Introductory Statement

I would like to thank the European Parliament for the invitation to provide testimony for your inquiry into the Electronic Mass Surveillance of EU Citizens. The suspicionless surveillance programs of the NSA, GCHQ, and so many others that we learned about over the last year endanger a number of basic rights which, in aggregate, constitute the foundation of liberal societies.

The first principle any inquiry must take into account is that despite extraordinary political pressure to do so, no western government has been able to present evidence showing that such programs are necessary. In the United States, the heads of our spying services once claimed that 54 terrorist attacks had been stopped by mass surveillance, but two independent White House reviews with access to the classified evidence on which this claim was founded concluded it was untrue, as did a Federal Court.

Looking at the US government's reports here is valuable. The most recent of these investigations, performed by the White House's Privacy and Civil Liberties Oversight Board, determined that the mass surveillance program investigated was not only ineffective -- they found it had never stopped even a single imminent terrorist attack -- but that it had no basis in law. In less diplomatic language, they discovered the United States was operating an unlawful mass surveillance program, and the greatest success the program had ever produced was discovering a taxi driver in the United States transferring $8,500 dollars to Somalia in 2007.

After noting that even this unimpressive success – uncovering evidence of a single unlawful bank transfer -- would have been achieved without bulk collection, the Board recommended that the unlawful mass surveillance program be ended. Unfortunately, we know from press reports that this program is still operating today.

I believe that suspicionless surveillance not only fails to make us safe, but it actually makes us less safe. By squandering precious, limited resources on "collecting it all," we end up with more analysts trying to make sense of harmless political dissent and fewer investigators running down real leads. I believe investing in mass surveillance at the expense of traditional, proven methods can cost lives, and history has shown my concerns are justified.

Despite the extraordinary intrusions of the NSA and EU national governments into private communications world-wide, Umar Farouk Abdulmutallab, the "Underwear Bomber," was allowed to board an airplane traveling from Europe to the United States in 2009. The 290 persons on board were not saved by mass surveillance, but by his own incompetence, when he failed to detonate the device. While even Mutallab's own father warned the US government he was dangerous in November 2009, our resources were tied up monitoring online games and tapping German ministers. That extraordinary tip-off didn't get Mutallab a dedicated US

investigator. All we gave him was a US visa.

Nor did the US government's comprehensive monitoring of Americans at home stop the Boston Bombers. Despite the Russians specifically warning us about Tamerlan Tsarnaev, the FBI couldn't do more than a cursory investigation -- although they did plenty of worthless computer-based searching - and failed to discover the plot. 264 people were injured, and 3 died. The resources that could have paid for a real investigation had been spent on monitoring the call records of everyone in America.

This should not have happened. I worked for the United States' Central Intelligence Agency. The National Security Agency. The Defense Intelligence Agency. I love my country, and I believe that spying serves a vital purpose and must continue. And I have risked my life, my family, and my freedom to tell you the truth.

The NSA granted me the authority to monitor communications world-wide using its mass surveillance systems, including within the United States. I have personally targeted individuals using these systems under both the President of the United States' Executive Order 12333 and the US Congress' FAA 702. I know the good and the bad of these systems, and what they can and cannot do, and I am telling you that without getting out of my chair, I could have read the private communications of any member of this committee, as well as any ordinary citizen. I swear under penalty of perjury that this is true.

These are not the capabilities in which free societies invest. Mass surveillance violates our rights, risks our safety, and threatens our way of life.

If even the US government, after determining mass surveillance is unlawful and unnecessary, continues to operate to engage in mass surveillance, we have a problem. I consider the United States Government to be generally responsible, and I hope you will agree with me. Accordingly, this begs the question many legislative bodies implicated in mass surveillance have sought to avoid: if even the US is willing to knowingly violate the rights of billions of innocents -- and I say billions without exaggeration -- for nothing more substantial than a "potential" intelligence advantage that has never materialized, what are other governments going to do?

Whether we like it or not, the international norms of tomorrow are being constructed today, right now, by the work of bodies like this committee. If liberal states decide that the convenience of spies is more valuable than the rights of their citizens, the inevitable result will be states that are both less liberal and less safe.

Thank you.

