Bundesgericht
Tribunal fédéral
Tribunale federale
Tribunal federal

{T 1/2}

1B 344/2014

Urteil vom 14. Januar 2015

I. öffentlich-rechtliche Abteilung

Besetzung
Bundesrichter Fonjallaz, Präsident,
Bundesrichter Merkli, Karlen, Eusebio, Chaix,
Gerichtsschreiber Forster.

Verfahrensbeteiligte
Oberstaatsanwaltschaft des Kantons Zürich, Florhofgasse 2, Postfach, 8090 Zürich,
Beschwerdeführerin,

gegen

Unbekannt.

Gegenstand
Grenzüberschreitende rückwirkende Überwachung des elektronischen Fernmeldedienstes bzw. sozialer Internet-Netzwerke,

Beschwerde gegen die Verfügung vom 8. September 2014 des Obergerichts des Kantons Zürich, Zwangsmassnahmengericht.

Sachverhalt:

A.
Die Staatsanwaltschaft II des Kantons Zürich führt eine Strafuntersuchung wegen Vergehen nach Art. 259 und Art. 261bis StGB. Sie wirft der noch unbekannten Täterschaft vor, im Sommer 2014 rassistische Postings auf einer Website eines sozialen Netzwerks veröffentlicht zu haben. Gegenüber einer in den USA domizilierten Internetservice-Providerin und deren Mitarbeitern verfügte die Staatsanwaltschaft am 27. August 2014 (gestützt auf Art. 273 StPO und Art. 32 lit. b des Internationalen Cybercrime-Übereinkommens) rückwirkend für sechs Monate die Herausgabe der sogenannten "IP-History" (der fraglichen Website und der beteiligten Teilnehmer-Profile) sowie der Registrierungsdaten der betreffenden Kunden. Ein entsprechendes Überwachungsgesuch der Staatsanwaltschaft vom 27. August 2014 wies das Obergericht des Kantons Zürich, Zwangsmassnahmengericht, mit Verfügung vom 8. September 2014 ab, soweit es darauf eintrat.

B.
Gegen die Verfügung des Zwangsmassnahmengerichtes gelangte die Oberstaatsanwaltschaft des Kantons Zürich mit Beschwerde vom 10. Oktober 2014 an das Bundesgericht. Sie beantragt die Aufhebung des angefochtenen Entscheides und die Genehmigung des Überwachungsgesuches.
Am 20. Oktober 2014 verzichtete das Obergericht auf eine Stellungnahme. Mit Eingabe vom 17. November 2014 beantragte die Oberstaatsanwaltschaft, das Urteil des Bundesgerichtes sei nicht zu veröffentlichen (eventualiter sei die Publikation auf die rechtlichen Erwägungen zu beschränken, subeventualiter sei der untersuchte

Sachverhalt in stark zusammengefasster Form zu veröffentlichen).

Erwägungen:

1.
Angefochten wird die abschlägige Behandlung eines Gesuches der Staatsanwaltschaft um Genehmigung von strafprozessualen Untersuchungsmassnahmen, welche nach Ansicht der Staatsanwaltschaft direkt von ihr zu verfügen und vom Zwangsmassnahmengericht (nach Art. 273 Abs. 2 StPO) zu bewilligen seien. Nichtgenehmigungen im Sinne von Art. 273 Abs. 2 StPO kann die Staatsanwaltschaft grundsätzlich mit Beschwerde in Strafsachen beim Bundesgericht anfechten (vgl. BGE 137 IV 340 E. 2.3 S. 344-346; nicht amtl. publizierte E. 1 von BGE 138 IV 232; Urteile 1B 19/2014 vom 28. Mai 2014 E. 1.3; 1B 441/2013 vom 6. Januar 2014 E. 1). Die vorliegende Beschwerde dient der Prüfung von grundsätzlichen Rechtsfragen im Schnittbereich zwischen Strafprozessrecht und internationaler Strafrechtshilfe. Zur Wahrnehmung ihrer Leitungs- und Koordinationsfunktion ist in Fällen wie dem vorliegenden auch die kantonale Oberstaatsanwaltschaft beschwerdebefugt (vgl. BGE 139 IV 25 E. 1 S. 27; Urteile 1B 109/2014 vom 3. November 2014 E. 1.5; 1B 158/2014 vom 25. Juni 2014 E. 1.1-1.7; 1B 193/2013 vom 12. Dezember 2013 E. 1.1-1.4).
Die übrigen Sachurteilsvoraussetzungen von Art. 78 ff. BGG sind erfüllt und geben zu keinen Bemerkungen Anlass.

2.
Das Zwangsmassnahmengericht wies das Ersuchen der Staatsanwaltschaft um Genehmigung einer rückwirkenden Überwachung des Fernmeldeverkehrs (mittels Erhebung von Kommunikations-Randdaten und sogenannten Bestandesdaten in den USA) ab, soweit es darauf eintrat. Weder das Internationale Cybercrime-Übereinkommen noch das Bundesrecht bilde eine Grundlage für eine direkte (grenzüberschreitende) Anordnung der fraglichen Untersuchungsmassnahmen. Diese könnten durch das Zwangsmassnahmengericht nicht bewilligt werden. Diesbezüglich sei vielmehr der Rechtshilfeweg zu beschreiten.

3.
In der Beschwerde wird Folgendes vorgebracht: Bei der von der Staatsanwaltschaft zur Edition verlangten IP-History handle es sich grundsätzlich um genehmigungsbedürftige Verbindungsdaten im Sinne von Art. 273 StPO. Im vorliegenden Fall erlaube Art. 32 lit. b des Internationalen Cybercrime-Übereinkommens, dass die Staatsanwaltschaft (nach einer Genehmigung durch das Zwangsmassnahmengericht) direkt auf die Verbindungsdaten zugreifen dürfe, ohne dafür den Rechtshilfeweg beschreiten zu müssen. Entgegen der in der Botschaft zum Cybercrime-Übereinkommen geäusserten Auffassung des Bundesrates genüge es, wenn der ausländische Provider, der zur Herausgabe der Daten befugt ist, seine Zustimmung dazu erklärt. Das zusätzliche Einverständnis einer weiteren berechtigten Person im Inland sei nicht erforderlich. Aufgrund ihrer Allgemeinen Geschäftsbedingungen sei die betroffene Providerfirma berechtigt, die fraglichen Daten an die schweizerischen Strafverfolgungsbehörden herauszugeben. Die Prüfung, ob die Zustimmung freiwillig erfolgt sei, obliege nicht dem Zwangsmassnahmengericht. Die Providerfirma habe in einer E-Mail vom 11. Juli 2014 ausdrücklich festgehalten, dass sie "bei Vorliegen eines rechtmässigen Entscheides der zuständigen Behörde
gewillt" sei, das Überwachungsgesuch zu prüfen und diesem allenfalls stattzugeben. Auch die übrigen Voraussetzungen (von Art. 273 StPO i.V.m. Art. 32 lit. b des Cybercrime-Übereinkommens) seien erfüllt. Was blosse Registrierungsdaten bzw. Bestandesdaten betrifft, handle es sich beim betroffenen ausländischen Internetservice-Provider um einen Dienstanbieter im Sinne von Art. 18 Abs. 1 lit. b des Cybercrime-Übereinkommens, weshalb die Staatsanwaltschaft von diesem Anbieter die Bestandesdaten (im Sinne von Art. 18 Abs. 3 des Übereinkommens bzw. Art. 14 BÜPF) direkt herausverlangen dürfe. Die Vorinstanz habe in diesem Zusammenhang das Bundesrecht verletzt.

4.

4.1. Die Schweizerische Strafprozessordnung vom 5. Oktober 2007 (StPO, SR 312.0) regelt die Verfolgung und Beurteilung der Straftaten nach Bundesrecht durch die Strafbehörden des Bundes und der Kantone (Art. 1 Abs. 1 StPO). Die Verfahrensvorschriften anderer Bundesgesetze bleiben vorbehalten (Art. 1 Abs. 2 StPO).

Die Gewährung der internationalen Rechtshilfe und das Rechtshilfeverfahren richten sich nur so weit nach der StPO, als andere Gesetze des Bundes und völkerrechtliche Verträge dafür keine Bestimmungen enthalten (Art. 54 StPO).

