

As a senior technician in Zoom, I've seen that Zoom (Zoom Video Communications, Inc.) secretly violates users data privacy all the time to meet U.S. government's requirement and to gain economic interests. Arbitrary copy, storage and utilizing of users personal data are common. Backdoor has been opened to monitor user behavior. Though I am not a professor in law and I can't point out which law Zoom violates, but I'm a man with good professional ethic, I should stand out to blow the whistle and tell the truth. As far as I know, Zoom' huge PR team will hire ways to cover up the facts and avoid their responsibility. Facts may disappear and even I myself will be threatened and sued. However, everyone has the right to know the truth and we need to fight against Zoom together to let them eat their own bitter fruit.

I . Do Zoom users really have data autonomy?

According to my working experiences, U.S. government departments like FBI, NSA ask Zoom to preserve user data of interest including those already deleted by users so that they can obtain any data in any time. In order to meet such requests, Zoom has developed a tool for “data preservation”, preserving users data indiscriminately. This tool helps secretly copy and preserve users' data such as meeting history and participants details, cloud recordings, chat message, pictures, files, Zuora (Billing system, zuora.com), SFDC(CRM system, salesforce.com), phone/address, billing address, and credit/debt cards through data cloning and mirroring. What's worse, if your account were added into the “Data Preservation” system with your appearance on the target list , even you don't have any illegal behavior, all of your

actions in Zoom will under direct surveillance and at the free disposal of law-enforcing departments. Even though you can delete your data at your will, Zoom and the government can still obtain all the backup data from the system. American government can fetch data of online users in the name of threatening national security. But are all these reasonable?

1.1 Zoom backs up users' data

In order to meet the requirements from American law-enforcing departments, Zoom established a separate big-data database in advantage of AWS cloud service. The tool of “data preservation” is developed on the base of this database. This database clones the production environment of Zoom so that Zoom users cannot delete their data in it and be unaware of being monitored. Zoom can find what the government needs secretly from this database. Meeting history and participants details, cloud recordings, chat message, pictures, files, Zuora (Billing system, zuora.com), SFDC(CRM system, salesforce.com), phone/address, billing address, and credit/debt cards are included in the database. Even within Zoom, this database and tools are highly confidential. Only legal department are authorized to use it.

1.2 Users cannot delete their data from the root

1.2.1 Code

Users cannot delete their data in Zoom from the root. In the data production environment, “fake deletion” has been

written into the source code. That means when a user clicks the delete button, the system just records this behavior without any concrete actions. Then the user thinks data has been deleted. In the meantime, all the data including those being “as if deleted” are backed up in the database.

The following picture shows the underlying source code of a recording file of Zoom video meeting.

“recording_status” means state of preservation.

1-in the process

100-done

101-being deleted

```

meeting_id` varchar(50) NOT NULL COMMENT 'meeting instance id',
`start` datetime NOT NULL,
`recording_status` tinyint(4) NOT NULL COMMENT '1-process,100-finish,101: deleted',
`end` datetime DEFAULT NULL,
`file_size` bigint(20) DEFAULT '0' COMMENT 'recording file size in byte',
`file_name` varchar(512) DEFAULT NULL COMMENT 'recording file name in s3',
`video_poster` varchar(512) DEFAULT NULL,
`video_width` int(11) DEFAULT NULL,
`video_height` int(11) DEFAULT NULL,
`passwd` varchar(64) DEFAULT NULL,
`options` bigint(10) DEFAULT NULL,
`create_time` datetime DEFAULT NULL,
`modify_time` datetime DEFAULT NULL,
PRIMARY KEY (`id`),
KEY `meeting_id` (`meeting_id`) USING BTREE,
KEY `start_time` (`start`) USING BTREE

```

When Zoom users delete their recording files under their accounts, the system just records a mark of

“recording_status=101” and hides the files. In fact, all these files are still saved on a specific path in the Zoom cloud service. The save path (“file_name”) is showed clearly in the following screenshot from Zoom production database.

id	meeting_id	start	recording_status	end	file_size	file_name	video_poster	video_width	video_height	passwd	option
00015941-a62c-...	DRn6FnSRT/uqPMk...	20	:43 100	20	0... 78458394	s3://zoom-cmr/cmr/fr...	0	0	0	NULL	18
000159db-8931-...	vC+RmEatTdKx70...	20	:24 100	20	3... 73718816	s3://zoom-cmr/cmr/fr...	0	0	0	NULL	18
0001614a-80e4-...	fBskVzA5SR58Ek9...	20	:44 100	20	1... 346334796	s3://zoom-cmr/cmr/fr...	0	0	0	NULL	18
00016c93-b5b1-...	xu78fZbXS2uzy0G...	20	:44 100	20	0... 35780483	s3://zoom-cmr/cmr/fr...	0	0	0	NULL	32
00017fea-e20d-...	NvXafspZT4eqivU...	20	:15 100	20	0... 580414816	s3://zoom-cmr/cmr/fr...	0	0	0	NULL	18
00018050-311c-...	xEkbZbIRQnak7Y0...	20	:45 100	20	2... 81692771	/opt/zoom/cmr-stora...	0	0	0	NULL	17
0001a5bf-55ef-...	edebnufuQa...73	20	:48 100	20	1... 666047077	s3://zoom-cmr/cmr/fr...	0	0	0	NULL	18

1.2.2 System

Zoom senior management asks the technology team to develop a tool of data preservation for American government. Leakage to the public of which is forbidden. This system is clearly introduced through an internal email. Within this email, the senior management said, “That way, customers can delete whatever they like, and we have our legally mandated record still intact”. Meanwhile, he proposed two requirements to the tech team. First of all, “All legal requests come with the requirement that they are kept confidential and we are precluded from disclosing the request to customers. Whatever system we establish must allow for this confidential treatment.” Secondly, U.S. government

sometimes requires that Zoom preserve new records that may be created and are responsive to the given notice. Zoom needs to make sure to have the ability to monitor ongoing activity following the mentioned requests.