I will now respond to the submitted questions. Please bear in mind that I will not be disclosing new information about surveillance programs: I will be limiting my testimony to information regarding what responsible media organizations have entered into the public domain. For the record, I also repeat my willingness to provide testimony to the United States Congress, should they decide to consider the issue of unconstitutional mass surveillance.

Rapporteur Claude Moraes MEP, S&D Group

Given the focus of this Inquiry is on the impact of mass surveillance on EU citizens, could you elaborate on the extent of cooperation that exists between the NSA and EU Member States in terms of the transfer and collection of bulk data of EU citizens?

- A number of memos from the NSA's Foreign Affairs Directorate have been published in the press.

One of the foremost activities of the NSA's FAD, or Foreign Affairs Division, is to pressure or incentivize EU member states to change their laws to enable mass surveillance. Lawyers from the NSA, as well as the UK's GCHQ, work very hard to search for loopholes in laws and constitutional protections that they can use to justify indiscriminate, dragnet surveillance operations that were at best unwittingly authorized by lawmakers. These efforts to interpret new powers out of vague laws is an intentional strategy to avoid public opposition and lawmakers' insistence that legal limits be respected, effects the GCHQ internally described in its own documents as "damaging public debate."

In recent public memory, we have seen these FAD "legal guidance" operations occur in both Sweden and the Netherlands, and also faraway New Zealand. Germany was pressured to modify its G-10 law to appease the NSA, and it eroded the rights of German citizens under their constitution. Each of these countries received instruction from the NSA, sometimes under the guise of the US Department of Defense and other bodies, on how to degrade the legal protections of their countries' communications. The ultimate result of the NSA's guidance is that the right of ordinary citizens to be free from unwarranted interference is degraded, and systems of intrusive mass surveillance are being constructed in secret within otherwise liberal states, often without the full awareness of the public.

Once the NSA has successfully subverted or helped repeal legal restrictions against unconstitutional mass surveillance in partner states, it encourages partners to perform "access operations." Access operations are efforts to gain access to the bulk communications of all major telecommunications providers in their jurisdictions, normally beginning with those that

handle the greatest volume of communications. Sometimes the NSA provides consultation, technology, or even the physical hardware itself for partners to "ingest" these massive amounts of data in a manner that allows processing, and it does not take long to access everything. Even in a country the size of the United States, gaining access to the circuits of as few as three companies can provide access to the majority of citizens' communications. In the UK, Verizon, British Telecommunications, Vodafone, Global Crossing, Level 3, Viatel, and Interoute all cooperate with the GCHQ, to include cooperation beyond what is legally required. http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq

By the time this general process has occurred, it is very difficult for the citizens of a country to protect the privacy of their communications, and it is very easy for the intelligence services of that country to make those communications available to the NSA -- even without having explicitly shared them. The nature of the NSA's "NOFORN," or NO FOREIGN NATIONALS classification, when combined with the fact that the memorandum agreements between NSA and its foreign partners have a standard disclaimer stating they provide no enforceable rights, provides both the NSA with a means of monitoring its partner's citizens without informing the partner, and the partner with a means of plausible deniability.

The result is a European bazaar, where an EU member state like Denmark may give the NSA access to a tapping center on the (unenforceable) condition that NSA doesn't search it for Danes, and Germany may give the NSA access to another on the condition that it doesn't search for Germans. Yet the two tapping sites may be two points on the same cable, so the NSA simply captures the communications of the German citizens as they transit Denmark, and the Danish citizens as they transit Germany, all the while considering it entirely in accordance with their agreements. Ultimately, each EU national government's spy services are independently hawking domestic accesses to the NSA, GCHQ, FRA, and the like without having any awareness of how their individual contribution is enabling the greater patchwork of mass surveillance against ordinary citizens as a whole.

The Parliament should ask the NSA and GCHQ to deny that they monitor the communications of EU citizens, and in the absence of an informative response, I would suggest that the current state of affairs is the inevitable result of subordinating the rights of the voting public to the prerogatives of State Security Bureaus. The surest way for any nation to become subject to unnecessary surveillance is to allow its spies to dictate its policy.