4.2. Das Bundesgesetz vom 20. März 1981 über internationale Rechtshilfe in Strafsachen (IRSG, SR 351.1) regelt, soweit andere Gesetze oder internationale Vereinbarungen nichts anderes bestimmen, alle Verfahren der zwischenstaatlichen Zusammenarbeit in Strafsachen, insbesondere die Rechtshilfe zur Unterstützung eines Strafverfahrens im Ausland nach dem dritten Teil IRSG (Art. 1 Abs. 1 lit. b IRSG). Gemäss dem Staatsvertrag vom 25. Mai 1973 zwischen der Schweizerischen Eidgenossenschaft und den Vereinigten Staaten von Amerika über gegenseitige Rechtshilfe in Strafsachen (RVUS, 0.351.933.6) verpflichten sich die Vertragsparteien, gestützt auf die Bestimmungen dieses Vertrags einander Rechtshilfe zu leisten in Ermittlungs- oder Gerichtsverfahren wegen strafbarer Handlungen, deren Ahndung unter die Gerichtsbarkeit des ersuchenden Staats oder eines seiner Gliedstaaten fällt (Art. 1 Ziff. 1 lit. a RVUS). Im ersuchten Staat dürfen bei Ausführung eines Ersuchens nach dem RVUS nur Zwangsmassnahmen angewendet werden, die sein Recht für Ermittlungs- oder Gerichtsverfahren wegen einer seiner Gerichtsbarkeit unterworfenen Handlung vorsieht (Art. 4 Ziff. 1 RVUS). Soweit der RVUS nichts anderes bestimmt, werden Ersuchen nach den üblichen
Vorschriften ausgeführt, die für Ermittlungen oder Verfahren im ersuchten Staat hinsichtlich einer unter seine Gerichtsbarkeit fallenden Straftat anzuwenden sind (Art. 9 Ziff. 1 RVUS). Die zuständigen Gerichts- und anderen Beamten in jedem der beiden Staaten werden mit allen ihnen nach ihrem Recht zur Verfügung stehenden Mitteln bei der Ausführung von Ersuchen des anderen Staats behilflich sein (Art. 9 Ziff. 3 RVUS). Kein Angehöriger des ersuchten Staats, der sich weigerte, nicht erzwingbare Auskünfte zu erteilen, oder gegen den im ersuchten Staat gemäss den Vorschriften des RVUS Zwangsmassnahmen angewendet werden mussten, darf im ersuchenden Staat nur deswegen irgendwelchen gesetzlich vorgesehenen Sanktionen ausgesetzt werden, weil er von seinem vertraglich vorgesehenen Weigerungsrecht Gebrauch gemacht hat (Art. 14 RVUS). Machen der ersuchte Staat, einer seiner Gliedstaaten oder eine Drittperson an Schriftstücken, Akten oder Beweisstücken, deren Herausgabe verlangt oder bewirkt wurde, Eigentum oder sonstige Rechte geltend, so richten sich diese nach dem Recht des Ortes, an dem sie erworben wurden. Eine Vorlage- oder Herausgabepflicht nach dem RVUS geht den im vorstehenden Satz erwähnten Rechten vor. Diese Rechte bleiben jedoch
anderweitig unberührt (Art. 21 RVUS). Wenn ein im RVUS vorgesehenes Verfahren die Rechtshilfe in Strafsachen zwischen den Vertragsparteien nach einem anderen Abkommen oder nach dem Recht im ersuchten Staat erleichtern würde, so wird für die Leistung solcher Rechtshilfe das Verfahren nach dem RVUS angewendet. Rechtshilfe und Verfahren nach irgendeinem anderen internationalen Vertrag oder Übereinkommen oder nach dem innerstaatlichen Recht in den Vertragsstaaten bleiben vom RVUS unberührt und werden dadurch weder ausgeschlossen, noch eingeschränkt (Art. 38 Ziff. 1 RVUS). Die Bestimmungen des RVUS gehen abweichenden Vorschriften des innerstaatlichen Rechts in den Vertragsstaaten vor (Art. 38 Ziff. 2 RVUS). Vertreter der Zentralstellen können, wenn es ratsam erscheint, ihre Meinungen über die Auslegung, Anwendung oder Durchführung des RVUS im Allgemeinen oder in Bezug auf besondere Fälle schriftlich austauschen oder sich für einen mündlichen Meinungsaustausch treffen (Art. 39 Ziff. 1 RVUS).

4.3. Am 1. Januar 2012 ist das Übereinkommen vom 23. November 2001 über die Cyberkriminalität (CCC, SR 0.311.43) für die Schweiz in Kraft getreten. Auch die Vereinigten Staaten von Amerika (USA) haben das Übereinkommen ratifiziert; es ist für die USA seit 1. Januar 2007 in Kraft.

4.3.1. In der Präambel zum CCC weisen die Mitgliedstaaten des Europarates und die übrigen Vertragsstaaten des Übereinkommens unter anderem darauf hin, dass zur wirksamen Bekämpfung der Computerkriminalität eine verstärkte, zügige und gut funktionierende internationale Zusammenarbeit in Strafsachen nötig sei. Zweck des Übereinkommens ist es (laut Art. 39 Abs. 1 CCC), die zwischen den Vertragsparteien bestehenden zwei- oder mehrseitigen Verträge oder Übereinkünfte in diesem Sinne zu ergänzen, insbesondere auch das Europäische Übereinkommen vom 20. April 1959 über die Rechtshilfe in Strafsachen (EUeR, SR 0.351.1).

4.3.2. In Kapitel II des Übereinkommens (Art. 2-22 CCC) werden die "innerstaatlich zu treffenden Massnahmen" geregelt. Zu den (gemäss Abschnitt 2: "Verfahrensrecht") innerstaatlich zu erlassenden verfahrensrechtlichen Bestimmungen (Art. 14-21 CCC) gehören insbesondere Regeln für die Erhebung von in elektronischer

Form vorhandenem Beweismaterial für Straftaten im Sinne von Art. 14 Abs. 2 lit. a-b CCC (Art. 14 Abs. 2 lit. c CCC). Jede Vertragspartei hat sodann die erforderlichen gesetzgeberischen und anderen Massnahmen zu treffen, damit ihre zuständigen Behörden die umgehende Sicherung (Art. 16-17 und Art. 29 CCC) bestimmter Computerdaten einschliesslich Verkehrsdaten (Art. 1 lit. d CCC), die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht (Art. 16 Abs. 1 CCC). Führt eine Vertragspartei ihre Verpflichtung nach Art. 16 Abs. 1 CCC so durch, dass eine Person im Wege einer Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, sicherzustellen, so trifft diese
Vertragspartei die erforderlichen gesetzgeberischen und anderen Massnahmen, um diese Person zu verpflichten, die Unversehrtheit dieser Computerdaten so lange wie notwendig, längstens aber 90 Tage, zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschliessend verlängert werden kann (Art. 16 Abs. 2 CCC). Jede Vertragspartei trifft in Bezug auf Verkehrsdaten (Art. 1 lit. d CCC), die nach Art. 16 CCC zu sichern sind, auch die erforderlichen gesetzgeberischen und anderen Massnahmen, um sicherzustellen, (a) dass die umgehende Sicherung von Verkehrsdaten unabhängig davon möglich ist, ob ein oder mehrere Diensteanbieter an der Übermittlung dieser Kommunikation beteiligt waren, und (b) dass Verkehrsdaten in einem solchen Umfang umgehend an die zuständige Behörde der Vertragspartei oder an eine von dieser Behörde bezeichnete Person weitergegeben werden, dass die Vertragspartei die Diensteanbieter und den Weg feststellen kann, auf dem die Kommunikation übermittelt wurde (Art. 17 Abs. 1 CCC).

4.3.3. Ebenfalls unter Kapitel II, Abschnitt 2 des Übereinkommens (innerstaatlich zu erlassende verfahrensrechtliche Normen) bestimmt Art. 18 Abs. 1CCC (unter dem Titel: Anordnung der Herausgabe) Folgendes:

"Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Massnahmen, um ihre zuständigen Behörden zu ermächtigen anzuordnen:
a. dass eine Person in ihrem Hoheitsgebiet bestimmte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden und die in einem Computersystem oder auf einem Computerdatenträger gespeichert sind, vorzulegen hat; und
b. dass ein Diensteanbieter, der seine Dienste im Hoheitsgebiet der Vertragspartei anbietet, Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat."

4.3.4. Art. 18 Abs. 3CCC definiert Bestandesdaten (im Sinne von Art. 18 Abs. 1 lit. b CCC) wie folgt:

"Im Sinne dieses Artikels bedeutet der Ausdruck 'Bestandsdaten' alle in Form von Computerdaten oder in anderer Form enthaltenen Informationen, die bei einem Diensteanbieter über Teilnehmer seiner Dienste vorliegen, mit Ausnahme von Verkehrsdaten oder inhaltsbezogenen Daten, und durch die Folgendes festgestellt werden kann:
a. die Art des genutzten Kommunikationsdienstes, die dafür getroffenen technischen Massnahmen und die Dauer des Dienstes;
b. die Identität des Teilnehmers, seine Post- oder Hausanschrift, Telefon- und sonstige Zugangsnummer sowie Angaben über Rechnungsstellung und Zahlung, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst zur Verfügung stehen;
c. andere Informationen über den Ort, an dem sich die Kommunikationsanlage befindet, die auf der Grundlage des Vertrags oder der Vereinbarung in Bezug auf den Dienst vorliegen."

