is located outside Europe, EU rules apply to search engine operators if they have a branch or a subsidiary in a Member State which promotes the selling of advertising space offered by the search engine;
- b) On the applicability of EU data protection rules to a search engine: Search engines are controllers of personal data. Google can therefore not escape its responsibilities before European law when handling personal data by saying it is a search engine. EU data protection law applies and so does the right to be forgotten.
- c) On the "Right to be forgotten": Individuals have the right - under certain conditions - to ask search engines to remove links with personal information about them.

This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purposes of the data processing (para 93 of the ruling). The court found that in this particular case the interference with a person's right to data protection could not be justified merely by the economic interest of the search engine. At the same time, the Court explicitly clarified that the right to be forgotten is not absolute but will always need to be balanced against other fundamental rights, such as the freedom of expression and of the media (para 85 of the ruling). A case-by-case assessment is needed considering the type of information in question, its sensitivity for the individual's private life and the interest of the public in having access to that information. The role the person requesting the deletion plays in public life might also be relevant.

Implications and precedence

The Court in its judgement did not elevate the right to be forgotten to a "super right" trumping other fundamental rights, such as the freedom of expression or the freedom of the media.

On the contrary, it confirmed that the right to get your data erased is not absolute and has clear limits. The request for erasure has to be assessed on a case-by-case basis. It only applies where personal data storage is no longer necessary or is irrelevant for the original purposes of the processing for which the data was collected. Removing irrelevant and outdated links is not tantamount to deleting content.

The Court also clarified, that a case-by-case assessment will be needed. Neither the right to the protection of personal data nor and the right to freedom of expression are absolute rights. A fair balance should be sought between the legitimate interest of internet users and the person's fundamental rights. Freedom of expression carries with it responsibilities and has limits both in the online and offline world.

This balance may depend on the nature of the information in question, its sensitivity for the person's private life and on the public interest in having that information. It may also depend on the personality in question: the right to be forgotten is certainly not about making prominent people less prominent or making criminals less criminal.

The case itself provides an example of this balancing exercise. While the Court ordered Google to delete access to the information deemed irrelevant by the Spanish citizen, it did not rule that the content of the underlying newspaper archive had to be changed in the name of data protection (paragraph 88 of the Court's ruling). **The Spanish citizens' data may still be accessible but is no longer ubiquitous. This is enough for the citizen's privacy to be respected.**

Google will have to assess deletion requests on a case-by-case basis and to apply the criteria mentioned in EU law and the European Court's judgment. These criteria relate to the accuracy, adequacy, relevance, including time passed and proportionality of the links, in relation to the purposes of the data processing (paragraph 93 of the ruling).

The criteria for accuracy and relevance for example may critically depend on how much time has passed since the original references to a person. While some search results linking to content on other web pages may remain relevant even after a considerable passage of time, others will not be so, and an individual may legitimately ask to have them deleted.

Refer: Factsheet on the “Right to be Forgotten” ruling (C-131/12).

BIBLIOGRAPHY

https://drive.google.com/folderview?id=0B_bK7-akJLapam10TnJvb0EzXzg&usp=sharing

The above given Google Drive link contains all the documents that were used in the creation of this primer and thus can be used by the delegates for initiating their research on the given agenda.