The right to be free unwarranted intrusion into our private effects -- our lives and possessions, our thoughts and communications -- is a human right. It is not granted by national governments and it cannot be revoked by them out of convenience. Just as we do not allow police officers to enter every home to fish around for evidence of undiscovered crimes, we must not allow spies to rummage through our every communication for indications of disfavored activities.

Could you comment on the activities of EU Member States intelligence agencies in these operations and how advanced their capabilities have become in comparison with the NSA?

- The best testimony I can provide on this matter without pre-empting the work of journalists is to point to the indications that the NSA not only enables and guides, but shares some mass surveillance systems and technologies with the agencies of EU member states. As it pertains to the issue of mass surveillance, the difference between, for example, the NSA and FRA is not one of technology, but rather funding and manpower. Technology is agnostic of nationality, and the flag on the pole outside of the building makes systems of mass surveillance no more or less effective.

In terms of the mass surveillance programmes already revealed through the press, what proportion of the mass surveillance activities do these programmes account for? Are there many other programmes, undisclosed as of yet, that would impact on EU citizens rights?

- There are many other undisclosed programs that would impact EU citizens' rights, but I will leave the public interest determinations as to which of these may be safely disclosed to responsible journalists in coordination with government stakeholders.

Shadow Rapporteur Sophie Int'Veld MEP, ALDE Group

Are there adequate procedures in the NSA for staff to signal wrongdoing?

- Unfortunately not. The culture within the US Intelligence Community is such that reporting serious concerns about the legality or propriety of programs is much more likely to result in your being flagged as a troublemaker than to result in substantive reform. We should remember that many of these programs were well known to be problematic to the legal offices of agencies such as the GCHQ and other oversight officials. According to their own documents, the priority of the overseers is not to assure strict compliance with the law and accountability for violations of law, but rather to avoid, and I quote, "damaging public debate," to conceal the fact that for-profit companies have gone "well beyond" what is legally required of them, and to avoid legal review of questionable programs by open courts. (http://www.theguardian.com/uk-news/2013/oct/25/leaked-memos-gchq-mass-surveillance-secret-snowden)

In my personal experience, repeatedly raising concerns about legal and policy matters with my co-workers and superiors resulted in two kinds of responses.

The first were well-meaning but hushed warnings not to "rock the boat," for fear of the sort of retaliation that befell former NSA whistleblowers like Wiebe, Binney, and Drake. All three men reported their concerns through the official, approved process, and all three men were subject to armed raids by the FBI and threats of criminal sanction. Everyone in the Intelligence Community is aware of what happens to people who report concerns about unlawful but authorized operations.

The second were similarly well-meaning but more pointed suggestions, typically from senior officials, that we should let the issue be someone else's problem. Even among the most senior individuals to whom I reported my concerns, no one at NSA could ever recall an instance where an official complaint had resulted in an unlawful program being ended, but there was a

unanimous desire to avoid being associated with such a complaint in any form.

Do you feel you had exhausted all avenues before taking the decision to go public?

- Yes. I had reported these clearly problematic programs to more than ten distinct officials, none of whom took any action to address them. As an employee of a private company rather than a direct employee of the US government, I was not protected by US whistleblower laws, and I would not have been protected from retaliation and legal sanction for revealing classified information about lawbreaking in accordance with the recommended process.

It is important to remember that this is legal dilemma did not occur by mistake. US whistleblower reform laws were passed as recently as 2012, with the US Whistleblower Protection Enhancement Act, but they specifically chose to exclude Intelligence Agencies from being covered by the statute. President Obama also reformed a key executive Whistleblower regulation with his 2012 Presidential Policy Directive 19, but it exempted Intelligence Community contractors such as myself. The result was that individuals like me were left with no proper channels.

Do you think procedures for whistleblowing have been improved now?

- No. There has not yet been any substantive whistleblower reform in the US, and unfortunately my government has taken a number of disproportionate and persecutory actions against me. US government officials have declared me guilty of crimes in advance of any trial, they've called for me to be executed or assassinated in private and openly in the press, they revoked my passport and left me stranded in a foreign transit zone for six weeks, and even used NATO to ground the presidential plane of Evo Morales - the leader of Bolivia - on hearing that I might attempt to seek and enjoy asylum in Latin America.