4.3.5. In Kapitel III des Übereinkommens (Art. 23-35 CCC) wird die "Internationale Zusammenarbeit" geregelt. Gemäss Art. 23CCC arbeiten die Vertragsparteien untereinander (im Einklang mit Kapitel III des Übereinkommens) "im grösstmöglichen Umfang zusammen, indem sie einschlägige völkerrechtliche Übereinkünfte über die internationale Zusammenarbeit in Strafsachen sowie Übereinkünfte, die auf der Grundlage einheitlicher oder auf Gegenseitigkeit beruhender Rechtsvorschriften getroffen wurden, und innerstaatliche Rechtsvorschriften für Zwecke der Ermittlungen oder Verfahren in Bezug auf Straftaten in Zusammenhang mit Com-

putersystemen und -daten oder für die Erhebung von Beweismaterial in elektronischer Form für eine Straftat anwenden".

4.3.6. Art. 25 Abs. 4(Satz 1) CCC legt Folgendes fest: Soweit in den Artikeln des Kapitels III des Übereinkommens "nicht ausdrücklich etwas anderes vorgesehen ist, unterliegt die Rechtshilfe den im Recht der ersuchten Vertragspartei oder in den anwendbaren Rechtshilfeverträgen vorgesehenen Bedingungeneinschliesslich der Gründe, aus denen die ersuchte Vertragspartei die Zusammenarbeit ablehnen kann".

4.3.7. Art. 26Abs. 1 CCC regelt die unaufgeforderte Übermittlung von Informationen wie folgt: "Eine Vertragspartei kann einer anderen Vertragspartei, soweit ihr innerstaatliches Rechtes erlaubt und ohne vorheriges Ersuchen, Informationen übermitteln, die sie im Rahmen eigener Ermittlungen gewonnen hat, wenn sie der Auffassung ist, dass die Übermittlung dieser Informationen der anderen Vertragspartei bei der Einleitung oder Durchführung von Ermittlungen oder Verfahren wegen nach diesem Übereinkommen umschriebener Straftaten helfen oder dazu führen könnte, dass diese Vertragspartei ein Ersuchen um Zusammenarbeit" nach dem Kapitel III "stellt."

4.3.8. Unter dem Titel 1: "Rechtshilfe bei vorläufigen Massnahmen" (Art. 29-30 CCC) bestimmt Art. 29CCC ("umgehende Sicherung gespeicherter Computerdaten") Folgendes:
Abs. 1: "Eine Vertragspartei kann eine andere Vertragspartei um Anordnung oder anderweitige Bewirkung der umgehenden Sicherung von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der anderen Vertragspartei befindet, und derentwegen die ersuchende Vertragspartei beabsichtigt, ein Rechtshilfeersuchen um Durchsuchung oder ähnlichen Zugriff, Beschlagnahme oder ähnliche Sicherstellung oder Weitergabe der Daten zu stellen."
Abs. 3: "Nach Eingang des von einer anderen Vertragspartei gestellten Ersuchens trifft die ersuchte Vertragspartei alle geeigneten Massnahmen zur umgehenden Sicherung der bezeichneten Daten in Übereinstimmung mit ihrem innerstaatlichen Recht. Für die Zwecke der Erledigung eines Ersuchens wird die beiderseitige Strafbarkeit als Voraussetzung für die Vornahme dieser Sicherung nicht verlangt."

4.3.9. Art. 30CCC ermöglicht eine umgehende Weitergabe gesicherter Verkehrsdaten (aufgrund eines Ersuchens nach Art. 29 CCC) wie folgt:
Abs. 1: "Stellt die ersuchte Vertragspartei bei der Erledigung eines Ersuchens nach Artikel 29 um Sicherung von Verkehrsdaten bezüglich einer bestimmten Kommunikation fest, dass ein Diensteanbieter in einem anderen Staat an der Übermittlung dieser Kommunikation beteiligt war, so gibt die ersuchte Vertragspartei Verkehrsdaten in so ausreichender Menge an die ersuchende Vertragspartei umgehend weiter, dass dieser Diensteanbieter und der Weg, auf dem die Kommunikation übermittelt wurde, festgestellt werden können."
Abs. 2: "Von der Weitergabe von Verkehrsdaten nach Absatz 1 darf nur abgesehen werden, wenn:
a. das Ersuchen eine Straftat betrifft, die von der ersuchten Vertragspartei als politische oder als mit einer solchen zusammenhängende Straftat angesehen wird; oder
b. die ersuchte Vertragspartei der Ansicht ist, dass die Erledigung des Ersuchens geeignet ist, ihre Souveränität, Sicherheit, öffentliche Ordnung (ordre public) oder andere wesentlichen Interessen zu beeinträchtigen."

4.3.10. Titel 2 regelt die "Rechtshilfe in Bezug auf Ermittlungsbefugnisse" (Art. 31-34 CCC) : Gemäss Art. 31CCC ("Rechtshilfe beim Zugriff auf gespeicherte Computerdaten") kann eine Vertragspartei "eine andere Vertragspartei um Durchsuchung oder ähnlichen Zugriff, um Beschlagnahme oder ähnliche Sicherstellung und um Weitergabe von Daten ersuchen, die mittels eines Computersystems gespeichert sind, das sich im Hoheitsgebiet der ersuchten Vertragspartei befindet, einschliesslich Daten, die nach Artikel 29 gesichert worden sind" (Abs. 1). "Die ersuchte Vertragspartei erledigt das Ersuchen, indem sie die in Artikel 23 bezeichneten völkerrechtlichen Übereinkünfte, sonstigen Übereinkünfte und Rechtsvorschriften anwendet und die anderen einschlägigen Bestimmungen" des Kapitels III "einhält" (Abs. 2).
Es handelt sich hier um eine (im Verhältnis zum RVUS) spezialrechtliche Regelung der förmlichen Rechtshilfe zwischen der Schweiz und den USA im Bereich der Cyber-Kriminalität (vgl. Art. 38 Ziff. 1 Satz 2 RVUS).

4.3.11. Schliesslich sieht das Übereinkommen in Art. 32 CCC auch noch gewisse grenzüberschreitende Straf-

verfolgungsbefugnisse vor, bei denen (ausnahmsweise) der förmliche Rechtshilfeweg (über Art. 29-31 CCC) vermieden werden kann. Art. 32CCC (”Grenzüberschreitender Zugriff auf gespeicherte Computerdaten”) lautet wie folgt:

”Eine Vertragspartei darf ohne die Genehmigungeiner anderen Vertragspartei:
a. auf öffentlich zugängliche gespeicherte Computerdaten (offene Quellen) zugreifen, gleichviel, wo sich die Daten geographisch befinden; oder
b. auf gespeicherte Computerdaten, die sich im Hoheitsgebiet einer anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die rechtmässige und freiwillige Zustimmung der Person einholt, die rechtmässig befugt ist, die Daten mittels dieses Computersystems an sie weiterzugeben.”

4.3.12. Am 28. Januar 2003 wurde ein Zusatzprotokoll zum Internationalen Cybercrime-Übereinkommen abgeschlossen, welches rassistische und fremdenfeindliche Handlungen über Computersysteme zum Gegenstand hat (Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems, ETS Nr. 189). Dieses Zusatzprotokoll wurde von der Schweiz am 9. Oktober 2003 unterzeichnet. Es trat am 1. März 2006 (nach den ersten fünf Ratifikationen) für diverse Vertragsstaaten in Kraft. Die Schweiz hat das Zusatzprotokoll zum Cybercrime-Übereinkommen bisher noch nicht ratifiziert. Die USA haben es nicht unterzeichnet.

4.4. Neben der eigentlichen geheimen (inhaltlichen) Überwachung des Post- und Fernmeldeverkehrs (Art. 270-272 i.V.m. Art. 269 StPO) sieht Art. 273 StPO die Möglichkeit vor, dass die Staatsanwaltschaft (ebenfalls zunächst geheime) Auskünfte einholt betreffend Verkehrs- und Rechnungsdaten bzw. Teilnehmeridentifikation (Art. 273 StPO). Auskünfte über solche sogenannten Randdaten des Fernmeldeverkehrs (seitens der Fernmeldedienst-Anbieterinnen) können sich darauf erstrecken, wann und mit welchen Personen oder Anschlüssen eine überwachte Person über den Fernmeldeverkehr Verbindungen gehabt hat (Art. 273 Abs. 1 lit. a StPO). Zudem können Erhebungen über Verkehrs- und Rechnungsdaten erfolgen (Art. 273 Abs. 1 lit. b StPO). Voraussetzung für solche Massnahmen ist erstens der dringende Verdacht eines Verbrechens oder Vergehens (oder einer Übertretung nach Art. 179septies StGB). Zweitens müssen hier die Voraussetzungen von Art. 269 Abs. 1 lit. b und c StPO erfüllt sein (Art. 273 Abs. 1 Ingress StPO). Wie die inhaltliche Kommunikationsüberwachung (Art. 272 Abs. 1 i.V.m. Art. 270 StPO) bedürfen Massnahmen nach Art. 273 StPO der Genehmigung durch das Zwangsmassnahmengericht (Art. 273 Abs. 2 StPO). Entsprechende Auskünfte können unabhängig von
der Dauer einer Überwachung und bis 6 Monate rückwirkend verlangt werden (Art. 273 Abs. 3 StPO, Art. 15 Abs. 3 BÜPF).