1.3 What data do Zoom provide to U.S. law-enforcing department?

Normally, these data include Meeting history and participants details, cloud recordings, chat messages, pictures, files, phone/address, billing address, credit/debt cards, billing history and address books. However, when U.S. government departments make requirements, they often give no just cause and ask for every information of one user. The following pictures partly show how they ask for data. For example, FBI, without any good reason, asked Zoom for 10 kinds of user data like private information, financial information, address. What's worse, miscellaneous provisions with words "all information" or "any information" are used to upgrade the scope and authority of acquiring data. From the legal instrument, wrongdoing of the user is not shown, but FBI is still able to acquire "all information" it wants. It could be imagined that FBI can acquire any information by this so-called "legal mean" if they want. Meanwhile, Zoom, turning a blind eye, have not taken the responsibility of protecting users' data and privacy.



U.S. Department of Justice
Federal Bureau of Investigation

One Justice Way Main: 972-559-5000
Dallas, Texas 75220-5220

Zoom
ATTN: Legal Department
55 Almaden Boulevard, 6th floor
San Jose, CA 95113

Re: Preservation of Records

Dear Custodian of Records:

The Federal Bureau of Investigation (FBI), United States Department of Justice, is requesting the preservation of the following user's Zoom account:

<https://zoom.us/j/701172052>
US: 166699006833, 701172052#
Webinar ID: 701 172 052

It is also requested that any and all subscriber records for the customer account associated with the accounts also be preserved.

Pursuant to Title 18, United States Code Section 2703(f), this letter is a formal request for the preservation of all stored communications, records, and other evidence in your possession regarding the accounts listed above pending further legal process.

I request that you not disclose the existence of this request to the subscriber or any other person, other than as necessary to comply with this request. If compliance with this request might result in a permanent or temporary termination of service to the Accounts, or otherwise alert any user of the Accounts as to your actions to preserve the information described below, please contact me as soon as possible and before taking action.

I request that you preserve, for a period of 90 days, the information described below currently in your possession in a form that includes the complete record. This request applies only retrospectively. It does not in any way obligate you to capture and preserve new information that arises after the date of this request. This request applies to the following items, whether in electronic or other form, including information stored on backup media, if available:

1. The contents of any communication or file stored by or for the Accounts and any associated accounts, and any information associated with those communications or files, such as the source and destination email addresses or IP addresses.
2. All records and other information relating to the Accounts and

any associated accounts including the following:

- a. subscriber names, user names, screen names, or other identities;
- b. mailing addresses, residential addresses, business addresses, e-mail addresses, and other contact information;
- c. length of service (including start date) and types of service utilized;
- d. records of user activity for any connections made to or from the Accounts, including the date, time, length, and method of connections, data transfer volume, user name, and source and destination Internet Protocol address;
- e. telephone or instrument number or other subscriber number or identity, including temporarily assigned network address;
- f. means and source of payment for the Accounts (including any credit card or bank accounts numbers) and billing records;
- g. correspondence and other records of contact by any person or entity about the Accounts, such as "Help Desk" notes; and
- h. any other records or evidence relating to the Accounts including Geolocation.

If there are any additional questions, please contact SA Kelly Luquette 817-716-9638.

Sincerely,

Matthew J. DeSarno
Special Agent in Charge

By: 
Derek Kleinmann
Supervisory Special Agent

CLONE - URGENT: Preservation Request - Middletown Police Department

*Search warrant to follow within 90 days

Records to Preserve:

- Billing address(es), e-mail address(es), authorized users, all associated telephone numbers, types of services, methods of payment, payment history, and dates and times of service and device activation and termination for all participants.
- Device identification including ICCID, IMEI, MEID, or ESN associated with this account.
- Log in and log out records.
- History of data connections, Internet Service Providers (ISP's), Internet Protocol (IP) logs, and dates/times accessed.
- All stored images, videos, or other media associated with virtual conference.
- In-coming and out-going SMS/MMS (text) messages.
- Any cloud storage services and access to contents of any cloud storage.

Zoom /  ZOOM-120137

Ticket # 1608269 USA DOJ Grand Jury Subpoena

For any and all accounts associated with the following identifiers:

Email: tamufor87@gmail.com Email: akembuom@gmail.com Email: akembuom@yahoo.com Email: Wilson.tita@gmail.com Email: frueric@gmail.com Telephone number: 443-622-6398

Telephone number: 651-206-8084

Telephone number: 346-757-5501

Telephone number: 240-640-8054

Provide the following records from the date of account creation to the present:

- Name(s) and address(es) of subscriber/customer (to include physical and e-mail address(es);
- Telephone and facsimile number(s) of subscriber/customer;
- Local and long distance telephone connection records, or records of session times and durations;
- Length of service (including start date) and types of service utilized
- Telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;
- Means and payment for such service (including any credit card or bank account number) and billing records
- Meeting title, initiation content, participants, meeting link, date time and duration and any activity recorded in meetings; and
- Message content, sender, recipients, date, time and read receipts to include shared files with file name, size and type

Zoom /  ZOOM-102526

Data Preservation - #1301352

Dear Engineering - Please ensure all data for these accounts and users including recordings, chats, and meeting history can not be deleted until this request is cleared.