What is your relationship with the Russian and Chinese authorities, and what are the terms on which you were allowed to stay originally in Hong Kong and now in Russia?

- I have no relationship with either government.

Shadow Rapporteur Jan Philipp Albrecht MEP, Greens Group

Could we help you in any way, and do you seek asylum in the EU?

- If you want to help me, help me by helping everyone: declare that the indiscriminate, bulk collection of private data by governments is a violation of our rights and must end. What happens to me as a person is less important than what happens to our common rights.

As for asylum, I do seek EU asylum, but I have yet to receive a positive response to the requests I sent to various EU member states. Parliamentarians in the national governments have told me that the US, and I quote, "will not allow" EU partners to offer political asylum to me, which is why the previous resolution on asylum ran into such mysterious opposition. I would

welcome any offer of safe passage or permanent asylum, but I recognize that would require an act of extraordinary political courage.

Can you confirm cyber-attacks by the NSA or other intelligence agencies on EU institutions, telecommunications providers such as Belgacom and SWIFT, or any other EU-based companies?

- Yes. I don't want to outpace the efforts of journalists, here, but I can confirm that all documents reported thus far are authentic and unmodified, meaning the alleged operations against Belgacom, SWIFT, the EU as an institution, the United Nations, UNICEF, and others based on documents I provided have actually occurred. And I expect similar operations will be revealed in the future that affect many more ordinary citizens.

Shadow Rapporteur Cornelia Ernst MEP, GUE Group

In your view, how far can the surveillance measures you revealed be justified by national security and from your experience is the information being used for economic espionage? What could be done to resolve this?

- Surveillance against specific targets, for unquestionable reasons of national security while respecting human rights, is above reproach. Unfortunately, we've seen a growth in untargeted, extremely questionable surveillance for reasons entirely unrelated to national security. Most recently, the Prime Minister of Australia, caught red-handed engaging in the most blatant kind of economic espionage, sought to argue that the price of Indonesian shrimp and clove cigarettes was a "security matter." These are indications of a growing disinterest among governments for ensuring intelligence activities are justified, proportionate, and above all accountable. We should be concerned about the precedent our actions set.

The UK's GCHQ is the prime example of this, due to what they refer to as a "light oversight regime," which is a bureaucratic way of saying their spying activities are less restricted than is proper (http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world). Since that light oversight regime was revealed, we have learned that the GCHQ is intercepting and storing unprecedented quantities of ordinary citizens' communications on a constant basis, both within the EU and without http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa). There is no argument that could convince an open court that such activities were necessary and proportionate, and it is for this reason that such activities are shielded from the review of open courts.

In the United States, we use a secret, rubber-stamp Foreign Intelligence Surveillance Court that only hears arguments from the government. Out of approximately 34,000 government requests over 33 years, the secret court rejected only 11. It should raise serious concerns for this committee, and for society, that the GCHQ's lawyers consider themselves fortunate to avoid the kind of burdensome oversight regime that rejects 11 out of 34,000 requests. If that's what heavy oversight looks like, what, pray tell, does the GCHQ's "light oversight" look like?

Let's explore it. We learned only days ago that the GCHQ compromised a popular Yahoo service to collect images from web cameras inside citizens' homes, and around 10% of these images they take from within people's homes involve nudity or intimate activities (http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo). In the same report, journalists revealed that this sort of webcam data was searchable via the NSA's XKEYSCORE system, which means the GCHQ's "light oversight regime" was used not only to capture bulk data that is clearly of limited intelligence value and most probably violates EU laws, but to then trade that data with foreign services without the knowledge or consent of any country's voting public.

We also learned last year that some of the partners with which the GCHQ was sharing this information, in this example the NSA, had made efforts to use evidence of religious conservatives' association with sexually explicit material of the sort GCHQ was collecting as a grounds for destroying their reputations and discrediting them (http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html). The "Release to Five Eyes" classification of this particular report, dated 2012, reveals that the UK government was aware of the NSA's intent to use sexually explicit material in this manner, indicating a deepening and increasingly aggressive partnership. None of these religious conservatives were suspected of involvement in terrorist plots: they were targeted on the basis of their political beliefs and activism, as part of a class the NSA refers to as "radicalizers."