4.5. Das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 6. Oktober 2000 (BÜPF, SR 780.1) regelt die Überwachung des Post- und Fernmeldeverkehrs, die angeordnet und durchgeführt wird: (a) im Rahmen eines Strafverfahrens des Bundes oder eines Kantons, (b) zum Vollzug eines Rechtshilfeersuchens nach dem IRSG und (c) im Rahmen der Suche und Rettung vermisster Personen (Art. 1 Abs. 1 BÜPF). Im Rahmen dieses Geltungsbereiches ist das BÜPF auf alle staatlichen, konzessionierten oder meldepflichtigen Anbieterinnen von Post- und Fernmeldedienstleistungen sowie Internet-Anbieterinnen anwendbar (Art. 1 Abs. 2 BÜPF).

4.6. Wird (nach Art. 269-273 StPO) eine Überwachung des Fernmeldedienstes angeordnet, prüft der Dienst des Bundes für die Überwachung des Post- und Fernmeldeverkehrs (nachfolgend: Dienst) unter anderem, ob die Überwachung eine gemäss dem anwendbaren Recht überwachungsfähige Straftat betrifft und von der zuständigen Behörde angeordnet worden ist (Art. 13 Abs. 1 lit. a i.V.m. Art. 2 Abs. 1 BÜPF). Er weist die Anbieterinnen von Fernmeldediensten an, die für die Überwachung notwendigen Massnahmen zu treffen (Art. 13 Abs. 1 lit. b BÜPF). Der Dienst nimmt von den Anbieterinnen den umgeleiteten Fernmeldeverkehr der überwachten Person entgegen, zeichnet diesen auf und liefert der anordnenden Behörde die Dokumente und Datenträger aus (Art. 13 Abs. 1 lit. c BÜPF i.V.m. Art. 269 f. StPO). Er nimmt von den Anbieterinnen Teilnehmeridentifikationen sowie Verkehrs- und Rechnungsdaten entgegen und leitet diese an die anordnende Behörde weiter (Art. 13 Abs.

1 lit. d BÜPF i.V.m. Art. 273 StPO).

4.7. Die Anbieterinnen von Fernmeldediensten liefern dem Dienst auch sogenannte Bestandesdaten über "bestimmte" Fernmeldeanschlüsse. Dazu gehören insbesondere Name und Adresse der Teilnehmerin oder des Teilnehmers (Art. 14 Abs. 1 BÜPF). Auf Gesuch hin erteilt der Dienst Auskünfte über solche Bestandesdaten an die eidgenössischen und kantonalen Behörden, welche eine Überwachung des Fernmeldeverkehrs anordnen oder genehmigen dürfen, zur Bestimmung der zu überwachenden Anschlüsse und Personen (Art. 14 Abs. 2 lit. a BÜPF). Art. 14 Abs. 4 BÜPF bestimmt für die strafrechtliche Verfolgung von Internetdelikten Folgendes: "Wird eine Straftat über das Internet begangen, so ist die Internet-Anbieterin verpflichtet, der zuständigen Behörde alle Angaben zu machen, die eine Identifikation des Urhebers oder der Urheberin ermöglichen".

4.8. Die Anbieterinnen von Fernmeldediensten sind verpflichtet, dem Dienst auf Verlangen den Fernmeldeverkehr der überwachten Person sowie die Teilnehmeridentifikation und Verkehrs- und Rechnungsdaten zuzuleiten. Ebenso haben sie die zur Vornahme der Überwachung notwendigen Informationen zu erteilen (Art. 15 Abs. 1 BÜPF i.V.m. Art. 269-273 StPO). Weiter sind sie verpflichtet, die für die Teilnehmeridentifikation notwendigen Daten sowie die Verkehrs- und Rechnungsdaten während sechs Monaten aufzubewahren (Art. 15 Abs. 3 BÜPF i.V.m. Art. 273 Abs. 3 StPO). Sie liefern die verlangten Teilnehmeridentifikationen sowie Verkehrs- und Rechnungsdaten so rasch als möglich und den Fernmeldeverkehr der überwachten Person soweit möglich in Echtzeit. Von ihnen angebrachte Verschlüsselungen müssen sie entfernen (Art. 15 Abs. 4 BÜPF). Die Anbieterinnen gewährleisten auch die Mitteilung der in Art. 14 Abs. 1 BÜPF genannten Bestandesdaten (Art. 15 Abs. 5 BÜPF). Sie müssen während mindestens zwei Jahren nach Aufnahme der Kundenbeziehung die Auskünfte nach Art. 14 BÜPF auch über Personen erteilen können, welche die Kundenbeziehung für Mobiltelefone nicht über ein Abonnementsverhältnis aufgenommen haben (Art. 15 Abs. 5bis BÜPF).

5.
Zunächst ist zu prüfen, ob und inwieweit das Zwangsmassnahmengericht (gestützt auf Art. 32 CCC i.V.m. Art. 273 StPO) die grenzüberschreitende rückwirkende Erhebung von Verkehrs- und Verbindungsdaten ("IP-History") beim ausländischen Provider durch die Staatsanwaltschaft hätte bewilligen müssen.

5.1. Bei Internetadressen ist die Angabe eines registrierten Inhabers des Fernmelde-Anschlusses bzw. eines Rechnungsadressaten (vgl. Art. 14 Abs. 1 i.V.m. Art. 13 Abs. 1 lit. d BÜPF) schon aus technischen Gründen nicht ohne weiteres möglich, da der Internetservice-Provider dem Internet-User in der Regel für jede Session eine neue IP-Adresse zuweist. Um den Teilnehmer zu identifizieren, muss der Provider somit zusätzlich alle zugewiesenen IP-Adressen abspeichern (vgl. dazu Thomas Hansjakob, Wichtige Entwicklungen der Bundesgerichtspraxis zu Überwachungen des Post- und Fernmeldeverkehrs, forum poenale 2013, S. 173 ff., 176; Sylvain Métille, Mesures techniques de surveillance et respect des droits fondamentaux, en particulier dans le cadre de l'instruction pénale et du renseignement, Diss. NE, Basel 2011, S. 40 ff.; Nicolai Seitz, Strafverfolgungsmassnahmen im Internet, Diss. Köln 2004, S. 9 ff.; Botschaft vom 27. Februar 2013 des Bundesrates zum Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs [Botschaft BÜPF], BBl 2013 2683, 2702 Ziff. 1.4.16, 2732 f., 2736, 2742 f., 2746, 2769 f.). Bei Straftaten, die über das Internet begangen werden, sind die dem schweizerischen Recht unterworfenen Dienstanbieterinnen
verpflichtet, der Polizei und der Staatsanwaltschaft alle (auch rückwirkenden) Angaben zu machen, die eine Identifikation des Urhebers ermöglichen (Art. 14 Abs. 4 i.V.m. Art. 1 Abs. 1-2 BÜPF sowie Art. 24b und Art. 27 VÜPF; vgl. BGE 139 IV 98 E. 4.8 S. 101 f.; 195 E. 2.2 S. 197). Gewisse Abgrenzungsfragen stellen sich, wenn der (Internet-) Anschluss den Strafverfolgungsbehörden nicht bereits bekannt ist, also wenn kein "typischer" Fall einer Bestandesdaten-Abfrage (im Sinne von Art. 14 Abs. 1 BÜPF) vorliegt (vgl. dazu unten, E. 6). Falls bei Untersuchungen wegen Internetdelikten bereits eine E-Mail-Adresse (bzw. ein Internetanschluss) bekannt ist, stellt die Ermittlung der betreffenden Registrierungsdaten grundsätzlich eine Bestandesdatenabfrage im Sinne von Art. 14 Abs. 4 BÜPF dar (vgl. Hansjakob, forum poenale 2013, S. 177; ders., in: Zürcher Kommentar StPO, 2. Aufl., Zürich 2014, Art. 273 N. 8). Wenn den Strafverfolgungsbehörden hingegen lediglich strafbare Internet- Kommunikationsaktivitäten bekannt geworden sind (zum Beispiel Postings auf sozialen Netzwerken) und über die Verbindungs-Randdaten der betreffenden Internet-Kommunikation die zugewiesenen IP-Adressen und registrierten Kunden erst eruiert werden sollen

(sogenannte "IP-History"), sind bei Überwachungen in der Schweiz die Vorschriften von Art. 273 StPO anwendbar (vgl. Botschaft BÜPF, BBl 2013 2683, 2743; BGE 126 I 50 E. 5-6 S. 60-67; s.a. unten, E. 6.2). Das Genehmigungsgesuch der Staatsanwaltschaft und die Beschwerde der Oberstaatsanwaltschaft stützen sich denn auch ausdrücklich auf diese Bestimmung.