Account ID: n0BotioERr2LSFBqkGZ2aQ

Account Number: 167211

Account ID: dCKkZ9tjRt-H27D1bitXpg

Account Number: 183278

Account ID: 4tCDE4jRQ7C0mcfQ_aJHJw

Account Number: 461645

Account ID: kEYfjLkKTj6s617GfA-0eg

Account Number: 499799

Account ID: jwPT_lwTSkSSwkliTLDm3A

Account Type: Free

Account Owner Email: contactjerrym@gmail.com

User ID: L3DHN0hwTxeC7gCyAsAexw

Account ID: 5WkqbZI9ReCEIGgTtAHNhg

Account Type: Free

Account Owner Email: marks@foumbergco.com

User ID: FOf15uzoRySzxej7mzi_3Q

II Monitoring Users through Backdoor System

2.1 Tracking Automated TOS Violators Termination System

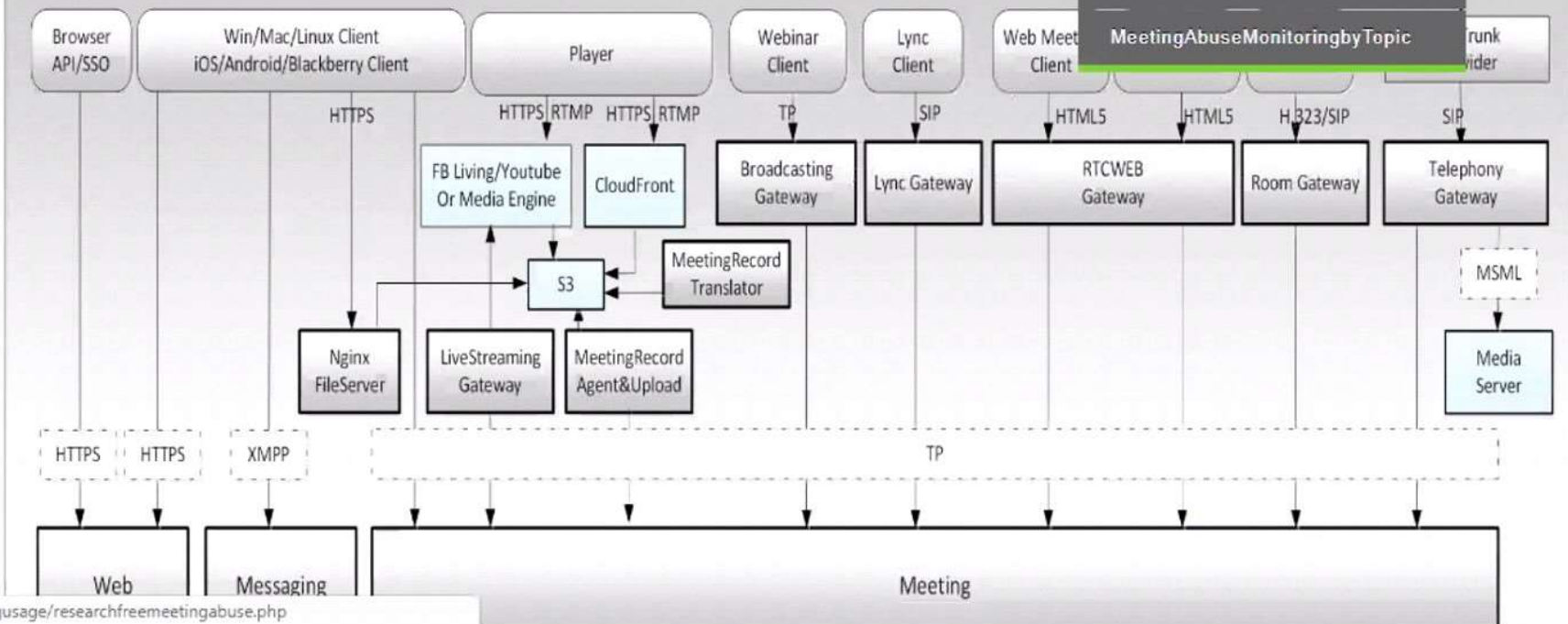
The Zoom headquarter has completed the R&D of a secret monitoring system long time ago. It is called "Tracking Automated TOS Violators Termination System" whose internal IP is "se.zipow.com/tos". No later than 2018, the system was put into application, monitoring free users as well as premium users and enterprise users.

Main functions of the system: automatic search of susceptible meetings; free access to meetings without password or host's authorization simply by the backdoor of the system; random analyze of video content from meetings; secret recordings of videos, audios, screenshots of meetings and production of reports or data accordingly to U.S. supervisory departments; termination of susceptible meetings and banning of relative accounts. The system is highly confidential and only opens to a few internal employees. Zoom may explain this system was developed for fighting crime. But Zoom has to acknowledge the system shows it has the ability to monitor users and it already does. People need to worry about whether Zoom will abuse the system for U.S. so-called "national security" or business purposes, and even randomly, frequently, indistinguishably monitor global users and steal their personal data at a large scale.

Welcome to Operation

- FreeMeetingUsageAbuse
- 24HMeetingUsageAbuse
- LargeWebinarMonitoring
- EmailAbuseMonitoringbyHostname
- MeetingAbuseMonitoringbyTopic

Zoom Video Architecture



The above picture shows the backend control interface of the system. The IP "zipow.com" belongs to Zoom and only a few staffs can visit it. From the picture, this system can monitor end-to-end conferences, telephone conferences, online conferences and relative emails. As for kinds of the meetings being monitored, free conferences, 24+ hours conferences and large webinars are all included. Also, it can monitor one specific host or meetings with a specific theme. In other words, Zoom can monitor any meeting of interest.

Not handle by autjob(need research) Report

[Tracking TOS Violators Detailed info](#)