I wonder if any members of this committee have ever advocated a position that the NSA, GCHQ, or even the intelligence services of an EU member state might attempt to construe as "radical"? If you were targeted on the basis of your political beliefs, would you know? If they sought to discredit you on the basis of your private communications, could you discover the culprit and prove it was them? What would be your recourse?

And you are parliamentarians. Try to imagine the impact of such activities against ordinary citizens without power, privilege, or resources. Are these activities necessary, proportionate, and an unquestionable matter of national security?

A few weeks ago we learned the GCHQ has hired scientists to study how to create divisions amongst activists and disfavored political groups, how they attempt to discredit and destroy private businesses, and how they knowingly plant false information to misdirect civil discourse (https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/).

To directly answer your question, yes, global surveillance capabilities are being used on a daily basis for the purpose of economic espionage. That a major goal of the US Intelligence Community is to produce economic intelligence is the worst kept secret in Washington.

In September, we learned the NSA had successfully targeted and compromised the world's major financial transaction facilitators, such as Visa and SWIFT, which released documents describe as providing "rich personal information," even data that "is not about our targets" (http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html). Again, these documents are authentic and unmodified - a fact the NSA itself has never once disputed.

In August, we learned the NSA had targeted Petrobras, an energy company (http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html). It would be the first of a long list of US energy targets.

But we should be clear these activities are not unique to the NSA or GCHQ. Australia's DSD targeted Sri Mulyani Indrawati, a finance minister and Managing Director of the World Bank (http://www.theguardian.com/world/2013/nov/18/australia-tried-to-monitor-indonesian-presidents-phone). Report after report has revealed targeting of G-8 and G-20 summits. Mass surveillance capabilities have even been used against a climate change summit.

Recently, governments have shifted their talking points from claiming they only use mass surveillance for "national security" purposes to the more nebulous "valid foreign intelligence purposes." I suggest this committee consider that this rhetorical shift is a tacit acknowledgment by governments that they recognize they have crossed beyond the boundaries of justifiable activities. Every country believes its "foreign intelligence purposes" are "valid," but that does not make it so. If we are prepared to condemn the economic spying of our competitors, we must be prepared to do the same of our allies. Lasting peace is founded upon fundamental fairness.

The international community must agree to common standards of behavior, and jointly invest in the development of new technical standards to defend against mass surveillance. We rely on common systems, and the French will not be safe from mass surveillance until Americans, Argentines, and Chinese are as well.

The good news is that there are solutions. The weakness of mass surveillance is that it can very easily be made much more expensive through changes in technical standards: pervasive, end-to-end encryption can quickly make indiscriminate surveillance impossible on a cost-effective basis. The result is that governments are likely to fall back to traditional, targeted surveillance founded upon an individualized suspicion. Governments cannot risk the discovery of their exploits by simply throwing attacks at every "endpoint," or computer processor on the end of a network connection, in the world. Mass surveillance, passive surveillance, relies upon unencrypted or weakly encrypted communications at the global network level.

If there had been better independent and public oversight over the intelligence agencies, do you think this could have prevented this kind of mass surveillance? What conditions would need to be fulfilled, both nationally and internationally?

- Yes, better oversight could have prevented the mistakes that brought us to this point, as could an understanding that defense is always more important than offense when it comes to matters of national intelligence. The intentional weakening of the common security standards upon which we all rely is an action taken against the public good.

The oversight of intelligence agencies should always be performed by opposition parties, as under the democratic model, they always have the most to lose under a surveillance state. Additionally, we need better whistleblower protections, and a new commitment to the importance of international asylum. These are important safeguards that protect our collective

human rights when the laws of national governments have failed.

European governments, which have traditionally been champions of human rights, should not be intimidated out of standing for the right of asylum against political charges, of which espionage has always been the traditional example. Journalism is not a crime, it is the foundation of free and informed societies, and no nation should look to others to bear the burden of defending its rights.

Shadow Rapporteur Axel Voss MEP, EPP Group

Why did you choose to go public with your information?