5.2. Zusätzliche (rechtliche und technische) Hindernisse ergeben sich, wenn inländische Strafverfolger - wie im vorliegenden Fall - auf Verbindungsdaten aus Internet-Kommunikation zugreifen wollen, die bei im Ausland domizilierten Providern gespeichert sind. Die (Ober-) Staatsanwaltschaft vertritt die Ansicht, dass im vorliegenden Fall die Voraussetzungen eines direkten Zugriffs auf die von einer in den USA domizilierten Internetservice-Providerfirma gespeicherten Verkehrs- und Verbindungsdaten ("IP-History") gemäss Art. 32 lit. b CCC erfüllt seien. Ein Rechtshilfeersuchen sei daher nicht erforderlich.

5.3. Vorbehältlich abweichender völkerrechtlicher Bestimmungen ist ein Staat aufgrund des Grundsatzes der Territorialität nicht berechtigt, eigene Strafverfolgungsmassnahmen auf dem Hoheitsgebiet eines anderen Staates vorzunehmen. Dies gilt namentlich für strafprozessuale Beweismittelbeschlagnahmungen oder Fernmeldeüberwachungen im Ausland (vgl. Botschaft BÜPF, BBl 2013 2683, 2689, 2708, 2742 unten; François Charlet/Cédric Boquet, De l'application de la LSCPT aux fournisseurs de services de VoIP, Jusletter vom 10. November 2014, Rz. 37; Andreas Donatsch/Stefan Heimgartner/Madeleine Simonek, Internationale Rechtshilfe, Zürich 2011, S. 4, 34 f.; Alexandre Dyens, Territorialité et ubiquité en droit pénal international suisse, Diss. LS, Basel 2014, S. 19 f.; Sabine Gless, Internationales Strafrecht, Basel 2011, Rz. 258; Stefan Heimgartner, Die internationale Dimension von Internetstraffällen - Strafhoheit und internationale Rechtshilfe in Strafsachen, in: Schwarzenegger/Arter/Jörg [Hrsg.], Internet-Recht und Strafrecht, Bern 2005, S. 117 ff., 120 ff., 135; Lukas Morscher, Aktuelle Entwicklungen im Technologie- und Kommunikationsrecht, ZBJV 147 [2011]177 ff., S. 214 f.; Dominic Ryser, "Computer Forensics", eine neue Herausforderung
für das Strafprozessrecht, in: Schwarzenegger/ rter/ Jörg [Hrsg.], Internet-Recht und Strafrecht, Bern 2005, S. 553 ff., 575 f.; Sandra Schweingruber, Cybercrime-Strafverfolgung im Konflikt mit dem Territorialitätsprinzip, Jusletter vom 10. November 2014, Rz. 4; Seitz, a.a.O., S. 366 f.; Lea Unseld, Internationale Rechtshilfe im Steuerrecht, Diss. ZH 2011, S. 6 f.; Robert Zimmermann, La coopération judiciaire internationale en matière pénale, 4. Aufl., Bern 2014, Rz. 568; s.a. BGE 139 III 236 E. 4.2 S. 237 f.; 120 Ib 97 E. 6b S. 111). Diesbezüglich ist grundsätzlich der ordentliche Weg der internationalen Rechtshilfe in Strafsachen zu beschreiten, im Bezug auf die sogenannte "akzessorische" Rechtshilfe mit den USA namentlich gestützt auf Art. 29-31 CCC bzw. Art. 1 Ziff. 1 lit. a RVUS (vgl. Art. 1 Abs. 1-2 und Art. 54 StPO i.V.m. Art. 1 Abs. 1 lit. b IRSG).

5.4. Die Vertragsstaaten des Internationalen Cybercrime-Übereinkommens (darunter die meisten europäischen Staaten, die USA, Kanada, Australien und Japan) haben festgestellt, dass die modernen Kommunikations- und Datenverarbeitungstechnologien eine Herausforderung für die Bekämpfung der Computer- und Internetkriminalität darstellen. Elektronische Daten werden, unabhängig vom Herkunfts- oder Aufbewahrungsort, innert Sekunden an beliebige Empfänger auf der ganzen Welt versandt oder an eine Vielzahl von Personen und Einrichtungen verbreitet. In Computersystemen gespeicherte Informationen können für einen bestimmten oder unbestimmten Personenkreis zugänglich gemacht, gezielt gesucht und entsprechend heruntergeladen werden. Staatsgrenzen bilden für den Informationsfluss im Internetzeitalter keine Hindernisse mehr, und die neuen Technologien führen in steigendem Masse dazu, dass die Aktivitäts- und die Erfolgsorte von deliktischem Verhalten geographisch weit auseinanderliegen können. Da der Anwendungsbereich der staatlichen Gesetzgebungen demgegenüber vom Territorialitätsgrundsatz begrenzt wird (vgl. oben, E. 5.3), muss die Strafverfolgung im Bereich des Cybercrime über adäquate Instrumente des internationalen Strafrechts unterstützt
werden (vgl. Präambel CCC; Council of Europe, Explanatory Report to the Convention on Cybercrime [Explanatory Report CCC], Ziff. 6, publ. auf: http://conventions.coe.int/treaty/en/reports/html/185.htm; Botschaft vom 18. Juni 2010 des Bundesrates über die Genehmigung und die Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität [Botschaft CCC], BBl 2010 4697, 4700 Ziff. 1.1; s.a. Annina Baltisser, Datenbeschädigung und Malware im Schweizer Strafrecht: Der Tatbestand des Art. 144bis StGB im Vergleich mit den Vorgaben der Cybercrime Convention und der deutschen Regelung, Diss. ZH 2013, S. 147-151; Heimgartner, a.a.O., S. 142 ff.; Eric Hilgendorf, Tendenzen und Probleme einer Harmonisierung des Internetstrafrechts auf Europäischer Ebene, in: Schwarzenegger/Arter/Jörg [Hrsg.], Internet-Recht und Strafrecht, Bern 2005, S.

257 ff., 268 ff.; Christian Schwarzenegger, Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001, in: Donatsch/Forster/Schwarzenegger [Hrsg.], Strafrecht, Strafprozessrecht und Menschenrechte, Festschrift für Stefan Trechsel zum 65. Geburtstag, Zürich 2002, S. 305 ff.; Seitz, a.a.O., S. 357 ff.).

5.5. Die international vereinheitlichten und spezifizierten Instrumente des Cybercrime-Übereinkommens (vgl. dazu oben, E. 4.3.1-4.3.11) versuchen insbesondere den Umständen Rechnung zu tragen, dass förmliche Rechtshilfeverfahren sich regelmässig aufwändig, kompliziert und langwierig gestalten und diverse Staaten keine oder nur eine relativ kurze "Vorratsdatenspeicherung" in Bezug auf die rückwirkende Erhebung von Randdaten des elektronischen Fernmeldeverkehrs kennen (vgl. Art. 273 Abs. 3 StPO; s.a. Art. 16 Abs. 2 CCC), weshalb der Ablauf der gesetzlichen Überwachungsfrist droht, noch bevor über ein hängiges Rechtshilfegesuch entschieden werden konnte (vgl. dazu Heimgartner, a.a.O., S. 134 ff.; Schweingruber, a.a.O., Rz. 5; Seitz, a.a.O., S. 355-357). Das Übereinkommen sieht diesbezüglich spezifische Instrumente vor, darunter die vorsorgliche umgehende Sicherung gespeicherter Computerdaten im Hinblick auf ein späteres Rechtshilfeersuchen ("Expedited preservation of stored computer data", Art. 29 CCC; s. dazu Heimgartner, a.a.O., S. 144 f.; Seitz, a.a.O., S. 358), die umgehende Weitergabe von Verkehrsdaten, welche aufgrund eines vorsorglichen Ersuchens (nach Art. 29 CCC) gesichert wurden (Art. 30 CCC, "Expedited disclosure of
preserved traffic data") sowie den direkten grenzüberschreitenden Zugriff in jenen Fällen, bei denen ein Berechtigter (etwa ein ausländischer Internetservice-Provider) der Datenerhebung zugestimmt hat (Art. 32 lit. b CCC, "Trans-border access to stored computer data with consent").