JobRunningTime	Account_ID	Type	Host_ID	Email	Status	SignupTime(GMT)	Meeting_ID	Meeting_Number	Meeting_StartTime(GMT)	Proof
54:33	-qIVKG4KQMwvwn7qhWc7LQ	PRO	_RhMqnXwRcC-a3oTJNpsauA	ima@gmail.com	Active	2019-12-25 42:45	Yyz7nKZXQuS4w9vbcxSXfg==	126415829	2019-12-25 23:42	
54:33	YgIVYon_ROCSkahp6ct9Qw	Free	zhWKWW9OSMK-x9gKx8QnQQ	jerryood21@gmail.com	Active	2019-12-25 12:25	vV6g56RdeZ6Y.EySyOjg==	5995404552	2019-12-25 54:16	
54:33	UUYILkldRW2Ac7wyUd3yaA	Free	VlIOnmo4RxGxgvldl7prw	sw4oud.com	Active	2019-12-25 15:05	zhiyWaVuQ-zKQjzbbo7KQ==	6262344458	2019-12-25 22:05	
54:33	Zto72-CYRcq7rgT96KY2ow	Free	vdigUCg8SIGqHZMV00TVXg	sear@gmail.com	Active	2019-12-25 15:58	+j5Q.cbtT5e4URiGs7jj0g==	486532039	2019-12-25 03:58	
54:33	cidew9rMSYeNaALdhSuAA	Free	uKIB1--dRbmXP3-vLfDXBw	grmrgrrrrrrrrrrr@gmail.com	Active	2019-12-25 25:26	sSR9b232T0WpBX51dTK4Gw==	2234015396	2019-12-25 33:25	
54:33	P01vilxoSneLihfxcj76w	Free	qzTi5bjQq2NB0jHSPntQ	ross@gmail.com	Active	2019-12-25 47:17	nawfWimoRJuzJY6svPaQ==	7379865810	2019-12-25 00:34	
54:33	bWalO2n3SymG_RDJAUX0XA	Free	rwithoutic68YY0zTPaDtUvziZ-agCC	robert27@gmail.com	Active	2019-12-25 53:00	mLCy5dwXRvS5tdXQ1ezqg==	4241052698	2019-12-25 34:44	
54:33	Tdczm2PXRrubwfE6dbobUbw	Free	EZBGSIaFSfCRDPxnNpVR-qQ	piggay.fun	Active	2019-12-25 33:31	ToXI4FcwQ7uzKskr6jrU9g==	7562690668	2019-12-25 20:51	
20:48	SgedzImRbi-EDFGXwaBjg	Free	Ur9KPwaBQdKZ-br5A-JGtQ	daeeur@icloud.com	Deactive	2019-12-25 34:57	cHGwWxzSB2gbvrhxEOFIw==	8718361678	2019-12-25 31:00	Report
20:45	6mNK6XvbTkW29w5ebVBMA	Free	J7kgO8_rZubR6K_nyORFQ	cgyathoo.com	Deactive	2019-12-25 51:00	TfbhXJLGt3tiZITtmBytgQ==	9615774714	2019-12-25 44:52	Report
20:41	Nrvoc4qHzRveNYhdk-QtRYg	Free	itQpvjfrYaMGgwP2rdDfg	piggay.fun	Deactive	2019-12-25 41:37	eE22wBMRHmcLsgJS0qfg==	2506881496	2019-12-25 56:36	Report
20:38	O0Du96iyTv6wnV_FRi53wA	Free	AJAqRoRpSySkpw2AfT33Q	slutmail.com	Deactive	2019-12-25 00:31	iPKyDcn4Sjezy1slwk7gHg==	953024552	2019-12-25 03:24	Report
20:30	OHkZPN-hRTu8X-mqog-cjQ	PRO	VcoKu7FZToOmglMKrCt5UQ	nathanwin020@gmail.com	Active	2019-12-25 33:46	PNLUwGDfQHytJMknRYotA==	312892932	2019-12-25 35:27	Report
19:54	OkId3vtHSL6jgFdhvdbMikg	Name Host 50+	UBm_gRr_RgisHa0btCQUoA	5b57d2@meeting11.com	Active	2019-12-25 42:49	l0Zlr1TWri6S9ioXO1COcQ==	565019903	2019-12-25 07:34	Report
19:53	N_112QHbRPu6OE0fv67SgA	PRO	kf76VqccTpKFtsOaVqbENA	bwfa@gmail.com	Active	2019-12-25 06:02	Dilnt228Si23hAghtCeKgww==	2226661069	2019-12-25 40:10	Report
21:20	Vo-ZQHn4QIK10Szi1Mfy3pw	Free	XJJWA7V2SEq0xh6KWgx-ow	dickenn@gmail.com	Deactive	2019-12-25 56:24	IIXSMLeSby-G2Brak8ccw==	8692943231	2019-12-25 09:03	Report
21:16	p6_uiqbmQwWT2nQHhCNFuG	Free	oHVpoU8USkymZFSmazCB7A	piggay.fun	Deactive	2019-12-25 52:55	uKmcr29DScilfnUpHjelA==	323370006	2019-12-25 23:05	Report
21:13	74cyQpjOSTK-X28acyto_w	Free	23nbmQWSRUW4el4p3agC6w	ravnail.com	Deactive	2019-12-25 54:23	ERQLpfBiSEKeJ2wqeImQDQ==	9064177581	2019-12-25 28:08	Report
21:09	c8HbrZN7Q_e_TsLOVEmlLow	Free with CC	0qlcwZ6XhTrGfsthf-NYJav	swegmail.com	Deactive	2019-12-25 33:01	GyiLedsaTzkp19F9Dc4ISQ==	2316393269	2019-12-25 37:18	Report

Tracking IOS Violators Detailed info

Type	Host_ID	Email	Status	SignupTime(GMT)	Meeting_ID	Meeting_Number	Meeting_StartTime(GMT)	Proof_Violation	Terminated?	TakeAction_Time	Total
Free	uKIB1--dRbmXP3-vLfDXBw	grra [REDACTED] gmmmmmmr@gmail.com	Active	20 [REDACTED] 09:25:26	tSR9b232T0WpBX51dTK4Gw==	2234015396	20 [REDACTED] 01:33:25	Report PIC1 PIC2	InProgress		81
Free	qzTI5bljQq2NB0jHSNPwtQ	ron [REDACTED] gmail.com	Active	20 [REDACTED] 21:47:17	nawfWimoRJu2uzJY6xvPaQ==	7379865810	20 [REDACTED] 00:00:34	Report	InProgress		82
Free	withoutc68YY0zTPaDtUvziZz-ag CC	rob [REDACTED] 7@gmail.com	Active	20 [REDACTED] 16:53:00	mLCy5dwXRvS5tdXQ1ezqg==	4241052698	20 [REDACTED] 01:34:44	Report PIC1 PIC2	InProgress		46
Free	EZBGSJaFSfCRDpXNpVR-qQ	pig [REDACTED] fun	Active	20 [REDACTED] 23:33:31	TtXI4FcvQ7uzKxkr6jzU9g==	7562690668	20 [REDACTED] 00:20:51	Report PIC1 PIC2	InProgress		294
.Q PRO	_RhMqnXwRcC-a3oTjNpauA	ims [REDACTED] gmail.com	Active	20 [REDACTED] 18:42:45	Yyz7nKZXQuS4w9vbcxSXfg==	126415829	20 [REDACTED] 01:23:42				
Free	vdigUCg8SIgqHZMFV00TVXg	sea [REDACTED] gmail.com	Active	20 [REDACTED] 21:15:58	Hj5QicbIT5e4URaGs7jj0g==	486532039	20 [REDACTED] 00:03:58				
Free	VH0Nmo4RvGxgvtvdl7prw	sw [REDACTED] ed.com	Active	20 [REDACTED] 01:15:05	zhlyWnVuQ+izKOjbtzo7KQ==	6262344458	20 [REDACTED] 01:22:05				
Free	zhWKW'W9OSMK-x9zKx8QrQQ	ier [REDACTED] od21@gmail.com	Active	20 [REDACTED] 17:12:25	vnVV6z56RdeZ6Y/EvSvOig==	5995404552	20 [REDACTED] 03:54:16				