- Secret laws and secret courts cannot authorize unconstitutional activities by fiat, nor can classification be used to shield an unjustified and embarrassing violation of human rights from democratic accountability. If the mass surveillance of an innocent public is to occur, it should be authorized as the result of an informed debate with the consent of the public, under a framework of laws that the government invites civil society to challenge in open courts.

That our governments are even today unwilling to allow independent review of the secret policies enabling mass surveillance of innocents underlines governments' lack of faith that these programs are lawful, and this provides stronger testimony in favor of the rightfulness of my actions than any words I might write.

Did you exhaust all possibilities before taking the decision to go public?

- Yes. I had reported these clearly problematic programs to more than ten distinct officials, none of whom took any action to address them. As an employee of a private company rather than a direct employee of the US government, I was not protected by US whistleblower laws, and I would not have been protected from retaliation and legal sanction for revealing classified information about lawbreaking in accordance with the recommended process.

It is important to remember that this is legal dilemma did not occur by mistake. US whistleblower reform laws were passed as recently as 2012, with the US Whistleblower Protection Enhancement Act, but they specifically chose to exclude Intelligence Agencies from being covered by the statute. President Obama also reformed a key executive Whistleblower regulation with his 2012 Presidential Policy Directive 19, but it exempted Intelligence Community contractors such as myself. The result was that individuals like me were left with no proper channels.

Are you aware that your revelations have the potential to put at risk lives of innocents and hamper efforts in the global fight against terrorism?

- Actually, no specific evidence has ever been offered, by any government, that even a single life has been put at risk by the award-winning journalism this question attempts to implicate.

The ongoing revelations about unlawful and improper surveillance are the product of a partnership between the world's leading journalistic outfits and national governments, and if you can show one of the governments consulted on these stories chose not to impede demonstrably fatal information from being published, I invite you to do so. The front page of every newspaper in the world stands open to you.

Did the Russian secret service approach you?

- Of course. Even the secret service of Andorra would have approached me, if they had had the chance: that's their job.

But I didn't take any documents with me from Hong Kong, and while I'm sure they were disappointed, it doesn't take long for an intelligence service to realize when they're out of luck. I was also accompanied at all times by an utterly fearless journalist with one of the biggest megaphones in the world, which is the equivalent of Kryptonite for spies. As a consequence, we spent the next 40 days trapped in an airport instead of sleeping on piles of money while waiting for the next parade. But we walked out with heads held high.

I would also add, for the record, that the United States government has repeatedly acknowledged that there is no evidence at all of any relationship between myself and the Russian intelligence service.

Who is currently financing your life?

- I am.

Shadow Rapporteur Timothy Kirkhope MEP, ECR Group

You have stated previously that you want the intelligence agencies to be more accountable to citizens, however, why do you feel this accountability does not apply to you? Do you therefore, plan to return to the United States or Europe to face criminal charges and answer questions in an official capacity, and pursue the route as an official whistle-blower?

- Respectfully, I remind you that accountability cannot exist without the due process of law, and even Deutsche Welle has written about the well-known gap in US law that deprived me of vital legal protections due to nothing more meaningful than my status as an employee of a private company rather than of the government directly (http://www.dw.de/us-whistleblower-laws-offer-no-protection/a-17391500). Surely no one on the committee believes that the measure of one's political rights should be determined by their employer.

Fortunately, we live in a global, interconnected world where, when national laws fail like this, our international laws provide for another level of accountability, and the asylum process provides a means of due process for individuals who might otherwise be wrongly deprived of it. In the face of the extraordinary campaign of persecution brought against me by my the United States government on account of my political beliefs, which I remind you included the grounding of the President of Bolivia's plane by EU Member States, an increasing number of national

governments have agreed that a grant of political asylum is lawful and appropriate.

Polling of public opinion in Europe indicates I am not alone in hoping to see EU governments agree that blowing the whistle on serious wrongdoing should be a protected act.

Do you still plan to release more files, and have you disclosed or been asked to disclose any information regarding the content of these files to Chinese and Russian authorities or any names contained within them?

As stated previously, there are many other undisclosed programs that would impact EU citizens' rights, but I will leave the public interest determinations as to which of these may be safely disclosed to responsible journalists in coordination with government stakeholders. I have not disclosed any information to anyone other than those responsible journalists.

Thank you.