5.6. Im vorliegenden Fall hat die Staatsanwaltschaft am 22. Juli 2014 (über die Einsatzzentrale des Fedpol) bei den zuständigen US-Behörden ein Gesuch um vorläufige umgehende Sicherung (Art. 29 CCC) der fraglichen Randdaten des Internetverkehrs gestellt ("Expedited preservation request", Art. 29 Abs. 2 CCC). Im Betreff des Gesuches wird auch noch eine umgehende Weitergabe von vorläufig gesicherten Verkehrsdaten (im Sinne von Art. 30 CCC) erwähnt. Art. 1 lit. d CCC definiert als "Verkehrsdaten" ("Traffic data") im Sinne des Übereinkommens "alle Computerdaten in Zusammenhang mit einer Kommunikation unter Nutzung eines Computersystems, die von einem Computersystem, das Teil der Kommunikationskette war, erzeugt wurden und aus denen der Ursprung, das Ziel, der Leitweg, die Uhrzeit, das Datum, der Umfang oder die Dauer der Kommunikation oder die Art des für die Kommunikation benutzten Dienstes hervorgeht". Die vom Übereinkommen verlangte (innerstaatliche) Zugriffsmöglichkeit auf solche Verkehrsdaten wird in der Schweiz (durch Art. 273 StPO i.V.m. Art. 13 Abs. 1 lit. d und Art. 15 Abs. 1-4 BÜPF) gewährleistet. In der Schweiz domizilierte und zugelassene Anbieterinnen müssen während sechs Monaten Randdaten des Fernmeldeverkehrs
speichern und (in den Fällen von Art. 273 StPO) auch rückwirkend Auskünfte geben.

5.7. Ob und inwieweit im Hinblick auf ein Rechtshilfeersuchen (Art. 31 CCC) das Gesuch der Staatsanwaltschaft um vorsorgliche "umgehende Sicherung" (Art. 29 CCC) zu bewilligen ist, und ob eine "umgehende Weitergabe von Verkehrsdaten" erfolgen kann, welche aufgrund des vorsorglichen Ersuchens gesichert wurden (Art. 30 CCC), hat nach den Bestimmungen des Übereinkommens die zuständige (nach Art. 29 CCC ersuchte) US-Behörde zu entscheiden (vgl. oben, E. 4.3.8-4.3.9). Diese Frage bildet denn auch nicht Gegenstand des angefochtenen Entscheides. Zu prüfen bleibt, ob hier die Voraussetzungen einer direkten grenzüberschreitenden Randdatenerhebung durch die Schweizer Strafverfolgungsbehörden erfüllt sind (Art. 32 CCC). Die Frage wird von der Staatsanwaltschaft und der Oberstaatsanwaltschaft bejaht, von der Vorinstanz hingegen verneint.

5.8. Art. 32 lit. a CCC ist im vorliegenden Fall nicht anwendbar. Das Ersuchen der Staatsanwaltschaft um Randdatenerhebung des Internet-Verkehrs bezieht sich nicht auf öffentlich zugängliche Daten (wie z.B. per Internet einsehbare offene Kommunikationsforen oder unbeschränkt zugängliche Webseiten und Dateien; vgl. dazu Seitz, a.a.O., S. 361-366).

5.9. Gemäss Art. 32 lit. b CCC darf eine Vertragspartei des Übereinkommens ohne die Genehmigungeiner anderen Vertragspartei auf gespeicherte Computerdaten, die sich im Hoheitsgebiet der anderen Vertragspartei befinden, mittels eines Computersystems in ihrem Hoheitsgebiet zugreifen oder diese Daten empfangen, wenn sie die ("rechtmässige und freiwillige") Zustimmung der Person einholt, die ("rechtmässig") befugt ist, die

Daten mittels dieses Computersystems an sie weiterzugeben. Der Explanatory Report nennt als Beispiel den Fall einer von einem Internetservice-Provider im Ausland gespeicherten E-Mail (vgl. Explanatory Report CCC, Ziff. 294; s.a. Heimgartner, a.a.O., S. 146; eingehend Seitz, a.a.O., S. 370-378.).
In der Botschaft zum Cybercrime-Übereinkommen wird die Auffassung vertreten, Art. 32lit. b CCC sei in dem Sinne "eng" auszulegen, dass jeweils die Zustimmung "einer Person im Inland"einzuholen sei, welche rechtmässig befugt ist, die Daten "an eine inländische Strafverfolgungsbehörde weiterzuleiten" (Botschaft CCC, BBl 2010 4697, 4738). Dieser Formulierung in der bundesrätlichen Botschaft kann nicht gefolgt werden. Sie findet weder im Wortlaut noch in den einschlägigen Materialien des Übereinkommens oder der Fachliteratur eine Stütze. Zudem widerspricht sie dem dargelegten Sinn und Zweck des multilateralen Vertrages (vgl. oben, E. 5.4-5.5).
Wie nachfolgend zu zeigen sein wird, setzt die Zustimmungsvoraussetzung von Art. 32 lit. b CCC dem Anwendungsbereich einer grenzüberschreitenden Erhebung von Daten bereits sehr enge Schranken (vgl. E. 5.10-5.11). Mit Art. 32 CCC haben sich die Vertragsstaaten auf einen minimalen (restriktiven) gemeinsamen Konsens für einen grenzüberschreitenden ("extraterritorialen") Zugriff geeinigt (vgl. Explanatory Report CCC, Ziff. 293; Vorentwurf und Erläuternder Bericht des EJPD vom März 2009 betreffend Genehmigung und Umsetzung des Übereinkommens des Europarates über die Cyberkriminalität [Bericht EJPD CCC], S. 43 Ziff. 2.3.11, Fn. 212; Seitz, a.a.O., S. 373 f.). Wenn zusätzlich (und entgegen dem Wortlaut von Art. 32 lit. b CCC) auch noch die Zustimmung einer (berechtigten) Person im Inland verlangt würde, würden die Hauptanliegen des CCC (Verbesserung der Bekämpfung der grenzüberschreitenden Cyberkriminalität, Erleichterung der Rechtshilfe bzw. partielle Lockerung des Erfordernisses des förmlichen Rechtshilfeweges) unterlaufen. Ausländische E-Mail-Konten oder Accounts von sozialen Netzwerken würden dem in Art. 32 lit. b CCC vorgesehenen direkten Zugriff praktisch vollständig entzogen, indem (bei im Ausland gespeicherten Daten) nur in
seltenen Fällen auch noch eine zustimmungsberechtigte inländische Person eruierbar sein dürfte, die dann auch noch ihre Zustimmung zur Datenerhebung erteilen müsste (vgl. auch Schweingruber, a.a.O., Rz. 13 f.).

5.10. Nach dem Gesagten kommen auch ausländische Personen bzw. Gesellschaften als Zustimmungsberechtigte im Sinne von Art. 32 lit. b CCC in Frage. Die rechtmässige Befugnis der Person, über die Daten zu verfügen und sie an eine staatliche Stelle weiterzuleiten, beurteilt sich primär nach dem nationalen Recht des Staates, in welchem die betreffende Person handelt (Botschaft CCC, BBl 2010 4697, 4738). Zustimmungs- und weiterleitungsberechtigt sind namentlich ausländische Internetprovider bzw. Anbieter von sozialen Netzwerken, welche sich in ihren Allgemeinen Nutzungsbedingungen bzw. Datenverwendungsrichtlinien ein solches Weiterleitungsrecht an in- und ausländische Strafverfolgungsbehörden gegenüber ihren Kunden ausbedungen haben (vgl. Explanatory Report CCC, Ziff. 294; Schweingruber, a.a.O., Rz. 16-18). Dass eine betroffene ausländische Providerfirma in diesem Sinne grundsätzlich berechtigt wäre, ihre Zustimmung zu einer direkten Datenherausgabe zu erklären, reicht indessen (nach dem klaren Wortlaut von Art. 32 lit. b CCC) für einen grenzübergreifenden Zugriff noch nicht aus: Vielmehr ist weiter zu prüfen, ob die anfragende Strafverfolgungsbehörde eine rechtswirksame "freiwillige Zustimmung" gegenüber der ausländischen
Providerfirma eingeholt hat. Eine konkludente freiwillige Zustimmung kann insbesondere angenommen werden, wenn der angefragte Internet-Provider (oder auch der Inhaber des betroffenen Kontos selbst) die Daten ohne Weiteres herausgibt (vgl. Schweingruber, a.a.O., Rz. 20; Botschaft CCC, BBl 2010 4697, 4738).