ToS Violation account detected/predicted by **Machine Learning**, if you found account belongs to false alarm from this page, pls report to

Account_ID	Host_ID	Email	Evidence_Pic	Account_Type	Status	C
N_1I2QHbRPu6OE0A6JSgA	kf76VqccTpKFt8OaVqbENA	bw673...@il.com	PIC1 PIC2	PRO	inprogress	#799480
MDdPzpN_S46WiusKs7gXCQ	6IBHB-iFRJOZp2QjU632cg	bwfce...@.com		PRO	open	deleted the picture, will capt
0kld3vThSL6jgFdhvdbMkg	UBm_gRr_RgisHa0btCQUoA	5b585...@eeting11.com	PIC1 PIC2	Name Host 50+		
0kld3vThSL6jgFdhvdbMkg	LgPubctbQOCQP4MiflIPzA	5b585...@eeting11.com	PIC1 PIC2	Name Host 50+		
0kld3vThSL6jgFdhvdbMkg	Jr5Eo64eTtK6fwbMUS2fw	5b585...@eeting11.com	PIC1 PIC2	Name Host 50+		
SIP5XSIBS5u8_RPjO2zqJQ	eqz5JUYMSOCJCV8F-IYeYw	5bf36...@eeting11.com	PIC1 PIC2	API Partner		
ZpGTIO1KQF-VStT_xDf1Nw	y9MwoNNsSqSXXkolEDELw	209ad...@room.net		PRO		
I-HPAwZPRJ-cKRLH-bcMZg	4XHyb0s0Q9qON128FX-Nfg	methic...@mail.com		PRO		
SIP5XSIBS5u8_RPjO2zqJQ	JHFtW1oNR6yoRsedv06U2g	5bf29...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	RIseloWvS3e8tmR07jZ7sg	5bf23...@eeting11.com	PIC1 PIC2	API Partner		
djM5i87bSCKeUM5qkv7CQ	Ulj-zRY5Q76-HxlFJeKLKA	ebost...@	PIC1 PIC2	Name Host 50+		
SIP5XSIBS5u8_RPjO2zqJQ	9syJQycLTxms4HjU1748Qg	5bf1e...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	Go9Vj3QyTAut_ROGIBMDqg	5bf1b...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	wqG2oPYSSNKdwPNH1SCiOQ	5bf13...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	LPkoDMGSzOebacsYvnWkQ	5bdc2...@eeting11.com	PIC1 PIC2	API Partner		
djM5i87bSCKeUM5qkv7CQ	13WK2XPYSH6X2Vp3711qrQ	Kelly...@u13.org	PIC1 PIC2	Name Host 50+		
jaeyS4OqTfWkRgqLDH3OOA	YrtFBg9pRa68PaNqj8K9Rw	scratch...@58@hotmail.com		PRO		
djM5i87bSCKeUM5qkv7CQ	EF4IjO8Rgoku8EcszMfAQ	pamel...@JU13.org	PIC1 PIC2	Name Host 50+	pending	Escalating to CSM/AE Team
KQIL0wDQqmk8L iROBzotA	8RXc47XRTW6HIUUI8fDrGw	SlapY...@mail.com		PRO	pending	#754893

Host_ID	Email	Status	SignupTime(GMT)	Meeting_ID	Meeting_Number	Meeting_StartTime(GMT)	Proof_Violation	Terminated?	TakeAction_Time	Total_P
IR	rw	Active	2021 01:15:05	zhWnV	62	21 01:22:05				
FS	VR-qQ	Active	2020 23:33:31	TtXl4Fcv	75	21 00:20:51				
2w	panuA	Active	2020 18:42:45	Yyz7nKZ	12	21 01:23:42				
49	KsQsQQ	Active	2021 17:12:25	vnVV6g5	59	20 23:54:16				
S	TVXg	Active	2020 21:15:58	-j5QcblT	48	21 00:03:58				
2b	XBw	Active	2020 09:25:26	SR9b232	22	21 01:33:25				
q2	vtQ	Active	2020 21:47:17	nawfWim	73	21 00:00:34				
TR	ag	Active	2020 16:53:00	mLCy5dw	42	21 01:34:44				
B6	GIQ	Deactive	2020 21:34:57	cHGwWx	87	20 23:31:00	Report PIC1 PIC2	Terminated	20	21 00:20:48175
R2	RFQ	Deactive	2022 10:51:00	TfbbXJLg	96	20 23:44:52	Report PIC1 PIC2	Terminated	20	21 00:20:45145
ja	0g	Deactive	2020 20:41:57	IE22-wB3	25	20 22:56:36	Report PIC1 PIC2	Terminated	20	21 00:20:41222
sS	T33Q	Deactive	2021 16:00:31	IPKyDcn4	95	20 23:03:24	Report PIC1 PIC2	Terminated	20	21 00:20:3885
Z7	C5UQ	Active	2020 09:33:46	PNLUwG	31	20 16:35:27	Report			
-8	UoA	Active	2025 10:42:49	10Zlr1Tw	56	20 22:07:34	Report			
TP	ENA	Active	2021 15:06:02	DiInt228	22	20 19:40:10	Report			
72	gx-ow	Deactive	2020 17:56:24	IsXSMLe	86	20 22:09:03	Report	Terminated	20	20 23:21:20279
U	qCB7A	Deactive	2020 19:52:55	uKmcR29	32	20 22:23:05	Report PIC1 PIC2	Terminated	20	20 23:21:16152
/S	agC6w	Deactive	2021 08:54:23	ERQLpfB	90	20 22:28:08	Report PIC1 PIC2	Terminated	20	20 23:21:1375
hT	aw	Deactive	2021 09:33:01	GyILedna	23	20 22:37:18	Report PIC1 PIC2	Terminated	20	20 23:21:0953

The above four pictures show how the system works. The first one displays how one can check “autojob historic terminated accounts reports” and “not handle by autojob reports” by clicking two buttons on the top left corner. Each meeting is monitored by one monitoring task. The sheets in the other three pictures explain detailed information of each monitoring task, including job running time, account ID, account type(paid or free), host ID and email, real-time

screenshots of meeting(which means the system can monitor the meeting without permission), type of action(auto or handle). The fourth picture shows the accounts being monitored, including paid/free accounts, business/name host 50+ accounts and API partners.