5.11. Im angefochtenen Entscheid wird hierzu Folgendes dargelegt: Die Staatsanwaltschaft habe ein Schreiben vom 1. Juli 2014 der betroffenen amerikanischen Internetservice-Providerfirma eingereicht. Dieses Schreiben beziehe sich zwar auf einen anderen untersuchten Fall, betreffe aber die analoge Frage der freiwilligen Zustimmung zur Datenherausgabe. Dem Schreiben sei zu entnehmen, dass das Unternehmen einen hoheitlichen Entscheid zur Frage erwarte, ob es gezwungen werden könne, die Daten direkt herauszugeben. Andernfalls bestehe es auf der Einhaltung des Rechtshilfeweges (vgl. angefochtener Entscheid, S. 6 oben). Der Vorinstanz ist darin beizupflichten, dass in der fraglichen Äusserung keine freiwillige Zustimmung zur direkten Datenherausgabe gesehen werden kann. Die Internet-Providerin besteht vielmehr auf dem förmlichen Rechtshilfeweg, sofern sich aus dem hier anwendbaren Recht, insbesondere aus Art. 32 lit. b CCC i.V.m. Art. 273 StPO, keine Verpflichtung zur direkten Datenherausgabe ergibt. Ohne freiwillige Zustimmung einer dazu berechtigten Person oder Gesellschaft besteht eine solche rechtliche Verpflichtung aber gerade nicht. Zwar beruft sich die Oberstaatsanwaltschaft in ihrer Beschwerde auf eine (weitere) E-Mail des

Rechtsdienstes der Providerfirma vom 11. Juli 2014. Auch diesem Schreiben lässt sich jedoch keine bedingungslose freiwillige Zustimmung zur Datenherausgabe entnehmen. Ebenso wenig liegt hier eine konkludente Zustimmung durch faktische Datenherausgabe vor.

5.12. Nach dem Gesagten sind die Voraussetzungen (von Art. 32 CCC) eines direkten grenzüberschreitenden Zugriffs auf Internetkommunikations-Randdaten (der vom Zwangsmassnahmengericht nach Art. 273 StPO zu bewilligen wäre) hier nicht erfüllt. Aus Art. 23, Art. 25 Abs. 4 und Art. 39 Abs. 3 CCC folgt, dass in allen Fällen, bei denen die (Ausnahme-) Voraussetzungen von Art. 32 CCC nicht gegeben sind, die fragliche Datenerhebung bzw. rückwirkende Überwachung im Ausland auf dem förmlichen Rechtshilfeweg (hier gestützt auf Art. 31 CCC bzw. das RVUS) zu beantragen ist. Die Vertragsstaaten des Übereinkommens haben sich (über die Bestimmungen von Art. 32 CCC hinaus) nicht auf weitergehende "extraterritoriale" Zugriffe von Strafverfolgungsbehörden einigen können (vgl. Explanatory Report CCC, Ziff. 293; Bericht EJPD CCC, S. 43 Ziff. 2.3.11, Fn. 212; Seitz, a.a.O., S. 373 f.). Vielmehr kamen sie überein, allfällige weitere direkte Zugriffsmöglichkeiten erst in einem späteren Stadium und aufgrund der bis dann erlangten Erfahrungen in Erwägung zu ziehen (vgl. Explanatory Report CCC, Ziff. 293). Die am 22. Juli 2014 von der Staatsanwaltschaft beantragte vorläufige Sicherung der einschlägigen Verkehrsdaten (Art. 29 CCC) dient denn auch (primär)
der Sicherstellung einer allfälligen Beweiserhebung auf dem förmlichen Rechtshilfeweg (Art. 31 CCC).

5.13. Auch das Schweizer Landesrecht enthält keine materielle Grundlage für die von der Staatsanwaltschaft beantragte direkte Randdatenerhebung (bzw. rückwirkende Fernmeldeüberwachung) im Ausland: Art. 273 StPO regelt entsprechende Zwangsmassnahmen im Inland, nämlich gegenüber (in der Schweiz domizilierten bzw. dem schweizerischen Recht unterworfenen) Fernmeldedienst-Anbieterinnen, welche (nach Art. 1 Abs. 1-2 i.V.m. Art. 13 Abs. 1 lit. d und Art. 15 Abs. 1-4 BÜPF) verpflichtet sind, entsprechende Randdaten des Fernmeldeverkehrs zu speichern und den zuständigen Behörden zur Verfügung zu halten. Für rechtshilfeweise Untersuchungshandlungen im Ausland sind hingegen die völkerrechtlichen Bestimmungen über die internationale Rechtshilfe in Strafsachen massgeblich (Art. 54 StPO i.V.m. Art. 1 Abs. 1 lit. b IRSG; analog für das deutsche Landesrecht s.a. Seitz, a.a.O., S. 371).

6.
Schliesslich bleibt noch zu prüfen, ob und inwieweit das Zwangsmassnahmengericht (gestützt auf Art. 18 Abs. 1 lit. b CCC i.V.m. Art. 14 BÜPF) die grenzüberschreitende Erhebung von blossen Bestandesdaten ("Registrierungsdaten" von Internetkunden) beim ausländischen Provider durch die Staatsanwaltschaft hätte bewilligen müssen.

6.1. Die (Ober-) Staatsanwaltschaft beruft sich diesbezüglich auf Art. 18 Abs. 1 lit. b CCC. Diese Bestimmung verpflichtet die Vertragsstaaten dazu, "gesetzgeberische und andere Massnahmen" zu treffen, damit ihre Behörden anordnen können, dass ein Diensteanbieter, der seine Dienste in ihrem Hoheitsgebiet anbietet, "Bestandsdaten in Zusammenhang mit diesen Diensten, die sich in seinem Besitz oder unter seiner Kontrolle befinden, vorzulegen hat". Dies ist im schweizerischen Recht (gestützt auf Art. 14 i.V.m. Art. 15 Abs. 5 und Abs. 5bis BÜPF i.V.m. Art. 265 StPO) gewährleistet (vgl. Botschaft CCC, BBl 2010 4697, 4721). Die Bestandesdaten (im Sinne von Art. 18 Abs. 1 lit. b CCC) werden in Art. 18 Abs. 3 CCC näher definiert (vgl. oben, E. 4.3.4).

6.2. Die Erhebung von Verbindungs -Randdaten bzw. die Teilnehmeridentifikation im Sinne von Art. 273 Abs. 1 StPO (dazu oben, E. 5) ist zu unterscheiden von der blossen Bestandesdaten -Auskunft (nach Art. 14 BÜPF) über registrierte Fernmeldeanschlüsse: Bei der Teilnehmeridentifikation (nach Art. 273 Abs. 1 lit. a StPO) werden Teilnehmer an konkreten Fernmeldeverbindungen über einen gewissen Zeitraum hinweg identifiziert ("Verbindungen hat oder gehabt hat"). Das heisst, es werden Verkehrsdaten von Kommunikationenerhoben und gestützt darauf Anschlüsse und Teilnehmer identifiziert. Hier muss nach schweizerischem Recht der dringende Verdacht eines Verbrechens oder Vergehens (Art. 273 Abs. 1 StPO) vorliegen. Ausserdem muss die Verbindungsdaten-Erhebung richterlich bewilligt werden (Art. 273 Abs. 2 StPO). Bei blossen Bestandesdaten-Auskünften (nach Art. 14 Abs. 1 BÜPF) hingegen sind die Anschlüsse den Strafverfolgungsbehörden bereits bekannt ("bestimmte Fernmeldeanschlüsse"), und es wird den auskunftsberechtigten Behörden lediglich mitgeteilt, wer als Inhaber bzw. Rechnungsadressat dieses Anschlusses bei den Anbieterinnen registriert ist. Es

werden hier also lediglich Bestandesdaten mitgeteilt, aber keine Verbindungsdaten zu Kommunikationen erhoben. Blosse Auskünfte über bekannte Anschlüsse (nach Art. 14 Abs. 1 BÜPF) werden daher nicht nur zu Strafverfolgungszwecken an die Staatsanwaltschaft erteilt, sondern auch an die Polizei zur Erfüllung polizeilicher Aufgaben (Art. 14 Abs. 2 lit. a-b BÜPF). Eine richterliche Bewilligung ist hier nicht erforderlich (vgl. Hansjakob, forum poenale 2013, S. 176 f.). Eine Bestandesdatenerhebung kann (nötigenfalls) über eine Editionsverfügung erfolgen (Art. 265 StPO).
Bei Straftaten, die über das Internet begangen werden, sind die dem schweizerischen Recht unterworfenen Dienstanbieterinnen verpflichtet, der Polizei und der Staatsanwaltschaft alle (auch rückwirkenden) Angaben zu machen, die eine Identifikation des Urhebers ermöglichen (Art. 14 Abs. 4 i.V.m. Art. 1 Abs. 1-2 BÜPF sowie Art. 24b und Art. 27 VÜPF; zur Abgrenzung gegenüber der Randdatenerhebung nach Art. 273 StPO s.a. oben, E. 5.1). Bei Erhebungen gemäss Art. 14 Abs. 4 BÜPF wird allerdings nur abgeklärt, wer einen bestimmten Internet-Anschluss benützt hat. Entsprechende Bestandesdaten müssen 10 Jahre rückwirkend ediert werden. Randdatenerhebungen nach Art. 273 StPO liegen demgegenüber vor, wenn eruiert werden soll, "wer wann mit wem" über das Internet "kommuniziert" hat (Hansjakob, Kommentar StPO, Art. 273 N. 8). Als Ausfluss des Territorialitätsgrundsatzes (vgl. oben, E. 5.3) sind in der Schweiz ansässige Tochter- oder Partnergesellschaften von ausländischen Providerfirmen, die in der Schweiz Daten speichern (sogenannte "Server Farms"), dem schweizerischen Recht (StPO/BÜPF) unterworfen (vgl. Morscher, a.a.O., S. 214 f.).