Meeting_ID: TtXI4FcwQ7uzKxkr6jzU9g==

Account_ID	Host_ID	email	Meeting_Number	Status	Meeting_topic	Start time
Tdczm2PXRtubwfE6dboUbw	EZBGSJaFSfCRDpXNpVR-qQ	pig[REDACTED]lay.fun	7562690668	InProgress	Super Piggy's Personal Meeting Room	20[REDACTED]0:51

Meeting Participants Info for meeting_id: TtXI4FcwQ7uzKxkr6jzU9g==

USERNAME	Email	IPADDR	COUNTRY	REGION	CITY	ZIPCODE	IS_HOST	JOINTIME	LEAVE	TIME	SECON
Super Piggy	pig[REDACTED]lay.fun	23.20.3.93	United States	Virginia	Ashburn	20149	1	20[REDACTED]00	21 20[REDACTED]2500	21 384	45
SUPER PIGGY	sup[REDACTED]@protonmail.com	162.217.29.152	United States	Ohio	Westerville	43082	0	20[REDACTED]00	21 254		
LONDON Lnd .	nort[REDACTED]n1090@gmail.com	86.14.162.143	United Kingdom	Wigan	Wigan	WN2	0	20[REDACTED]00	21 20[REDACTED]6970	21 673	1515
SmokerDave	Gre[REDACTED]e19@hotmail.com	173.61.230.235	United States	New Jersey	Trenton	08610	0	20[REDACTED]00	21 20[REDACTED]6680	21 341	2313
KΩεB West SL= UT(801) ΩmegA™	slcr[REDACTED]an1987@gmail.com	24.11.86.154	United States	Utah	Salt Lake City	84123	0	20[REDACTED]00	21 20[REDACTED]8940	21 148	2901
???...its a methstery!	sco[REDACTED]ac@gmail.com	174.0.22.159	Canada	Alberta	Calgary	T3J	0	20[REDACTED]00	21 20[REDACTED]1850	21 167	4028
gatobrazil	gate[REDACTED]69@gmail.com	200.158.158.249	Brazil	Sao Paulo	Sao Paulo		0	20[REDACTED]00	21 20[REDACTED]8480	21 873	1483
ucTopMB Miami	ucto[REDACTED]gmail.com	192.119.166.20	United States	Minnesota	Saint Paul	55124	0	20[REDACTED]00	21 20[REDACTED]3360	21 146	450
meTh becomes her (NYC)	you[REDACTED]ejoeking@gmail.com	98.15.57.236	United States	New York	Jackson Heights	11372	0	20[REDACTED]00	21 20[REDACTED]3450	21 825	601

The above picture shows an example. The basic information of every meeting participant is recorded including username, email, IP, address (country, region, city, zipcode), join/leave time, duration and etc..

Tracking Automated TOS Violators Termination Detailed info

Termination Time(GMT)	Account_ID	Type	Host_ID	Email	Status	SignupTime (GMT)	Proof_Violation	Terminated?	TookAction_Steps
2022-09-01 12:00	QV94tSzOK-Q	Free	MV9uiG2muQ	me@bom	Deactivated	2022-09-01 12:00	Report	Terminated	Forceuserlogout:[host_id: "MV9uiG2muQ", email: "me@bom"] ForceForbiddenUser:[account_id: "QV94tSzOK-Q", host_id: "MV9uiG2muQ", email: "me@bom"] ForceClosedMeeting:[meeting_number: "2591j6T": "PBA+1j6T"] SentNotificationEmail:[email: "me@bom"]
2022-09-01 21:00	CRm7VRGmq	Free	ihxApQ	dri@bom	Deactivated	2022-09-01 21:00	Report	Terminated	Forceuserlogout:[host_id: "ihxApQ", email: "dri@bom"] ForceForbiddenUser:[account_id: "CRm7VRGmq", host_id: "ihxApQ", email: "dri@bom"] ForceClosedMeeting:[meeting_number: "5882JU": ""] SentNotificationEmail:[email: "dri@bom"]
2022-09-01 21:00	7KXIBR7Kvsw	Free without CC	HO5_K5EJsQ	21@alite	Deactivated	2022-09-01 21:00	Report	Terminated	Forceuserlogout:[host_id: "HO5_K5EJsQ", email: "21@alite"] ForceForbiddenUser:[account_id: "7KXIBR7Kvsw", host_id: "HO5_K5EJsQ", email: "21@alite"]

This picture shows how TATVTS deals with “suspicious meeting” with three ways below: namely forcing user to log out, blocking the user and terminating the meeting. Normally they are combined together.

2.2 Zoom backend management system

Zoom backend management system has top authority over all Zoom accounts. It is designed to help manage Zoom user accounts. However, this system has some backdoor functions which may violate user privacy data. Zoom may use this privilege to deal with troublesome users rambunctiously. Some functions are beyond imagination. Here I will introduce its function of logging into user's account with user credentials. When a Zoom employee clicks the button "Login zoom us with this user Cred", he can log into this user's account in the same way the user himself deals with his own account. In this way, the employee has the same right to deal with this user's account, checking everything of the account, using the user's private key to see any confidential files, meeting records, IM chats, emails, telephone recordings and billings. This means the so-called "ee2e" encryption measure is meaningless. Besides this privilege, Zoom can modify or delete user's local data, and even remotely control or implant a backdoor on relative devices like Zoom Room through this system. Compared to managing user accounts by backend database, this system makes it more convenient for Zoom staff to monitor user behaviors and fetch their data ignoring encryption measure. The following pictures are some screenshots of the system and part of the codes.



ADMIN

User

Account

Audit

Feedback

Satisfaction

Billing Cancel Log

System Properties

CIDR Rule

REPORT

Daily Report

Weekly Report

Monthly Report

MJT Report

JMF Report

Free Trial Report

Top 100 Meeting Usage Report

Named Host Report

Edu Report

Active Host Report

API Report

User Admin

Account ID: XEgbgF [redacted]

Account Name: Carolina [redacted]

Account Type: Pro (Named Host)

Account Owner ID: 9ACXoXS [redacted]

Account Owner Email: car [redacted]

Account Owner Type: Work Email

User ID: 9ACX [redacted]

JID: 9ac [redacted]@xmpp.zoom.us

Sync User To XMPP

Switch JID

Force user log out

User Name: [redacted] Vargas (Owner)

User Email: car [redacted]@yahoo.com **Activate** Enable

User Login: Work Email

User Type: Pro

Meeting Capacity: 100 **Save**

Login zoom.us with this user cred



ADMIN

User

Account

Audit

Feedback

Satisfaction

Billing Cancel Log

System Properties

CIDR Rule

REPORT

Daily Report

Weekly Report

Monthly Report

MJT Report

JMF Report

Free Trial Report

Top 100 Meeting Usage Report

Named Host Report

Edu Report

Active Host Report

API Report

User Admin

Account ID: 0XK [redacted]

Account Name: Sml [redacted]

Account Type: Pro (Named Host)

Account Owner ID: ciG [redacted]

Account Owner Email: [redacted]@gmail.com

Account Owner Type: Work Email

User ID: ciG [redacted]

JID: [redacted]@xmpp.zoom.us

Sync User To XMPP

Switch JID

Force user log out

User Name: [redacted] (Owner)

User Email: [redacted]@gmail.com **Activate** Enable

User Login: Work Email

User Type: Pro

Meeting Capacity: 100 **Save**

Login zoom.us with this user cred

us02web.zoom.us/meeting/8

REQUEST A DEMO1.888.799

zoom

SOLUTIONS ▾PLANS & PRICINGCONTACT SALES

SCHEDULE A MEETINGJOIN A MEETING

PERSONAL

My Meetings > Manage

Profile

Meetings

Webinars

Recordings

Settings

ADMIN

> User Management

> Room Management

> Account Management

> Advanced

Attend Live Training

Video Tutorials

Knowledge Base

Topic

Time

Add to

Meeting ID

Meeting Password

Invite Link

Video

Audio

Meeting Options

Eastern Time (US and Canada)

Google Calendar

Outlook Calendar (.ics)

Yahoo Calendar

Require meeting password

https://us02web.zoom.us/j/85

Host

Participant

Telephone and Computer Audio

Dial from United States of America

Enable join before host

Mute participants upon entry

Enable waiting room

Only authenticated users can join

Record the meeting automatically in the cloud

```
<#if __loginUser.role == 1 || __loginUser.role == 8 || __loginUser.role == 19>
  <div class="control-group">
    <label class="control-label">Premium Type:</label>
    <div class="controls">
      <#if user.isPremiumUser()>
        <span>Yes</span> &nbsp; <#if __loginUser.role == 1> <button id="btnDisablePremiumType" class="btn btn-primary btn-danger">Disable</button> </#if>
      <#else>
        <span>No</span> &nbsp; <#if __loginUser.role == 1> <button id="btnEnablePremiumType" class="btn btn-primary">Enable</button> </#if>
      </#if>
    </div>
  </div>
</#if>
<#if __loginUser.role == 1 || __loginUser.role == 8 || __loginUser.role == 9 || __loginUser.role == 10 || __loginUser.role == 12 || __loginUser.role == 16 || __loginUser.role == 19>
  <div class="control-group">
    <div class="controls">
      <a class="btn btn-primary btn-large" href="@url value="/user/admin/login_web?id=${userInfo.id?url}&sns=${userInfo.snsType}"/>" target="_blank">Login zoom.us with this user cred</a> <br/>
    </div>
  </div>
</#if>
```

```

import com.saasbee.webapp.Constants;
import com.saasbee.webapp.audit.AuditAction;
import com.saasbee.webapp.audit.AuditMgr;
import com.saasbee.webapp.audit.AuditRole;
import com.saasbee.webapp.audit.AuditSource;
import com.saasbee.webapp.audit.AuditUserRole;
import com.saasbee.webapp.audit.AuditUserType;
import com.saasbee.webapp.cache.CacheClient;
import com.saasbee.webapp.cache.CacheEngine;
import com.saasbee.webapp.configuration.GlobalConfig;
import com.saasbee.webapp.domain.Account;
import com.saasbee.webapp.domain.AccountUser;
import com.saasbee.webapp.domain.Meeting;
import com.saasbee.webapp.domain.User;
import com.saasbee.webapp.domain.UserProfile;
import com.saasbee.webapp.domain.UserProfileExt2;
import com.saasbee.webapp.domain.UserSns;
import com.saasbee.webapp.exception.ErrorCode;
import com.saasbee.webapp.exception.common.FileUploadException;
import com.saasbee.webapp.exception.common.PolicyException;
import com.saasbee.webapp.exception.common.TokenException;
import com.saasbee.webapp.exception.meeting.MeetingAlreadyStartedException;

```

“Saasbee.com” is owned by Zoom, and all of Zoom’s source code is marked with the “saasbee”.

```

@RequestMapping("/user/admin/login_web")
public void userAdminLoginWeb(@RequestParam("id") String id, HttpServletRequest request, HttpServletResponse response, ModelMap model) throws Exception {
    UserEntity loginUser = sessionManager.getUser();
    boolean isDevEnv = GlobalConfig.getInstance().isDevEnv();

    User user = null;
    int snsType = ServletRequestUtils.getIntParameter(request, "sns", -1);
    String email = ServletRequestUtils.getStringParameter(request, "email", "");
    if (snsType >= 0) {
        user = userService.getUserByIdAndType(id, snsType);
    } else {
        List<User> snsList = userService.listUserByUserIds(Arrays.asList(id));
        if (snsList != null && !snsList.isEmpty()) {
            user = snsList.get(0);
        }
    }
}

```

III Breaking promise and using user data for machine learning

Eric Yuan, the CEO of Zoom, once proclaimed that “We now commit to all of our customers that we will not use any

of their audios, videos, chats, screen sharing, attachments and other communications like poll results, whiteboard and reactions to train our AI models or third-party AI models”. From what I know, Zoom is eager to develop AI, because the company needs AI to find out illegitimacy in video conferencing to avoid compliance risk, to identify fraud users to reduce economic losses, and to analyze business trend and focus of service to gain more profits.