6.3. Zur "anderen Rechtshilfe" (im dritten Teil IRSG) gehört auch die sogenannte unaufgeforderte Übermittlung von Beweismitteln und Informationen (Art. 67a IRSG). Auch in diesem Bereich ist das IRSG anwendbar, soweit internationale Vereinbarungen nichts anderes bestimmen (Art. 1 Abs. 1 lit. b IRSG). Soweit Schweizer Strafverfolgungsbehörden (gestützt auf Art. 14 i.V.m. Art. 1 Abs. 1-2 BÜPF) Bestandesdaten bei Providern in der Schweiz direkt erheben können, dürfen sie die Daten unter den Voraussetzungen des einschlägigen Rechtshilferechts (insbesondere von Art. 26 Abs. 1 CCC i.V.m. Art. 67a IRSG) auch unaufgefordert (ohne förmliches Rechtshilfeersuchen) an eine interessierte ausländische Strafverfolgungsbehörde übermitteln. Im Falle einer zulässigen unaufgeforderten Übermittlung durch Schweizer Ermittlungsbehörden ist keine vorgängige Bewilligung durch eine Schweizer Rechtshilfebehörde oder das Zwangsmassnahmengericht nötig (vgl. BGE 140 IV 123; 139 IV 137 E. 4.3-4.6 S. 141 ff.; 130 II 236 E. 6.1-6.2 S. 244 f.; 129 II 544; 125 II 238). Umgekehrt (und auf den vorliegenden Fall bezogen) könnten die zuständigen US-Strafverfolgungsbehörden (unter den Voraussetzungen von Art. 26 i.V.m. Art. 18 Abs. 1 lit. b und Abs. 3 CCC bzw. der einschlägigen Strafverfahrens- und Rechtshilfenormen des US-Rechts) ihnen in den USA zugängliche Bestandesdaten (oder andere von ihnen ermittelte Informationen) "unaufgefordert" an die Zürcher Staatsanwaltschaft oder an das Bundesamt für Justiz (Zentralstelle USA) übermitteln (vgl. auch Art. 39 Ziff. 1 RVUS).

6.4. Die (Ober-) Staatsanwaltschaft stellt sich auf den Standpunkt, Art. 18 Abs. 1 lit. b CCC sei (über das Dargelegte hinaus) auf alle - auch im Ausland domizilierten - Internet-Provider anwendbar, die in der Schweiz ihre Dienste "anbieten". Insofern dürfe die Staatsanwaltschaft auch ausländische Anbieterinnen direkt anweisen, ihr (im Ausland erhältliche) Bestandesdaten auszuliefern (so auch Schweingruber, a.a.O., Rz. 25-28). Dieser Auslegung ist nicht zu folgen: Da das Cybercrime-Übereinkommen über die Fälle von Art. 32 CCC hinaus keinen grenzüberschreitenden direkten Zugriff im Ausland erlaubt (vgl. dazu oben, E. 5.12), kann sich Art. 18 Abs. 1 lit. b CCC nur auf im Inland domizilierte und zugelassene Fernmeldedienst-Anbieterinnen beziehen, welche dort über registrierte Bestandesdaten ihrer Kunden verfügen. Dabei kann es sich auch um "Server Farms" von ausländischen Internetservice-Providern handeln, welche im Inland Daten speichern. Art. 18 Abs. 1 lit. b CCC regelt (anders als Art. 32 CCC) keinen Fall einer zulässigen grenzüberschreitenden Strafverfolgungsmassnahme. Nach dem Wortlaut der Bestimmung und ihrer systematischen Stellung (in Kapitel II, Abschnitt 2 des Übereinkommens) bezieht sie sich auf die innerstaatlich zu erlassenden verfahrensrechtlichen Bestimmungen (vgl. dazu oben, E. 4.3.2-4.3.3 und E. 6.1). Auch der Wortlaut von Art. 25 Abs. 4 Satz 1 CCC (vgl. oben, E. 4.3.6) lässt keinen Zweifel daran, dass die rechtshilferechtlichen strafprozessualen Zugriffsmöglichkeiten (insbesondere die grenzüberschreitenden) im Kapitel III des Übereinkommens abschliessend geregelt sind (vgl. auch Bericht EJPD CCC, S. 43 Ziff. 2.3.11, Fn. 212).

6.5. Für die Herausgabe von Bestandesdaten bei in den USA domizilierten Anbieterinnen ist folglich (gemäss Art. 23, Art. 25 Abs. 4 und Art. 31 CCC sowie dem RVUS) das von den US-amerikanischen Behörden

anzuwendende Amts- und Rechtshilferecht massgeblich. Ob und inwieweit eine unaufgeforderte Übermittlung solcher Daten (ohne förmliches Rechtshilfeersuchen im Sinne von Art. 31 CCC) nach Art. 26 CCC (bzw. US-Recht) möglich und geboten wäre, hat nicht das kantonale Zwangsmassnahmengericht (grenzübergreifend) zu entscheiden, sondern (auf entsprechende informelle Anfrage der Schweizer Behörden hin) die sachlich zuständigen Behörden der USA (vgl. auch Art. 54 StPO i.V.m. Art. 1 Abs. 1 lit. b IRSG). Auch Art. 26 Abs. 1 CCC verweist für dessen Anwendbarkeit ausdrücklich auf das innerstaatliche Recht des übermittelnden Staates (vgl. oben, E. 4.3.7; s.a. Art. 38 Ziff. 1 Satz 2 RVUS). Nachdem weder im Völkerrecht noch im schweizerischen Landesrecht eine entsprechende Rechtsgrundlage besteht, kann ein extraterritorialer Bestandesdaten-Zugriff auch nicht über ein schweizerisches Gerichtsurteil im Sinne einer "anderen Massnahme" (Art. 18 Abs. 1 Ingress CCC) erfolgen. Für eine "Genehmigung" eines Gesuches um Erhebung von Bestandesdaten war das Zwangsmassnahmengericht im Übrigen weder nach der StPO zuständig (Bestandesdaten im Inland, vgl. dazu oben, E. 6.1-6.2), noch nach dem hier anwendbaren Rechtshilferecht bzw. US-Recht (Bestandesdaten im Ausland).

7.
Zusammenfassend ergibt sich, dass für die von der Staatsanwaltschaft beabsichtigten Datenerhebungen (bzw. rückwirkenden Überwachungen) in den USA der Weg der internationalen Rechtshilfe in Strafsachen zu beschreiten ist. Das Zwangsmassnahmengericht hat das Gesuch um Genehmigung einer direkten grenzüberschreitenden Erhebung von Randdaten des Internetverkehrs (gestützt auf Art. 32 CCC i.V.m. Art. 273 StPO) zu Recht abgewiesen. Für eine "Genehmigung" der rechtshilfeweisen Herausgabe von Bestandesdaten war es gar nicht zuständig. Die Beschwerde gegen den abschlägigen Entscheid der Vorinstanz ist folglich als unbegründet abzuweisen.
Es sind weder Gerichtskosten zu erheben, noch Parteientschädigungen auszurichten (Art. 66 Abs. 4 i.V.m. Art. 68 Abs. 3 BGG).
Entgegen dem Antrag der Oberstaatsanwaltschaft ist das vorliegende Grundsatzurteil amtlich zu publizieren. Dem prozessualen Subeventualantrag der Oberstaatsanwaltschaft (betreffend Anonymisierung) wird insoweit stattgegeben, dass der Sachverhalt in der Weise redigiert und anonymisiert wird, dass keine Rückschlüsse auf den konkreten Gegenstand der Untersuchung, das betroffene soziale Netzwerk und die inkriminierten Teilnehmer gezogen werden können.

Demnach erkennt das Bundesgericht:

1.
Die Beschwerde wird abgewiesen.

2.
Es werden keine Gerichtskosten erhoben.

3.
Dieses Urteil wird der Oberstaatsanwaltschaft und dem Obergericht des Kantons Zürich, Zwangsmassnahmengericht, schriftlich mitgeteilt.

Lausanne, 14. Januar 2015

Im Namen der I. öffentlich-rechtlichen Abteilung
des Schweizerischen Bundesgerichts

Der Präsident: Fonjallaz

Der Gerichtsschreiber: Forster