3.1 With AI, Zoom, under the guidance of law enforcement, uses TATVTS against users

Tracking Automated TOS Violators Termination System mentioned above could automatically detect suspicious meetings via machine learning, join meetings without password and host’s permission, analyse meeting content and secretly take photos and videos of attendees and meeting content. Trained by data collected in the system, TATVTS becomes more intelligent in identifying meetings and users in which law enforcement has interest. Thus data of many innocent users becomes the samples for machine learning and users’ data privacy, like video conferencing, becomes unprotected. From the screenshots below, we could see the system uses machine learning to monitor meetings.

ToS Violation account detected/predicted by **Machine Learning**, if you found account belongs to false alarm from this page, pls report to

Account_ID	Host_ID	Email	Evidence_Pic	Account_Type	Status	C
N_1I2QHbRPu6OE0A6JSgA	xf76VqccTpKFt8OaVqbENA	bw673...@il.com	PIC1 PIC2	PRO	inprogress	#799480
MDdPzpN_S46WiusKs7gXCQ	6IBHB-iFRJOZp2QjU632cg	bwfce...@.com		PRO	open	deleted the picture, will capt
0klid3vIhSL6jgFdhvdbMkg	UBm_gRr_RgisHa0btCQUoA	5b585...@eeting11.com	PIC1 PIC2	Name Host 50+		
0klid3vIhSL6jgFdhvdbMkg	LgPubctbQOCQP4MiflIPzA	5b585...@eeting11.com	PIC1 PIC2	Name Host 50+		
0klid3vIhSL6jgFdhvdbMkg	Jr5Eo64eTtK6fwbMUS2fww	5b585...@eeting11.com	PIC1 PIC2	Name Host 50+		
SIP5XSIBS5u8_RPjO2zqJQ	eqz5JUYMSOCJCV8F-IYeYw	5bf36...@eeting11.com	PIC1 PIC2	API Partner		
ZpGTIO1KQF-VStT_xDf1Nw	y9MwoNNsSqSXXkolEDELw	209ad...@room.net		PRO		
I-HPAwZPRJ-cKRLH-bcMZg	4XHyb0s0Q9qON128FX-Nfg	methic...@mail.com		PRO		
SIP5XSIBS5u8_RPjO2zqJQ	JHFtW1oNR6yoRsedv06U2g	5bf29...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	RIseloWvS3e8tmR07jZ7sg	5bf23...@eeting11.com	PIC1 PIC2	API Partner		
djM5i87bSCKeUM5qkv7CQ	Ulj-zRY5Q76-HxlFJeKLKA	ebosti...@.com	PIC1 PIC2	Name Host 50+		
SIP5XSIBS5u8_RPjO2zqJQ	9syJQycLTxms4HjU1748Qg	5bf1e...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	Go9Vj3QyTAut_ROGIBMDqg	5bf1b...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	wqG2oPYSSNKdwPNH1SCiOQ	5bf13...@eeting11.com	PIC1 PIC2	API Partner		
SIP5XSIBS5u8_RPjO2zqJQ	LPkoDMGSzOebacsYvnWkQ	5bdc2...@eeting11.com	PIC1 PIC2	API Partner		
djM5i87bSCKeUM5qkv7CQ	13WK2XPYSH6X2Vp3711qrQ	Kelly...@u13.org	PIC1 PIC2	Name Host 50+		
jaeyS4OqTfWkRgqLDH3OOA	YrtFBg9pRa6SPzNqj8K9Rw	scratch...@hotmail.com		PRO		
djM5i87bSCKeUM5qkv7CQ	EF4IjO8Rgoku8EcszMfAQ	pamel...@IU13.org	PIC1 PIC2	Name Host 50+	pending	Escalating to CSM/AE Team
KQIL0wDQqmk8L iROBzotA	8RXc47XRTW6HIUUI8tDrGw	SlapY...@mail.com		PRO	pending	#754893

3.2 Feeding user data to AI for commercial use

Fraudulence against Zoom(like credit fraudulence) costed Zoom huge profits losses. To deal with it,



Zoom, based on its data warehouse, uses machine learning to automatically identify the meeting data and user accounts. The machine learning processing screenshot below shows how Zoom locates fraudulent users via big data. Higher scores mean higher correlation with fraudulent accounts found before.

3.3 Machine learning is required by senior managements for commercial use

The picture below shows emails of management of Zoom's business department, in which he admits that big data department shall use machine learning to find out new business models and trend.

Please find our approach and high level execution plan below:

Step 1: Identify business questions, metrics/facts and dimensions (using the "by" analysis) necessary to support the business initiatives.

Step 2: Identify key performance indicators against which success of the business initiatives will be measured.

Step 3: Identify key tasks, decisions, and the flow of information required to support the critical metrics and success factors. Get buy-in from data and process owners to support the initiative. Build data cleansing (iterative) processes as needed.

Step 4: Build data pipeline from supporting data sources including measures, dimensional attributes, granularity, update frequency, storage location, and access methods. Build technology architecture and implement new technologies for scalable data stores.

Step 5: Provide ad-hoc reporting (reactive) and run machine learning algorithm (proactive) to find patterns and trends in data to support new pivots in business.

Team is super excited about this new responsibility and looking forward to take on this challenge. Here's to a new journey for Zoom.... Please stay tuned for more updates and process on how you can leverage this team for your data needs.

Thanks,



Sunil Madan

Head of Business Services

Zoom Video Communications

Call 408-780-3933 | Click zoom.us | Zoom 4082035159



[Refer a Friend](#)

[Zoom recognized in 2016 Gartner Critical Capabilities Report](#)

Gartner.

PS:

The things showed above give the picture of Zoom's privacy infringement. Later I may release more inside stories about the company to guarantee users' right to know and their data privacy right.